

**Development of a Class of Non-Associative Algebras:
Applications in Cryptography and Coding Theory**



By

Nazli Sanam

**Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN
2021**

**Development of a Class of Non-Associative Algebras:
Applications in Cryptography and Coding Theory**



By

Nazli Sanam

Supervised

By

Dr. Asif Ali

**Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN
2021**

Development of a Class of Non-Associative Algebras: Applications in Cryptography and Coding Theory



A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT
FOR THE DEGREE OF

**DOCTOR OF PHILOSOPHY
IN
MATHEMATICS**

By

Nazli Sanam

**Department of Mathematics
Quaid-i-Azam University, Islamabad
PAKISTAN
2021**

Dedicated

to

my Precious Family

Author's Declaration

I, **Nazli Sanam**, hereby state that my PhD thesis titled **Development of a Class of Non-Associative Algebras: Applications in Cryptography and Coding Theory** is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the university has the right to withdraw my PhD degree.



Name of Student: **Nazli Sanam**

Date: **3-June-2021**

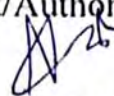
Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**Development of a Class of Non-Associative Algebras: Applications in Cryptography and Coding Theory**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and **Quaid-i-Azam University** towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Student/Author Signature



Name: **Nazli Sanam**

Development of a Class of Non-Associative Algebras:

Applications in Cryptography and Coding Theory

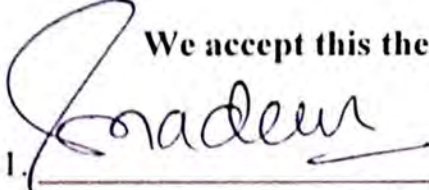
By

Nazli Sanam


CERTIFICATE

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF THE
DOCTOR OF PHILOSOPHY IN MATHEMATICS

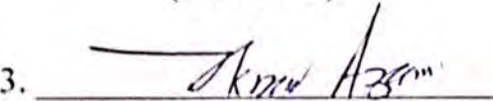
We accept this thesis as conforming to the required standard

1. 

Prof. Dr. Sohail Nadeem
(Chairman)

2. 

Dr. Asif Ali
(Supervisor)

3. 

Prof. Dr. Akbar Azam
(External Examiner)

4. 

Dr. Tahir Mehmood
(External Examiner)

Department of Mathematics, COMSATS
University, Park Road Chak Shahzad,
Islamabad.

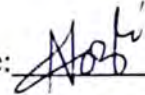
Department of Mathematics & Statistics
International Islamic University, Sector H-
10 Islamabad.

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2021

Certificate of Approval

This is to certify that the research work presented in this thesis entitled Development of a Class of Non-Associative Algebras: Applications in Cryptography and Coding Theory was conducted by Ms. Nazli Sanam under the kind supervision of Dr. Asif Ali. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in field of Mathematics from Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan.

Student Name: Ms. Nazli Sanam

Signature: 

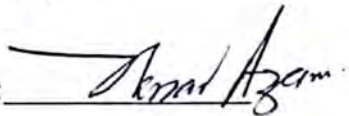
External committee:

a) External Examiner 1:

Name: **Prof. Dr. Akbar Azam**

Designation: Professor

Office Address: Department of Mathematics, COMSATS University, Park Road Chak Shahzad, Islamabad.

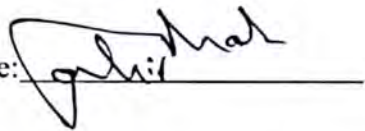
Signature: 

b) External Examiner 2:

Name: **Dr. Tahir Mehmood**

Designation: Assistant Professor

Office Address: Department of Mathematics & Statistics, Faculty of Basics Applied Sciences International Islamic University, Islamabad.

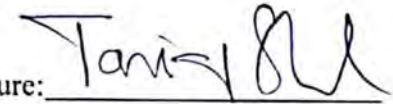
Signature: 

c) Internal Examiner

Name: **Dr. Asif Ali**

Designation: Associate Professor

Office Address: Department of Mathematics, QAU Islamabad.

Signature: 

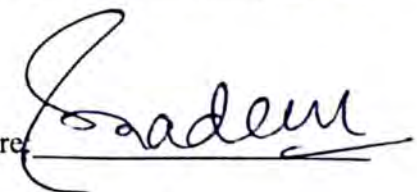
Supervisor Name:

Dr. Asif Ali

Signature: 

Name of Dean/ HOD

Prof. Dr. Sohail Nadeem

Signature: 

Acknowledgments

All praise and gratitude for Allah (SWT), the Merciful Lord, the Creator, Who guides me in darkness, helps me in difficulties and enables me to reach the ultimate stage with courage. Special appreciation for the last Prophet Mohammad (PBUH).

This achievement is made possible as a collective effort from the contributors, both directly or indirectly. This is the time now to extend my gratitude to the people who supported during this research period and played vital role in various forms to achieve this milestone.

First of all, I would like to express my sincerest thanks and appreciation to my supervisor Dr. Asif Ali for his council and valuable guidance in my Ph.D study and related research. I express the deepest gratitude to my respected Professor Dr. Tariq Shah for his continuing guidance and suggestions. His confidence in my abilities and constant encouragement pushed through the difficult parts of the research . It would not have been possible without his kind support and thoughtful ideas.

I wish to express my heartiest thanks to my father Mr. Abdul Ghani, the one who can never ever be thanked enough for his prayers, overwhelming love, kindness and care he bestows upon me. I am extremely thankful to my sisters Naghmana Gulshan, Aliya Tabassam, Afshan Noreen and my brother Muhammad Ijaz Ghani for their encouragement and support. I am thankful to my nephew Muhammad Usama for the proofreading of this thesis.

A very special thanks to my dear husband Sheikh Sobish Imtiaz, not only for his constant emotional support and motivation during this challenging period of my life but also for his help in the computational work included in my thesis. I have no words to express my gratitude to my lovely kids Safa Saman and Shaamir Sultan. I must apologise them for not giving them proper time during my period of research.

I also thank my professors, from the Department of Mathematics, for their effort in

providing an excellent research environment and my PhD colleagues for their good company during my studies. I extend my heartiest and deepest thanks to Dr. Afshan Batool and Dr. Asma Razzaque for always being there for help during my research. I am also thankful to Dr. Sadia Midhat, Dr. Saira Husnain, Dr. Irum Batool, Dr. Ayesha Usman, Ms. Saira Jehangir and Ms. Dania Saleem for their moral support. I am also grateful to the administrative staff of mathematics department, in particular, Mr. Zahoor Jan and Mr. Sajid Mehmood for their cooperation and support at every time.

In the end, I would like to mention my beloved student Ms. Zain Majeed for believing in me and being a constant support.

Nazli Sanam

Preface

One of the peculiarity of mathematics is that its thorniest contradictions bloom into beautiful theories. According to Albert Einstein, "Pure mathematics is, in its way the poetry of logical ideas." Mathematics (in particular pure mathematics) has gone through many revolutionary changes over a period of almost one century and it morphed into new shapes with time.

Initially, rings and algebra were considered to be associative and commutative and in some cases associative only. Since the mid of 19th century, many non-associative structures have been introduced so far. For instance, Octonions, Cayley numbers, Lie algebras, Jordan algebras, Lie structures, alternative rings, loops and loop rings. Non-associative ring theory has flourished as an independent branch of algebra, having links with other branches of mathematics and other fields for instance, biology, physics and other sciences.

In 1972, Kazim and Naseeruddin [77] presented a generalization of a commutative semigroup and called it a left almost semigroup (LA-semigroup). An LA-semigroup is a groupoid satisfying the identity: $(ab)c = (cb)a$, which is known as the left invertive law. An LA-semigroup is non-associative and non-commutative, nevertheless it holds properties that are normally found in associative and commutative algebraic structures. Mushtaq and Kamran [100] in the year 1996, extended the idea of an LA-semigroup to a left almost group (LA-group). Despite being a non-associative algebraic structure, an LA-group interestingly resembles to an abelian group. LA-semigroups and LA-groups are considered by many authors to establish useful results to explore their properties and structures. In 2010, Shah and Rehman [131] combined the two structures to introduce a Left almost ring (LA-ring). It is an additive LA-group and multiplicative LA-semigroup along with the two distributive laws. They generalized a commutative semigroup ring to present an LA-ring, which consists of finitely non-zero functions with domain a commutative semigroup and co-domain an LA-ring.

In the current decade, many researchers have put forward their contribution to the development of this particular non-associative non-commutative structure and its generalizations. Major contributors include T. Shah and his co-researchers [113, 125, 128, 131–135], who not only studied the structural properties of LA-rings and its generalizations, but explored their applications to intuitionistic fuzzy and soft sets. They introduced the concepts of LA-integral domain, LA-field, LA-modules and a generalization of LA-rings called near LA-ring. Furthermore, they discussed the properties of ideals in LA-rings and M-systems in LA-rings. They proved the existence of a non-associative LA-ring and defined a Special LA-ring. Moreover, Shah and Kousar [127] studied the intuitionistic fuzzy normal sub-rings in LA-rings. Shah and Razzaque [129, 130], defined soft LA-rings and discussed soft ideals and M-systems in soft LA-rings. Rehman and Razzaque [109, 112], discussed the notions of projective and injective LA-modules, free LA-modules, split sequences in LA-modules and later they extended the applications of soft set theory to LA-rings and presented soft LA-modules and exact sequences of soft LA-modules. Hussain and his co-authors [55–60], focused on congruences and the notions of direct product and direct sum in LA-ring, LA-module and their generalizations. They introduced an LA-semiring as a generalization of LA-ring.

A number of researchers studied LA-rings from different aspects, a brief look-over to their work is mentioned in this thesis. The aim of this thesis is to explore those areas of LA-ring theory which are still to be uncovered. Some notions have just been introduced but are not further investigated in details by any researcher. For instance LA-domain, LA-fields and special LA-rings. We not only promote these concepts but also provide their different applications. The existing literature lacks examples of LA-rings with order greater than 18, we formulate an algorithm to obtain LA-rings of greater orders using LA-rings with small orders. Moreover, we study some new aspects of the soft LA-rings by investigating soft intersection LA-rings. We fuse generalized rough sets with soft sets to define generalized rough soft sets. We also introduce generalized rough and generalized rough soft LA-rings. Further, we explore the applications of LA-rings to Coding theory by introducing DNA codes over a special LA-field and to cryptography by constructing S-boxes over special LA-rings.

Chapter wise description

This thesis comprises of seven chapters:

Chapter 1 contains some basic concepts and results on LA-rings, soft sets, soft LA-rings, rough sets, Coding theory, DNA codes, cryptography and S-box, which are directly related to our work.

Chapter 2 is a detailed survey on LA-rings and its generalizations. It contains a comprehensive study of the progress of enduring literature on LA-rings and enumerates their several applications in different directions so far. The information provided in this chapter will be an unending source of motivation for future research on LA-ring theory.

Chapter 3 is devoted to our work regarding developments and enhancements in LA-ring theory. Rehman et al. defined a special LA-ring in 2013, as a special case of an LA-ring that is an additive abelian group. In Section 3.1, we compare the two notions and use software MACE4 to find an example of a non-associative special LA-ring, we also find example of an LA-ring that fails to become a special LA-ring. In 2011, Shah and Rehman presented few basic characteristics and properties of LA-rings including some conditions that cannot hold in an LA-ring, as they make it an additive abelian group. It was observed that, these conditions when hold in an LA-ring, turns it into a special LA-ring. We present these conditions as some criterion for an LA-ring to be a special LA-ring. Rehman et al. in 2013 demonstrated the existence of non-associative LA-ring, they used MACE4 to obtain different examples of non-associative LA-rings and LA-fields. MACE4 exhausted at the Order 64 and they couldn't explore examples of LA-rings having order greater than 18. Since our focus is on special LA-rings, we use the same software to find examples of non-associative special LA-rings, but it gave up at order 49 and the greatest order special LA-ring that we obtain has order 32. The urge to search for higher order special LA-rings motivated us to the construction of an algorithm, that takes a special LA-ring of order n as input and gives a special LA-ring of order n^{m+1} as output, where $n \geq 2$ and m are positive integers. Same algorithm can be used to obtain LA-rings (that are not special LA-rings) of greater orders. Examples of special LA-rings and the above mentioned algorithm are given in Section 3.2. In Section 3.3, we illustrate how a commutative and associative ring R and an LA-semigroup L together give rise to a special LA-ring called an LA-semigroup ring and denoted as $R[L]$. It contains finitely non-zero functions having R as codomain, codomain, similar to a group ring, semigroup ring or a loop ring. The domain in our case

is an LA-semigroup. The discussion in this section is based on the and basic results that hold in $R[L]$ and further depend on the properties of R and L . In Section 3.4, for the first time the concept of concept of divisibility in LA-rings is discussed, we introduce the notions of prime and irreducible elements, prime and maximal left ideals and study their mutual connections. Few results directly follow from the commutative ring theory, but some require the constraint of idempotency. An ordinary LA-ring cannot be idempotent, as the condition of idempotency makes it a special LA-ring. But in case of special LA-rings we have the liberty of considering the condition of idempotency. The Section 3.5 is about polynomial formation over special LA-rings. The main idea of this section is to discuss factorization of such polynomials. For this purpose we present Division Algorithm, Remainder theorem and Factorization theorem for polynomials over a special LA-ring. Due to lack of associativity and commutativity in a special LA-ring, these theorems are stated and proved in a different manner from their classical versions. We also introduce Euclidean LA-domain and special LA-field extensions in this section.

In Chapter 4, we explore some applications of LA-rings in soft set theory. The soft set theory is a successful tool to study the vagueness in data, it is a relatively new approach to handle uncertainty of the information in many situations. In Section 4.1, we connect the generalized rough sets with soft sets to get a hybrid model of generalized rough soft sets or T-rough soft sets. A decision making algorithm based on T-rough soft sets is constructed. We introduce T-rough LA-rings and T-rough soft LA-rings and studied the properties of their ideals. Some new notions are defined and a decision making method for T-rough soft LA-rings is also included in this section. In Section 4.2, soft-intersection special LA-rings are introduced and some fundamental properties of soft-intersection LA-rings and soft-intersection ideals of LA-rings are discussed. We show how a soft-intersection ring and a soft-intersection LA-semigroup give rise to a soft-intersection special LA-ring.

In Chapter 5, we find applications of LA-rings in Coding theory and construct linear cyclic codes over special LA-rings. In Section 5.1, we briefly introduce special LA-vector space as a generalization of LA-module. Section 5.2 provides the construction of linear cyclic codes over special LA-fields and in Section 5.3, we study DNA cyclic codes over a special LA-field of order 4 denoted F_{SLA4} . F_{SLA4} is a reasonable choice for constructing DNA codes as it has a one-to-one correspondence with the DNA alphabet $\{A, C, G, T\}$, where A, C, G and T denote Adenine, Cytosine, Guanine and Thymine which are the nu-

cleotides or the building blocks of DNA. The joining of the two oppositely oriented strands of DNA is facilitated by the bonding of the nucleotides present on each strand and is called the process of hybridization. Several techniques have been proposed so far to construct a set of DNA codewords that are not likely to make unwanted bonds with one another by hybridization. An efficient Algorithm for the construction of reversible complement cyclic codes over F_{SLA_4} is included in this section. These codes are highly suitable for DNA computations as they satisfy the ‘Hamming constraint’ and the ‘Reverse-complement constraint’ that ensure a reliable process of hybridization. The codes constructed in this section are generalization of the reversible complement cyclic codes over the Galois field $GF(4)$ of order 4. For computational convenience, we choose to construct codes of odd lengths only.

Chapter 6 is about the applications of LA-rings and algebras in Cryptography. Cryptography is the way of keeping the information confidentiality using mathematical approaches and methods. The substitution box (S-box) is one of the main components of symmetric key cryptosystem. Typically, the S-boxes are constructed over a Galois field, hence a Galois cyclic group and some other commutative and associative algebraic structures. In Section 6.1, small (4×4) S-boxes are designed over a special LA-field of order 16, accordingly these will be utilized in light weight cryptography. The purpose of these S-boxes designing is to increase the robustness due to non-associative and non-commutative behavior of LA-rings. We have used the Majority Logic Criterion (MLC) to judge the strength of these newly formed S-boxes in image encryption. Thus S-boxes are obtained are having high resistance against existing cryptanalysis attacks. A watermarking application of these S-boxes is given along with their comparison in the context.

In Section 6.2, A triplet of 8×8 S-boxes is designed using an LA-ring of order 512. The motivation behind the designing of these S-boxes is to upsurge the robustness and broaden the key space due to non-associative and non-commutative behavior of the algebraic structure under consideration and increase 65,536 times the key space. Thus, the obtained S-boxes having significant level of resistance against existing cryptanalysis attack. A novel color image encryption application is anticipated in which initially these 3 S-boxes are being used to produce confusion in three layers of a standard RGB image. However, for the sake of diffusion 3D Arnold chaotic map is used in the proposed encryption scheme. A comparison with some of existing chaos and S-box dependent color

image encryption schemes specs the performance results of the anticipated RGB image encryption and observed as approaching the standard prime level.

Lastly in Chapter 7 we give conclusion of our work and also give some future prospects of this study.

Contents

1	Background and Preliminaries	10
1.1	Left Almost Rings (LA-rings)	10
1.2	Soft Sets, Soft LA-rings and Rough Sets	11
1.2.1	Soft LA-rings	13
1.2.2	Rough Sets and Generalized Rough Sets	13
1.3	Coding Theory and DNA Computing	14
1.3.1	The Structure of DNA and the Process of Hybridization	15
1.3.2	DNA Coding	16
1.4	Cryptography	17
1.4.1	Boolean Functions and their Properties	18
1.4.2	Theory of S-box	19
2	A Survey on LA-ring Theory and its Generalizations	21
2.1	2010-2011	22
2.2	2012-2013	23
2.3	2014-2015	24
2.4	2016-2018	25
2.5	2019-2020	26
3	Developments in LA-ring Theory	28
3.1	LA-rings to Special LA-rings	28
3.2	Examples of a Non-associative Special LA-ring and Extensions of LA-rings	31
3.2.1	Examples of Special LA-rings of Smaller Orders	31
3.2.2	Constructing the Special LA-ring $\sum_{l=0}^{l=m} w^l R_{SLA_n}$	32
3.3	LA-semigroup rings	37

3.3.1	Basic Structure	37
3.3.2	Representation of Elements of N	40
3.3.3	Sub LA-rings and Ideals in LA-semigroup Rings	43
3.3.4	Homomorphisms and LA-Semigroup Rings	47
3.4	Divisibility Theory in LA-Domains	51
3.4.1	LA-field and LA-integral Domain	52
3.4.2	Prime and Maximal Left Ideals	52
3.4.3	Divisibility in LA-rings	54
3.4.4	Prime and Irreducible Elements	57
3.5	Polynomial Formation of a Special LA-ring	60
3.5.1	Factorization of the Polynomials over a Special LA-ring	61
3.5.2	Euclidean LA-domain and LA-field Extension	66
4	Developments in Soft LA-rings	69
4.1	Generalized Rough Soft LA-rings	69
4.1.1	Generalized Rough Soft Sets	70
4.1.2	Generalized Rough LA-rings	72
4.1.3	Generalized Rough Soft LA-rings	78
4.2	Soft Intersection LA-rings	87
4.2.1	Soft Intersection LA-groups	88
4.2.2	Soft Intersection LA-rings	89
4.2.3	Construction of SI-special LA-rings and SI-ideals	97
5	Applications to Coding Theory	103
5.1	Special LA-Vector Space	103
5.2	Linear Cyclic Codes over a Special LA-field for DNA Computations	104
5.3	DNA Cyclic Codes over a Special LA-field	108
6	Applications to Cryptography	113
6.1	Cryptosystem Design over a Special LA-field	113
6.1.1	S-box Construction over a Non-associative LA-field of Order 16	114
6.1.2	Majority Logic Criterion for the Analysis of S-Boxes	120
6.1.3	Differential Cryptanalysis on LA-field F_{SLA} based S-box	120
6.1.4	Propagation Ratio	123

6.1.5	Watermarking Applications	123
6.2	LA-ring Based Construction of 8×8 S-boxes with an Image Encryption Application	124
6.2.1	Generating Algorithm for Pair of S-boxes	126
6.2.2	Key Space Analysis	130
6.2.3	Performance analysis of S-boxes	131
6.2.4	RGB Image Encryption	133
6.2.5	Texture Analysis of Image Encryption	137
6.2.6	Analyses of Experimental Work	142
6.2.7	Security Measurement	146
6.2.8	Randomness of Test for Cipher	147
7	Conclusions	150

Chapter 1

Background and Preliminaries

This chapter serves as the introduction of our research work. The basic concepts and definitions are included that provide background information for the material in the proceeding chapters. The concise history and basic properties of LA-rings, soft sets, soft LA-rings, rough sets, coding theory, DNA coding, cryptography and S-boxes are discussed in this chapter. The preliminaries of these structures, definitions and some fundamental results are provided which have direct relation with our work. This chapter has four sections. In the first section, some basic definitions and results of LA-rings which are repeatedly used in further discussion are provided. The second section deals with soft sets, soft LA-rings and rough sets. Third section is about Coding theory, DNA structure and DNA computations. In the last section, we throw some light upon basics of cryptography.

1.1 Left Almost Rings (LA-rings)

A groupoid satisfying the condition " $(ab)c = (cb)a$ " (known as the left invertive law), is said to be an LA-semigroup [77]. Clearly, a commutative semigroup is an LA-semigroup. Later this concept was extended and LA-group [100] was defined as an LA-semigroup L containing a left identity element ' e ' and inverses of each of its elements. In case of an additive LA-group the left identity would be called left zero element and would be denoted by ' 0 .' For more details on LA-groups we recommend: [124]. The two concepts gave rise to LA-ring [131] as a new kind of non-associative rings, which is in fact a non-empty set R_{LA} equipped with an operation of addition that makes it an "LA-group," a multiplication operation with respect to which it is an "LA-semigroup" and the two distributive laws of

multiplication over addition. Shah and Shah [134], discovered some fundamental properties of LA-rings. For instance, they proved that an LA-ring always satisfies the "medial law $(ab)(cd) = (ac)(bd)$ " and in case if it has (multiplicative) left identity element 'e' then it satisfies the "paramedial law $(ab)(cd) = (db)(ca)$." Shah and Rehman [131], developed the notion of zero divisors in LA-rings as an analogue of the same for associative rings. An LA-integral domain is an LA-ring having a left identity element and holding no zero divisors, while an LA-field is an LA-ring which contains left identity element and the inverse of each of its non zero elements. A subset of an LA-ring with at least one element is called its sub LA-ring if it is itself an LA-ring. A left (right) ideal of an LA-ring R_{LA} is a sub LA-ring S such that $R_{LA}S \subseteq S$ ($SR_{LA} \subseteq S$). A left as well as a right ideal is called an ideal. Further, Shah and Rehman [132], defined a "principal left ideal" generated by an element $a \in R_{LA}$, as the set $\langle a \rangle = R_{LA}a = \{ra : r \in R_{LA}\}$ where R_{LA} is an LA-ring with left identity. If an element $0 \neq a \in R_{LA}$ possesses multiplicative inverse it would be called a unit in R_{LA} . Rehman [110], showed that the set of all units in an LA-ring is an LA-group.

Though the idea of a quotient LA-ring was already introduced in [131], Shah and Raees [128], defined a quotient LA-ring using a left ideal. Let R_{LA} be an LA-ring with left identity and K be a left ideal of R_{LA} , $R_{LA}/K = \{K + r : r \in R_{LA}\}$ is an LA-ring containing $K + e$ as left identity. Here 'e' is the left identity element in R_{LA} . The elements in R_{LA}/K are called additive cosets and satisfy the following two properties:

1. for $a \in R_{LA}$, $K + a = K$ iff $a \in K$.
2. for $a, b \in R_{LA}$, $K + a = K + b$ iff $b - a \in K$.

1.2 Soft Sets, Soft LA-rings and Rough Sets

The Fuzzy set theory is one of the ancient tools used to handle vagueness and uncertainties in the data. Molodtsov [97], presented the soft set theory as a generalization of the fuzzy set theory, which deals with such problems in a parametric fashion. Many applications of this theory can be observed in different fields such as operation research, game theory, smoothness of functions, Perron integration, Riemann integration, probability theory and measure theory. Maji et al. [90], stepped forward and applied soft sets to find solution of a decision making problem. They presented different operations on soft sets. The theory was

further enhanced by many researchers, several new notions and operations were discovered [14, 119]. An important step was the introduction of soft relations and functions that was achieved by Babitha and Sunil in [19].

Molodtsov [97] defined a soft set as a parameterised family of sets. For an initial universe U with power set denoted by $P(U)$ and a subset A of a collection E of parameters, (f, A) denotes a soft set where f is a function from A into $P(U)$. Later Çağman and Enginoğlu redefined soft sets and their operations. The new operations are more practical for further study of soft set theory and improvement of many results. Following definitions of soft set and related operations are taken from [28].

Definition 1.2.1. "A soft set g_A over U is a set defined by a function g_A representing a mapping $g_A : E \rightarrow P(U)$ with $g_A(a) = \emptyset$ for all elements a of E which are not in A .

A soft set over U can be represented by the set of ordered pairs

$$g_A = \{(a, g_A(a)) : a \in E, g_A(a) \in P(U)\}.$$

Clearly soft set is a parameterized family of subsets of the set U . Throughout, $S(U)$ would denote the set of all soft sets over U ."

Definition 1.2.2. "Let g_A be a soft set over U , then

1. If $g_A(a) = \emptyset$ for each $a \in E$, then g_A is called a empty soft set, denoted by g_\emptyset .
2. If $g_A(a) = U$; for all $x \in A$, then g_A is called A-universal soft set, denoted by $g_{\bar{A}}$. If $A = E$, then the A-universal soft set is called universal soft set denoted by $g_{\bar{E}}$."

Definition 1.2.3. "For two soft sets g_A and g_B be over U ,

1. g_A is called a soft subset of g_B , denoted $g_A \widetilde{\subseteq} g_B$, if $g_A(a) \subseteq g_B(a)$ for each $a \in E$.
2. g_A and g_B are said to be soft equal denoted $g_A = g_B$, if $g_A(a) = g_B(a)$ for all $a \in E$.
3. the union of g_A and g_B is denoted by $g_A \widetilde{\cup} g_B$ is the soft set defined by the approximation function $g_{A \widetilde{\cup} B}(a) = g_A(a) \cup g_B(a)$, for each $a \in E$.
4. the intersection of g_A and g_B is denoted by $g_A \widetilde{\cap} g_B$ is the soft set defined by the approximation function $g_{A \widetilde{\cap} B}(a) = g_A(a) \cap g_B(a)$, for each $a \in E$, such that $g_A(a), g_B(a) \neq \emptyset$.

5. the \wedge -product of g_A and g_B , denoted by $g_A \tilde{\wedge} g_B$, is the soft set defined by the function $g_{A \tilde{\wedge} B} : E \times E \rightarrow P(U)$, $g_{A \tilde{\wedge} B}(x, y) = g_A(a) \cap g_B(b)$, for all $(a, b) \in E \times E$, such that $g_A(a), g_B(b) \neq \emptyset$.
6. the \vee -product of g_A and g_B , denoted by $g_A \tilde{\vee} g_B$, is the soft set defined by the function $g_{A \tilde{\vee} B} : E \times E \rightarrow P(U)$, $g_{A \tilde{\vee} B}(a, b) = g_A(a) \cup g_B(b)$, for all $(a, b) \in E \times E$."

1.2.1 Soft LA-rings

Aktaş and Çağman [9] are the first to find applications of soft set theory in algebra. They defined a soft group and discussed its fundamental features. Then Acar et al. [3] presented the idea of soft rings and the notion of a soft LA-semigroup was set forth by Aslam et al. in [18]. To study more soft algebraic structures we recommend: [16, 29, 45, 72, 87].

Shah et al. [129, 130], made a new approach to extend the study of soft rings and introduced soft LA-rings. Here we are restating the definitions of soft LA-rings and related concepts from [129, 130], using Çağman's definition for soft sets.

Definition 1.2.4. Let R_{LA} be an LA-ring. A "soft LA-ring" over R_{LA} is a non-empty soft set g_A over R_{LA} with the property that for each $a \in E$, if $g_A(a) \neq \emptyset$ then $g_A(a)$ is a sub LA-ring of R_{LA} .

Definition 1.2.5. An "idealistic soft LA-ring" over R_{LA} is a non-empty soft set g_A over R_{LA} such that; $g_A(a)$ is an ideal of R_{LA} for each $a \in E$ whenever $g_A(a) \neq \emptyset$.

Definition 1.2.6. A non-empty subset g_B of a soft LA-ring g_A over R_{LA} is said to be;

1. a soft M-system, if for every $g_B(a), g_B(b) \in g_B$, there is some $g_A(x) \in g_A$ such that $g_B(a)(g_A(x)g_B(b)) \in g_B$.
2. a soft P-system, if for all $g_B(a) \in g_B$, there is some $g_A(x) \in g_A$ with the property that $g_B(a)(g_A(x)g_B(a)) \in g_B$.

1.2.2 Rough Sets and Generalized Rough Sets

Pawlak [106] introduced "rough set theory" as a novel branch of uncertainty mathematics having close relation with the "fuzzy set theory." Both rough and soft sets are generalizations of classical sets and complement each other. The lower and upper rough approximation spaces are sets with multiple memberships, while fuzzy sets are concerned with

partial memberships. The frequent progress of these two theories establishes a framework for "soft computing," initiated by Zadeh [152]. Soft Computing not only includes rough sets, but fuzzy logic, probabilistic reasoning, belief networks, neural networks, evolutionary computing, machine learning and chaos theory.

The theory presented by Pawlak is based on an equivalence relation τ on a non-empty finite set U called the universe. The pair (U, τ) is termed as an approximation space. Following are the definitions of the lower and upper approximations of a $D \subseteq U$.

$$\underline{\tau}(D) = \{x \in U : [x]_{\tau} \subseteq D\} \quad (1.2.1)$$

$$\overline{\tau}(D) = \{x \in U : [x]_{\tau} \cap D \neq \emptyset\}. \quad (1.2.2)$$

The pair $(\underline{\tau}(D), \overline{\tau}(D))$ is rough set. In case, if $\underline{\tau}(D) = \overline{\tau}(D)$ then we say D is definable. Fundamentals of rough sets can be seen in [106].

Pawlak's approximations require some equivalence relation and sometimes due to incomplete information, such an equivalence relation is hard to establish. To overcome this problem, Couois et al. [33] introduced a T-rough set as a generalized Pawlak's rough set, which is based on a set valued mapping. Davvaz [37] further improved the notion of generalized approximation spaces and discussed generalized rough sets.

Definition 1.2.7. [147] "For two non-empty sets V and W , and a set valued map $T : V \rightarrow P^*(W)$ (where $P^*(W)$ denotes the collection of all non-empty subsets of W), the triplet (V, W, T) is called a generalized approximation space or generalized rough set. If L is a subset of W , then the lower and upper approximations of L are defined as:

$$\underline{T}(L) = \{x \in V | T(x) \subseteq L\} \quad (1.2.3)$$

and

$$\overline{T}(L) = \{x \in V | T(x) \cap L \neq \emptyset\}. \quad (1.2.4)$$

The pair $(\underline{T}(L), \overline{T}(L))$ is called a T-rough set (generalized rough set)."

For more details on generalized rough sets we recommend [13].

1.3 Coding Theory and DNA Computing

Coding theory is the science that deals with the detection and correction of errors that occur when some information is transmitted through some communication channel. The

data is usually carried in form of string of symbols or bits from a transmitter to a receiver. Error-correcting codes are significant for achieving higher reliability that is required in modern data transmission and storage systems. Some relevant definitions from [101] are given below:

"If A is a finite set with $q(> 1)$ symbols that can be transmitted, then any non-empty subset C of A^n is called a q -ary code of length n over A . Where n is a positive integer greater than 1, A^n is the set of all n -tuples of elements of A and A is called the alphabet of transmission. Each element of C is called a codeword."

"The Hamming distance between two codewords of same length is the number of positions at which the corresponding symbols differ. It is named after the American mathematician Richard Hamming." A linear code is defined to be a subspace of the vector space F^n over a finite field F . It is an error correcting code.

The mapping $\sigma : F^n \rightarrow F^n$ such that,

$$\sigma(a_1, a_2, \dots, a_n) = (a_n, a_1, \dots, a_{n-1}) \quad (1.3.1)$$

is a linear transformation and is called the cyclic shift. A linear code C , that is invariant under the cyclic shift is called a cyclic code. That is, for all $a \in C$, $\sigma(a) \in C$.

1.3.1 The Structure of DNA and the Process of Hybridization

Deoxyribonucleic acid (DNA) is the fundamental programming unit of life with incredible density of data. It carries all the genetic information and instructions required to build and run a human body. DNA consists of two long strings called polynucleotides or DNA strands, each consisting of four building blocks called nucleotides viz: "Adenine," "Cytosine," "Guanine" and "Thymine" denoted by the letters A , C , G and T respectively, each strand has distinct polar ends called 3' end and 5' end. The two oppositely oriented and twisted strands of DNA form a double helix. Joining of the two strands is facilitated by the formation of hydrogen bonds between the nucleotides. This process is called hybridization or base pairing and it follows the Watson-Crick complement (WCC) model, which states that each A joins with a T and each C with a G and conversely. The complements of A , C , G and T are T , G , C and A respectively. The two strands are combined in opposite direction and in reversed order. For instance, a DNA $5' - ACGATTC - 3'$ strand will be coupled with strand $3' - TGCTAAG - 5'$.

1.3.2 DNA Coding

DNA computing is a blend of genetic data analysis and computational science, so that the computational difficulties may be addressed. Adleman [5], first demonstrated DNA computing while solving a tough (NP-complete) computational problem. He utilized the notion of DNA hybridization on which any DNA computation is based.

A DNA code has to satisfy at least one of the constraints, namely: "the Hamming constraint for a distance d , the reverse constraint, the reverse-complement constraint, and the fixed GC-constraint." For more details we recommend to see [92].

The advancements in the applications of algebraic coding to the DNA codes stimulated the interest of coding theorists to use rings for the construction of DNA codes. Because of having an equivalence with the DNA alphabet $\{A, C, G, T\}$, rings and fields consisting of four elements are particularly used for DNA codes. In [117], Rykov et al. introduced the DNA codes, that are quaternary reversible complement cyclic codes, they considered the reverse constraint only. Gaborit and King [47], presented some new constructions for additive and linear codes over four-letter alphabets, particularly, they constructed DNA codes over $GF(4)$. Their codes satisfy either a reversible complement constraint, a GC-content constraint or both. Abualrub et al. [1], developed cyclic codes having large number of codewords over $GF(4)$. Then more DNA cyclic codes over the ring $F_2 + uF_2$ were constructed in [53, 82]. Moreover, the construction of additive self dual codes over $GF(4)$ and Linear self dual codes over \mathbb{Z}_4 that are suitable for DNA computations were studied in [137] and [43] respectively.

Gradually researcher's interest shifted to the construction of DNA codes over fields and rings of order 4^n , where $n \in \mathbb{N}$ for DNA computing applications. For instance, in 2012, Yildiz and Siap [151], for first time considered the ring $F_2[u]/(u^4 - 1)$ to develop DNA "cyclic codes." Bennanni et.al in [21] generated DNA codes from the cyclic codes over the ring $F_2[u]/(u^6)$, using edit distance. Bayram et al. [20], investigated linear, cyclic and constacyclic codes over $F_4[v]/(v^2 - v)$, they provided some examples of DNA codes over that ring that attain Griesmer bound. In [161], Zhu et al. studied the construction of the DNA cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$. Dertli and Cengellenmis in [38], explored the DNA codes generated from the cyclic codes over $\mathbb{Z}_4 + w\mathbb{Z}_4$ and $\mathbb{Z}_4 + w\mathbb{Z}_4 + v\mathbb{Z}_4 + uv\mathbb{Z}_4$, they established a link with elements of these rings and DNA codons. Limbachiya et al. [83] introduced some new families of DNA codes over the ring $\mathbb{Z}_4 + w\mathbb{Z}_4$.

1.4 Cryptography

Cryptology is the science dealing with storage and data communication in secure and typically secret form. There are two further subdivisions of cryptology viz; cryptography and cryptanalysis. Cryptography is the way of keeping the information secrecy using mathematical methods. Whereas cryptanalysis is the art of cracking encrypted information by the means of mathematical and computational devices. It is powerful enough to breach the cryptographic security systems, without accessing the cryptographic key, and it obtains permissions to the content of encrypted communications. Although, both cryptography and cryptanalysis aim at the same target, however the methods and techniques for cryptanalysis have been modified radically throughout the history of cryptography.

Some common terminologies are used in cryptography. An original message is called plaintext and the coded message, a ciphertext. Encryption (or enciphering) is the process through which a plaintext is converted into the ciphertext, while the conversion of ciphertext into its original form is called decryption (or deciphering). The cryptography secures the information through the encryption and decryption and it has two major kinds; "symmetric key cryptography" and "asymmetric key cryptography."

"Symmetric key cryptography" involves the encryption and decryption of information using a common confidential code, called the encryption key or simply a key. While in the "asymmetric key cryptography," a pair of private and public keys is used for the enciphering and deciphering of information respectively. A cryptographic technique or a cipher is a safe procedure of transferring a confidential message over some line of communication. It comprises a formal mathematical algorithm to encrypt or decrypt the data. Symmetric key cryptosystems are either stream ciphers or block ciphers. A bit is most basic unit of information in computing and a group of 8 bits is called a byte. The algorithm of a block cipher works on fixed-length groups of bits, known as blocks. Typically, modern block ciphers involve the operations of substitution and permutation on plain text data bytes and in the process of substitution, a substitution box (S-box) is used to replace an input block with another output block [15].

1.4.1 Boolean Functions and their Properties

Boolean algebra, a branch of algebra named after the mathematician George Boole (1815-1864) is a wide-ranging area in itself. In the following, we present some fundamentals on Boolean functions that are necessary for the understanding of S-box theory.

Consider the m -dimensional vector space \mathbb{Z}_2^m over the Galois field $\mathbb{Z}_2 = \{0, 1\}$. \mathbb{Z}_2^m comprises of 2^m binary sequences of length m and it is facilitated with the scalar product $\langle \cdot, \cdot \rangle: \mathbb{Z}_2^m \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$. Where

$$\langle x, y \rangle = \bigoplus_{k=1}^m x_k \odot y_k.$$

Here \odot and \oplus denote respectively the multiplication and addition over \mathbb{Z}_2 .

Definition 1.4.1. "A Boolean function is a function h from \mathbb{Z}_2^m to \mathbb{Z}_2 . The truth table of h is a (0,1)-sequence defined by $(h(x_0), h(x_1), \dots, h(x_{2^m} - 1))$, ordered by the lexicographic ordering."

Definition 1.4.2. [35] "A linear Boolean function is a function $L_\gamma: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$ defined by

$$L_\gamma(x) = \gamma_1 x_1 \oplus \gamma_2 x_2 \oplus \dots \oplus \gamma_m x_m,$$

where $\gamma_j x_j$ is the bitwise AND of the j -th bits of γ and x , while \oplus represents bitwise XOR."

Definition 1.4.3. [61] "Affine Boolean functions is a collection of linear Boolean functions together with their compliments

$$A_{\gamma,c} = L_\gamma(x) \oplus c,$$

where $x \in \mathbb{Z}_2^m$. A sequence of affine (linear) functions is called an affine (linear) sequence."

Definition 1.4.4. [35] "The class of all single valued Boolean functions is given by

$$G_m = \{g|g: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2\}. \quad (1.4.1)$$

The collection of all affine Boolean functions in G_m is denoted as

$$A_m = \{g|g: g \in G_m \text{ and } g \text{ is affine } \}, \quad (1.4.2)$$

and the set of all linear Boolean functions in G_m is given by

$$L_m = \{g|g: g \in G_m \text{ and } g \text{ is linear } \}." \quad (1.4.3)$$

Remark 1.4.5. All linear functions and their negations form the set of all affine functions.

Definition 1.4.6. " The nonlinearity of a Boolean function h is defined to be the distance between h and the set of all affine linear functions."

1.4.2 Theory of S-box

Boolean functions provide a framework for symmetric cryptographic systems. They are used to design S-boxes in block ciphers and are their nonlinear elements. Boolean functions with higher nonlinearity and excellent cryptographic properties have great significance in the construction of block ciphers.

A routine sequel of the single output Boolean function theory is to extend it to the Boolean functions with multiple outputs, along with referred as a substitution box (S-box) [144]. The connection betwixt the input and output bits regarding dimension and inimitability engenders numerous S-boxes. An $m \times l$ S-box is a function $\varphi : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^l$ from m input to l output binary bits, while the total number of inputs and outputs are 2^m and 2^l respectively. Then, an S-box is fair a collection of l single output Boolean functions joint in a fixed manner. The dimension of an S-box has an upshot on the exclusivity of the output and the input, which may affect the characteristics of S-box. In case, if we have an S-box with dimension $m \times l$, where $l < m$ (that is the input bits are greater in number compared to output bits), then there would be repetition of certain entries in the S-box. However, an $m \times m$ S-box, might whichever contain different entries, where all the inputs are mapped to distinct outputs, or some of them may duplicate various entries of the S-box. Injective as well as surjective S-boxes are called bijective S-boxes and they possess inverses (see [4, 61]). One of the key parts of all the cryptosystems is S-box, which styles the system non linear. While improving a symmetric (or private-key) cryptosystem, that is built as a substitution-permutation network (S-P network) (DES or AES-like system), most of the nonlinearity is felt in the S-boxes portion of the algorithm. This permits rest of the algorithm to be linear. Modest softness in the S-boxes can hence result in cryptosystems, that are just broken. S-boxes are used as an irritating scheme that authorises robustness of cryptographic algorithms. Hence, in order to figure a secure cryptosystem the design of S-boxes have to be cryptographically resilient [4, 66, 144]. In traditional and modern cryptography, the S-boxes are normally built over finite Galois fields ($GF(2^m)$ for $2 \leq$

$m \leq 8$), such as AES [36], Residue Prime S-box [67], Gray S-box [138], APA S-box [34], Xyi S-box [148], Skipjack S-box [81] and S_8 AES S-box.

Chapter 2

A Survey on LA-ring Theory and its Generalizations

Until the mid of 19th century, the rings and algebras considered were only the associative (and commutative) rings and algebras, for instance, numbers rings, functions rings, and the rings of abelian group endomorphisms. Later on, the introduction of non-associative rings and algebras brought a significant change.

Non-associative ring has flourished as a stand alone branch of algebra, having connections with several branches of mathematics and other fields, for instance, biology, physics and other sciences.

In the year 1843, J.T. Graves introduced the very first non-associative rings, called Octonions. In 1845, Arthur Cayley constructed an abstract non-associative ring consisting of Cayley numbers. Later in 1870, Sophus Lie introduced an interesting class of non associative rings called Lie theory. Furthermore, in 1930 a German researcher, Zorn opened up a discussion on Alternative rings [157–160]. For details see: ‘Jacobson’ [69], ‘Albert’ [11] and ‘Dubisch and Perlis’ [40]. Further in 1932-1933, a German researcher Jordan introduced some non-associative structures, which were named after him as Jordan structures. These structures play a pivotal role in quantum group theory and also appear in recent fundamental physics theories. Further, the non-associative structure of loop was introduced in 1930’s [107]. The details of loop theory can be found in [10, 11, 23, 25]. Bruck [24], introduced a non-associative loop ring in 1944.

In 1972, Kazim and Naseeruddin [77], introduced a left almost semigroup (LA-semigroup) (also known as an Abel Grassman-groupoid (AG-groupoid)) and defined it to be

a groupoid S satisfying the left invertive law i.e. for each a, b, c in S , $(ab)c = (cb)a$. An LA-semigroup is a mid way structure between a semi group and a groupoid. In the year 1996, Mushtaq and Kamran outstretched the concept of Left almost semigroup to left almost group (LA-group or AG-group) [100]. An LA-semigroup S becomes an LA-group when it contains a left identity element and each element of S possesses an inverse within S . Some basic properties of LA-groups are presented in [124].

In the year 2010, Shah and Rehman [131], extended the notions of LA-group and LA-semigroup to present a new ring structure, where the operations ‘+’ and ‘.’ are non-associative, and named it as a left almost ring (LA-ring). It is in fact an upshot of LA-group and LA-semigroup. Due to their non-commutative and non-associative nature, LA-rings have been emergent as a utilitarian non-associative class which instinctively would have practical contributions to the development of the non-associative ring theory. It is defined as: "a non-empty set R_{LA} having more than one element, such that $(R_{LA}, +)$ is an LA-group and (R_{LA}, \cdot) is an LA-semigroup and holds both left and right distributive laws." An LA-ring (R, \oplus, \cdot) can always be obtained from a commutative ring $(R, +, \cdot)$, where $a \oplus b = b - a$ and the operation of multiplication ‘.’ is same as in R . For detailed study of structure of LA-rings and their generalizations we recommend: [108, 110, 133, 134].

2.1 2010-2011

In [131], the authors generalized the notion of a commutative semigroup ring $R[X; S]$ of a commutative semigroup S over an associative ring R and constructed a non-associative LA-ring $R_{LA}[X^s; s \in S]$ comprising of finitely nonzero functions from a semigroup S into an LA-ring R_{LA} . They also defined the concepts of degree and order of an element in $R_{LA}[X^s; s \in S]$ parallel to $R[X; S]$. However, it also contains associative ring structures. They gave definitions of LA-field and LA-integral domain and in the same paper, they presented the ideas of an LA-module, quotient LA-ring and LA-ring homomorphism. In the same year, Shah et al. [135] introduced topological LA-groups and topological LA-rings as generalized topological groups and topological rings respectively. They proved that "the product of any collection of topological LA-rings is again a topological LA-ring and a sub LA-ring of a topological LA-ring inherits the property of being a topological LA-ring."

Shah and Shah [134], in the year 2011, presented some fundamental properties and useful facts about LA-rings that are helpful to understand the basic structure of LA-rings. The results studied by them are useful for future research and developments. Along with basic results, they proved that an LA-ring can never be idempotent and also right distributive property implies left distributive property in an LA-ring with left identity 'e'. Later in 2011, Shah et al. [128] proceeded to promote the concept of LA-module introduced in [131] and developed the substructures of LA-modules, their operations and elementary properties. They also defined quotient of an LA-module by its LA-sub module. They also demonstrated the dissimilarity of an LA-module to the standard idea of a module. In the same year, Shah et al. [133] presented a generalization of LA-rings and introduced the concept of near left almost rings (nLA-rings) $(R_{LA}, +, \cdot)$. Here R_{LA} is an additive LA-group and with respect to multiplication it is an LA-semigroup, where one sided distributive property holds. They observed that many properties that usually hold in near rings and LA-rings are also valid for nLA-rings but unlike near-ring, in an nLA-ring the zero symmetric part and the constant part do not exist. In wake of its structural properties an nLA-ring behaves similar to a commutative ring and a commutative near ring yet it is non-commutative and non-associative. In addition, Shah et al. [125] in 2011 gave a characterization of nLA-rings through their ideals. They presented the necessary and sufficient conditions for an nLA-ring to be direct sum of its ideals. Moreover, they discovered that the sum of ideals is again an ideal but the product of ideals is just a left ideal.

2.2 2012-2013

In the year 2012, Shah and Rehman [132] provided some characterizations of LA-rings relative to several properties of their ideals. They established the necessary and sufficient conditions for an LA-ring to be fully prime. Furthermore, they included some discussion on M-system, P-sysetm, I-system, subtracting sets in an LA-ring and proved the conditions under which a left ideal becomes an M -system, P-system or an I -system. Furthermore, they showed that "a subtractive subset of an LA-ring is semi-subtractive and a quasi-prime ideal of an LA-ring with left identity is semi-subtractive."

In 2012, Shah et al. [127] extended the notion of fuzzy normal subrings in associative rings to define intuitionistic fuzzy normal LA-subrings of LA-rings. The authors broaden

the notions for LA-rings and established some concepts for intuitionistic fuzzy normal LA-subrings of LA-rings. They also investigated the conditions under which an intuitionistic fuzzy set becomes an intuitionistic fuzzy normal sub LA-ring of an LA-ring R_{LA} .

In 2013, Rehman et al. [113] made a major development, when they established the existence of a non-associative LA-ring by giving some non-trivial examples. They used a mathematical software Mace 4 to establish these examples. The authors, due to the existence of non-trivial LA-rings, were able to nullify the confusion regarding associative multiplication since the first examples of LA-rings were trivial. They also introduced in the same paper, a special LA-ring as: an additive abelian group, multiplicative LA-semigroup with both distributive laws. Later in 2013, Gaketem [48] worked on a generalization of an LA-ring called a P-regular nLA-ring and explored some properties of its quasi-ideals.

2.3 2014-2015

Alghamdi and Sahraoui [12] in 2014, established a tensor product of LA-modules as an expansion of the notion of an LA-module introduced in [131]. The newly constructed structure acts similar to the conventional tensor product of typical modules over a ring, albeit the LA-groups and LA-modules are not required to be abelian. They provided some generalizations of fundamental results of the ordinary tensor. In the same year, Yiarayong [149], carried out a study on left ideals, left primary and weakly left primary ideals in LA-rings and studied their mutual relationships. Gaketem in 2014 [49], preferred to call a left almost ring (LA-ring) as Abel-Grassmann ring (AG-ring), defined c-prime, 3-prime, weakly prime ideal of AG-ring and studied their mutual relation. Also in 2014, Kellil in his paper [78], introduced the notions of an LA-semiring, a strong LA-semiring and then a *-LA-semiring. Many results obtained for semirings are also valid in the new setting. The author investigated the relationship between the additive and multiplicative idempotents and also proved that in case of a strong LA-semiring S , the set of multiplicative idempotents; $E^*(S)$ is closed under multiplication and so $(S, +, \cdot)$ is an orthodox strong LA-semiring.

In the year 2015, Hussain and Khan [58] used congruence relations to provide some new characterizations of LA-rings and demonstrated that how each LA-ring homomorphism gives rise to a congruence relation on LA-rings using some good examples. Further,

they discussed quotient LA-rings and proved isomorphism theorems for LA-rings. In the same year, Shah and Razzaque [129], for the first time investigated soft LA-rings and explored their several algebraic properties. Previously the applications of soft set theory were restricted to associative structures only. The authors introduced soft M-systems, soft P-systems, soft I-systems and studied soft irreducible ideals, soft strongly irreducible ideals soft quasi-prime ideals and soft quasi-semiprime ideals for their properties. Later in 2015, Hussain et al. in their paper [60], extended the notion of congruences on semigroups to the congruences of LA-modules and proved the corresponding analogs of isomorphism theorems. They defined internal and external direct sum of the LA-submodules and established an isomorphism between them.

2.4 2016-2018

In the year 2016, Shah et al. [130] extended the idea of soft rings from theoretical viewpoint. They developed some more applications of soft set theory to LA-rings and instituted the notions of soft ideals and soft prime ideals in soft LA-rings. They also investigated idealistic soft LA-rings, soft LA-ring homomorphism and presented several good examples for the illustration of these concepts. In the same year, Hussain and Firdous [55] defined the direct product of LA-rings, which is itself an LA-ring. They used properties of direct product to give a characterization of LA-rings. In the same year, Rahman et al. [108] presented left almost semirings (LA-semirings) as another generalization of LA-rings. They defined congruence relation and homomorphism of LA-semirings and proved that each homomorphism defines a congruence relation on an LA-semiring. In the same paper, they also provided analogs of isomorphism theorems. Also in 2016, Yiarayong et al. [150] promoted some already defined notions of LA-semirings and further developed the substructures and operations on substructures for an LA-semiring. Further in 2016, Rehman et al. [111], investigated the notions of (α, β) -fuzzy (bi-, generalized bi-, quasi-, interior) ideals in LA-rings. They identified lower and upper parts of these structures and characterized regular LA-rings using the identified properties of these structures.

In the year 2017, Hussain et al. [57] characterized nLA-rings by using ideals, defined a fully idempotent near left almost ring and discussed some of their properties. They instituted the concepts of prime ideals, fully prime ideals, irreducible ideals, M-systems, P-

systems and I-systems in a near left almost ring and explored their properties. In the same year, Rehman and Razzaque [112], discussed the notions of projective and injective LA-modules, free LA-modules, split sequences in LA-modules and proved several associated results.

Also in 2017, Rehman et al. in their paper [114] introduced LA-hyperrings and explored some of their useful characterizations through their hyperideals and hypersystems. Razzaque and Rehman in 2017 [109], extended the applications of soft set theory to LA-rings and presented the ideas of soft LA-modules, soft homomorphisms, exact sequences of soft LA-modules and investigated some of their properties. They also obtained a characterization theorem of soft LA-modules. In the same year, Ahmed [6] introduced the notion of an LA-Noetherian in an LA-ring and near left almost ring. Furthermore, they extended the notion of ideal in an LA-ring and LA-module over LA-ring and its substructure to LA-Noetherian.

Hussain et al. in 2018 [56], generalized the concept of congruences from left almost rings [55] to near left almost rings. They showed that from every homomorphism one can get a congruence relation on near left almost rings and provided analogues of the isomorphism theorems.

2.5 2019-2020

In the year 2019, Hussain et al. [59] expanded the notion of quasi and bi-ideals from LA-semigroups to LA-rings and explored many interesting and elegant properties of quasi and bi-ideals. Further, they discussed quasi and bi-ideals in regular LA-rings and intra regular LA-rings. In the same year, Omayao [103] extended the idea of k -ideals and full k -ideals of semiring to near left almost ring. They defined an additive inversive near left almost ring and proved some properties similar to semirings. Moreover, they focused on restriction in k -ideals and established some results of full k -ideals and k -closure in an additive inversive n LA-ring.

Kauser et al. have significant contributions to the theory of LA-rings in the years 2019 and 2020. In their paper [73], they defined the notion of direct product of finite fuzzy normal subrings over nonassociative and non-commutative rings (LA-ring) and investigated the some basic properties of direct product of fuzzy normal subrings. Later in [74], they

extended the characterizations of fuzzy bi-ideal and fuzzy quasi-ideal in an associative ring to fuzzy left (resp. right, interior, quasi-, bi-, generalized bi-) ideals in LA-rings. They also characterized regular (intra-regular, both regular and intra-regular) LA-rings in terms of such ideals. In the same year, Kauser et al. [76] initiated study on the generalization of the fuzzification of ideals in LA-ring and characterized different classes of LA-ring in terms of intuitionistic fuzzy left (resp. right, bi-, generalized bi-, (1, 2)-) ideals. In the continuation, they studied LA-rings by their anti fuzzy bi-ideals [75] in the year 2020. They characterized the different classes of LA-rings in terms of anti fuzzy left (resp. right, bi-, generalized bi-, (1, 2)-) ideals. Recently in 2020, Khachorncharoenkul et al. [79] introduced left almost seminearrings which generalize LA-semirings, nLA-rings and LA-rings. Some related properties of left almost seminearrings are investigated. Moreover, the ideal structure and its properties are studied and the isomorphism theorems are also included.

Chapter 3

Developments in LA-ring Theory

The LA-ring theory is progressing rapidly since its inception. A good number of researchers have contributed to its evolution and several new notions regarding LA-rings have been introduced so far. Still there is big margin for discoveries in this area and in this chapter we include some of our contributions.

3.1 LA-rings to Special LA-rings

Rehman et al. [131], proved the existence of non-associative LA-rings and LA-fields, and discussed their several special cases. They introduced a special LA-ring and provided an example of a special LA-ring comprising of 8 elements, using a software MACE 4 [95]. Where a special LA-ring is an LA-ring that is additive abelian group. Clearly, a special LA-ring is an LA-ring but an LA-ring may not be a special LA-ring. In this section, we give certain constraints under which an LA-ring becomes a special LA-ring.

Following example is an illustration of a non-associative special LA-ring having order 8. This example is obtained using MACE 4.

Example 3.1.1. Consider $R_{SLA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$, with addition and multiplication tables on next page.

It can be easily observed from the operation tables that, with respect to addition, R_{SLA} is an abelian group and with respect to multiplication, R_{SLA} is a non associative LA-semigroup. The two distributive laws are satisfied and hence $(R_{SLA}, +, \cdot)$ is a non-associative special LA-ring.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	4	1	5	2	6	3	7
3	0	5	3	6	6	3	5	0
4	0	2	4	6	1	3	5	7
5	0	3	6	5	5	6	3	0
6	0	6	5	3	3	5	6	0
7	0	7	7	0	7	0	0	7

A special LA-ring is an LA-ring, but the converse doesn't hold. Following is the example of an LA-ring which is not a special LA-ring.

Example 3.1.2. [113] Consider $R_{SLA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with addition and multiplication as:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	2	0	3	1	6	4	7	5
2	1	3	0	2	5	7	4	6
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	6	4	7	5	2	0	3	1
6	5	7	4	6	1	3	0	2
7	7	6	5	4	3	2	1	0

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	4	4	0	0	4	4	0
2	0	4	4	0	0	4	4	0
3	0	0	0	0	0	0	0	0
4	0	3	3	0	0	3	3	0
5	0	7	7	0	0	7	7	0
6	0	7	7	0	0	7	7	0
7	0	3	3	0	0	3	3	0

Then $(R_{LA}, +)$ is a non-associative LA-group and (R_{LA}, \cdot) is a non-associative LA-semigroup.

Although an LA-ring may not be a special LA-ring but we can counter few situations, where LA-rings with certain condition becomes a special LA-ring.

Theorem 3.1.3. An LA-ring R_{LA} becomes a special LA-ring if and only if the following condition is satisfied:

$$(\mu + \nu) + \omega = \nu + (\mu + \omega) \text{ for all } \mu, \nu, \omega \in R.$$

Proof. Let R_{LA} be a special LA-ring then commutativity and associativity of addition together imply that $(\mu + \nu) + \omega = \nu + (\mu + \omega)$.

Conversely, let R_{LA} be an LA-ring with the given condition. Taking $\nu = 0$ we have $(\mu + 0) + \omega = 0 + (\mu + \omega) = \mu + \omega$. using the left invertive law we have $(\mu + 0) + \omega = (\omega + 0) + \mu = 0 + (\omega + \mu) = \omega + \mu$. $(R, +)$ is commutative as well as associative and hence $(R_{LA}, +, \cdot)$ is a special LA-ring. ■

Proposition 3.1.4. An LA-ring R_{LA} containing left identity ‘ e ’ becomes a special LA-ring if $e + e = e$.

Proof. From [134], for an LA-ring R_{LA} $(\mu + \nu)(\omega + \varsigma) = (\nu + \mu)(\varsigma + \omega)$ for all $\mu, \nu, \omega, \varsigma \in R_{LA}$. Now if $e + e = e$, then taking $\mu = \nu = e$ in the above equation gives $\omega + \varsigma = \varsigma + \omega$ for all $\omega, \varsigma \in R_{LA}$. This implies that $(R_{LA}, +)$ is an abelian group. ■

Proposition 3.1.5. A cancellative LA-ring R_{LA} containing left identity ‘ e ’ becomes a special LA-ring if $e + e \neq 0$. (Where a cancellative LA-ring is an LA-ring in which both cancellation laws hold).

Proof. From [134] in an LA-ring R_{LA} , $(\mu + \nu)(\omega + \varsigma) = (\nu + \mu)(\varsigma + \omega)$ for all $\mu, \nu, \omega \in R_{LA}$. If $e + e \neq 0$, then taking $\omega = \varsigma = e$ in the above equation and by cancellation we have $\mu + \nu = \nu + \mu$ for each $\mu, \nu \in R_{LA}$. This implies that $(R_{LA}, +)$ is an abelian group. ■

Proposition 3.1.6. An LA-ring R_{LA} with $\mu^2 = \mu$ for all $\mu \in R_{LA}$ is a special LA-ring.

Proof. From [134] for all μ in an LA-ring R_{LA} , $\mu^2 = (\mu + 0)^2$. So $\mu = \mu^2 = (\mu + 0)^2 = \mu + 0$. This implies that $(R_{LA}, +)$ is an abelian group. ■

An element μ in an LA-ring R_{LA} , is said to be idempotent if $\mu^2 = \mu$ and R_{LA} is called idempotent if its each element is idempotent.

Theorem 3.1.7. An idempotent LA-ring R_{LA} is a special LA-ring.

Proof. Let $\mu \in R_{LA}$, then our hypothesis and Corollary 6 [134], $\mu = \mu^2 = (\mu + 0)^2 = \mu + 0$ imply that R_{LA} is an additive abelian group. ■

3.2 Examples of a Non-associative Special LA-ring and Extensions of LA-rings

While proving the existence of a non-associative LA-ring, Rehman et al. [113], explored some good examples of LA-rings. By investigating the tables up to order 63 using Mace4 [95], they could obtain examples of non-associative LA-rings of order 8,9,12 and 18 only. Due to memory exhaustion, MACE 4 exit at order 64. So the question "what is the next order after 18 for which non-associative LA-ring exists?" remained unanswered.

In this section, we first discuss the existence of non-associative special LA-rings using MACE 4. Moreover, we construct non-associative special LA-rings of higher orders by extending previously known special LA-rings. We construct a special LA-ring $\sum_{l=0}^{l=m} w^l R_{SLA_n}$ with order n^{m+1} . Here 'm' is a positive integer and R_{SLA_n} is a special LA-ring of order 'n'. We propose a computational method for this purpose and provide an algorithm. Using this algorithm we construct examples of special LA-rings of higher orders in small time. The similar approach can be used to obtain LA-rings of higher orders.

Throughout this section we denote a special LA-ring of order n by R_{SLA_n} .

3.2.1 Examples of Special LA-rings of Smaller Orders

Following is an example of a special LA-ring of order 4.

Example 3.2.1. We consider the following non-associative special LA-ring $R_{SLA_4} = \{0, 1, 2, 3\}$ with left identity 1. It is any easy observation that R_{SLA_4} is a special LA-field.

+	0	1	2	3	·	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	0	3	2	1	0	1	2	3
2	2	3	0	1	2	0	3	1	2
3	3	2	1	0	3	0	2	3	1

Through MACE 4 we find that, the least possible order of a special LA-ring is 4. Using MACE4 and checking the tables, we get to know that non-associative special LA-rings only exist of orders 4,8,9,12,16,18,24 and 32. Due to memory exhaustion, MACE4 exits at

order 49. Therefore the order after 32 for which non-associative special LA-ring exists was not found at this stage. This is an intriguing problem to figure out. To continue search for non-associative special LA-rings of higher orders we establish the extensions of previously known special LA-rings.

3.2.2 Constructing the Special LA-ring $\sum_{l=0}^{l=m} w^l R_{SLA_n}$

Let R_{SLA_n} is a special LA-ring of order n . We can construct a set $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ (with $w^{m+1} = 0$) consisting of the elements of the type $\sum_{l=0}^{l=m} a_l w^l$, where all a_l belong to R_{SLA_n} and m is a positive integer. Now \mathfrak{R} is a special LA-ring with respect to the following operations:

$$\sum_{l=0}^{l=m} a_l w^l + \sum_{l=0}^{l=m} b_l w^l = \sum_{l=0}^{l=m} (a_l + b_l) w^l \quad (3.2.1)$$

and

$$\sum_{l=0}^{l=m} a_l w^l \cdot \sum_{l=0}^{l=m} b_l w^l = \sum_{l=0}^{l=m} c_l w^l, \quad (3.2.2)$$

for $\sum_{l=0}^{l=m} a_l w^l, \sum_{l=0}^{l=m} b_l w^l$ in \mathfrak{R} . Where $c_l = \sum_{i+j=l} a_i b_j$ and $w^{m+1} = 0$.

From Equations 3.2.1 and 3.2.2, it is clear that the operations in \mathfrak{R} follow from the operations in R_{SLA_n} and it is not difficult to show that $(\sum_{l=0}^{l=m} w^l R_{SLA_n}, +, \cdot)$ is a special LA-ring. To understand the structure of the special LA-ring \mathfrak{R} , the addition and multiplication tables for \mathfrak{R} . We design the following algorithm to construct the addition and multiplication tables for \mathfrak{R} .

Algorithm:

Input: A special LA-ring $(R_{SLA_n}, +, \cdot)$ and the addition and multiplication tables for R_{SLA_n} .

Step 1 Generate n^{m+1} elements $\sum_{l=0}^{l=m} a_l w^l$ for all a_l in R_{SLA_n} .

Step 2 Select one element from step 1 to get $x = \sum_{l=0}^{l=m} a_l w^l$.

Step 3 Iterate over elements in step 1 to get $y = \sum_{l=0}^{l=m} b_l w^l$.

Step 4 Add x and y to get $x + y$.

Step 5 Store results of step 4 in a row for x of step 2.

Step 6 Multiply x with y to get xy .

Step 7 Store results of step 6 in a row for x of step 2.

Step 8 Repeat steps 2 to 5 for each x in step 1 to get addition table.

Step 9 Repeat steps 2, 3, 6 and 7 for each x in step 1 to get multiplication table.

Following examples are two demonstrations of the above algorithm.

Example 3.2.2. Consider the non-associative special LA-field $R_{SLA_4} = \{0, 1, 2, 3\}$ of order 4 from Example 3.2.1. Then $R_{SLA_4} + wR_{SLA_4} = \{0, 1, 2, 3, w, 1+w, 2+w, 3+w, 2w, 1+2w, 2+2w, 3+2w, 3w, 1+3w, 2+3w, 3+3w\}$, consisting of $4^2 = 16$ elements. $R_{SLA_4} + wR_{SLA_4}$ is a non-commutative special LA-ring of characteristic 2 with $w^2 = 0$ or with the LA-ring isomorphism $R_{SLA_4} + wR_{SLA_4} \cong R_{SLA_4}[x]/\langle x^2 \rangle$. In $R_{SLA_4} + wR_{SLA_4}$ an element $a + bw$ is a unit if and only if $a \neq 0$. So there are 12 units in $R_{SLA_4} + wR_{SLA_4}$. Namely, $1, 2, 3, 1+w, 2+w, 3+w, 1+2w, 2+2w, 3+2w, 1+3w, 2+3w$ and $3+3w$.

+	0	1	2	3	w	1+w	2+w	3+w	2w	1+2w	2+2w	3+2w	3w	1+3w	2+3w	3+3w
0	0	1	2	3	w	1+w	2+w	3+w	2w	1+2w	2+2w	3+2w	3w	1+3w	2+3w	3+3w
1	1	0	3	2	1+w	w	3+w	2+w	1+2w	2w	3+2w	2+2w	1+3w	3w	3+3w	2+3w
2	2	3	0	1	2+w	3+w	w	1+w	2+2w	3+2w	2w	1+2w	2+3w	3+3w	3w	1+3w
3	3	2	1	0	3+w	2+w	1+w	w	3+2w	2+2w	1+2w	2w	3+3w	2+3w	1+3w	3w
w	w	1+w	2+w	3+w	0	1	2	3	3w	1+3w	2+3w	3+3w	2w	1+2w	2+2w	3+2w
1+w	1+w	w	3+w	2+w	1	0	3	2	1+3w	3w	3+3w	2+3w	1+2w	2w	3+2w	2+2w
2+w	2+w	3+w	w	1+w	2	3	0	1	2+3w	3+3w	3w	1+3w	2+2w	3+2w	2w	1+2w
3+w	3+w	2+w	1+w	w	3	2	1	0	3+3w	2+3w	1+3w	3w	3+2w	2+2w	1+2w	2w
2w	2w	1+2w	2+2w	3+2w	3w	1+3w	2+3w	3+3w	0	1	2	3	w	1+w	2+w	3+w
1+2w	1+2w	2w	3+2w	2+2w	1+3w	3w	3+3w	2+3w	1	0	3	2	1+w	w	3+w	2+w
2+2w	2+2w	3+2w	2w	1+2w	2+3w	3+3w	3w	1+3w	2	3	0	1	2+w	3+w	w	1+w
3+2w	3+2w	2+2w	1+2w	2w	3+3w	2+3w	1+3w	3w	3	2	1	0	3+w	2+w	1+w	w
3w	3w	1+3w	2+3w	3+3w	2w	1+2w	2+2w	3+2w	w	1+w	2+w	3+w	0	1	2	3
1+3w	1+3w	3w	3+3w	2+3w	1+2w	2w	3+2w	2+2w	1+w	w	3+w	2+w	1	0	3	2
2+3w	2+3w	3+3w	3w	1+3w	2+2w	3+2w	2w	1+2w	2+w	3+w	w	1+w	2	3	0	1
3+3w	3+3w	2+3w	1+3w	3w	3+2w	2+2w	1+2w	2w	3+w	2+w	1+w	w	3	2	1	0

and

·	0	1	2	3	w	1+w	2+w	3+w	2w	1+2w	2+2w	3+2w	3w	1+3w	2+3w	3+3w
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	w	1+w	2+w	3+w	2w	1+2w	2+2w	3+2w	3w	1+3w	2+3w	3+3w
2	0	3	1	2	3w	3+3w	1+3w	2+3w	w	3+w	1+w	2+w	2w	3+2w	1+2w	2+2w
3	0	2	3	1	2w	2+2w	3+2w	1+2w	3w	2+3w	3+3w	1+3w	w	2+w	3+w	1+w
w	0	w	2w	3w	0	w	2w	3w	0	w	2w	3w	0	w	2w	3w
1+w	0	1+w	2+2w	3+3w	w	1	2+3w	3+2w	2w	1+3w	2	3+w	3w	1+2w	2+w	3
2+w	0	3+w	1+2w	2+3w	3w	3+2w	1+w	2	w	3	1+3w	2+2w	2w	3+3w	1	2+w
3+w	0	2+w	3+2w	1+3w	2w	2+3w	3	1+w	3w	2+2w	3+w	1	w	2	3+3w	1+2w
2w	0	3w	w	2w	0	3w	w	2w	0	3w	w	2w	0	3w	w	2w
1+2w	0	1+3w	2+w	3+2w	w	1+2w	2	3+3w	2w	1+w	2+3w	3	3w	1	2+2w	3+w
2+2w	0	3+3w	1+w	2+2w	3w	3	1+2w	2+w	w	3+2w	1	2+3w	2w	3+w	1+3w	2
3+2w	0	2+3w	3+w	1+2w	2w	2+w	3+3w	1	3w	2	3+2w	1+w	w	2+2w	3	1+3w
3w	0	2w	3w	w	0	2w	3w	w	0	2w	3w	w	0	2w	3w	w
1+3w	0	1+2w	2+3w	3+w	w	1+3w	2+2w	3	2w	1	2+w	3+3w	3w	1+w	2	3+2w
2+3w	0	3+2w	1+3w	2+w	3w	3+w	1	2+2w	w	3+3w	1+2w	2	2w	3	1+w	2+3w
3+3w	0	2+2w	3+3w	1+w	2w	2	3+w	1+3w	3w	2+w	3	1+2w	w	2+3w	3+2w	1

$R_{SLA_4} + wR_{SLA_4}$ has only three ideals $I_0 = \{0\} \subseteq I_w \subseteq R_{SLA_4} + wR_{SLA_4}$. Where $I_w = (R_{SLA_4} + wR_{SLA_4})w = \{0, w, 2w, 3w\}$. Clearly $R_{SLA_4} + wR_{SLA_4}$ is a principal ideal special LA-ring and also a local special LA-ring having I_w as its maximal ideal. Since all the ideals of $R_{SLA_4} + wR_{SLA_4}$ are in a chain so, $R_{SLA_4} + wR_{SLA_4}$ is a chain special LA-ring.

The notions of chain LA-ring, local LA-ring, principal ideal and maximal ideal are analogs of the same concepts for associative rings.

Example 3.2.3. Consider the special LA-ring with identity $R_{SLA_8} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with the additive and multiplicative tables on the next page.

+	0	1	2	3	4	5	6	7
0	6	5	0	2	7	4	3	1
1	5	6	1	7	2	3	4	0
2	0	1	2	3	4	5	6	7
3	2	7	3	6	5	1	0	4
4	7	2	4	5	6	0	1	3
5	4	3	5	1	0	2	7	6
6	3	4	6	0	1	7	2	5
7	1	0	7	4	3	6	5	2

·	0	1	2	3	4	5	6	7
0	4	0	2	1	3	7	6	5
1	3	4	2	0	1	5	6	7
2	2	2	2	2	2	2	2	2
3	1	3	2	4	0	7	6	5
4	0	1	2	3	4	5	6	7
5	5	7	2	5	7	6	2	6
6	6	6	2	6	6	2	2	2
7	7	5	2	7	5	6	2	6

Here the zero element is ‘2’ and the left identity element is ‘4’. Units in R_{SLA8} are: 0, 1, 3 and 4. The set $R = R_{SLA8} + wR_{SLA8} + w^2R_{SLA8}$ (with $w^3 = 0$) is a special LA-ring with $8^3 = 512$ elements.

As the addition and multiplication tables are large so we didn’t include them completely over here.

+	$0 + 0w + 0w^2 \dots 7 + 7w + 7w^2$
$0 + 0w + 0w^2$	$6 + 6w + 6w^2 \dots 1 + w + w^2$
·	· ... ·
·	· ... ·
·	· ... ·
$7 + 7w + 7w^2$	$1 + w + w^2 \dots 2 + 2w + 2w^2$

·	$0 + 0w + 0w^2 \dots 7 + 7w + 7w^2$
$0 + 0w + 0w^2$	$4 + 6w + w^2 \dots 5 + 2w + 5w^2$
·	· ... ·
·	· ... ·
·	· ... ·
$7 + 7w + 7w^2$	$7 + 2w + 7w^2 \dots 6 + 2w + 6w^2$

We are adding few of our observations about that ring. The left identity element in \mathfrak{R} is ‘422’. $a + bw + cw^2$ is a unit in \mathfrak{R} if and only if ‘a’ has inverse in R_{SLA8} . So, there are 256 units in \mathfrak{R} . $\mathfrak{R} = R_{SLA8} + wR_{SLA8} + w^2R_{SLA8}$ is isomorphic to the quotient special LA-ring $R_{SLA8}[x]/\langle x^3 \rangle$. \mathfrak{R} is not a local special LA-ring as the ideals $\mathfrak{R}(2 + 0w + 0w^2)$, $\mathfrak{R}(5 + 0w + 0w^2)$, $\mathfrak{R}(5 + 0w + 2w^2)$, $\mathfrak{R}(5 + 2w + 0w^2)$, $\mathfrak{R}(5 + 2w + 2w^2)$, and $\mathfrak{R}(6 + 0w + 0w^2)$ are all maximal ideals. Furthermore, these ideals are not in a chain so \mathfrak{R} is not a chain special LA-ring. Since the ideal $\langle 2 + 6w + 2w^2, 2 + 6w + 5w^2 \rangle$ is not a principal ideal, hence \mathfrak{R} fails to be a principal ideal special LA-ring.

After a careful study of some example of the special LA-ring $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$, for different values of m and n we observe some special features of \mathfrak{R} . There are some

properties that are possessed by R_{SLA_n} , but they may not hold in \mathfrak{R} . Our observations and findings about \mathfrak{R} stated below:

Observations

1. The special LA-ring $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ is isomorphic to the quotient special LA-ring $R_{SLA_n}[x]/\langle x^{m+1} \rangle$.
2. The order of special LA-ring $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ is n^{m+1} .
3. An element $\sum_{l=0}^{l=m} a_l w^l$ is a unit in $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ if and only if a_0 holds inverse in R_{SLA_n} .
4. If R_{SLA_n} is a special LA-field, it is not necessary that $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ is a special LA-field.
5. $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ is not necessarily a chain special LA-ring.
6. $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ is not necessarily a local special LA-ring.
7. Each ideal in $\mathfrak{R} = \sum_{l=0}^{l=m} w^l R_{SLA_n}$ need not be a principal ideal.

Remarks on Running Times

We used a computer system with processor:

$$Intel® Core™ i5 – 2410M CPU @ 2.30GHz \times 4,$$

RAM: 6 GB and python version 3.6 for the computation process. For the special LA-rings $\sum_{l=0}^{l=m} w^l R_{SLA_n}$ with $n = 4$ and $m = 1$ the whole process of generating 16 elements and then the construction of addition and multiplication tables took a fraction of a second. Similar is the case when $m = 2$ and elements are 64. As we increase ‘ n ’ and ‘ m ’ the process time increases. For instance, there are 1024 elements in $\sum_{l=0}^{l=4} w^l R_{SLA_4}$ and total construction time is 30.28 seconds and for $\sum_{l=0}^{l=6} w^l R_{SLA_4}$ with 16384 elements the processing time is approximately 6 and a half hour. Moreover, $\sum_{l=0}^{l=2} w^l R_{SLA_8}$ has 512 elements takes approximately 10 seconds but, $\sum_{l=0}^{l=3} w^l R_{SLA_8}$ has 4096 elements and it takes approximately 12 minutes.

3.3 LA-semigroup rings

This section is about LA-semigroup ring $R[L]$, which consists of finitely non-zero functions from an LA-semigroup L to a commutative and associative ring R . We observe that $R[L]$ is in fact a special LA-ring and it can be considered as an analog of the group ring [96], semigroup ring [52] and loop ring [24]. and study the formation of its sub LA-rings, ideals and homomorphisms using the same for the corresponding LA-semigroup L and ring R . For the quasi, bi and interior ideals in an LA-semigroup L and R , we established quasi, bi and interior ideals in an LA-semigroup ring $R[L]$. We also see that, if R is a Noetherian (Artinian) ring, then so is the corresponding LA-semigroup ring $R[L]$ for any LA-semigroup L .

Throughout this section, R represents a commutative and associative ring and L denotes an LA-semigroup.

3.3.1 Basic Structure

Consider a commutative and associative ring $(R, +, \cdot)$ and let L be an LA-semigroup under binary operation \star . Let $N = \{\varphi | \varphi : L \rightarrow R, \text{ where } \varphi \text{ are finitely nonzero}\}$. Define the binary operation $+$ in N as $(\varphi + \psi)(s) = \varphi(s) + \psi(s)$. Then $(N, +)$ is an abelian group. As for $\varphi, \psi \in N$, $\varphi(s), \psi(s) \in R$ (for each $s \in L$), so $(\varphi + \psi)(s) = \varphi(s) + \psi(s) \in R$ and hence $\varphi + \psi \in N$.

Let $\varphi, \psi \in N$. As $\varphi(s), \psi(s) \in R$, so by the commutative law in $(R, +)$, we have

$$\begin{aligned}(\varphi + \psi)(s) &= \varphi(s) + \psi(s) \\ &= \psi(s) + \varphi(s) \\ &= (\psi + \varphi)(s).\end{aligned}$$

Hence $\varphi + \psi = \psi + \varphi$.

Thus commutative law holds in N .

Now for $\varphi, \psi, \vartheta \in N$, $\varphi(s), \psi(s), \vartheta(s) \in R$, and by the associative law in $(R, +)$, we have

$$\begin{aligned}
 ((\varphi + \psi) + \vartheta)(s) &= (\varphi + \psi)(s) + \vartheta(s) \\
 &= (\varphi(s) + \psi(s)) + \vartheta(s) \\
 &= \varphi(s) + (\psi(s) + \vartheta(s)) \\
 &= \varphi(s) + (\psi + \vartheta)(s) \\
 &= (\varphi + (\psi + \vartheta))(s).
 \end{aligned}$$

Hence $(\varphi + \psi) + \vartheta = \varphi + (\psi + \vartheta)$.

Thus associative law for addition holds in N .

Consider the mapping $o : L \rightarrow R$ with $o(s) = 0$ for each $s \in L$,

$$\begin{aligned}
 (o + \varphi)(s) &= 0 + \varphi(s) \\
 &= \varphi(s).
 \end{aligned}$$

$\Rightarrow o + \varphi = \varphi$.

Thus o is the additive identity in N .

For each $\varphi \in N$, there is a map $-\varphi : L \rightarrow R$ such that $(-\varphi)(s) = -\varphi(s)$ for every $s \in L$ and

$$\begin{aligned}
 ((-\varphi) + \varphi)(s) &= (-\varphi(s)) + \varphi(s) \\
 &= -\varphi(s) + \varphi(s) \\
 &= 0 \\
 &= o(s).
 \end{aligned}$$

$\Rightarrow (-\varphi) + \varphi = o$.

Thus, each element in $(N, +)$ posses inverse and therefore, $(N, +)$ is an abelian group.

Now we define binary operation ' \odot ' in N as follows:

$$\varphi \odot \psi(s) = \sum_{\kappa \star u = s} \varphi(\kappa)\psi(u).$$

It can be shown that, (N, \odot) is an LA-semigroup. As for $\varphi(\kappa)$ and $\psi(u) \in R$, $\kappa, u \in (L, \star)$ and (R, \cdot) is a commutative and associative, $(\varphi \odot \psi)(s) \in R$. $\varphi \odot \psi \in N$, since φ, ψ are finitely nonzero on L .

For $\varphi, \psi, \vartheta \in N$ and $s \in L$, consider

$$\begin{aligned}
[(\varphi \odot \psi) \odot \vartheta](s) &= \sum_{\kappa \star u = s} (\varphi \odot \psi)(\kappa) \vartheta(u) \\
&= \sum_{\kappa \star u = s} \left[\sum_{\kappa = \omega \star \nu} ((\varphi(\omega) \psi(\nu))) \right] \vartheta(u) \\
&= \sum_{(\omega \star \nu) \star u = s} (\varphi(\omega) \psi(\nu)) \vartheta(u) \\
&= \sum_{(u \star \nu) \star \omega = s} (\vartheta(u) \psi(\nu)) \varphi(\omega).
\end{aligned}$$

As (L, \star) is an LA-semigroup, so $(\omega \star \nu) \star u = (u \star \nu) \star \omega$ for all $\omega, \nu, u \in (L, \star)$. Hence

$$\begin{aligned}
[(\varphi \odot \psi) \odot \vartheta](s) &= \sum_{(\kappa \star \nu) \star u = s} (\varphi(\kappa) \psi(\nu)) \vartheta(u) \\
&= \sum_{(u \star \nu) \star \kappa = s} (\vartheta(u) \psi(\nu)) \varphi(\kappa) \\
&= \sum_{k' \star \kappa = s} \left[\sum_{k' = u \star \nu} (\vartheta(u) \psi(\nu)) \right] \varphi(\kappa) \\
&= \sum_{k' \star \kappa = s} (\vartheta \odot \psi)(k') \varphi(\kappa) \\
&= [(\vartheta \odot \psi) \odot \varphi](s).
\end{aligned}$$

Thus (N, \odot) is an LA-semigroup.

It is simple to establish that the operation ‘ \odot ’ is distributive over ‘+’. As $\varphi(\kappa), \psi(u)$ and $\vartheta(u) \in R$ and distributive laws hold in R , so

$$\begin{aligned}
[\varphi \odot (\psi + \vartheta)](s) &= \sum_{\kappa \star u = s} \varphi(\kappa) (\psi + \vartheta)(u) \\
&= \sum_{\kappa \star u = s} \varphi(\kappa) (\psi(u) + \vartheta(u)) \\
&= \sum_{\kappa \star u = s} (\varphi(\kappa) \psi(u) + \varphi(\kappa) \vartheta(u)) \\
&= \sum_{\kappa \star u = s} \varphi(\kappa) \psi(u) + \sum_{\kappa \star u = s} \varphi(\kappa) \vartheta(u) \\
&= (\varphi \odot \psi)(s) + (\varphi \odot \vartheta)(s) \\
&= [\varphi \odot \psi + \varphi \odot \vartheta](s).
\end{aligned}$$

Thus, $\varphi \odot (\psi + \vartheta) = \varphi \odot \psi + \varphi \odot \vartheta$. Similarly, $(\psi + \vartheta) \odot \varphi = \psi \odot \varphi + \vartheta \odot \varphi$. Hence, $(N, +, \odot)$ is a special LA-ring.

3.3.2 Representation of Elements of \mathbf{N}

Consider R to be an associative ring and L an LA-semigroup. We define $R[L]$ to be the set of all formal linear combinations of the form $\sum_{\varrho \in L} \mu_{\varrho} \varrho$, where $\mu_{\varrho} \in R$ for all $\varrho \in L$ and μ_{ϱ} are finitely non-zero.

The support of an element $\sum_{\varrho \in L} \mu_{\varrho} \varrho$ in $R[L]$ is defined to be the set of elements in L that appear effectively in that expression, that is

$$Supp(\sum_{\varrho \in L} \mu_{\varrho} \varrho) = \{\varrho \in L : \mu_{\varrho} \neq 0\} \quad (3.3.1)$$

Thus support of any element in $R[L]$ is a finite set. It follows from our definition that the element $\sum_{\varrho \in L} \mu_{\varrho} \varrho = \sum_{\varrho \in L} \nu_{\varrho} \varrho$ in $R[L]$, if and only if $\mu_{\varrho} = \nu_{\varrho}$, for all $\varrho \in L$.

We define the sum of any two elements $\sum_{\varrho \in L} \mu_{\varrho} \varrho$ and $\sum_{\varrho \in L} \nu_{\varrho} \varrho$ in $R[L]$ componentwise as:

$$\sum_{\varrho \in L} \mu_{\varrho} \varrho + \sum_{\varrho \in L} \nu_{\varrho} \varrho = \sum_{\varrho \in L} (\mu_{\varrho} + \nu_{\varrho}) \varrho \quad (3.3.2)$$

and their product by

$$\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\varrho \in L} \nu_{\varrho} \varrho = \sum_{\varrho, h \in L} \mu_{\varrho} \varrho h \nu_h \quad (3.3.3)$$

The above formula can be modified as:

$$\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\varrho \in L} \nu_{\varrho} \varrho = \sum_{u \in L} c_u u \text{ where } c_u = \sum_{\varrho h = u} \mu_{\varrho} \nu_h. \quad (3.3.4)$$

It is easy to verify that $(R[L], +)$ is an additive abelian group and $(R[L], \cdot)$ is a groupoid and in case if R is a commutative ring then $(R[L], \cdot)$ is an LA-semigroup and also the two distributive laws hold. Hence $R[L]$ is a special LA-ring.

We now define $R \times R[L] \rightarrow R[L]$ as $(c, \sum_{\varrho \in L} \mu_{\varrho} \varrho) \rightarrow \sum_{\varrho \in L} (c \mu_{\varrho}) \varrho$. From the fact that R is an R -module, it follows that $R[L]$ is also an R -module.

$R[L]$ is infact the special LA-ring N . Where the function $\varphi : L \rightarrow R$ is represented as $\varphi = \sum_{\varrho \in L} \varphi(\varrho) \varrho$ or simply $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ where $\mu_{\varrho} = \varphi(\varrho)$ for all $\varrho \in L$.

In case if R contains identity 1, then $i : L \rightarrow R[L]$ such that for each $x \in L$, $i(x) = \sum_{\varrho \in L} \mu_{\varrho} \varrho$, where $\mu_x = 1$ and $\mu_{\varrho} = 0$ if $\varrho \neq x$ is an embedding of L into $R[L]$. Thus L can be regarded as a subset of $R[L]$ and we can say that L is a basis of $R[L]$ over R . As R is commutative, the rank of a free module over R is well defined. Thus, if L is finite, the $rank(R[L])$ over R is precisely $|L|$.

If L has a left identity ‘ e ’ then we may consider the mapping $\pi : R \rightarrow R[L]$ given by: $\pi(k) = \sum_{\varrho \in L} \mu_{\varrho} \varrho$, where $\mu_e = k$ and $\mu_{\varrho} = 0$ if $\varrho \neq e$. It is not difficult to show that π is an LA-ring monomorphism and we can thus also regard R as a sub LA-ring of $R[L]$.

In wake of the above identifications, for $k \in R$ and $\varrho \in L$, $rg = gr$ in $R[L]$. Following is an evident example of an LA-semigroup ring.

Example 3.3.1. Let $L = \{s, u, v\}$, such that (L, \cdot) is an LA-semigroup, where

\cdot	s	u	v
s	s	s	s
u	s	s	v
v	s	u	s

Consider $R = \mathbb{Z}_2 = \{0, 1\}$ then for $\varphi \in \mathbb{Z}_2[L]$,

$$\varphi = \mu_s s + \mu_u u + \mu_v v$$

so that $\mathbb{Z}_2[L] = \{0, s, u, v, s + u, s + v, u + v, s + u + v\}$ is an LA-semigroup ring with the operations defined as:

$+$	0	s	u	v	$s + u$	$s + v$	$u + v$	$s + u + v$
0	0	s	u	v	$s + u$	$s + v$	$u + v$	$s + u + v$
s	s	0	$s + u$	$s + v$	u	v	$s + u + v$	$u + v$
u	u	$s + u$	0	$u + v$	s	$s + u + v$	v	$s + v$
v	v	$s + v$	$u + v$	0	$s + u + v$	s	u	$s + u$
$s + u$	$s + u$	u	s	$s + u + v$	0	$u + v$	$s + v$	v
$s + v$	$s + v$	v	$s + u + v$	s	$u + v$	0	$s + u$	u
$u + v$	$u + v$	$s + u + v$	v	u	$s + v$	$s + u$	0	s
$s + u + v$	$s + u + v$	$u + v$	$s + v$	$s + u$	v	u	s	0

and

\cdot	0	s	u	v	$s + u$	$s + v$	$u + v$	$s + u + v$
0	0	0	0	0	0	0	0	0
s	0	s	s	s	0	0	0	s
u	0	s	s	v	0	$s + v$	$s + v$	v
v	0	s	u	s	$s + u$	0	$s + u$	u
$s + u$	0	0	0	$s + v$	0	$s + v$	$s + v$	$s + v$
$s + v$	0	0	$s + u$	0	$s + u$	0	$s + u$	$s + u$
$u + v$	0	0	$s + u$	$s + v$	$s + u$	$s + v$	$u + v$	$u + v$
$s + u + v$	0	s	u	v	$s + u$	$s + v$	$u + v$	$s + u + v$

Proposition 3.3.2. If I and J are two subsets of R then

$$I[L] \cap J[L] = (I \cap J)[L]. \quad (3.3.5)$$

Proof. Let $x \in I[L] \cap J[L]$ then $x \in I[L]$ and $x \in J[L]$. That is $x = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ with all $\mu_{\varrho} \in I$ and $x = \sum_{\varrho \in L} \nu_{\varrho} \varrho$ with all $\nu_{\varrho} \in J$. So that, $\sum_{\varrho \in L} \mu_{\varrho} \varrho = \sum_{\varrho \in L} \nu_{\varrho} \varrho$. That is, $\mu_{\varrho} = \nu_{\varrho} \in I \cap J$ for all $\varrho \in L$. This implies that, $x = \sum_{\varrho \in L} \mu_{\varrho} \varrho = \sum_{\varrho \in L} \nu_{\varrho} \varrho \in (I \cap J)[L]$. Hence, $I[L] \cap J[L] \subseteq (I \cap J)[L]$.

On the other hand, let $y \in (I \cap J)[L]$. Then $y = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ where $\mu_{\varrho} \in I \cap J$, that is $\mu_{\varrho} \in I$ and $\mu_{\varrho} \in J$ for all $\varrho \in L$. So that $y = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in I[L]$ and $y = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in J[L]$ and hence $y = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in I[L] \cap J[L]$. Which implies that, $(I \cap J)[L] \subseteq I[L] \cap J[L]$. Thus, $I[L] \cap J[L] = (I \cap J)[L]$. ■

Proposition 3.3.3. If I and J are two subsets on R then

$$I[L] \cup J[L] \subseteq (I \cup J)[L]. \quad (3.3.6)$$

Proof. Let $x \in I[L] \cup J[L]$ then $x \in I[L]$ or $x \in J[L]$. That is $x = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ with all $\mu_{\varrho} \in I$ or $x = \sum_{\varrho \in L} \nu_{\varrho} \varrho$ with all $\nu_{\varrho} \in J$. So there exist $\mu_{\varrho} \in I \cup J$ such that $x = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ or there exist $\nu_{\varrho} \in I \cup J$ such that $x = \sum_{\varrho \in L} \nu_{\varrho} \varrho$. In either case, $x \in (I \cup J)[L]$ and hence, $I[L] \cup J[L] \subseteq (I \cup J)[L]$. ■

The converse of the above proposition may not hold in general and for illustration we have the following example.

Example 3.3.4. Let $R = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with subsets $I = \{2, 3\}$ and $J = \{2, 5\}$, then $I \cup J = \{2, 3, 5\}$. Consider the LA-semigroup $L = \{x, y, z\}$ such that:

·	x	y	z
x	x	x	x
y	z	z	z
z	x	x	x

$I[L] = \{2x + 2y + 2z, 2x + 2y + 3z, 2x + 3y + 2z, 3x + 2y + 2z, 3x + 3y + 2z, 3x + 2y + 3z, 2x + 3y + 3z, 3x + 3y + 3z\}$ and $J[L] = \{2x + 2y + 2z, 2x + 2y + 5z, 2x + 5y + 2z, 5x + 2y + 2z, 5x + 5y + 2z, 5x + 2y + 5z, 2x + 5y + 3z, 5x + 5y + 5z\}$.

$I[L] \cup J[L] = \{2x + 2y + 2z, 2x + 2y + 3z, 2x + 3y + 2z, 3x + 2y + 2z, 3x + 3y + 2z, 3x +$

$2y + 3z, 2x + 3y + 3z, 3x + 3y + 3z, 2x + 2y + 5z, 2x + 5y + 2z, 5x + 2y + 2z, 5x + 5y + 2z, 5x + 2y + 5z, 2x + 5y + 3z, 5x + 5y + 5z\}$.

On the other hand,

$(I \cup J)[L] = \{2x + 2y + 2z, 2x + 2y + 3z, 2x + 3y + 2z, 3x + 2y + 2z, 3x + 3y + 2z, 3x + 2y + 3z, 2x + 3y + 3z, 3x + 3y + 3z, 2x + 2y + 5z, 2x + 5y + 2z, 5x + 2y + 2z, 5x + 5y + 2z, 5x + 2y + 5z, 2x + 5y + 3z, 5x + 5y + 5z, 2x + 3y + 5z, 2x + 5y + 3z, 3x + 2y + 5z, 5x + 2y + 3z, 3x + 5y + 2z, 5x + 3y + 2z, 3x + 3y + 5z, 3x + 5y + 3z, 5x + 3y + 3z, 3x + 5y + 5z, 5x + 3y + 5z, 5x + 5y + 3z\}$.

Clearly, $I[L] \cup J[L] \subseteq (I \cup J)[L]$ but $(I \cup J)[L] \not\subseteq I[L] \cup J[L]$.

3.3.3 Sub LA-rings and Ideals in LA-semigroup Rings

There are some ideals in LA-semigroup rings which can be established from the ideals in rings and LA-semigroups.

Proposition 3.3.5. Let T be a sub ring of a commutative and associative ring R and M be a sub LA-semigroup of an LA-semigroup L , then:

1. $T[L] = \{\sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} \in T \text{ for all } \varrho \in L\}$ is a sub LA-ring of $R[L]$.
2. $R[M] = \{\sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} \in R \text{ for all } \varrho \in M\}$ is a sub LA-ring of $R[L]$.
3. $T[M] = \{\sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} \in T \text{ for all } \varrho \in M\}$ is a sub LA-ring of $R[L]$.

Proof. The proof is straightforward so eliminated. ■

In the same manner, one can obtain ideals in an LA-semigroup ring using ideals of R and L in different ways as given in the following proposition.

Proposition 3.3.6. If I is a left (right or two sided) ideal of a commutative and associative ring R and B is a left (right or two-sided) ideal of an LA-semigroup L , then

1. $I[L] = \{\sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} \in I \text{ for all } \varrho \in L\}$ is a left (right or two-sided) ideal of $R[L]$.
2. $R[B] = \{\sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} \in R \text{ for all } \varrho \in B\}$ is a left (right or two-sided) ideal of $R[L]$.

3. $I[B] = \{\sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} \in I \text{ for all } \varrho \in B\}$ is a left (right or two-sided) ideal of $R[L]$.

The succeeding example shows that it is not necessary that all the ideals in $R[L]$ are of the type $I[L], R[B]$ or $I[B]$ for any ideals I and B of R and L respectively.

Example 3.3.7. consider the LA-semigroup ring of the Example 3.3.1. Then $R = \mathbb{Z}_2 = \{0, 1\}$ has only two ideals $I_1 = \{0\}$ and $I_2 = \{0, 1\} = \mathbb{Z}_2$. On the other hand, only ideals of L are $B_1 = \{x\}$ and $B_2 = \{x, y, z\} = L$. The ideals of $\mathbb{Z}_2[L]$ are $K_1 = \{0\}, K_2 = \{0, x\}, K_3 = \{0, x + y, x + z, y + z\}$ and $K_4 = \{0, x, y, z, x + y, x + z, y + z, x + y + z\} = \mathbb{Z}_2[L]$. The ideal $K_3 \neq I[L], R[B]$ or $I[B]$ for any ideals I and B of R and L respectively.

Proposition 3.3.8. For a commutative and associative ring R and an LA-semigroup L , if $A = \{\sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} \in R, \varrho \in L\}$ is an ideal in the LA-semigroup ring $R[L]$, then $B = \{\sum \mu_{\varrho} : \varrho \in L\}$ is an ideal in R . Where L has left identity ‘ e ’.

Proof. By definition of an ideal, $o = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ (such that all $\mu_{\varrho} = 0$) belongs to A . Thus for $0 \in R, 0 = \sum_{\varrho \in L} \mu_{\varrho} \in B$ where $\mu_{\varrho} = 0$ for all $\varrho \in L$. Hence $B \neq \emptyset$. Now for $\sum_{\varrho \in L} \mu_{\varrho}$ and $\sum_{\varrho \in L} \nu_{\varrho} \in B$, there exist $\sum_{\varrho \in L} \mu_{\varrho} \varrho$ and $\sum_{\varrho \in L} \nu_{\varrho} \varrho$ in A , such that $\sum_{\varrho \in L} \mu_{\varrho} \varrho - \sum_{\varrho \in L} \nu_{\varrho} \varrho = \sum_{\varrho \in L} (\mu_{\varrho} - \nu_{\varrho}) \varrho \in A$ because A is an ideal of R . So $\sum_{\varrho \in L} (\mu_{\varrho} - \nu_{\varrho}) \in B$. That is $\sum_{\varrho \in L} \mu_{\varrho} - \sum_{\varrho \in L} \nu_{\varrho} \in B$. Further let $k \in R$ and $\sum_{\varrho \in L} \mu_{\varrho} \in B$, where $\sum_{\varrho \in L} \mu_{\varrho} \varrho \in A$, then $k(\sum_{\varrho \in L} \mu_{\varrho} \varrho) = \sum_{\varrho \in L} \kappa \mu_{\varrho} \varrho$. Since A is an ideal of $R[L]$ and $k = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$ also, where $\mu_{\varrho} = k$, if $\varrho = e$ and $\mu_{\varrho} = 0$ otherwise. Now $k(\sum_{\varrho \in L} \mu_{\varrho} \varrho) = \sum_{\varrho \in L} (\kappa \mu_{\varrho}) \varrho \in A$ and $\sum_{\varrho \in L} \kappa \mu_{\varrho} \in B$. ■

Proposition 3.3.9. Consider L be an LA-semigroup having left identity ‘ e ’. For an ideal I of $R, I = I^*$, where

$$I^* = \left\{ \sum_{\varrho \in L} \mu_{\varrho} : \sum_{\varrho \in L} \mu_{\varrho} \varrho \in I[L] \right\}. \quad (3.3.7)$$

Proof. Let $\mu \in I$, then $\mu = \mu e + \sum_{e \neq \varrho \in L} 0 \varrho \in I[L]$. Also $\mu = \mu + \sum_{e \neq \varrho \in L} 0 \in I^*$. This implies that, $I \subseteq I^*$. Now let $x \in I^*$, then $x = \sum_{\varrho \in L} \mu_{\varrho} \in I^*$ where $\sum_{\varrho \in L} \mu_{\varrho} \varrho \in I[L]$. This implies that, $\mu_{\varrho} \in I$ for all $\varrho \in L$. Since I is an ideal in R so $\sum_{\varrho \in L} \mu_{\varrho} \in I$ and hence, $I^* \subseteq I$. Therefore $I = I^*$. ■

Proposition 3.3.10. Let T be a subset of R , if $T[L]$ is an ideal in $R[L]$ then T is an ideal in R .

Proof. As $T[L]$ is an ideal in $R[L]$ so $0 \in T[L]$ where $0 = \sum_{\varrho \in L} 0\varrho \in T[L]$. Thus for $0 \in R, 0 \in T$ and $T \neq \emptyset$. Let $\mu, \nu \in T$ then $\mu e + \sum_{e \neq \varrho \in L} 0\varrho \in T[L]$ and $\nu e + \sum_{e \neq \varrho \in L} 0\varrho \in T[L]$. Since $T[L]$ is an ideal in $R[L]$, $(\mu - \nu)e + \sum_{e \neq \varrho \in L} 0\varrho \in T[L]$ and $\mu - \nu \in T$. Now let $k \in R$ and $\mu \in T$ then, $ke + \sum_{e \neq \varrho \in L} 0\varrho \in R[L]$ and $\mu e + \sum_{e \neq \varrho \in L} 0\varrho \in T[L]$. Since $T[L]$ is an ideal in $R[L]$, $(k\mu)e + \sum_{e \neq \varrho \in L} 0\varrho \in T[L]$ This implies that $k\mu \in T$. Also, $(\mu k)e + \sum_{e \neq \varrho \in L} 0\varrho \in T[L]$ and $\mu k \in T$. Hence, T is an ideal in R . ■

Recall that a ring R is direct sum of its ideals I_1, I_2, \dots, I_n denoted $R = I_1 \oplus I_2 \oplus \dots \oplus I_n$, if and only if $R = I_1 + I_2 + \dots + I_n$ and $I_i \cap I_j = \{0\}$ if $i \neq j$.

Theorem 3.3.11. Let I_1, I_2, \dots, I_n be ideals of a commutative and associative ring R such that $R = I_1 \oplus I_2 \oplus \dots \oplus I_n$, then for an LA-semigroup L , the LA-semigroup ring $R[L] = I_1[L] \oplus I_2[L] \oplus \dots \oplus I_n[L]$. Where for each $i = 1, \dots, n$, $I_i[L] = \{\sum_{\varrho \in L} \mu_{i\varrho} \varrho : \mu_{i\varrho} \in I_i \text{ for all } \varrho \in L\}$.

Proof. For $\varphi \in R[L]$, $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ and since $R = I_1 \oplus I_2 \oplus \dots \oplus I_n$ for each $\mu_{\varrho} \in R$, there exists unique $\mu_{i\varrho} \in I_i$ for all $i = 1, \dots, n$ such that, $\mu_{\varrho} = \sum_{i=1}^n \mu_{i\varrho}$. So, $\varphi = \sum_{\varrho \in L} (\sum_{i=1}^n \mu_{i\varrho}) \varrho = \sum_{i=1}^n (\sum_{\varrho \in L} \mu_{i\varrho} \varrho) \in I_1[L] + I_2[L] + \dots + I_n[L]$. Thus $R[L]$ is contained in $I_1[L] + I_2[L] + \dots + I_n[L]$. But since each $I_i[L]$ is an ideal in $R[L]$, so $I_1[L] + I_2[L] + \dots + I_n[L]$ is contained in $R[L]$. Hence $R[L] = I_1[L] + I_2[L] + \dots + I_n[L]$.

Now let $i \neq j$ and $x \in I_i[L] \cap I_j[L]$, then $x \in I_i[L]$ and $x \in I_j[L]$. That is $x = \sum_{\varrho \in L} \mu_{i\varrho} \varrho$ also $x = \sum_{\varrho \in L} \mu_{j\varrho} \varrho$, where $\mu_{i\varrho} \in I_i$, and $\mu_{j\varrho} \in I_j$, for all $\varrho \in L$. Thus $\mu_{i\varrho} = \mu_{j\varrho}$, for all $\varrho \in L$. So, $\mu_{i\varrho}, \mu_{j\varrho} \in I_i \cap I_j = \{0\}$ for all $\varrho \in L$ i.e. $\mu_{i\varrho} = \mu_{j\varrho} = 0$, for all $\varrho \in L$ and $x = 0$. So, $I_i[L] \cap I_j[L] = \{0\}$ and hence $R[L] = I_1[L] \oplus I_2[L] \oplus \dots \oplus I_n[L]$. ■

Definition 3.3.12. A Sub LA-ring Q of an LA-ring R_{LA} is said to be its quasi ideal if $R_{LA}Q \cap QR_{LA} \subseteq Q$.

Theorem 3.3.13. If A is a quasi-ideal of L then for a commutative and associative ring R , $R[A]$ is quasi-ideal of $R[L]$, for any LA-semigroup L .

Where

$$R[A] = \left\{ \sum_{\varrho \in L} \mu_{\varrho} \varrho : \mu_{\varrho} = 0 \text{ if } \varrho \notin A \right\}. \quad (3.3.8)$$

Proof. Being a quasi ideal of L , A is its sub LA-semigroup. By the Proposition 3.3.5, $R[A]$ is a sub LA-semigroup ring. Let $x \in R[A]R[L] \cap R[L]R[A]$ then $x \in R[A]R[L]$ and

$x \in R[L]R[A]$. We have, $x = \sum_{finite} \varphi\psi$ where, $\varphi = \sum_{\varrho \in A} \mu_{\varrho}\varrho$ and $\psi = \sum_{\varrho \in L} \nu_{\varrho}\varrho$ also $x = \sum_{finite} \vartheta\delta$ where, $\vartheta = \sum_{\varrho \in L} \omega_{\varrho}\varrho$ and $\delta = \sum_{\varrho \in A} \varsigma_{\varrho}\varrho$.

Now, $x = \sum_{finite} \varphi\psi = \sum_{finite} (\sum_{\varrho \in A} \mu_{\varrho}\varrho \sum_{\varrho \in L} \nu_{\varrho}\varrho) = \sum_{finite} (\sum_{\varrho \in A, h \in L} \mu_{\varrho}\nu_h\varrho h) = \sum_{finite} (\sum_{u \in AS} \varrho_u u)$.

Also, $x = \sum_{finite} \vartheta\delta = \sum_{finite} (\sum_{\varrho \in L} \omega_{\varrho}\varrho \sum_{\varrho \in A} \varsigma_{\varrho}\varrho) = \sum_{finite} (\sum_{\varrho \in L, h \in A} \omega_{\varrho}\varsigma_h\varrho h) = \sum_{finite} (\sum_{u \in SA} \varrho_u u)$. This implies that $x \in R[AS]$ and $x \in R[SA]$. That is, $x \in R[AS] \cap R[SA] = R[AS \cap SA] \subseteq R[A]$. Thus, $R[A]R[L] \cap R[L]R[A] \subseteq R[A]$. Hence, $R[A]$ is a quasi-ideal of $R[L]$. ■

Definition 3.3.14. A Sub LA-ring B of an LA-ring R_{LA} is said to be its bi-ideal if $(BR_{LA})B \subseteq B$.

Theorem 3.3.15. If A is a bi-ideal of an LA-semigroup L then for a commutative and associative ring R , $R[A]$ is a bi-ideal of $R[L]$, for any LA-semigroup L .

Proof. Since A is a bi-ideal of L , it is its sub LA-semigroup. By the Proposition 3.3.5, $R[A]$ is a sub LA-semigroup ring. Let $\alpha \in (R[A]R[L])R[A]$ then,

$\alpha = \sum_{finite} (\sum_{finite} \varphi\psi)\vartheta$ where, $\varphi = \sum_{\varrho \in A} \mu_{\varrho}\varrho$, $\psi = \sum_{\varrho \in L} \nu_{\varrho}\varrho$ and $\vartheta = \sum_{\varrho \in A} \omega_{\varrho}\varrho$.

Now, $\alpha = \sum_{finite} \sum_{finite} (\varphi\psi)\vartheta = \sum_{finite} \sum_{finite} (\sum_{\varrho \in A} \mu_{\varrho}\varrho \sum_{\varrho \in L} \nu_{\varrho}\varrho) \sum_{\varrho \in A} \omega_{\varrho}\varrho = \sum_{\varrho \in A, h \in L, \varrho \in A} (\mu_{\varrho}\nu_h)\omega_{\varrho}(\varrho h)\varrho = \sum_{u \in (AS)_A} k_u u$. This implies that, $\alpha \in R_{(AS)_A} \subseteq R[A]$ so that $\alpha \in R[A]$. Thus, $(R[A]R[L])R[A] \subseteq R[A]$ and hence $R[A]$ is a bi-ideal of $R[L]$. ■

Definition 3.3.16. A Sub LA-ring A of an LA-ring R_{LA} is called its Interior ideal if $(R_{LA}A)R_{LA} \subseteq A$.

Theorem 3.3.17. If A is an interior ideal of L then for a commutative and associative ring R , $R[A]$ is an interior ideal of $R[L]$, for any LA-semigroup L .

Proof. As A is an interior ideal of L , it is its sub LA-semigroup. By the Proposition 3.3.5, $R[A]$ is a sub LA-semigroup ring. Let $\alpha \in (R[L]R[A])R[L]$ then $\alpha = \sum_{finite} (\sum_{finite} \varphi\psi)\vartheta$ where, $\varphi = \sum_{\varrho \in L} \mu_{\varrho}\varrho$, $\psi = \sum_{\varrho \in A} \nu_{\varrho}\varrho$, $\vartheta = \sum_{\varrho \in L} \omega_{\varrho}\varrho$.

Now, $\alpha = \sum_{finite} \sum_{finite} (\varphi\psi)\vartheta = \sum_{finite} \sum_{finite} (\sum_{\varrho \in L} \mu_{\varrho}\varrho \sum_{\varrho \in A} \nu_{\varrho}\varrho) \sum_{\varrho \in L} \omega_{\varrho}\varrho = \sum_{\varrho \in L, h \in A, \varrho \in L} (\mu_{\varrho}\nu_h)c_{\varrho}(\varrho h)\varrho = \sum_{u \in (SA)_L} k_u u$. This implies that, $\alpha \in R_{[(SA)_L]} \subseteq R[A]$ and $\alpha \in R[A]$. Thus, $(R[L]R[A])R[L] \subseteq R[A]$ and $R[A]$ is an interior ideal of $R[L]$. ■

3.3.4 Homomorphisms and LA-Semigroup Rings

Ring homomorphisms and LA-semigroup homomorphisms provide us with different examples of LA-ring homomorphisms which are illustrated in the succeeding proposition:

Proposition 3.3.18. Let R and R' be commutative and associative rings and let L and L' be LA-semigroups. If $\tau : R \rightarrow R'$ is a ring homomorphism and $\phi : L \rightarrow L'$ be an LA-semigroup homomorphism then:

1. $\theta : R[L] \rightarrow R'[L]$ is a LA-ring homomorphism, where for all $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$\theta(\varphi) = \theta\left(\sum_{\varrho \in L} \mu_{\varrho}\right) = \sum_{\varrho \in L} \tau(\mu_{\varrho})\varrho. \quad (3.3.9)$$

And the kernel of θ is given by

$$\ker(\theta) = \left\{ \varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L] : \mu_{\varrho} \in \ker(\tau), \text{ for all } \varrho \in L \right\}. \quad (3.3.10)$$

2. $\theta : R[L] \rightarrow R[\phi(L)]$ is an LA-ring homomorphism, where for all $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$\theta(\varphi) = \theta\left(\sum_{\varrho \in L} \mu_{\varrho}\right) = \sum_{\varrho \in L} \mu_{\varrho} \phi(\varrho). \quad (3.3.11)$$

The kernel of θ is given by

$$\ker(\theta) = \left\{ \varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L] : \mu_{\varrho} = 0, \text{ for all } \varrho \in L \right\}. \quad (3.3.12)$$

3. $\theta : R[L] \rightarrow R'[\phi(L)]$ is an LA-ring homomorphism, where for all $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$\theta(\varphi) = \theta\left(\sum_{\varrho \in L} \mu_{\varrho}\right) = \sum_{\varrho \in L} \tau(\mu_{\varrho})\phi(\varrho). \quad (3.3.13)$$

The kernel of θ is given by

$$\ker(\theta) = \left\{ \varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L] : \mu_{\varrho} \in \ker(\tau), \text{ for all } \varrho \in L \right\}. \quad (3.3.14)$$

Remark 3.3.19. 1. If τ and ϕ defined in the Proposition 3.3.18 are bijections, then so is θ in each case.

2. If $R \cong R'$ then $R[L] \cong R'[L]$.

3. If $L \cong L'$ then $R[L] \cong R[L']$.

Note that if $\tau : R \rightarrow R'$ is a ring epimorphism and I is an ideal in R then $\tau(I) = \{\tau(\mu) : \mu \in I\}$ is an ideal in R' .

Proposition 3.3.20. Consider a commutative ring R and an LA-semigroup L . If, I is an ideal in R , then

$$\theta(I[L]) = (\tau(I))[L]. \quad (3.3.15)$$

Where θ is the LA-ring homomorphism defined in the Proposition 3.3.18 part 1 and τ is a ring epimorphism.

From ring theory, if $\tau : R \rightarrow R'$ is a ring homomorphism and I' is an ideal in R' then $\tau^{-1}(I') = \{\mu \in R : \tau(\mu) \in I'\}$ is an ideal in R .

Proposition 3.3.21. Let R and R' be commutative and associative rings and let L be an LA-semigroup. If I' is an ideal in R' , then

$$\theta^{-1}(I'[L]) = (\tau^{-1}(I'))[L]. \quad (3.3.16)$$

Where θ is the LA-ring homomorphism defined in the Proposition 3.3.18 part 1 and τ is a ring homomorphism.

Also If $\phi : L \rightarrow L'$ is an LA-semigroup epimorphism and A is an ideal in L then $\phi(A) = \{\phi(\varrho) : \varrho \in A\}$ is an ideal in L' .

Proposition 3.3.22. Consider a commutative and associative ring R . Let L and L' be two LA-semigroups. If A is an ideal in L , then

$$\theta(R[A]) = R[\phi(A)]. \quad (3.3.17)$$

Where θ is the LA-ring homomorphism defined in the Proposition 3.3.18 part 2 and ϕ is an LA-semigroup epimorphism.

Recall that if $\phi : L \rightarrow L'$ is an LA-semigroup homomorphism and A' is an ideal in L' then $\phi^{-1}(A') = \{\varrho \in L \mid \phi(\varrho) \in A'\}$ is an ideal in L .

Proposition 3.3.23. Let L and L' be LA-semigroups and let R be a commutative and associative ring, if A' is an ideal in L' , then

$$\theta^{-1}(R[A']) = R[\phi^{-1}(A')]. \quad (3.3.18)$$

Where θ is the LA-ring homomorphism defined in the Proposition 3.3.18 part 2 and ϕ is an LA-semigroup homomorphism.

The following two results are based on isomorphisms.

Theorem 3.3.24. Consider two commutative and associative rings R and R' and let L be an LA-semigroup. Then

$$(R \times R')[L] \cong R[L] \times R'[L].$$

Proof. Define $\theta : (R \times R')[L] \rightarrow R[L] \times R'[L]$, such that

$$\theta\left(\sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho\right) = \left(\sum_{\varrho \in L} \mu_{\varrho}\varrho, \sum_{\varrho \in L} \mu'_{\varrho}\varrho\right) \quad (3.3.19)$$

Let $\sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho, \sum_{\varrho \in L} (\nu_{\varrho}, \nu'_{\varrho})\varrho \in (R \times R')[L]$, then

$$\begin{aligned} \sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho + \sum_{\varrho \in L} (\nu_{\varrho}, \nu'_{\varrho})\varrho &= \sum_{\varrho \in L} (\mu_{\varrho} + \nu_{\varrho}, \mu'_{\varrho} + \nu'_{\varrho})\varrho \\ \theta\left(\sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho + \sum_{\varrho \in L} (\nu_{\varrho}, \nu'_{\varrho})\varrho\right) &= \theta\left(\sum_{\varrho \in L} (\mu_{\varrho} + \nu_{\varrho}, \mu'_{\varrho} + \nu'_{\varrho})\varrho\right) \\ &= \left(\sum_{\varrho \in L} (\mu_{\varrho} + \nu_{\varrho})\varrho, \sum_{\varrho \in L} (\mu'_{\varrho} + \nu'_{\varrho})\varrho\right) \\ &= \left(\sum_{\varrho \in L} \mu_{\varrho}\varrho + \sum_{\varrho \in L} \nu_{\varrho}\varrho, \sum_{\varrho \in L} \mu'_{\varrho}\varrho + \sum_{\varrho \in L} \nu'_{\varrho}\varrho\right) \\ &= \left(\sum_{\varrho \in L} \mu_{\varrho}\varrho, \sum_{\varrho \in L} \mu'_{\varrho}\varrho\right) + \left(\sum_{\varrho \in L} \nu_{\varrho}\varrho, \sum_{\varrho \in L} \nu'_{\varrho}\varrho\right) \\ &= \theta\left(\sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho\right) + \theta\left(\sum_{\varrho \in L} (\nu_{\varrho}, \nu'_{\varrho})\varrho\right). \end{aligned}$$

and

$$\begin{aligned} \sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho \sum_{\varrho \in L} (\nu_{\varrho}, \nu'_{\varrho})\varrho &= \sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})(\nu_{\varrho}, \nu'_{\varrho})\varrho = \sum_{\varrho, h \in L} (\mu_{\varrho}\nu_h, \mu'_{\varrho}\nu'_h)\varrho h \\ \theta\left(\sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho \sum_{\varrho \in L} (\nu_{\varrho}, \nu'_{\varrho})\varrho\right) &= \theta\left(\sum_{\varrho, h \in L} (\mu_{\varrho}\nu_h, \mu'_{\varrho}\nu'_h)\varrho h\right) \\ &= \left(\sum_{\varrho, h \in L} \mu_{\varrho}\nu_h\varrho h, \sum_{\varrho, h \in L} \mu'_{\varrho}\nu'_h\varrho h\right) \\ &= \left(\sum_{\varrho \in L} \mu_{\varrho}\varrho \sum_{\varrho \in L} \nu_{\varrho}\varrho, \sum_{\varrho \in L} \mu'_{\varrho}\varrho \sum_{\varrho \in L} \nu'_{\varrho}\varrho\right) \\ &= \left(\sum_{\varrho \in L} \mu_{\varrho}\varrho, \sum_{\varrho \in L} \mu'_{\varrho}\varrho\right) \left(\sum_{\varrho \in L} \nu_{\varrho}\varrho, \sum_{\varrho \in L} \nu'_{\varrho}\varrho\right) \\ &= \theta\left(\sum_{\varrho \in L} (\mu_{\varrho}, \mu'_{\varrho})\varrho\right) \theta\left(\sum_{\varrho \in L} (\nu_{\varrho}, \nu'_{\varrho})\varrho\right). \end{aligned}$$

So θ is a homomorphism.

One can easily verify that θ is a bijection. ■

Theorem 3.3.25. Let I be an ideal of a commutative and associative ring R and let L be an LA-semigroup. Then

$$R[L]/I[L] \cong (R/I)[L]. \quad (3.3.20)$$

Proof. $R[L]/I[L] = \{\psi + I[L] \mid \psi \in R[L]\}$ and $(R/I)[L] = \sum_{\varrho \in L} (\mu_{\varrho} + I) \varrho \mid \mu_{\varrho} + I \in R/I\}$

Define $\theta : R[L]/I[L] \rightarrow (R/I)[L]$

by $\theta(\psi + I[L]) = \theta(\sum_{\varrho \in L} \nu_{\varrho} + I[L]) = \sum_{\varrho \in L} (\nu_{\varrho} + I) \varrho$.

$$\begin{aligned} \theta(\varphi + I[L] + \psi + I[L]) &= \theta(\varphi + \psi + I[L]) \\ &= \theta\left(\sum_{\varrho \in L} ((\mu_{\varrho} + \nu_{\varrho}) + I[L])\right) \\ &= \sum_{\varrho \in L} (\mu_{\varrho} + \nu_{\varrho} + I) \varrho \\ &= \sum_{\varrho \in L} (\mu_{\varrho} + I) \varrho + \sum_{\varrho \in L} (\nu_{\varrho} + I) \varrho \\ &= \theta(\varphi + I[L]) + \theta(\psi + I[L]). \end{aligned}$$

Also

$$\begin{aligned} \theta((\varphi + I[L])(\psi + I[L])) &= \theta(\varphi\psi + I[L]) \\ &= \theta\left(\left(\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{h \in L} \nu_h h\right) + I[L]\right) \\ &= \sum_{\varrho \in L} (\mu_{\varrho} \nu_h + I) gh \\ &= \sum_{\varrho \in L} (\mu_{\varrho} + I)(\nu_h + I) gh \\ &= \left(\sum_{\varrho \in L} (\mu_{\varrho} + I) \varrho\right) \left(\sum_{h \in L} (\nu_h + I) h\right) \\ &= \theta(\varphi + I[L]) \theta(\psi + I[L]). \end{aligned}$$

So θ is a homomorphism.

It is not difficult to see that θ is bijective. ■

Definition 3.3.26. A Noetherian (an Artinian) LA-ring is an LA-ring R_{LA} , that satisfies the ascending (decending) chain condition for its ideals. In other words, provided any chain of ideals in R_{LA} ;

$I_1 \subseteq \cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$ ($I_1 \supseteq \cdots \supseteq I_{k-1} \supseteq I_k \supseteq I_{k+1} \supseteq \cdots$) there exists an index n such that:

$$I_n = I_{n+1} = \cdots .$$

Theorem 3.3.27. For a commutative and associative ring R , if R is Noetherian then so is $R[L]$ for any LA-semigroup L .

Proof. Let $K_1 \subseteq K_2 \subseteq \dots \subseteq K_n \subseteq \dots$ be an ascending chain of ideals in $R[L]$. Then $K_i \subseteq K_{i+1} \Rightarrow \hat{K}_i \subseteq \hat{K}_{i+1}$, where, $\hat{K} = \{\sum_{\varrho \in L} \mu_\varrho : \sum_{\varrho \in L} \mu_\varrho \varrho \in K\}$. Because, if $\alpha \in \hat{K}_i$ then $\alpha = \sum_{\varrho \in L} \mu_\varrho$, where $\sum_{\varrho \in L} \mu_\varrho \varrho \in K_i$. Now, $K_i \subseteq K_{i+1}$ implies that $\sum_{\varrho \in L} \mu_\varrho \varrho \in K_{i+1}$. Then, $\sum_{\varrho \in L} \mu_\varrho \in \hat{K}_{i+1}$. Which implies that, $\hat{K}_1 \subseteq \hat{K}_2 \subseteq \dots \subseteq \hat{K}_n \subseteq \dots$ be an ascending chain of ideals in R . Since R is a noetherian ring so, there exists a positive integer n , such that $\hat{K}_n = \hat{K}_m$ for all $m \geq n$. Now, let $\varphi \in K_n$ then $\varphi = \sum_{\varrho \in L} \mu_\varrho \varrho$ and $\sum_{\varrho \in L} \mu_\varrho \in \hat{K}_n = \hat{K}_m \Rightarrow \sum_{\varrho \in L} \mu_\varrho \in \hat{K}_m$. So that, $\varphi = \sum_{\varrho \in L} \mu_\varrho \varrho \in K_m$. Thus, $K_n \subseteq K_m$. Similarly $K_m \subseteq K_n$ and this implies that $K_n = K_m$ for all $m \geq n$. Hence, $R[L]$ is Noetherian. ■

Similarly, it is not hard to prove the following theorem.

Theorem 3.3.28. If R is Artinian then so is $R[L]$ for any LA-semigroup L .

3.4 Divisibility Theory in LA-Domains

Divisibility has a great significance in commutative ring theory due to its relation with the ideal structure of these rings. The concept of divisibility in LA-rings has not been introduced so far. In this section, we establish the useful notion of divisibility for the LA-rings and explore their ideal structure in more detail. This section includes the concepts of prime and irreducible elements and prime and maximal ideals. Most of the results proved in this chapter use ‘medial law’ and ‘paramedial law’ from [134].

3.4.1 LA-field and LA-integral Domain

In order to start a study on divisibility theory in LA-rings, we first need to establish few concepts and results regarding LA-fields and LA-integral domains.

Shah and Rehman in their paper [131], introduced the notions of LA-integral domain or simply an LA-domain and an LA-field. In the following, we provide our findings for the two.

The succeeding result is obvious, as cancellation laws imply non-existence of zero divisors.

Theorem 3.4.1. An LA-ring is cancellative if and only if it is an LA-Integral Domain.

Theorem 3.4.2. Every LA-field is an LA-integral Domain.

Proof. Assume that R_{LA} is an LA-field, then for each non-zero element $\mu \in R_{LA}$, its multiplicative inverse $\mu^{-1} \in R_{LA}$. Let $\mu, \nu \in R_{LA}$ such that $\mu\nu = 0$ and $\nu \neq 0$, then $\nu^{-1} \in R_{LA}$. Now $\mu\nu = 0$ implies that $(\mu\nu)\nu^{-1} = 0\nu^{-1}$ or $(\nu^{-1}\nu)\mu = 0$. That is $\mu = 0$. R_{LA} has no right zero divisors.

Suppose $\mu\nu = 0$ with $\mu \neq 0$. $\mu\nu = 0$ implies that $(e\mu)\nu = 0$, so, $\Rightarrow (\mu\nu)e = 0$. Since R_{LA} has no right zero divisors and $e \neq 0$, this implies that $\nu\mu = 0$ and $\mu \neq 0$, so again due to non existence of right zero divisors in R_{LA} , $\nu = 0$. Hence, R_{LA} has no left zero divisors. ■

Following theorem is analogue of the same for associative rings.

Theorem 3.4.3. Every finite LA-integral domain is an LA-field.

Definition 3.4.4. An LA-integral domain is called a principal left ideal LA-integral domain if each of its left ideals is a principal left ideal.

3.4.2 Prime and Maximal Left Ideals

Definition 3.4.5. A left ideal \mathcal{P} of an LA-ring R_{LA} is called a prime left ideal iff for any left ideals I_1, I_2 of R_{LA} , $I_1I_2 \subseteq \mathcal{P}$ implies that $I_1 \subseteq \mathcal{P}$ or $I_2 \subseteq \mathcal{P}$.

The succeeding theorem yields an alternate definition of a prime left ideal.

Theorem 3.4.6. Let R_{LA} be an LA-ring with ‘ e ’ as left identity. A left ideal \mathcal{P} of R_{LA} is left prime ideal iff for any $\mu, \nu \in R_{LA}$, $\mu\nu \in \mathcal{P} \Rightarrow \mu \in \mathcal{P}$ or $\nu \in \mathcal{P}$.

Proof. Let \mathcal{P} be a prime ideal. Consider $\mu, \nu \in R_{LA}$ with $\mu\nu \in \mathcal{P}$. Then

$$\begin{aligned} (R_{LA}\mu)(R_{LA}\nu) &= (R_{LA}R_{LA})(\mu\nu) \\ &= R_{LA}(\mu\nu) \\ &\subseteq R_{LA}\mathcal{P} \\ &\subseteq \mathcal{P} \end{aligned}$$

As \mathcal{P} is a prime ideal, so, $R_{LA}\mu \subseteq \mathcal{P}$ or $R_{LA}\nu \subseteq \mathcal{P}$. Hence, $\mu = e\mu \in R_{LA}\mu \subseteq \mathcal{P} \Rightarrow \mu \in \mathcal{P}$ or $\nu = e\nu \in R_{LA}\nu \subseteq \mathcal{P} \Rightarrow \nu \in \mathcal{P}$

Converse is straightforward. ■

Definition 3.4.7. A proper left ideal \mathcal{M} of an LA-ring R_{LA} is called a maximal left ideal if no proper left ideal of R_{LA} contains \mathcal{M} .

We now characterize prime ideals and maximal ideals in an LA-ring containing left identity, by the quotient LA-rings formed by these ideals.

Theorem 3.4.8. Let R_{LA} be an LA-ring with ‘ e ’ as left identity and \mathcal{P} be a proper left ideal of R_{LA} . Then \mathcal{P} is a prime left ideal iff R_{LA}/\mathcal{P} is an LA-integral domain.

Proof. Let \mathcal{P} be a prime left ideal of R_{LA} . Since R_{LA} is an LA-ring with left identity, the quotient ring R_{LA}/\mathcal{P} is also an LA-ring with left identity. We now show that R_{LA}/\mathcal{P} has no zero divisors. Let $\mathcal{P} + \mu, \mathcal{P} + \nu \in R_{LA}/\mathcal{P}$, and $(\mathcal{P} + \mu)(\mathcal{P} + \nu) = \mathcal{P}$. Then $\mathcal{P} + \mu\nu = \mathcal{P}$, which implies that $\mu\nu \in \mathcal{P}$. Since \mathcal{P} is a prime left ideal, either $\mu \in \mathcal{P}$ or $\nu \in \mathcal{P}$, that is either $\mathcal{P} + \mu = \mathcal{P}$ or $\mathcal{P} + \nu = \mathcal{P}$. Thus R_{LA}/\mathcal{P} has no zero divisors. This implies that R_{LA}/\mathcal{P} is an LA-integral domain.

Conversely, suppose R_{LA}/\mathcal{P} is an LA-integral domain. Let $\mu\nu \in \mathcal{P}$ then $\mathcal{P} = \mathcal{P} + \mu\nu$, and $\mathcal{P} = (\mathcal{P} + \mu)(\mathcal{P} + \nu)$. As R_{LA}/\mathcal{P} is an integral domain, $\mathcal{P} + \mu = \mathcal{P}$ or $\mathcal{P} + \nu = \mathcal{P}$. Thus, $\mu \in \mathcal{P}$ or $\nu \in \mathcal{P}$ and so, \mathcal{P} is a prime left ideal. ■

Theorem 3.4.9. Let R_{LA} be an LA-ring with ‘ e ’ as left identity and \mathcal{M} be a proper left ideal of R_{LA} . Then \mathcal{M} is a maximal left ideal iff R_{LA}/\mathcal{M} is an LA-field.

Proof. Suppose that \mathcal{M} is a maximal left ideal. Since R_{LA} is an LA-ring with left identity, R_{LA}/\mathcal{M} is an LA-ring with left identity ‘ e ’. Let $\mathcal{M} + \mu \in R_{LA}/\mathcal{M}$ such that $\mathcal{M} + \mu \neq \mathcal{M}$. Consider

$$T = \{\kappa + \mu\lambda : \kappa \in \mathcal{M}, \lambda \in R_{LA}\}$$

then it is not difficult to show that T is a left ideal of R_{LA} properly containing \mathcal{M} . Since \mathcal{M} is a maximal left ideal, we have $T = R_{LA}$, so there are elements $\kappa \in \mathcal{M}$ and $\nu \in R$ such that $e = \kappa + \mu\nu$. Thus, $\mathcal{M} + (\kappa + \mu\nu) = \mathcal{M} + e$ and so $\mathcal{M} + \mu\nu = \mathcal{M} + e$. Hence, $\mathcal{M} + \mu$ has an inverse in R_{LA}/\mathcal{M} . This shows that each non-zero element of R_{LA}/\mathcal{M} is a unit and so R_{LA}/\mathcal{M} is an LA-field.

Conversely, assume that R_{LA}/\mathcal{M} is an LA-field. Let J be a left ideal of R_{LA} such that $\mathcal{M} \subset J \subseteq R_{LA}$. There exists $\eta \in J$ such that $\eta \notin \mathcal{M}$. Then $\mathcal{M} + \eta \neq \mathcal{M}$ and so there exists $\mathcal{M} + v \in R_{LA}/\mathcal{M}$ such that $(\mathcal{M} + v)(\mathcal{M} + \eta) = \mathcal{M} + e$. Thus, $\mathcal{M} + v\eta = \mathcal{M} + e$ which implies that $e - v\eta \in \mathcal{M} \subset J$. Also since J is a left ideal of R_{LA} , $v\eta \in J$. So $e = (e - v\eta) + v\eta \in J$. This implies that $J = R_{LA}$. Therefore, \mathcal{M} is maximal. ■

Remark 3.4.10. In an LA-ring with left identity each maximal left ideal is a prime left ideal.

3.4.3 Divisibility in LA-rings

From [124], it follows that commutativity implies associativity in LA-rings, the operation ‘ \cdot ’ in an LA-ring is non-commutative. So the division in an LA-ring is not that simple as it is in the case of a commutative and associative ring. An element μ in an LA-ring R_{LA} may divide another element ν in R_{LA} either from left or from right or from both sides.

Definition 3.4.11. Let R_{LA} be a LA-ring with left identity ‘ e ’. Then for $\mu, \nu \in R_{LA}$, μ is said to divide ν from left (right) denoted $\mu|_L\nu$ ($\mu|_R\nu$) if there exists $\alpha \in R_{LA}$ ($\varrho \in R_{LA}$) such that $\nu = \mu\alpha$ ($\nu = \varrho\mu$). An element μ is said to divide ν denoted $\mu|\nu$, if either $\mu|_L\nu$ or $\mu|_R\nu$. μ and ν are said to be associates of each other if $\mu|\nu$ and $\nu|\mu$.

Proposition 3.4.12. Let R_{LA} be a LA-ring with ‘ e ’ as left identity then for $\mu, \nu, \alpha \in R_{LA}$:

1. $\mu|\mu, e|\mu, \mu|0$.
2. If $\mu|\nu$ and $\nu|\alpha$ then $\mu|\alpha$.
3. $\mu|e$ iff μ is a unit.
4. If $\mu|_L\nu$ and $\nu|_L\alpha$ then $\mu|_L\alpha$.
5. If $\alpha|_L\mu$ and $\alpha|_L\nu$ then for all $\eta, v \in R$, $\alpha|_R(\mu\eta + \nu v)$.

Proof. 1. As $\mu = e\mu$, $\mu|_R\mu$ and $e|_L\mu$. So, $\mu|\mu$ and $e|\mu$. As for $0 \in R_{LA}$, $0 = 0\mu = \mu 0$, therefore, $\mu|0$.

2. If $\mu|\nu$ then $\mu|_L\nu$ or $\mu|_R\nu$ and there exist $\varrho_1, \varrho_2 \in R_{LA}$ such that $\nu = \mu\varrho_1$ or $\nu = \varrho_2\mu$. If $\nu|\alpha$ then $\nu|_L\alpha$ or $\nu|_R\alpha$ and there exist $\varrho_3, \varrho_4 \in R_{LA}$ such that $\alpha = \nu\varrho_3$ or $\alpha = \varrho_4\nu$. Now If $\nu = \mu\varrho_1$ and $\alpha = \nu\varrho_3$ then $\alpha = (\mu\varrho_1)\varrho_3 = (\varrho_3\varrho_1)\mu$. If $\nu = \mu\varrho_1$ and $\alpha = \varrho_4\nu$ then $\alpha = \varrho_4(\mu\varrho_1) = (e\varrho_4)(\mu\varrho_1) = (e\alpha)(\varrho_4\varrho_1) = \mu(\varrho_4\varrho_1)$. If $\nu = \varrho_2\mu$ and $\alpha = \nu\varrho_3$ then $\alpha = (\varrho_2\mu)\varrho_3 = (\varrho_2\mu)(e\varrho_3) = (\varrho_2\mu)(e\varrho_3) = \mu((\varrho_2e)\varrho_3)$. If $\nu = \varrho_2\mu$ and $\alpha = \varrho_4\nu$ then $\alpha = \varrho_4(\varrho_2\mu) = (e\varrho_4)(\varrho_2\mu) = (\mu\varrho_4)(\varrho_2e) = ((\varrho_2e)\varrho_4)\mu$. So in each case $\mu|\alpha$.

3. Let μ be a unit then $\mu\mu^{-1} = e \Rightarrow \mu|e$.

Conversely, let $\mu|e$ then $\mu|_L e$ or $\mu|_R e$ and there exist $\varrho, \alpha \in R_{LA}$ such that either $e = \mu\varrho$ or $e = \beta\mu$. In either case μ is a unit.

4. Let $\mu|_L\nu$ and $\nu|_L\alpha$ then there exist $\varrho_1, \varrho_2 \in R_{LA}$ such that $\nu = \mu\varrho_1$ and $\alpha = \nu\varrho_2$, so that $\alpha = \nu\varrho_2 = (\mu\varrho_1)\varrho_2 = (\varrho_2\varrho_1)\mu$. So $\mu|_L\alpha$.

5. Let $\alpha|_L a$ and $\alpha|_L\nu$ then there exist $\varrho_1, \varrho_2 \in R$ such that $\mu = \alpha\varrho_1$ and $\nu = \alpha\varrho_2$, so that $\mu\eta + \nu\nu = (\alpha\varrho_1)\eta + (\alpha\varrho_2)\nu = (\eta\varrho_1)\alpha = (y d_2)\alpha = (\eta\varrho_1 + \nu\varrho_2)\alpha$. This implies that $\alpha|_R\mu\eta + \nu\nu$.

■

Proposition 3.4.13. Let R_{LA} be a LA-ring with ‘ e ’ as left identity if for $\mu, \nu \in R_{LA}$, $\mu|_R\nu$ then for an element α in R_{LA} , $\mu\alpha|_R\nu\alpha$.

Proof. If $\mu|_R\nu$ then there exists $\varrho \in R_{LA}$ such that $\nu = \varrho\mu$. Then $\nu\alpha = (\varrho\mu)\alpha = (\varrho\mu)(e\alpha) = (\varrho e)(\mu\alpha)$. So $\mu\alpha|_R\nu\alpha$. ■

Corollary 3.4.14. Let R_{LA} be a LA-ring. If for $\mu, \nu \in R_{LA}$, $\mu|_L\nu$ then for an idempotent element α in R_{LA} , $\mu\alpha|_L\nu\alpha$.

Proof. If $\mu|_L\nu$ then there exists $\varrho \in R_{LA}$ such that $\nu = \mu\varrho$. Then $\nu\alpha = (\mu\varrho)\alpha = (\mu\varrho)(\alpha\alpha) = (\mu\alpha)(\varrho\alpha)$ so $\mu\alpha|_L\nu\alpha$. ■

Proposition 3.4.15. Let μ, ν be elements in an LA-ring R_{LA} with left identity ‘ e ’. Then $\mu|_R\nu$ iff $R_{LA}\nu \subseteq R_{LA}\mu$.

Proof. Let $\mu|_{R\nu}$ then there exist α such that $\nu = \alpha\mu$. Let $\lambda \in R_{LA\nu}$ then $\lambda = \kappa\nu$ for some $\kappa \in R_{LA}$. Now $\lambda = \kappa(\alpha\mu) = (e\kappa)(\alpha\mu) = (\mu\kappa)(\alpha e) = ((\alpha e)\kappa)\mu \in R_{LA\mu}$. This implies that, $R_{LA\nu} \subseteq R_{LA\mu}$.

Conversely, let $R_{LA\nu} \subseteq R_{LA\mu}$ then $\nu = e\nu \in R_{LA\nu} \subseteq R_{LA\mu} \Rightarrow \nu \in R_{LA\mu}$. That is $\nu = \vartheta\mu$ for some $\vartheta \in R_{LA}$. Hence, $\mu|_{R\nu}$ ■

Corollary 3.4.16. Let μ, ν be elements in an LA-ring R_{LA} with left identity ‘ e ’ with μ an idempotent. Then $\mu|_{R\nu}$ iff $R_{LA\nu} \subseteq R_{LA\mu}$.

Proof. By Proposition 3.4.15, $\mu|_{R\nu}$ iff $R_{LA\nu} \subseteq R_{LA\mu}$. Consider that $\mu|_{L\nu}$ then there exists $\alpha \in R_{LA}$ such that $\nu = \mu\alpha$, let $\lambda \in R_{LA\nu}$ then $\lambda = \varrho\nu$ for some $\varrho \in R_{LA}$. Now $\vartheta = \varrho(\mu\alpha) = \mu(\varrho\alpha) = (\mu\mu)(\varrho\alpha) = ((\varrho\alpha)\mu)\mu \in R_{LA\mu}$. We have, $R_{LA\nu} \subseteq R_{LA\mu}$.

Conversely, let $R_{LA\nu} \subseteq R_{LA\mu}$ then $\nu = e\nu \in R_{LA\nu} \subseteq R_{LA\mu}$. This implies that, $\nu \in R_{LA\mu}$. That is $\nu = \vartheta\mu$ for some $\vartheta \in R_{LA}$ and hence, $\mu|_{R\nu}$. ■

Corollary 3.4.17. Let μ, ν be idempotent elements in an LA-ring R_{LA} with left identity ‘ e ’. Then μ and ν are associates iff $R_{LA\nu} \subseteq R_{LA\mu}$.

Theorem 3.4.18. Let R_{LA} be an LA-ring with ‘ e ’ as left identity;

1. ϱ is a unit iff $\varrho|\lambda$ for all $\lambda \in R_{LA}$.
2. ϱ is a unit iff $\langle \varrho \rangle = R_{LA}\varrho = R_{LA}$.
3. If $\mu = \nu\lambda$ (with $\lambda \in R_{LA}$ is a unit) then μ and ν are associates.

Proof. 1. Let ϱ be a unit then $\varrho^{-1}\varrho = \varrho\varrho^{-1} = e$. Let $\lambda \in R_{LA}$, then $\lambda = e\lambda = (\varrho\varrho^{-1})\lambda = (\lambda\varrho^{-1})\varrho$. This implies that $\varrho|_{R\lambda}$ that is $\varrho|\lambda$, for all $\lambda \in R_{LA}$.

Conversely, let $\varrho|\lambda$, for all $\lambda \in R_{LA}$. then $\varrho|e$ for $e \in R_{LA}$. By the Proposition 3.4.12 λ is a unit.

2. Let ϱ be a unit then $\varrho\varrho^{-1} = \varrho^{-1}\varrho = e$ By part 1, $\varrho|\lambda$ for all $\lambda \in R_{LA}$. Let $\mu \in R_{LA}$, $\mu = e\mu = (\varrho\varrho^{-1})\mu = (\mu\varrho^{-1})\varrho \in R_{LA}\varrho = \langle \varrho \rangle$. So, $R_{LA} \subseteq \langle \varrho \rangle$ but $\langle \varrho \rangle$ is an ideal of R_{LA} , so $\langle \varrho \rangle = R_{LA}$.

Conversely, let ϱ be an element in R_{LA} such that $\langle \varrho \rangle = R_{LA}$. Let $\lambda \in R_{LA}$, then $\lambda \in \langle \varrho \rangle = R_{LA}\varrho$ and $\lambda = \vartheta\varrho$ for some $\vartheta \in R_{LA}$. This implies that $\varrho|_{R\lambda}$ that us $\varrho|\lambda$ for all $\lambda \in R_{LA}$. By part 1, ϱ is a unit.

3. Let $\mu = \nu\lambda$ with $\lambda \in R_{LA}$ is a unit then $\nu|_L\mu$ or $\nu|\mu$. $\mu\lambda^{-1} = (\nu\lambda)\lambda^{-1} = (\lambda^{-1}\lambda)\nu = e\nu = \nu$. So, $\mu|_L\nu$ or $\mu|\nu$. Hence μ and ν are associates.

■

3.4.4 Prime and Irreducible Elements

We now define prime and irreducible elements in an LA-rings and study their relationship in a certain type of special LA-integral domain. Where, a special LA-integral domain is an special LA-ring which is an LA-domain.

Definition 3.4.19. A non-zero and non-unit element ρ in an LA-ring R_{LA} with left identity ‘ e ’ is called a prime element if for any $\mu, \nu \in R_{LA}$, $\rho|\mu\nu \Rightarrow \rho|\mu$ or $\rho|\nu$.

Definition 3.4.20. A non-zero and non-unit element β in an LA-ring R_{LA} with left identity ‘ e ’ is called an irreducible element if for any $\mu, \nu \in R_{LA}$, $\beta = \mu\nu$ then either μ is a unit or ν is a unit.

The following example illustrates that in an LA-ring with left identity ‘ e ,’ in general there is no relationship between a prime and an irreducible element.

Example 3.4.21. Let $R_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ be an LA-ring with the following additive and multiplicative tables:

+	0	1	2	3	4	5	6	7
0	1	2	3	0	6	7	5	4
1	0	1	2	3	4	5	6	7
2	3	0	1	2	7	6	4	5
3	2	3	0	1	5	4	7	6
4	6	5	7	4	1	3	2	0
5	7	4	6	5	3	1	0	2
6	4	6	5	7	0	2	1	3
7	5	7	4	6	2	0	3	1

·	0	1	2	3	4	5	6	7
0	5	1	4	3	2	0	6	7
1	1	1	1	1	1	1	1	1
2	4	1	5	3	0	2	6	7
3	3	1	3	1	3	3	1	1
4	0	1	2	3	4	5	6	7
5	2	1	0	3	5	4	6	7
6	7	1	7	1	7	7	1	1
7	6	1	6	1	6	6	1	1

Here the left identity element is $e = 4$, 3 is prime as well as irreducible element and 6, 7 are irreducible but not prime elements.

Now consider the LA-ring $R_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with the following additive and multiplicative tables:

+	0	1	2	3	4	5	6	7
0	2	3	0	1	6	7	4	5
1	3	2	1	0	5	4	7	6
2	0	1	2	3	4	5	6	7
3	1	0	3	2	7	6	5	4
4	6	5	4	7	2	1	0	3
5	7	4	5	6	1	2	3	0
6	4	7	6	5	0	3	2	1
7	5	6	7	4	3	0	1	2

·	0	1	2	3	4	5	6	7
0	1	4	2	5	7	3	6	0
1	0	1	2	3	4	5	6	7
2	2	2	2	2	2	2	2	2
3	3	5	2	6	3	6	2	5
4	7	0	2	5	1	3	6	4
5	5	3	2	6	5	6	2	3
6	6	6	2	2	6	2	2	6
7	4	7	2	3	0	5	6	1

Here the left identity element is $e = 2, 3$ and 5 are prime as well as irreducible elements and 6 is a prime element that is not irreducible.

Proposition 3.4.22. If in an LA-ring R_{LA} , ρ is an idempotent element in R_{LA} . ρ is prime element iff $R_{LA}\rho$ is a prime left ideal.

Proof. Let $\mu, \nu \in R_{LA}$ such that $\mu\nu \in R_{LA}\rho$ then $\mu\nu = \vartheta\rho$ for some $\vartheta \in R_{LA}$. This implies that $\rho|\mu\nu$. Since ρ is a prime then $\rho|\mu$ or $\rho|\nu$. If $\rho|\mu$ then there exist $\alpha_1, \alpha_2 \in R_{LA}$ such that $\mu = \rho\alpha_1$ or $\mu = \alpha_2\rho$. If $\mu = \rho\alpha_1$ then $\mu = (\rho\rho)\alpha_1 = (\alpha_1\rho)\rho \in R_{LA}\rho$. Now, if $\mu = \alpha_2\rho$ then $\mu \in R_{LA}\rho$. Similarly, if $\rho|\nu$ then $\nu \in R_{LA}\rho$. Hence, $R_{LA}\rho$ is a left prime ideal.

Conversely, assume that $R_{LA}\rho$ be a prime left ideal. Let $\rho|\mu\nu$, this implies that there exist $\alpha_1, \alpha_2 \in R_{LA}$ such that $\mu\nu = \rho\alpha_1$ $\mu\nu = \alpha_2\rho$. Now, $\mu\nu = \rho\alpha_1 = (\rho\rho)\alpha_1 = (\alpha_1\rho)\rho \in R_{LA}\rho$. As $R_{LA}\rho$ is a prime left ideal so $\mu \in R_{LA}\rho$ or $\nu \in R_{LA}\rho$. That $\rho|\mu$ or $\rho|\nu$. On the other hand, $\mu\nu = \alpha_2\rho \in R_{LA}\rho$. As $R_{LA}\rho$ is a prime left ideal so $\mu \in R_{LA}\rho$ or $\nu \in R_{LA}\rho$. That is $\rho|\mu$ or $\rho|\nu$. Hence, ρ is a prime element. ■

Theorem 3.4.23. Let R_{LA} be an idempotent LA-integral domain. An element β is irreducible in R_{LA} iff $R_{LA}\beta$ is maximal in the set of all proper principal left ideals.

Proof. If β is irreducible then $R_{LA}\beta$ is a proper ideal of R_{LA} . Let $R_{LA}\beta \subseteq R_{LA}\varrho$, (where $R_{LA}\varrho$ is a proper principal left ideal). This implies that $\beta \in R_{LA}\varrho$ and $\beta = \eta\varrho$ for

some $\eta \in R_{LA}$. As β is irreducible, so either η is a unit. ϱ is a unit contradicts that $R_{LA}\varrho$ is a proper ideal of R_{LA} . Hence η is a unit. $\eta^{-1}\beta = \eta^{-1}(\eta\varrho) = \eta^{-1}((\eta\eta)\varrho) = \eta^{-1}((\varrho\eta)\eta) = (\varrho\eta^{-1})(\eta\eta) = (\varrho\eta^{-1})\eta = (\eta\eta^{-1})\varrho = e\varrho = \varrho$. This shows that $\varrho \in R_{LA}\beta$ and $R_{LA}\varrho \subseteq R_{LA}\beta$. $R_{LA}\beta = R_{LA}\varrho$ implies that $R_{LA}\beta$ is maximal in the set of all proper principal left ideals.

Conversely, suppose on the contrary that β is not irreducible then $\beta = \mu\nu$, where neither μ nor ν is a unit. If $\mu \in R_{LA}\beta$ then $\mu = \lambda\beta$ for some $\lambda \in R_{LA}$. $\beta = \mu\nu = (\lambda\beta)\nu = (\lambda(\beta\beta))\nu = (\beta(\lambda\beta))\nu = (\nu(\lambda\beta))\beta$. By the cancellation law, $e = \nu(\lambda\beta)$, but ν is not a unit so $\mu \notin R_{LA}\beta$ and $R_{LA}\beta \subset R_{LA}\mu$. Also $R_{LA}\mu \subset R_{LA}$, as μ is not a unit. This contradicts the maximality of proper principal ideals. Hence β is irreducible. ■

Corollary 3.4.24. If R_{LA} is an idempotent principal left ideal LA-integral domain, then β is irreducible in R_{LA} iff $R_{LA}\beta$ is a maximal left ideal.

Following theorem shows that in an idempotent LA-integral domain, every prime element is irreducible.

Theorem 3.4.25. Let R_{LA} be an idempotent LA-integral domain, then every prime element is irreducible.

Proof. Let $\mu, \nu \in R_{LA}$ such that $\rho = \mu\nu$ then $\rho|\mu\nu$. Since ρ is a prime element so $\rho|\mu$ or $\rho|\nu$. If $\rho|\mu$ then there exist $\alpha_1, \alpha_2 \in R_{LA}$ such that $\mu = \rho\alpha_1$ or $\mu = \alpha_2\rho$. If $\mu = \rho\alpha_1$ then $\rho = \mu\nu = (\rho\alpha_1)\nu = (\nu\alpha_1)\rho$ or using cancellation law, $e = \nu\alpha_1$ and hence ν is a unit. If $\mu = \alpha_2\rho$ then $\rho = \mu\nu = (\alpha_2\rho)\nu = (\alpha_2(\rho\rho))\nu = (\rho(\alpha_2\rho))\nu = (\nu(\alpha_2\rho))\rho$ or $e\rho = (\nu(\alpha_2\rho))\rho$. By cancellation law unit.

On the other hand, if $\rho|\nu$ then there exist $\varrho_1, \varrho_2 \in R_{LA}$ such that $\nu = \rho\varrho_1$ or $\nu = \varrho_2\rho$. If $\nu = \rho\varrho_1$ then $\rho = \mu\nu = \mu(\rho\varrho_1) = \rho(\mu\varrho_1) = (\rho\rho)(\mu\varrho_1) = ((\mu\varrho_1)\rho)\rho = ((\rho\varrho_1)\mu)\rho$ or $e\rho = ((\rho\varrho_1)\mu)\rho$. By cancellation law $e = (\rho\varrho_1)\mu$. Hence μ is a unit. If $\nu = \varrho_2\rho$ then $\rho = \mu\nu = \mu(\varrho_2\rho) = \mu(\varrho_2(\rho\rho)) = \mu(\rho(\varrho_2\rho)) = \rho(\mu(\varrho_2\rho)) = (\rho\rho)(\mu(\varrho_2\rho)) = ((\mu(\varrho_2\rho))\rho)\rho = ((\rho(\varrho_2\rho))\mu)\rho$ or $e\rho = ((\rho(\varrho_2\rho))\mu)\rho$. By cancellation law $e = (\rho(\varrho_2\rho))\mu$. Hence μ is a unit. So in all the cases ρ is an irreducible element. ■

Theorem 3.4.26. Let R_{LA} be an idempotent principal left ideal LA-integral domain. Then an element in R_{LA} is prime iff it is irreducible.

Proof. By Theorem 3.4.25, every prime is irreducible.

Conversely, let β be irreducible then by the Corollary 3.4.24 $R_{LA}\beta$ is a maximal left ideal. By the Remark 3.4.10, $R_{LA}\beta$ is prime left ideal and by the Proposition 3.4.22 β is a prime. ■

3.5 Polynomial Formation of a Special LA-ring

This section is about the formation of polynomials (in one indeterminate) having coefficients from a special LA-ring as a finitely non-zero function from non-negative integers into a special LA-ring. The collection of such polynomials is itself a special LA-ring. In this section, we examine the division algorithm, remainder theorem and the factorization theorem for these polynomials. This section also includes the notions of irreducible polynomial over a special LA-ring, Euclidean special LA-domain and special LA-field extension.

The Special LA-ring of polynomials over a special LA-ring is an analog of the polynomial ring over associative rings. Shah and Rehman in [131] constructed an LA-ring of finitely non-zero functions from a commutative semigroup into an LA-ring. In the similar way we can construct a special LA-ring of finitely non-zero functions from the set of all non-negative integers \mathbb{Z}_0 into a special LA-ring R_{SLA} and call it the special LA-ring of polynomials over a special LA-ring. We denote it by $R_{SLA}[t, \mathbb{Z}_0]$ or simply by $R_{SLA}[t]$, where the symbol ' t ' is a 'variable' or 'indeterminant' that is totally unrelated to the special LA-ring R_{SLA} and do not represent the elements of R_{SLA} . Each element in $R_{SLA}[t]$ is called a polynomial over R_{SLA} and would be represented as :

$$p(t) = a_0 + a_1t + a_2t^2 + \dots + a_nt^n \quad (3.5.1)$$

where each a_i is an element in R_{SLA} . If the special LA-ring has a left identity ' e ,' then we can identify the polynomial $0 + et + 0t^2 + 0t^3 + \dots + 0t^n$ with ' t '. In that case t would be treated as a special member of $R_{SLA}[t]$ and a polynomial whose leading coefficient is ' e ' is called a monic polynomial. We write et^n simply as t^n and $(-a_n)t^n$ as $-a_nt^n$. If R_{SLA} has left identity ' e ' then, $R_{SLA}[t]$ also has ' e ' as its left identity. The support of $p = \sum_{i=0}^k a_it^i$, is denoted as: $Supp(p) = \{i : a_i \neq 0\}$. The order of p is defined as $ord(p) = \min(supp(p))$ and its degree as: $deg(p) = \max(supp(p))$. Likewise the polynomials over an associative ring, the degree of any nonzero polynomial is hence a

non-negative integer; no degree is assigned to the zero polynomial. The non-zero constant polynomials have degree 0.

Now we restate Lemma 2 [131], for a special LA-ring as:

Lemma 3.5.1. 1. If R_{SLA} is a special LA-ring with left identity, then for $p, q \in R_{SLA}[t]$,

$$\deg(p \cdot q) \leq \deg p + \deg q.$$

2. If R_{SLA} is a special LA-integral domain, then $\deg(p \cdot q) = \deg p + \deg q$.

Following example is an illustration of Lemma 3.5.1, part 1.

Example 3.5.2. Consider the special LA-ring R_{LA} of the Example 3.1.1; Let $p(t) = 3t^3 + 4t^2 + t + 7$ and $q(t) = 7t^3 + 6t^2 + 5t + 2$ then, $\deg p = \deg q = 3$ and $p \cdot q = (3t^3 + 4t^2 + t + 7)(7t^3 + 6t^2 + 5t + 2) = 2t^5 + t^4 + t^3 + t^2 + 2t + 7$.

Here $\deg(p(t)q(t)) < \deg p + \deg q$.

It follows from Lemma 3.5.1, that if R_{SLA} is a special LA-integral domain, then so is its polynomial special LA-ring $R_{SLA}[t]$. Though many properties of a special LA-ring R_{SLA} are carried over to the associated polynomial special LA-ring $R_{SLA}[t]$ but for no special LA-ring R_{SLA} does $R_{SLA}[t]$ forms a special LA-field. In fact, when R_{SLA} is a special LA-field (or for that matter a special LA-integral domain), no element of $R_{SLA}[t]$ which has positive degree can hold a multiplicative inverse. For, suppose that $p(t) \in R[t]$, with $\deg p(t) > 0$; if $p(t)q(t) = e$ for some $q(t) \in R[t]$, we could obtain the contradiction $0 = \deg(e) = \deg(p(t)q(t)) = \deg p(t) + \deg q(t) \neq 0$.

3.5.1 Factorization of the Polynomials over a Special LA-ring

To study the factorization of polynomials over a special LA-ring, we start with the division algorithm for polynomials over a special LA-ring.

Theorem 3.5.3. (Division Algorithm) Let R_{LA} be a Special LA-ring with left identity and $p_1(t), p_2(t) \neq 0$ be polynomials in $R_{SLA}[t]$, with the leading coefficient of $p_2(t)$ a unit element.

1. Then there exist unique polynomials $q_1(t), r_1(t) \in R_{SLA}[t]$ so that

$$P_1(t) = q_1(t)p_2(t) + r_1(t), \text{ where either } r_1(t) = 0 \text{ or } \deg(r_1(t)) < \deg(p_2(t)).$$

2. There exist unique polynomials $q_2(t), r_2(t) \in R_{SLA}[t]$ so that

$$p_1(t) = p_2(t)q_2(t) + r_2(t), \text{ where either } r_2(t) = 0 \text{ or } \deg(r_2(t)) < \deg(p_2(t)).$$

Proof. 1. The proof of Part 1 is an analogue of proof of the classical division algorithm see [26].

2. If $p_1(t) = 0$ or $\deg p_1(t) < \deg p_2(t)$, then it is obvious to take $q_1(t) = 0$ and $r_1(t) = p_1(t)$. In case, when the $\deg p_1(t) \geq \deg p_2(t)$, we prove the result by induction on the $\deg p_1(t) = n$. If $\deg p_1(t) = \deg p_2(t) = 0$, then we have $q_1(t) = ((p_2(t))^{-1}e)p_1(t)$ and $r_1(t) = 0$. Now, assume that the result is true for all polynomials of degree less than ‘ n ’. Let $p_1(t) = a_0 + a_1t + \dots + a_nt^n$ be a polynomial with degree ‘ n ’ and $p_2(t) = b_0 + b_1t + \dots + b_mt^m$ have degree m , with $n \geq m$. The polynomial

$$p'_1(t) = p_1(t) - p_2(t)(a_n(b_m^{-1}e))t^{n-m} \quad (3.5.2)$$

has degree less than ‘ n ’ since the coefficient of t^n is $a_n - b_m(a_n(b_m^{-1}e)) = 0$. Therefore, by the induction hypothesis, there exist polynomials $q'(t), r'(t) \in R_{SLA}[t]$ such that

$$p'_1(t) = q'(t)p_2(t) + r'(t), \quad (3.5.3)$$

where $r'(t) = 0$ or $\deg r'(t) < \deg p_2(t)$. Substituting the representation of $p'_1(t)$ in Equation 3.5.3 in to Equation 3.5.2 and solving for $p_1(t)$, we obtain

$$\begin{aligned} p_1(t) &= p_2(t)(q' + a_n(b_m^{-1}e)t^{n-m}) + r'(t) \\ &= p_2(t)q_2(t) + r_2(t), \end{aligned}$$

where $q_2(t) = q' + a_n(b_m^{-1}e)t^{n-m}$ and $r_2(t) = r'(t)$. This is the desired representation of $p_1(t)$. Now we show the uniqueness of $q_2(t)$ and $r_2(t)$.

Suppose there are polynomials $q'_2(t)$ and $r'_2(t) \in R_{SLA}[t]$ so that

$$p_1(t) = p_2(t)q_2(t) + r_2(t) = p_2(t)q'_2(t) + r'_2(t),$$

where $r_2(t) = 0$ or $\deg r_2(t) < \deg p_2(t)$, $r'_2(t) = 0$ or $\deg r'_2(t) < \deg p_2(t)$. Then,

$$r_2(t) - r'_2(t) = p_2(t)(q'_2(t) - q_2(t)).$$

Suppose $r_2(t) - r'_2(t) \neq 0$. Since the leading coefficient of $p_2(t)$ is a unit,

$$\deg(p_2(t)(q'_2(t) - q_2(t))) = \deg(q'_2(t) - q_2(t)) + \deg p_2(t) \geq \deg p_2(t).$$

This implies that

$$\deg(r_2(t) - r'_2(t)) \geq \deg p_2(t),$$

which is not possible since $\deg r_2(t), \deg r'_2(t) < \deg p_2(t)$. Therefore,

$$r_2(t) - r'_2(t) = 0 \quad \text{or} \quad r_2(t) = r'_2(t).$$

Thus,

$$0 = p_2(t)(q'_2(t) - q_2(t)). \quad (3.5.4)$$

As b_m is a unit, $\deg(p_2(t)(q'_2(t) - q_2(t))) \geq 0$ unless $q'_2(t) - q_2(t) = 0$. Thus from Equation 3.5.4, $q'_2(t) - q_2(t) = 0$ or $q'_2(t) = q_2(t)$.

■

Definition 3.5.4. For a polynomial $p(t) \in R_{SLA}[t]$, if $p(t) = q(t)s(t)$ for some $q(t), s(t) \in R_{SLA}[t]$ then we say $q(t)$ divides $p(t)$ from left side. Similarly if $p(t) = s(t)q(t)$ for some $q(t), s(t) \in R_{SLA}[t]$ then we say $q(t)$ divides $p(t)$ from right side.

The polynomials $q_1(t)$ and $r_1(t)$ that appear in the division algorithm would be called respectively, the quotient and the remainder on dividing $p_1(t)$ by $p_2(t)$ from right, while $q_2(t)$ and $r_2(t)$ would be called correspondingly the quotient and the remainder on dividing $p_1(t)$ by $p_2(t)$ from left. It is important to notice that if $p_2(t)$ is a monic polynomial or if R_{SLA} is a special LA-field then, we don't need to suppose that the leading coefficient of $p_2(t)$ is a unit.

Dobbs [39], presented the remainder theorem and factorization theorem for polynomials over noncommutative but associative coefficient rings. Following his method of proof, we present the following theorem.

Theorem 3.5.5. (Remainder Theorem) Let R_{SLA} be a special LA-ring with left identity 'e'. Let $\alpha \in R_{SLA}$, then $p(t) = \sum_{i=0}^n a_i t^i \in R_{SLA}[t]$ be a polynomial of degree $n \geq 1$. Then:

1. There exists unique polynomial $q_1(t) \in R_{SLA}[t]$ of degree $n - 1$ and $r_1 \in R_{SLA}$ such that $p(t) = q_1(t)(t - \alpha) + r_1$ with $r_1 = a_0 + (a_1 e)\alpha + (\alpha(a_2 e))\alpha + \dots + (\alpha(\alpha(\dots\alpha(a_n e)))\alpha$.
2. There exists unique polynomial $q_2(t) \in R_{SLA}[t]$ of degree $n - 1$ and $r_2 \in R_{SLA}$ such that $p(t) = (t - \alpha)q_2(t) + r_2$ with $r_2 = a_0 + \alpha a_1 + \alpha(\alpha a_2) + \dots + \alpha(\alpha(\alpha(\dots\alpha a_n)))$.

Proof. 1. By applying the division algorithm and dividing $p(t)$ by $t - \alpha$ from right, we have unique $q_1(t)$ and $r_1(t)$ in $R_{SLA}[t]$ such that $p(t) = q_1(t)(t - \alpha) + r_1(t)$, where $r_1(t) = 0$ or $\text{degr}_1 < 1$. Hence $r_1(t)$ is a constant polynomial say r_1 . Let us suppose that $q_1(t) = \sum_{i=0}^{n-1} b_i t^i \in R_{SLA}[t]$. Now $p(t) = q_1(t)(t - \alpha) + r_1(t)$ implies that:

$$a_n t^n + a_{n-1} t^{n-1} + \dots + a_0 = (b_{n-1} t^{n-1} + \dots + b_0)(t - \alpha) + r_1.$$

Using the distributive law, expanding and then equating the corresponding coefficients of $t^n, t^{n-1}, t^{n-2}, \dots, t^2, t$ and 1 , we get the following system of equations:

$$a_n = b_{n-1}e$$

$$a_{n-1} = -b_{n-1}\alpha + b_{n-2}e$$

$$a_{n-2} = -b_{n-2}\alpha + b_{n-3}e$$

...

$$a_2 = -b_2\alpha + b_1e$$

$$a_1 = -b_1\alpha + b_0e$$

$$a_0 = -b_0\alpha + r_1$$

On simplification we get, $a_n = b_{n-1}e$, $a_i = -b_i\alpha + b_{i-1}e$ for $i = n - 1, n - 2, \dots, 1$ and $a_0 = -b_0\alpha + r_1$. From these equations, we get $b_{n-1} = a_n e$, $b_{i-1} = (a_i + b_i\alpha)e$ for $i = 1, \dots, n - 1$ and from the last equation, $r_1 = a_0 + b_0\alpha$. By successive substitution of these values we get,

$$\begin{aligned} r_1 &= a_0 + ((a_1 + b_1\alpha)e)\alpha = a_0 + (a_1e)\alpha + (\alpha b_1)\alpha = a_0 + (a_1e)\alpha + (\alpha(a_2 + b_2\alpha)e)\alpha = \\ &= a_0 + (a_1e)\alpha + (\alpha(a_2e))\alpha + (\alpha(\alpha b_2))\alpha = \dots = a_0 + (a_1e)\alpha + (\alpha(a_2e))\alpha + \dots + \\ &= (\alpha(\alpha(\dots\alpha(a_n e))))\alpha. \end{aligned}$$

2. By analogous reasoning, starting with

$$a_n t^n + a_{n-1} t^{n-1} + \dots + a_0 = (t - \alpha)(c_{n-1} t^{n-1} + \dots + c_0) + r_2, \quad (3.5.5)$$

using the distributive law and equating the corresponding coefficients of the various powers of t . Solving for r_2 and c_{i-1} , and then on successive substitution we get the result $r_2 = a_0 + \alpha a_1 + \alpha(\alpha a_2) + \dots + \alpha(\alpha(\dots(\alpha a_n)))$.

■

Corollary 3.5.6. (Factorization Theorem) Let R_{SLA} be a special LA-ring with left identity e , $p(t) = \sum_{i=0}^n a_i t^i \in R_{SLA}[t]$ and $\alpha \in R_{SLA}$. Then:

1. The following two conditions are equivalent:

- (a) There exists $q_1(t) \in R_{SLA}[t]$ such that $p(t) = q_1(t)(t - \alpha)$;
- (b) $a_0 + (a_1 e)\alpha + (\alpha(a_2 e))\alpha + \dots + (\alpha(\alpha(\dots\alpha(a_n e)))\alpha = 0$.

2. The following two conditions are equivalent:

- (a) There exists $q_2(t) \in R_{SLA}[t]$ such that $p(t) = (t - \alpha)q_2(t)$;
- (b) $a_0 + \alpha a_1 + \alpha(\alpha a_2) + \dots + \alpha(\alpha(\alpha(\dots(\alpha a_n))) = 0$.

Proof. The proof is straightforward. ■

Following example shows that the polynomials $q_1(t)$ and $q_2(t)$ of Theorem 3.5.5 need not be equal and also r_1 and r_2 of the same theorem may not be same.

Example 3.5.7. Consider the special LA-ring $R_{SLA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of Example 3.1.1. Let $p(t) = 7t^3 + 4t^2 + 5t + 2$ and $\alpha = 3 \in R_{SLA}$. Then $p(t) = q_1(t)(t - 3) + r_1$ where $q_1(t) = 7t^2 + 2t$ and $r_1 = 2$. On the other hand $p(t) = (t - 3)q_2(t) + r_2$ where $q_2(t) = 7t^2 + 4t + 3$ and $r_2 = 4$. Clearly $q_1(t)$ is different from $q_2(t)$ and r_1 is different from r_2 .

The succeeding example is an instant application of the Factorization theorem.

Example 3.5.8. Consider the special LA-ring $R_{SLA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of Example 3.1.1 with left identity $e = 1$. Let $p(t) = 3t^2 + 2t + 1$. As for $\alpha = 1 \in R_{SLA}$, $1 + (2e)\alpha + (\alpha(3e))\alpha = 0$ so, by the factorization theorem $t + 1$ divides $p(t)$ from left side. On division we have $p(t) = (t + 1)(3t + 1)$. On the other hand, for $\alpha = 1 \in R_{SLA}$, $1 + \alpha 2 + \alpha(\alpha 3) = 0$ so, by the factorization theorem $t + 1$ divides $p(t)$ from right side. On division we find $p(t) = (5t + 1)(t + 1)$.

The discussion now takes an interesting turn with the introduction of an irreducible polynomial over a special LA-ring.

Definition 3.5.9. Let R_{SLA} be a special LA-ring with left identity. We call a non-constant polynomial $p(t) \in R_{SLA}[t]$ irreducible over R_{SLA} , or an irreducible polynomial in $R_{SLA}[t]$, if $p(t)$ is not a product of two positive degree polynomials in $R_{SLA}[t]$. Otherwise, $p(t)$ is termed reducible in $R_{SLA}[t]$.

Definition 3.5.9 holds only for polynomials with positive degree; constant polynomials are neither reducible nor irreducible. It is an easy observation that, any one degree polynomial $at + b$, $a \neq 0$, is irreducible in $R_{SLA}[t]$, where R_{SLA} is a special LA-ring with left identity. It may happen that a given polynomial is irreducible when viewed as an element of one special LA-ring, yet reducible in another. So to mention whether a polynomial is reducible or irreducible without specifying the coefficient special LA-ring involved doesn't make sense.

Example 3.5.10. The polynomial $p(t) = 2t^2 + 3t + 3 = (2t + 3)(3t + 1)$ so it is reducible over the special LA-field R_{SLA_4} of Example 3.2.1, but it is irreducible over the special LA-ring R_{SLA} of Example 3.1.1.

Remark 3.5.11. If n is odd then $t^n - 1$ can be uniquely factorized as a product of distinct irreducible polynomials.

3.5.2 Euclidean LA-domain and LA-field Extension

We now define the notion of a Euclidean norm on an LA-integral domain R_{LA} . This is essentially no more than a measure of size in R_{LA} .

Definition 3.5.12. A Euclidean norm on an LA-integral domain R_{LA} is a function v mapping the non zero elements of R_{LA} into the non negative integers satisfying the following conditions:

1. For all $a, b \in R_{LA}$ with $b \neq 0$, there exist q_1, q_2, r_1 and r_2 in R_{LA} such that $a = bq_1 + r_1$ and $a = q_2b + r_2$, where either $r_1 = 0$, $r_2 = 0$, $v(r_1) < v(b)$ or $v(r_2) < v(b)$.
2. For all $a, b \in R_{LA}$, where neither a nor b is 0, $v(a) \leq v(ab)$ and $v(b) \leq v(ab)$.

An LA-integral domain R_{LA} with a Euclidean norm on it is called a Euclidean LA-domain.

If F_{SLA} is a special LA-field, then $F_{SLA}[t]$ is a Euclidean special LA-domain, for the function v defined by $v(f(t)) = 2^{(\text{degree } f(t))}$ for $f(t) \in F_{SLA}[t]$, and $f(t) \neq 0$ is a Euclidean norm. Condition (1) holds by Theorem 3.5.3, and Condition (2) holds since the degree of the product of two polynomials is the sum of their degrees.

Theorem 3.5.13. In a Euclidean Special LA-domain every left ideal is a principal left ideal.

Proof. Let R_{SLA} be a Euclidean special LA-domain with Euclidean norm v , and let N be a left ideal in R_{SLA} . If $N = \{0\}$ then $N = \langle 0 \rangle$ and N is a principal left ideal in R_{SLA} . Now suppose that $N \neq \{0\}$. Then there exists $b \neq 0$ in N . Let us choose b such that $v(b)$ is minimal among all $v(t)$ for $t \in N$, we claim that $N = \langle b \rangle$. Let $a \in N$. Then by condition (1) of the Euclidean LA-domain, there exist q_1, q_2, r_1 and r_2 in R_{SLA} such that $a = bq_1 + r_1$ and $a = q_2b + r_2$, where either $r_1 = 0, r_2 = 0, v(r_1) < v(b)$ or $v(r_2) < v(b)$. Now from $a = q_2b + r_2, r_2 = a - q_2b$ and $a, b \in N$, so that $r_2 \in N$ since N is an ideal. Thus $v(r_2) < v(b)$ is impossible by our choice of b . Hence $r_2 = 0$, so $a = q_2b$. Since a was arbitrarily chosen element from N , we see that $N = \langle b \rangle$. ■

Remark 3.5.14. For a special LA-field $F_{SLA}, F_{SLA}[t]$ is a principal left ideal LA-domain by Theorem 3.5.13.

Definition 3.5.15. An LA-ring R_{LA} is called an LA^* -Ring if it satisfies the following identity. For all $a, b, c \in R_{LA}, (ab)c = b(ac)$.

Proposition 3.5.16. Let a, b be elements in an LA^* -ring R_{LA} with left identity 'e'. Then $a|b$ iff $R_{LAB} \subseteq R_{LAA}$.

Proof. Let $a|_R b$ then there exist c such that $b = ca$. Let $s \in Rb$ then $s = kb$ for some $k \in R_{LA}$. Now $s = k(ca) = (ek)(ca) = (ak)(ce) = ((ce)k)a \in R_{LAA} \Rightarrow R_{LAB} \subseteq R_{LAA}$.

Consider that $a|_L b$ then there exists $c \in R_{LA}$ such that $b = ac$, let $s \in R_{LAB}$ then $s = ub$ for some $u \in R_{LA}$. Now $t = u(ac) = (au)c = (cu)a \in R_{LAA} \Rightarrow R_{LAB} \subseteq R_{LAA}$.

Conversely, Let $R_{LAB} \subseteq R_{LAA}$ then $b = eb \in R_{LAB} \subseteq R_{LAA} \Rightarrow b \in R_{LAA}$. That is $b = ta$ for some $t \in R_{LA} \Rightarrow a|_R b$ and hence $a|b$. ■

Theorem 3.5.17. Let R_{LA} be an LA^* -integral domain. An element q is irreducible in R_{LA} iff $R_{LA}q$ is maximal in the set of all proper principal left ideals.

Proof. If q is irreducible then $R_{LA}q$ is a proper ideal of R_{LA} . Let $R_{LA}q \subseteq R_{LAd}$, (where R_{LAd} is a proper principal left ideal). This implies that $q \in R_{LAd}$ and $q = xd$ for some $t \in R_{LA}$. As q is irreducible, either d or t is a unit. d is a unit contradicts that R_{LAd} is a proper ideal of R_{LA} . Hence t is a unit. $t^{-1}q = t^{-1}(xd) = (xt^{-1})d = ed = d$. This shows that $d \in R_{LA}q$ and $R_{LAd} \subseteq R_{LA}q$. $R_{LA}q = R_{LAd}$ implies that $R_{LA}q$ is maximal in the set of all proper principal left ideals.

Conversely, suppose on the contrary that q is not irreducible then $q = ab$, where neither a nor b is a unit. If $b \in R_{LA}q$ then $b = rq$ for some $r \in R_{LA}$. $q = ab = a(rq) = (ar)q$. By the cancellation law $e = ar$. But a is not a unit so $b \notin R_{LA}q$ and by the Proposition 3.5.16, $R_{LA}q \subset R_{LA}b$. Also $R_{LA}b \subset R_{LA}$, as b is not a unit. This contradicts the maximality of $R_{LA}q$ in the set of all proper principal ideals. Hence q is irreducible. ■

Corollary 3.5.18. If R_{LA} is a principal left ideal LA^* -integral domain then q is irreducible in R_{LA} iff $R_{LA}q$ is a maximal left ideal.

Remark 3.5.19. Its not difficult to observe that if a special LA-ring R_{SLA} is an LA^* -Ring then, the corresponding polynomial special LA-ring $R_{SLA}[t]$ is also an LA^* -Ring.

Theorem 3.5.20. Let F_{SLA} be a special LA^* -field and let $f(t)$ be an irreducible polynomial in $F_{SLA}[t]$. Then there exists an extension special LA-field E of F_{SLA} such that $E = F_{SLA}[t]/\langle f(t) \rangle$.

Proof. By Theorem 3.5.17 $\langle f(t) \rangle$ is a maximal left ideal in $F_{SLA}[t]$. So $F_{SLA}[t]/\langle f(t) \rangle$ is a special LA^* -field. We claim that F_{SLA} can be identified with a sub special LA^* -field of $F_{SLA}[t]/\langle f(t) \rangle$ in a natural way by use of the map $\pi : F_{SLA} \rightarrow F_{SLA}[t]/\langle f(t) \rangle$ given by

$$\pi(a) = a + \langle f(t) \rangle \quad (3.5.6)$$

for $a \in F_{SLA}$. This map is one to one, for if $\pi(a) = \pi(b)$, that is, if $a + \langle f(t) \rangle = b + \langle f(t) \rangle$ for some $a, b \in F_{SLA}$, then $(a - b) \in \langle f(t) \rangle$, so $a - b$ must be a multiple of the polynomial $f(t)$, which being irreducible has degree ≥ 1 . Now if $a, b \in F_{SLA}$ then $a - b \in F_{SLA}$. So we must have $a - b = 0$, so $a = b$. Its not hard to show that ψ is an LA-ring homomorphism that maps F_{SLA} one-to-one onto a subfield of $F_{SLA}[t]/\langle f(t) \rangle$. ■

Example 3.5.21. Let F_{SLA} be a special LA^* -field. Then $f(t) = t$ is an irreducible polynomial over F_{SLA} so by the Theorem 3.5.20, $F_{SLA}[t]/\langle t \rangle$ is a special LA^* -field.

Chapter 4

Developments in Soft LA-rings

4.1 Generalized Rough Soft LA-rings

Hybrid models combining Fuzzy sets, rough sets and soft sets have appeared in different presentations and settings. For instance, Dubois and Prade [41] worked on fuzzy sets and fuzzy rough set. Feng [46] combined fuzzy sets, rough sets and soft sets all together and introduced some new concepts, such as rough soft sets, soft rough sets, soft rough fuzzy sets. Maji et al. [91] presented fuzzy soft set theory. Many researchers found the applications of these hybrid models to the decision making (see: [44, 116, 143]), and few explored their applications to some algebraic structures such as [104, 154]. In particular, Ghosh and Samanta defined rough soft groups [51], Wang and Zhan studied rough soft semigroups based on fuzzy ideals [142], Zhan and Davvaz introduced rough soft rings [153] and Zhan et al. presented rough soft hemirings [155]. All these studies are based on the Pawlak's approximation spaces which depend upon some equivalence relation. Sometimes, due to incomplete information such an equivalence relation is hard to establish. From this point of view, we introduce upper and lower approximations of soft sets under a set valued mapping ' T ' and explored an application of generalized rough soft sets (T-rough soft sets) in decision making. Since every Pawlak's rough set can be considered as a generalized rough set [147], every rough soft set may be considered as a T-rough soft set. So, the existing rough soft algebraic structures may be considered as the respective T-rough soft structures.

In this section, we propose the idea of a generalized rough soft set or a T-rough soft set. Also T-rough LA-rings are defined and their properties are discussed. Using the new definition of soft LA-ring from Chapter 1, we define a T-rough soft LA-ring. T-rough soft

idealistic LA-rings are established and T-rough soft M-systems and P-systems in T-rough soft LA-rings are also investigated. Algorithms for the decision making based on T-rough soft sets and T-rough soft LA-ring are also constructed in this section.

4.1.1 Generalized Rough Soft Sets

We use Definition 1.2.7 to define a T-rough soft set and then explore few of its properties.

Definition 4.1.1. Consider two non-empty sets V and W and $T : V \rightarrow P^*(W)$ be a set valued mapping, (where $P^*(W) = P(W) \setminus \emptyset$). Let g_A be a soft set over W . Then $T_*(g_A) = g_{A*}$ and $T^*(g_A) = g_A^*$ denote respectively the upper and lower approximations of g_A relative to T . Both are soft sets over V with the approximation functions given by;

$$g_{A*}(a) = T_*(g_A(a)) = \{b \in V | T(b) \subseteq g_A(a)\} \quad (4.1.1)$$

and

$$g_A^*(a) = T^*(g_A(a)) = \{b \in V | T(b) \cap g_A(a) \neq \emptyset\}, \quad (4.1.2)$$

where $a \in A$. We call the operators T_* and T^* , the lower and upper T-rough approximation operators on soft sets.

Throughout this section, a T-rough soft set would be denoted by TRS set, $P^*(W)$ will denote the collection of all non-empty subsets of W and the symbol T would represent a set valued mapping.

The following theorem illustrates few properties of lower and upper T-rough approximation of soft sets.

Theorem 4.1.2. Consider two non-empty sets V and W with a set valued map $T : V \rightarrow P^*(W)$. Let g_A and g_B be soft sets over W . Then,

1. $g_A \tilde{\subseteq} g_B \Rightarrow g_{A*} \tilde{\subseteq} g_{B*}$ and $g_A^* \tilde{\subseteq} g_B^*$.
2. $g_A \tilde{\cap} g_B = g_{A*} \tilde{\cap} g_{B*}$.
3. $g_A \tilde{\cap} g_B^* \tilde{\subseteq} g_A^* \tilde{\cap} g_B^*$.
4. $g_A \tilde{\cup} g_B = g_{A*} \tilde{\cup} g_{B*}$.

$$5. g_{A \cup B}^* = g_A^* \tilde{\cup} g_B^*.$$

$$6. g_{A \wedge B}^* = g_A^* \tilde{\wedge} g_B^*.$$

$$7. g_{A \wedge B}^* \tilde{\subseteq} g_A^* \tilde{\wedge} g_B^*.$$

$$8. g_{A \vee B}^* \tilde{\supseteq} g_A^* \tilde{\vee} g_B^*.$$

$$9. g_{A \vee B}^* = g_A^* \tilde{\vee} g_B^*.$$

Proof. The proof is straightforward so omitted. ■

Applications of TRS Sets in Decision Making

Zhan and Zhu [156] suggested a decision making algorithm for rough soft sets. Considering their technique as an inspiration, we present a TRS sets based decision making method. This method would set a basis of generalized rough soft sets and decision making methods in different fields such as: intelligent systems and information sciences and so on.

Algorithm

The novel method selects the finest parameter e of a given soft set g_A over a universe U . Equivalently, e is the most expected candidate on g_A with respect to a set valued mapping from one universe U' to the collection of non-empty subsets of another universe U .

Let U and U' be two universes and E be a collection of associated parameters. Consider g_A to be an original description soft set over U , where $A = \{e_1, e_2, \dots, e_m\} \subseteq E$. For a set valued mapping $T : U' \rightarrow P^*(U)$, consider T^* and T_* to be the upper and lower T-rough approximation operators. The algorithm for decision making for the TRS sets is as follows:

Step 1 Input: the original description universe U and another universe U' . $T : U' \rightarrow P^*(U)$ a set valued mapping with T^* and T_* , the upper and lower T-rough approximation operators. A soft set g_A over U .

Step 2 Compute $T_*(g_A) = g_{A_*}$ and $T^*(g_A) = g_{A^*}$ on g_A , the lower and upper TRS approximation operators respectively.

Step 3 Form the weighted tables of the soft sets g_A , g_{A_*} and g_{A^*} in accordance with the

weights determined by the selection committee.

Step 4 Compute the different values of $\|g_A(e_i)\| = \frac{|g_A^*(e_i)| - |g_{A^*}(e_i)|}{|g_A(e_i)|} \times w_i$.

Step 5 Find the minimum value $\|g_A(e_k)\|$ of $\|g_A(e_i)\|$.

Step 6 The decision is e_k .

The following example is an illustration of the method stated above.

Example 4.1.3. A restaurant in Pakistan has to select a chef closest to the desired cooking skills. The set of desired skills is $U = \{u_1, u_2, u_3, u_4, u_5, u_6\}$. Where, u_i stand for baking skills, knowledge of measurement units, presentation skills, work experience, knowledge of continental recipes and knowledge of local recipes respectively. They are asked to make the set $U' = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$ of recipes from the menu of the restaurant. Where, t_j stand for the Pineapple cake, Sushi, Panna cotta, Chinese noodles, Pizza, Chapli kebabs and Mexican enchiladas respectively. The mapping $T : U' \rightarrow P^*(U)$ maps each recipe onto the skill required for it. Hence, $T(t_1) = \{u_1, u_2, u_3, u_4\}$, $T(t_2) = \{u_3, u_4, u_5\}$, $T(t_3) = \{u_3, u_4, u_5\}$, $T(t_4) = \{u_4, u_5\}$, $T(t_5) = \{u_1, u_4, u_5\}$, $T(t_6) = \{u_4, u_6\}$ and $T(t_7) = \{u_1, u_2, u_3, u_4, u_5\}$. Now, there are four candidates to be judged, denoted by $A = \{e_1, e_2, e_3, e_4\}$. Each candidate has the skills $g_A(e_1) = \{u_1, u_6\}$, $g_A(e_2) = \{u_1, u_2, u_4, u_5, u_6\}$, $g_A(e_3) = \{u_3, u_6\}$ and $g_A(e_4) = \{u_2, u_4, u_5\}$, respectively.

Now suppose that the weights considered by the restaurant for the parameters are as: for the parameter e_1 , $w_1 = 0.7$, for the parameter e_2 , $w_2 = 0.5$, for the parameter e_3 , $w_3 = 0.6$ and for the parameter e_4 , $w_4 = 0.3$. Then Table 4.1 represents the weighted soft set g_A . Following the above Algorithm and the Definition 4.1.1, we can find two soft sets g_{A^*} and g_A^* over U' represented by the Table 4.2 and Table 4.3 respectively.

Calculating $\|g_A(e_1)\| = 1.4$, $\|g_A(e_2)\| = 0.4$, $\|g_A(e_3)\| = 1.5$ and $\|g_A(e_4)\| = 0.6$, we get the minimum value of $\|g_A(e_i)\|$ is $\|g_A(e_2)\| = 0.4$. Thus, e_2 is the expected candidate for selection.

4.1.2 Generalized Rough LA-rings

Here we introduce generalized LA-rings as a new approach to LA-ring theory. We define set valued homomorphism (SV homomorphism) and strong set valued homomorphism (SSV homomorphism) for the LA-rings as analogs of the same for the associative rings defined in [147]. We discuss several properties held by the upper and lower approximations.

U	e_1	e_2	e_3	e_4
	w_1	w_2	w_3	w_4
u_1	1	1	0	0
u_2	0	1	0	1
u_3	0	0	1	0
u_4	0	1	0	1
u_5	0	1	0	1
u_6	1	1	1	0

Table 4.1: table for weighted soft set g_A

U'	e_1	e_2	e_3	e_4
	w_1	w_2	w_3	w_4
t_1	0	0	0	0
t_2	0	0	0	0
t_3	0	0	0	0
t_4	0	1	0	1
t_5	0	1	0	0
t_6	0	1	0	0
t_7	0	0	0	0

Table 4.2: table for the soft set g_{A^*}

Pawlak's Roughness in LA-rings

Definition 4.1.4. [58] Let $(R_{LA}, +, \cdot)$ be an LA-ring and τ be a relation on R_{LA} . If for all $\mu, \nu, \alpha \in R_{LA}$, $(\mu, \nu) \in \tau$ implies that $(\alpha + \mu, \alpha + \nu)$ and $(\alpha \cdot \mu, \alpha \cdot \nu) \in \tau$ then τ is said to be left compatible. It is right compatible if $(\mu, \nu) \in \tau$ implies $(\mu + \alpha, \nu + \alpha)$ and $(\mu \cdot \alpha, \nu \cdot \alpha) \in \tau$. τ is called compatible if for all $\mu, \nu, \alpha, \beta \in R_{LA}$, if (μ, ν) and $(\alpha, \beta) \in \tau$, then $(\mu + \alpha, \nu + \beta)$ and $(\mu \cdot \alpha, \nu \cdot \beta)$ also belong to τ . A left (right) compatible equivalence relation is said to be a left (right) congruence relation, while a compatible equivalence relation is called a congruence relation.

Definition 4.1.5. Let τ be a congruence relation on an LA-ring R_{LA} . Then the approximation of R_{LA} is defined by $\tau(D) = (\underline{\tau}(D), \bar{\tau}(D))$ for each $D \in \mathcal{P}(R_{LA})$, (where

U'	e_1	e_2	e_3	e_4
	w_1	w_2	w_3	w_4
t_1	1	1	1	1
t_2	0	1	1	1
t_3	0	1	1	1
t_4	0	1	0	1
t_5	1	1	0	1
t_6	1	1	1	1
t_7	1	1	1	1

Table 4.3: table for the soft set g_A^*

$P^*(R_{LA}) = P(R_{LA}) \setminus \{\emptyset\}$ and

$$\underline{\tau}(D) = \{x \in U : [x]_{\tau} \subseteq D\}$$

and

$$\bar{\tau}(D) = \{x \in U : [x]_{\tau} \cap D \neq \emptyset\}.$$

Generalized Roughness in LA-rings

Throughout this section, R_{LA} and S_{LA} would denote LA-rings and $P^*(S_{LA})$, the set of all non-empty subsets of S_{LA} . The succeeding definition is an analogue of the definition 3.1 [147]

Definition 4.1.6. Let R_{LA} and S_{LA} be two LA-rings. A mapping $T_{LA} : R \rightarrow P^*(S_{LA})$ is called an SV-homomorphism if for all $\mu, \nu \in R_{LA}$,

1. $T(\mu) + T(\nu) \subseteq T(\mu + \nu)$,
2. $-T(\mu) \subseteq T(-\mu)$,
3. $T(\mu)T(\nu) \subseteq T(\mu\nu)$.

T is called an SSV homomorphism if

1. $T(\mu) + T(\nu) = T(\mu + \nu)$,
2. $-T(\mu) = T(-\mu)$,

$$3. T(\mu)T(\nu) = T(\mu\nu),$$

for all $\mu, \nu \in R_{LA}$.

Example 4.1.7. 1. Let I be an ideal of an LA-ring R_{LA} . Then the mapping $T : R_{LA} \rightarrow P^*(R_{LA})$ defined by $T(a) = I + a$ for all $a \in R_{LA}$ is an SV-homomorphism.

2. Let R_{LA} and S_{LA} be two LA-rings. Then the function $T : R_{LA} \rightarrow P^*(S_{LA})$ defined by $T(a) = S_{LA}$, for all $a \in R_{LA}$ is an SV-homomorphism. If S_{LA} has a left identity e , then T is an SSV-homomorphism.

3. Let R_{LA}, S_{LA} be two LA-rings. Then $T : R_{LA} \rightarrow P^*(S_{LA})$ defined by $T(a) = \{0\}$ for all $a \in R_{LA}$ is an SSV-homomorphism.

4. Let R_{LA} be an LA-ring. Then the map $T : R_{LA} \rightarrow P^*(R_{LA} \times R_{LA})$ such that $T(a) = \{(a, 0)\}$ for all $a \in R_{LA}$ is an SSV-homomorphism.

5. Let $f : R_{LA} \rightarrow S_{LA}$ be an LA-ring homomorphism. Then the function $T : R_{LA} \rightarrow P^*(S_{LA})$ defined by $T(a) = \{f(r)\}$ for all $a \in R_{LA}$ is an SSV-homomorphism.

Let Z and N be two non-empty subsets of an LA-ring R_{LA} . Then their product is defined by

$$ZN = \left\{ \sum_{finite} x_i y_i = \dots((x_1 y_1 + x_2 y_2) + x_3 y_3) + \dots + x_{n-1} y_{n-1} + x_n y_n; \text{ where } x_i \in Z \text{ and } y_i \in N \right\}.$$

Proposition 4.1.8. Let $T : R_{LA} \rightarrow P^*(S_{LA})$ be an SV homomorphism. If $\emptyset \neq Z, N \subseteq S_{LA}$, then:

$$1. \overline{T}(Z) + \overline{T}(N) \subseteq \overline{T}(Z + N),$$

$$2. -\overline{T}(Z) \subseteq \overline{T}(-Z),$$

$$3. \overline{T}(Z)\overline{T}(N) \subseteq \overline{T}(ZN).$$

Proof. 1. Let ' α ' be an element in $\overline{T}(Z) + \overline{T}(N)$. Then $\alpha = \mu + \nu$, where μ belong to $\overline{T}(Z)$ and ν belong to $\overline{T}(N)$. Then $T(\mu) \cap Z \neq \emptyset$ and $T(\nu) \cap N \neq \emptyset$. Thus we have $\beta, \gamma \in S_{LA}$ such that $\beta \in T(\mu) \cap Z$ and $\gamma \in T(\nu) \cap N$, which indicates that $\beta \in T(\mu)$, $\beta \in Z$, $\gamma \in T(\nu)$ and $\gamma \in N$. Therefore, $\beta + \gamma \in T(\mu) + T(\nu) \subseteq T(\mu + \nu)$

and $\beta + \gamma \in Z + N$. Thus, $\beta + \gamma \in T(\mu + \nu) \cap Z + N$. So, $T(\mu + \nu) \cap Z + N \neq \emptyset$. Consequently, $\mu + \nu \in \overline{T}(Z + N)$. Hence, $\alpha \in \overline{T}(Z + N)$ and $\overline{T}(Z) + \overline{T}(N) \subseteq \overline{T}(Z + N)$.

2. Let α be an element in $-\overline{T}(Z)$. Then $\alpha = -\beta$, where $\beta \in \overline{T}(Z)$. Then $T(\beta) \cap Z \neq \emptyset$. Now $T(\alpha) = T(-\beta) \supseteq -T(\beta)$. So, $-T(\beta) \cap -Z \neq \emptyset$ implies that $T(\alpha) \cap -Z \neq \emptyset$. Hence, μ belongs to $\overline{T}(-Z)$ and therefore, $-\overline{T}(Z) \subseteq \overline{T}(-Z)$.
3. Let $\alpha \in \overline{T}(Z)\overline{T}(N)$. Then $\alpha = \sum_{finite} \mu_i \nu_i$, where all $\mu_i \in \overline{T}(Z)$ and all $\nu_i \in \overline{T}(N)$. Then for all i , $T(\mu_i) \cap Z \neq \emptyset$ and $T(\nu_i) \cap N \neq \emptyset$. Therefore, for each i , there exist $\beta_i, \gamma_i \in S_{LA}$ such that $\beta_i \in T(\mu_i) \cap Z$ and $\gamma_i \in T(\nu_i) \cap N$, which implies that each $\beta_i \in T(\mu_i), \beta_i \in Z, \gamma_i \in T(\nu_i)$ and $\gamma_i \in N$. Now from the definition of T and ZN , we have $\sum_{finite} \beta_i \gamma_i \in T(\sum_{finite} \mu_i \nu_i)$ and $\sum_{finite} \beta_i \gamma_i \in ZN$. Thus, $\sum_{finite} \beta_i \gamma_i \in T(\alpha) \cap ZN$, so $T(\alpha) \cap ZN \neq \emptyset$. It follows that $\alpha \in \overline{T}(ZN)$; therefore, $\overline{T}(Z)\overline{T}(N) \subseteq \overline{T}(ZN)$.

■

Proposition 4.1.9. For an SSV homomorphism $T : R_{LA} \rightarrow P^*(S_{LA})$ and $\emptyset \neq Z, N \subseteq S_{LA}$,

1. $\underline{T}(Z) + \underline{T}(N) \subseteq \underline{T}(Z + N)$,
2. $-\underline{T}(Z) = \underline{T}(-Z)$,
3. $\underline{T}(Z)\underline{T}(N) \subseteq \underline{T}(ZN)$.

Proof. 1. For an element α in $\underline{T}(Z) + \underline{T}(N)$, there exist μ in $\underline{T}(Z)$ and ν in $\underline{T}(N)$, such that $\alpha = \mu + \nu$. Therefore $T(\mu) \subseteq \underline{T}(Z)$ and $T(\nu) \subseteq \underline{T}(N)$. Thus, $T(\mu) + T(\nu) \subseteq Z + N$. Therefore $T(\mu + \nu) \subseteq Z + N$. This implies that $\alpha \in \underline{T}(Z + N)$ and hence, $\underline{T}(Z) + \underline{T}(N) \subseteq \underline{T}(Z + N)$.

2. Let $\alpha \in -\underline{T}(Z)$. Then $\alpha = -\beta$, where $\beta \in \underline{T}(Z)$. Then $T(\beta) \subseteq Z$. Now $T(\alpha) = T(-\beta) = -T(\beta) \subseteq -Z$. So, $T(\alpha) \subseteq -Z$. Hence, $\alpha \in \underline{T}(-Z)$; therefore, $-\underline{T}(Z) \subseteq \underline{T}(-Z)$. Whereas, for $\alpha \in \underline{T}(-Z)$, $T(\alpha) \subseteq -Z$. That is, $-T(\alpha) \subseteq Z$. It follows that $T(-\alpha) \subseteq Z$. This implies that $-\alpha \in \underline{T}(Z)$ or $\alpha \in -\underline{T}(Z)$; therefore, $\underline{T}(-Z) \subseteq -\underline{T}(Z)$. Hence, $-\underline{T}(Z) = \underline{T}(-Z)$.

3. Let $\alpha \in \underline{T}(Z)\underline{T}(N)$. Then $\alpha = \sum_{finite} \mu_i \nu_i$, where all $\mu_i \in \underline{T}(Z)$ and all $\nu_i \in \underline{T}(N)$. Then for all i , $T(\mu_i) \subseteq Z$ and $T(\nu_i) \subseteq N$. By the definition of T and ZN , we have $\sum_{finite} T(\mu_i)T(\nu_i) \subseteq ZN$. Which implies that $T(\alpha) \subseteq ZN$. So, $\alpha \in \underline{T}(ZN)$; therefore, $\underline{T}(Z)\underline{T}(N) \subseteq \underline{T}(ZN)$.

■

The following example shows that equality in Proposition 4.1.8 and the Proposition 4.1.9 may not hold.

Example 4.1.10. Consider the LA-ring $R_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ obtained using [95] with the following additive and multiplicative tables on the next page.

+	0	1	2	3	4	5	6	7	·	0	1	2	3	4	5	6	7
0	2	3	4	5	6	7	0	1	0	5	4	2	3	1	0	6	7
1	3	2	5	4	7	6	1	0	1	0	1	2	3	4	5	6	7
2	0	1	2	3	4	5	6	7	2	2	2	2	2	2	2	2	2
3	1	0	3	2	5	4	7	6	3	7	7	2	2	7	7	2	2
4	6	7	0	1	2	3	4	5	4	1	0	2	3	5	4	6	7
5	7	6	1	0	3	2	5	4	5	4	5	2	3	0	1	6	7
6	4	5	6	7	0	1	2	3	6	6	6	2	2	6	6	2	2
7	5	4	7	6	1	0	3	2	7	3	3	2	2	3	3	2	2

Here the left additive identity is 2. Consider the SSV-homomorphism of Example 4.1.7 part 4.

1. Let $Z = N = \{(2, 2)\} \cup \{(1, x) | x \in R_{LA}\}$. Then $\overline{T}(Z) + \overline{T}(N) = \{2\}$, $\overline{T}(Z+N) = \{2, 5\}$ and $\underline{T}(Z) + \underline{T}(N) = \{2\}$, $\underline{T}(Z+N) = \{2, 5\}$.
2. Let $Z = \{(3, 2)\}$ and $N = \{(7, 2), (6, 1), (4, 5)\}$. Then $\overline{T}(Z)\overline{T}(N) = \{2\}$, $\overline{T}(ZN) = \{2, 7\}$ and $\underline{T}(Z)\underline{T}(N) = \{2\}$, $\underline{T}(ZN) = \{2, 7\}$.

Proposition 4.1.11. Let R_{LA} and S_{LA} be LA-rings and Z be a sub LA-ring of S_{LA} .

1. If $T : R_{LA} \rightarrow P^*(S_{LA})$ is an SV-homomorphism, then $\overline{T}(Z)$ is a sub LA-ring of R_{LA} .

2. If $T : R_{LA} \rightarrow P^*(S_{LA})$ is an SSV-homomorphism, then $\underline{T}(Z)$ is a sub LA-ring of R_{LA} .

Proof. 1. Let $\alpha, \beta \in \overline{T}(Z)$. Then $T(\alpha) \cap Z \neq \emptyset$ and $T(\beta) \cap Z \neq \emptyset$. Thus, there exist elements μ, ν in S_{LA} so that $\mu \in T(\alpha) \cap Z$ and $\nu \in T(\beta) \cap Z$. Thus $\mu \in T(\alpha)$, $\mu \in Z$ and $\nu \in T(\beta)$, $\nu \in Z$. Therefore, $\mu - \nu \in T(\alpha) - T(\beta) \subseteq T(\alpha - \beta)$, $\mu - \nu \in Z$ and $\mu\nu \in T(\alpha)T(\beta) \subseteq T(\alpha\beta)$, $\mu\nu \in Z$. So, $T(\alpha - \beta) \cap Z \neq \emptyset$ and $T(\alpha\beta) \cap Z \neq \emptyset$. Therefore, $\alpha - \beta \in \overline{T}(Z)$ and $\alpha\beta \in \overline{T}(Z)$.

2. For α, β in $\underline{T}(Z)$, $T(\alpha) \subseteq Z$ and $T(\beta) \subseteq Z$. So that, $T(\alpha - \beta) = T(\alpha) - T(\beta) \subseteq Z$ and $T(\alpha\beta) = T(\alpha)T(\beta) \subseteq Z$. Therefore, $\alpha - \beta \in \underline{T}(Z)$ and $\alpha\beta \in \underline{T}(Z)$.

■

Proposition 4.1.12. Let R_{LA} and S_{LA} be LA-rings and Z be an ideal of S_{LA} .

1. If $T : R_{LA} \rightarrow P^*(S_{LA})$ is an SV-homomorphism, then $\overline{T}(Z)$ is an ideal of R_{LA} .
2. If $T : R_{LA} \rightarrow P^*(S_{LA})$ is an SSV-homomorphism, then $\underline{T}(Z)$ is an ideal of R_{LA} .

Proof. 1. By the Proposition 4.1.11, $\overline{T}(Z)$ is a sub LA-ring of R_{LA} . Let $\rho \in R_{LA}$ and $\alpha \in \overline{T}(Z)$. Then $T(\alpha) \cap Z \neq \emptyset$, and there is an element μ in S_{LA} such that $\mu \in T(\alpha) \cap Z$. Thus $\mu \in T(\alpha)$ and $\mu \in Z$. Since $\rho \in R_{LA}$, there exists $\varrho \in S_{LA}$ such that $\varrho = T(\rho)$. Now, we have $\varrho\mu \in T(\rho)T(\alpha) \subseteq T(\rho\alpha)$ and $\mu\varrho \in T(\alpha)T(\rho) \subseteq T(\alpha\rho)$. That is $\varrho\mu \in T(\rho\alpha)$ and $\mu\varrho \in T(\alpha\rho)$. On the other hand $\varrho\mu \in T(\rho)\mu \subseteq S_{LA}Z \subseteq Z$ and $\mu\varrho \in \mu T(\rho) \subseteq ZS_{LA} \subseteq Z$. Thus, $\varrho\mu, \mu\varrho \in Z$. Therefore, $T(\rho\alpha) \cap Z \neq \emptyset$ and $T(\alpha\rho) \cap Z \neq \emptyset$. This implies that $\rho\alpha, \alpha\rho \in \overline{T}(Z)$.

2. By the Proposition 4.1.11, $\underline{T}(Z)$ is a sub LA-ring of R_{LA} . Let $\rho \in R_{LA}$ and $\alpha \in \underline{T}(Z)$. Then $T(\alpha) \subseteq Z$. Since $\rho \in R_{LA}$, $T(\rho) \subseteq S_{LA}$. It follows that $T(\rho\alpha) = T(\rho)T(\alpha) \subseteq S_{LA}Z \subseteq Z$ and $T(\alpha\rho) = T(\alpha)T(\rho) \subseteq ZS_{LA} \subseteq Z$. This implies that $\rho\alpha, \alpha\rho \in \underline{T}(Z)$.

■

4.1.3 Generalized Rough Soft LA-rings

In this section, we make a new approach to the LA-ring theory via soft sets and rough sets. We introduce and explore T-rough soft LA-rings (TRS LA-rings), idealistic TRS

LA-rings, T-rough soft M-systems (TRS M-systems) and T-rough soft P-systems (TRS P-systems) over TRS LA-rings with the help of relevant examples obtained using Mace 4 [95].

Definition 4.1.13. Consider two LA-rings R_{LA} and S_{LA} and a set valued map $T : R_{LA} \rightarrow P^*(S_{LA})$. A non-empty soft set g_A over S_{LA} is said to be a lower (upper) TRS LA-ring over S_{LA} when $T_*(g_A) = g_{A*}$ ($T^*(g_A) = g_A^*$) is a soft LA-ring over R_{LA} . That is, $g_{A*}(\alpha)$ ($g_A^*(\alpha)$) is an Sub LA-ring of R_{LA} for each $\alpha \in E$. Moreover, if g_{A*} and g_A^* are soft LA-rings over R_{LA} then g_A would be called a TRS LA-ring.

Example 4.1.14. Let $R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ be the LA-ring from Example 3.1.2 and g_A be a soft set over S_{LA} , where $E = A = R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $g_A(\alpha) = \{\beta \in S_{LA} | \alpha.\beta \in \{0, 7\}\}$ for all $\alpha \in A$ Then, $g_A(0) = g_A(3) = g_A(5) = g_A(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $g_A(1) = g_A(2) = g_A(4) = g_A(7) = \{0, 3, 5, 6\}$. Define a function $T : R_{LA} \rightarrow P^*(S_{LA})$ such that $T(0) = T(3) = T(4) = T(7) = \{0, 3\}$ and $T(1) = T(2) = T(5) = T(6) = \{0, 7\}$. Then, for all $\alpha \in A$, $g_A^*(\alpha) = \{0, 1, 2, 3, 4, 5, 6, 7\}$, while $g_{A*}(0) = g_{A*}(3) = g_{A*}(5) = g_{A*}(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $g_{A*}(1) = g_{A*}(2) = g_{A*}(4) = g_{A*}(7) = \{0, 3, 4, 7\}$. Which are sub LA-rings of R_{LA} and hence g_{A*} and g_A^* are soft LA-rings over R_{LA} implying that g_A is a TRS LA-ring over S_{LA} .

Lemma 4.1.15. Let g_A and g_B be two soft LA-rings over an LA-ring R_{LA} . Then, $g_A \tilde{\cap} g_B = g_A \tilde{\cap} g_B$ is a soft LA-ring over R_{LA} if it is non-empty.

Proof. The proof follows directly from Theorem 1 [130]. ■

Theorem 4.1.16. Let R_{LA} and S_{LA} be two LA-rings and consider a set valued mapping $T : R_{LA} \rightarrow P^*(S_{LA})$. Consider two soft sets g_A and g_B over S_{LA} where g_{A*} and g_{B*} are soft LA-rings over R_{LA} . Then, $g_A \tilde{\cap} g_{B*}$ is a soft LA-ring over R_{LA} if $g_{A*} \tilde{\cap} g_{B*}$ is non-empty.

Proof. By Lemma 4.1.15, $g_{A*} \tilde{\cap} g_{B*}$ is a soft LA-ring over R_{LA} . By Theorem 4.1.2, $f_{A \tilde{\cap} B*} = g_{A*} \tilde{\cap} g_{B*}$, and so $g_A \tilde{\cap} g_{B*}$ is a soft LA-ring over R_{LA} .

■

Remark 4.1.17. In case of upper TRS LA-rings, the above theorem may not hold.

Example 4.1.18. Let $R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ be an LA-ring, with the following additive and multiplicative tables:

+	0	1	2	3	4	5	6	7
0	2	3	4	5	6	7	0	1
1	3	2	5	4	7	6	1	0
2	0	1	2	3	4	5	6	7
3	1	0	3	2	5	4	7	6
4	6	7	0	1	2	3	4	5
5	7	6	1	0	3	2	5	4
6	4	5	6	7	0	1	2	3
7	5	4	7	6	1	0	3	2

·	0	1	2	3	4	5	6	7
0	5	4	2	3	1	0	6	7
1	0	1	2	3	4	5	6	7
2	2	2	2	2	2	2	2	2
3	7	7	2	2	7	7	2	2
4	1	0	2	3	5	4	6	7
5	4	5	2	3	0	1	6	7
6	6	6	2	2	6	6	2	2
7	3	3	2	2	3	3	2	2

Let g_A and g_B be two soft sets over S_{LA} , where $E = R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $A = B = \{1, 3, 5, 7\}$. $g_A(1) = \{3, 4\}$ and $g_A(3) = g_A(5) = g_A(7) = \{5, 6\}$, and $g_B(1) = \{4, 5, 6\}$, $g_B(3) = \{4, 5\}$ and $g_B(5) = g_B(7) = \{5, 6\}$.

Define a set valued mapping $T : R_{LA} \rightarrow P^*(S_{LA})$ so that $T(0) = T(1) = T(4) = T(5) = \{0\}$, $T(2) = \{4, 6\}$, $T(3) = \{0, 2\}$, $T(6) = \{3, 7\}$ and $T(7) = \{1, 5, 6\}$.

Then, $g_A^*(1) = \{2, 6\}$ and $g_A^*(3) = g_A^*(5) = g_A^*(7) = \{2, 7\}$. On the other hand, $g_B^*(1) = g_B^*(3) = g_B^*(5) = g_B^*(7) = \{2, 7\}$. Which are all Sub LA-rings of R_{LA} and hence g_A^* and g_B^* are soft LA-rings over R_{LA} .

Clearly, $g_{A^*} \tilde{\cap} g_{B^*}$ is non-empty. By Lemma 4.1.15, $g_{A^*} \tilde{\cap} g_{B^*}$ is a soft LA-ring over R_{LA} . Now $g_{A^*} \tilde{\cap} g_{B^*} = g_{A^* \tilde{\cap} B^*}$, where $g_{A^* \tilde{\cap} B^*}(\alpha) = g_A(\alpha) \cap g_B(\alpha)$ for each $\alpha \in E$, such that $g_A(\alpha), g_B(\alpha) \neq \emptyset$. Now, $g_{A^* \tilde{\cap} B^*}(1) = \{4\}$, $g_{A^* \tilde{\cap} B^*}(3) = \{5\}$ and $g_{A^* \tilde{\cap} B^*}(5) = g_{A^* \tilde{\cap} B^*}(7) = \{5, 6\}$. $g_{A^* \tilde{\cap} B^*}^*(\alpha) = \{\beta \in R_{LA} | T(\beta) \cap g_{A^* \tilde{\cap} B^*}(\alpha) \neq \emptyset\}$ for all $\alpha \in E$, such that $g_A(\alpha), g_B(\alpha)$ are non empty. Then, $g_{A^* \tilde{\cap} B^*}^*(1) = \{2\}$, $g_{A^* \tilde{\cap} B^*}^*(3) = \{7\}$, $g_{A^* \tilde{\cap} B^*}^*(5) = g_{A^* \tilde{\cap} B^*}^*(7) = \{2, 7\}$. As $g_{A^* \tilde{\cap} B^*}^*(3)$ is not an Sub LA-ring of R_{LA} . Hence $g_{A^* \tilde{\cap} B^*}^*$ is not a soft LA-ring over R_{LA} .

Lemma 4.1.19. Let g_A and g_B be two soft LA-rings over an LA-ring R_{LA} . Then, $g_{A \cup B} = g_A \tilde{\cup} g_B$ is a soft LA-ring over R_{LA} if $g_A \tilde{\subseteq} g_B$ or $g_A \supseteq g_B$.

Proof. The proof follows directly from Theorem 3 [130]. ■

Theorem 4.1.20. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a set valued mapping. Consider two soft sets g_A and g_B over S_{LA} with g_A^* and g_B^* soft LA-rings over R_{LA} . Then, $g_{A \cup B}^*$ is a soft LA-ring over R_{LA} if $g_A^* \subseteq g_B^*$ or $g_B^* \subseteq g_A^*$.

Proof. If $g_A^* \subseteq g_B^*$ or $g_B^* \subseteq g_A^*$, then it follows from Lemma 4.1.19 that $g_A^* \tilde{\cup} g_B^*$ is a soft LA-ring over R_{LA} . By Theorem 4.1.2, $g_{A \cup B}^* = g_A^* \tilde{\cup} g_B^*$. Thus, $g_{A \cup B}^*$ is a soft LA-ring over R_{LA} . ■

Remark 4.1.21. For the lower TRS LA-rings, the above theorem may not hold.

Example 4.1.22. Let $R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ be the LA-ring of Example 4.1.18. Let g_A and g_B be two soft sets over S_{LA} , where $E = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $A = B = \{1, 3, 5, 7\}$ and $g_A(1) = \{0, 2, 4, 5\}$, $g_A(3) = \{0, 3, 4\}$, $g_A(5) = \{0, 3, 4, 7\}$ and $g_A(7) = \{0, 1, 2, 3, 4\}$. Also, $g_B(1) = \{0, 2, 4\}$, $g_B(3) = \{0, 3, 4, 6\}$, $g_B(5) = \{0, 3, 4\}$ and $g_B(7) = \{0, 1, 2, 3, 4, 5\}$.

Define a mapping $T : R_{LA} \rightarrow P^*(S_{LA})$ such that $T(0) = T(1) = \{2, 6\}$, $T(4) = T(5) = \{5, 7\}$, $T(2) = \{4\}$, $T(3) = \{0, 1\}$, $T(6) = \{0, 2\}$ and $T(7) = \{0, 3\}$.

Then, $g_{A^*}(1) = \{2, 6\}$, $g_{A^*}(3) = g_{A^*}(5) = \{2, 7\}$ and $g_{A^*}(7) = \{2, 3, 6, 7\}$. On the other hand, $g_{B^*}(1) = \{2, 6\}$, $g_{B^*}(3) = g_{B^*}(5) = \{2, 7\}$ and $g_{B^*}(7) = \{2, 3, 6, 7\}$. All of these are sub LA-rings of R_{LA} and hence g_{A^*} and g_{B^*} are soft LA-rings over R_{LA} . By Lemma 4.1.19, $g_{A^*} \tilde{\cup} g_{B^*}$ is a soft LA-ring over R_{LA} .

Now, $g_A \tilde{\cup} g_B = g_{A \cup B}$, where $g_{A \cup B}(\alpha) = g_A(\alpha) \cup g_B(\alpha)$ for all $\alpha \in E$. Then, $g_{A \cup B}(1) = \{0, 2, 4, 5, 7\}$, $g_{A \cup B}(3) = \{0, 3, 4, 6\}$, $g_{A \cup B}(5) = \{0, 3, 4, 7\}$, $g_{A \cup B}(7) = \{0, 1, 2, 3, 4, 5\}$. $g_{A \cup B^*}(\alpha) = \{\beta \in R_{LA} | T(\beta) \subseteq g_{A \cup B}(\alpha)\}$ for all $\alpha \in E$. Then we have $g_{A \cup B^*}(1) = \{2, 4, 5, 6\}$, $g_{A \cup B^*}(3) = g_{A \cup B^*}(5) = \{2, 7\}$ and $g_{A \cup B^*}(7) = \{2, 3, 6, 7\}$. As $g_{A \cup B^*}(1)$ is not a sub LA-ring of R_{LA} . Therefore, $g_{A \cup B^*}$ is not a soft LA-ring over R_{LA} .

Theorem 4.1.23. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a set valued mapping. Consider two soft sets g_A and g_B over S_{LA} where g_{A^*} and g_{B^*} are soft LA-rings over R_{LA} . Then, $g_{A \tilde{\wedge} B^*}$ is a soft LA-ring over R_{LA} if $g_{A^*} \tilde{\wedge} g_{B^*}$ is non-empty.

Proof. By Theorem 1 [130], $g_{A^*} \tilde{\wedge} g_{B^*}$ is a soft LA-ring over R_{LA} . By Theorem 4.1.2, $g_{A \tilde{\wedge} B^*} = g_{A^*} \tilde{\wedge} g_{B^*}$, and so $g_{A \tilde{\wedge} B^*}$ is a soft LA-ring over R_{LA} . ■

Remark 4.1.24. In case of upper TRS LA-rings, the above theorem may not hold.

Example 4.1.25. In Example 4.1.18, we have two soft sets over S_{LA} . Clearly $g_A^* \tilde{\wedge} g_B^*$, is non-empty. Now $g_A \tilde{\wedge} g_B = g_{A \tilde{\wedge} B}$, where $g_{A \tilde{\wedge} B}(\alpha, \gamma) = g_A(\alpha) \cap g_B(\gamma)$ for all $(\alpha, \gamma) \in E \times E$, such that $g_A(\alpha), g_B(\gamma) \neq \emptyset$. $g_{A \tilde{\wedge} B^*}(\alpha, \gamma) = \{\beta \in R_{LA} | T(\beta) \cap g_{A \tilde{\wedge} B}(\alpha, \gamma) \neq \emptyset\}$ for all $(\alpha, \gamma) \in E \times E$, such that $g_A(\alpha), g_B(\gamma) \neq \emptyset$. Then, $g_{A \tilde{\wedge} B^*}(5, 3) = g_A(5) \cap g_B(3) = \{5\}$

and $g_{A\tilde{\wedge}B}^*(5, 3) = \{7\}$, which is not a sub LA-ring of R_{LA} . Hence $g_{A\tilde{\wedge}B}^*$ is not a soft LA-ring over R_{LA} .

Lemma 4.1.26. Let g_A and g_B be two soft LA-rings over an LA-ring R_{LA} . Then, $g_{A\tilde{\vee}B} = g_A\tilde{\vee}g_B$ is a soft LA-ring over R_{LA} if $g_A\tilde{\subseteq}g_B$ or $g_A\tilde{\supseteq}g_B$.

Proof. $g_A\tilde{\vee}g_B = g_{A\tilde{\vee}B}$ where $g_{A\tilde{\vee}B}(\alpha, \gamma) = g_A(\alpha)\tilde{\cup}g_B(\gamma)$ for all $(\alpha, \gamma) \in C$. Whether $g_A\tilde{\subseteq}g_B$ or $g_A\tilde{\supseteq}g_B$, in both cases $g_{A\tilde{\vee}B}(\alpha, \gamma)$ is a sub LA-ring of R_{LA} for all $(\alpha, \gamma) \in E \times E$. Hence, $g_{A\tilde{\vee}B}$ is a soft LA-ring over R_{LA} . ■

Theorem 4.1.27. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a set valued mapping. Let g_A and g_B be two soft sets over S_{LA} such that g_A^* and g_B^* are soft LA-rings over R_{LA} . Then, $g_{A\tilde{\vee}B}^*$ is a soft LA-ring over R_{LA} if $g_A^*\tilde{\subseteq}g_B^*$ or $g_A^*\tilde{\supseteq}g_B^*$.

Proof. If $g_A^*\tilde{\subseteq}g_B^*$ or $g_A^*\tilde{\supseteq}g_B^*$, then it follows from Lemma 4.1.26 that $g_{A\tilde{\vee}B}^*$ is a soft LA-ring over R_{LA} . By Theorem 4.1.2, $g_{A\tilde{\vee}B}^* = g_A^*\tilde{\vee}g_B^*$ and this implies that $g_{A\tilde{\vee}B}^*$ is a soft LA-ring over R_{LA} . ■

Remark 4.1.28. The above theorem may not be true for lower TRS LA-rings.

Example 4.1.29. From Example 4.1.22, we have two soft sets over S_{LA} . Clearly $g_{A\tilde{\vee}B}^*$ is non-empty. Now $g_{A\tilde{\vee}B} = g_{A\tilde{\vee}B}$, where $g_{A\tilde{\vee}B}(\alpha, \gamma) = g_A(\alpha) \cup g_B(\gamma)$ for all $(\alpha, \gamma) \in E \times E$. $g_{A\tilde{\vee}B}^*(\alpha, \gamma) = \{\beta \in R_{LA} | T(\beta) \subseteq g_{A\tilde{\vee}B}(\alpha, \gamma)\}$ for all $(\alpha, \gamma) \in E \times E$. Then, $g_{A\tilde{\vee}B}(5, 7) = g_A(5) \cup g_B(7) = \{0, 1, 2, 3, 4, 5, 7\}$ and $g_{A\tilde{\vee}B}^*(5, 7) = \{2, 3, 4, 5, 6, 7\}$. which is not a sub LA-ring of R_{LA} . Hence $g_{A\tilde{\vee}B}^*$ is not a soft LA-ring over R_{LA} .

Theorem 4.1.30. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a set-valued homomorphism. If g_A is a soft LA-ring over S_{LA} , then g_A is an upper TRS LA-ring over S_{LA} .

Proof. Since g_A is a soft LA-ring over S_{LA} , $g_A(\alpha)$ is a sub LA-ring of S_{LA} , for each $\alpha \in E$. Now $g_A^*(\alpha) = \{\beta \in R_{LA} | T(\beta) \cap g_A(\alpha) \neq \emptyset\}$. Let $\mu, \nu \in g_A^*(\alpha)$, then $T(\mu) \cap g_A(\alpha) \neq \emptyset$ and $T(\nu) \cap g_A(\alpha) \neq \emptyset$, then there exist $\eta, \delta \in R_{LA}$ such that $\eta \in T(\mu) \cap g_A(\alpha)$ and $\delta \in T(\nu) \cap g_A(\alpha)$, that is, $\eta \in T(\mu)$, $\delta \in T(\nu)$ and $\eta, \delta \in g_A(\alpha)$.

$g_A(\alpha)$ is a sub LA-ring of S_{LA} , then $\eta\delta, \eta - \delta \in g_A(\alpha)$. By Definition 4.1.6, $\eta - \delta \in T(\mu) - T(\nu) \subseteq T(\mu - \nu)$ and $\eta\delta \in T(\mu)T(\nu) \subseteq T(\mu\nu)$. Thus, $\eta - \delta \in T(\mu - \nu) \cap g_A(\alpha)$ and $\eta\delta \in T(\mu\nu) \cap g_A(\alpha)$, which implies, $T(\mu - \nu) \cap g_A(\alpha) \neq \emptyset$ and $T(\mu\nu) \cap g_A(\alpha) \neq \emptyset$.

Then, $\mu - \nu, ab \in g_A^*(\alpha)$. This shows that $g_A^*(\alpha)$ is a sub LA-ring of R_{LA} for all $\alpha \in E$. Hence, g_A^* is a soft LA-ring over R_{LA} , and so, g_A is an upper TRS LA-ring over S_{LA} . ■

Corollary 4.1.31. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a strong set-valued homomorphism. If g_A is a soft LA-ring over S_{LA} , then g_A is an upper TRS LA-ring over S_{LA} .

Theorem 4.1.32. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a strong set-valued homomorphism. If g_A is a soft LA-ring over S_{LA} , then g_A is a lower TRS LA-ring over S_{LA} .

Proof. Since g_A is a soft LA-ring over S_{LA} , and $g_A(\alpha)$ is a sub LA-ring of S_{LA} , for all $\alpha \in E$. Now for all $\alpha \in E$, $g_{A*}(\alpha) = \{\beta \in R_{LA} | T(\beta) \subseteq g_A(\alpha)\}$ Let $\mu, \nu \in g_{A*}(\alpha)$, then $T(\mu) \subseteq g_A(\alpha)$ and $T(\nu) \subseteq g_A(\alpha)$.

$g_A(\alpha)$ is a sub LA-ring of S_{LA} , then by Definition 4.1.6, $T(\mu - \nu) = T(\mu) - T(\nu) \subseteq g_A(\alpha)$ and $T(\mu\nu) = T(\mu)T(\nu) \subseteq g_A(\alpha)$. Then, $\mu - \nu, \mu\nu \in g_{A*}(\alpha)$. This shows that $g_{A*}(\alpha)$ is a sub LA-ring of R_{LA} for all $\alpha \in E$. Hence, g_{A*} is a soft LA-ring over R_{LA} , and so, g_A is a lower TRS LA-ring over S_{LA} . ■

Idealistic TRS LA-rings

This section is about the investigation of idealistic TRS LA-rings.

Definition 4.1.33. A non-empty soft set g_A over S_{LA} is said to be a lower (upper) idealistic TRS LA-rings over S_{LA} , if $g_{A*}(g_A^*)$ is idealistic soft LA-ring over R_{LA} , that is, $g_{A*}(\alpha)(g_A^*(\alpha))$ is an ideal of R_{LA} for all $\alpha \in E$, such that $g_{A*}(\alpha) \neq \emptyset(g_A^*(\alpha) \neq \emptyset)$. Moreover g_A is called an idealistic TRS LA-ring over S_{LA} if g_{A*} and g_A^* are idealistic soft LA-rings over R_{LA} .

Example 4.1.34. Consider the LA-ring $R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of Example 4.1.10. Let $E = R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and let g_A be a soft set over S_{LA} , where $A = \{1, 3, 5, 7\}$. $g_A(1) = \{4, 5\}$, $g_A(3) = g_A(5) = \{4, 5, 6\}$ and $g_A(7) = \{0, 4, 5, 6\}$. Define a set valued mapping $T : R_{LA} \rightarrow P^*(S_{LA})$ such that $T(0) = T(1) = T(4) = T(5) = \{1, 2\}$, $T(2) = \{4, 5\}$, $T(3) = T(7) = \{0, 6\}$ and $T(6) = \{5, 6\}$.

Then, $g_{A*}(1) = \{2\}$, $g_{A*}(3) = g_{A*}(5) = \{2, 6\}$ and $g_{A*}(7) = \{2, 3, 6, 7\}$ and $g_A^*(1) = \{2\}$ and $g_A^*(3) = g_A^*(5) = g_A^*(7) = \{2, 3, 6, 7\}$. Which are all ideals of

R_{LA} and hence g_{A^*} and g_A^* are soft idealistic LA-rings over R_{LA} implying that g_A is an idealistic TRS LA-rings over S_{LA} .

Remark 4.1.35. Since it is evident from Example 9 [130], that a soft LA-ring over an LA-ring R_{LA} may not be an idealistic soft LA-ring over R_{LA} . So, for another LA-ring S_{LA} , if $T : R_{LA} \rightarrow P^*(S_{LA})$ is a set-valued mapping then a TRS LA-ring over S_{LA} may not be a idealistic TRS LA-ring over S_{LA} .

Theorem 4.1.36. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a set-valued homomorphism. If g_A is an idealistic soft LA-ring over S_{LA} , then g_A is an upper idealistic TRS LA-ring over S_{LA} .

Proof. If, g_A is an idealistic soft LA-ring over S_{LA} , then $g_A(\alpha)$ is an ideal of S_{LA} , for all $\alpha \in E$, such that $g_A(\alpha) \neq \emptyset$. Now $g_A^*(\alpha) = \{\beta \in R_{LA} | T(\beta) \cap g_A(\alpha) \neq \emptyset\}$. Let $\mu, \nu \in g_A^*(\alpha)$, then $T(\mu) \cap g_A(\alpha) \neq \emptyset$ and $T(\nu) \cap g_A(\alpha) \neq \emptyset$, so there exist $\eta, \delta \in R_{LA}$ such that $\eta \in T(\mu) \cap g_A(\alpha)$ and $\delta \in T(\nu) \cap g_A(\alpha)$, that is, $\eta \in T(\mu), \delta \in T(\nu)$ and $\eta, \delta \in g_A(\alpha)$.

Since $g_A(\alpha)$ is an ideal of S_{LA} , $\eta - \delta \in g_A(\alpha)$. By Definition 4.1.6, $\eta - \delta \in T(\mu) - T(\nu) \subseteq T(\mu - \nu)$ and $\eta\delta \in T(\mu)T(\nu) \subseteq T(\mu\nu)$. Thus, $\eta - \delta \in T(\mu - \nu) \cap g_A(\alpha)$, which implies, $T(\mu - \nu) \cap g_A(\alpha) \neq \emptyset$. Then, $\mu - \nu \in g_A^*(\alpha)$. Now let $\rho \in R_{LA}$ and $\xi \in g_A^*(\alpha)$ then there exists $\vartheta \in T(\rho)$. Since $\xi \in g_A^*(\alpha)$, there exists $\varsigma \in T(\xi) \cap g_A(\alpha)$. We have $\vartheta\varsigma \in T(\rho)T(\xi) \subseteq T(\rho\xi)(\varsigma\vartheta \in T(\xi)T(\rho) \subseteq T(\xi\rho))$. On the other hand, since $g_A(\alpha)$ is an ideal of S_{LA} , $\vartheta\varsigma, \varsigma\vartheta \in g_A(\alpha)$. This implies that $T(\rho\xi) \cap g_A(\alpha) \neq \emptyset(T(\xi\rho) \cap g_A(\alpha) \neq \emptyset)$ and $\rho\xi, \xi\rho \in g_A^*(\alpha)$. This shows that $g_A^*(\alpha)$ is an ideal of R_{LA} for all $\alpha \in E$, such that $g_A^* \neq \emptyset$. Hence, g_A^* is an idealistic soft LA-ring over R_{LA} , and so, g_A is an upper idealistic TRS LA-ring over S_{LA} . ■

Corollary 4.1.37. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be an SV-homomorphism. If g_A is an idealistic soft LA-ring over S_{LA} , then g_A is an upper idealistic TRS LA-ring over S_{LA} .

Theorem 4.1.38. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be an SSV homomorphism. If g_A is an idealistic soft LA-ring over S_{LA} , then g_A is a lower idealistic TRS LA-ring over S_{LA} .

Proof. If, g_A is an idealistic soft LA-ring over S_{LA} , then $g_A(\alpha)$ is an ideal of S_{LA} , for all $\alpha \in E$, such that $g_A(\alpha) \neq \emptyset$. Now $g_{A*}(\alpha) = \{\beta \in R_{LA} | T(\beta) \subseteq g_A(\alpha)\}$ Let $\mu, \nu \in g_{A*}(\alpha)$, then $T(\mu) \subseteq g_A(\alpha)$ and $T(\nu) \subseteq g_A(\alpha)$.

Since $g_A(\alpha)$ is an ideal of S_{LA} , by Definition 4.1.6, $T(\mu - \nu) = T(\mu) - T(\nu) \subseteq g_A(\alpha)$ and then $\mu - \nu \in g_{A*}(\alpha)$. Now let $\rho \in R_{LA}$ and $\xi \in g_{A*}(\alpha)$. Since $\xi \in g_{A*}(\alpha)$, $T(\xi) \subseteq g_A(\alpha)$. Since $g_A(\alpha)$ is an ideal of S_{LA} , $T(\rho\xi) = T(\rho)T(\xi) \subseteq g_A(\alpha)$ ($T(\xi\rho) = T(\xi)T(\rho) \subseteq g_A(\alpha)$.) So, $\rho\xi, \xi\rho \in g_{A*}(\alpha)$. This shows that $g_{A*}(\alpha)$ is an ideal of R_{LA} for all $\alpha \in E$, such that $g_{A*}(\alpha) \neq \emptyset$. Hence, g_{A*} is an idealistic soft LA-ring over R_{LA} , and so g_A is a lower idealistic TRS LA-ring over S_{LA} . ■

TRS M-systems and P-systems over TRS Soft LA-rings

In this section we introduce TRS M-systems and P-systems in LA-rings.

Definition 4.1.39. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a set valued mapping, where $P^*(S_{LA})$ represents the collection of all non-empty subsets of S_{LA} . Let g_A be a TRS LA-ring over S_{LA} . A non empty soft set g_B over S_{LA} is said to be a lower (upper) TRS M-system over g_A if,

1. g_B is a soft subset of g_A .
2. $g_{B*}(g_B^*)$ is a soft M-system over $g_{A*}(g_A^*)$ that is, for $g_{B*}(\mu), g_{B*}(\nu) \in g_{B*}$ there exists $g_{A*}(\alpha) \in g_{A*}$ such that $g_{B*}(\mu)(g_{A*}(\alpha)g_{B*}(\nu)) \in g_{B*}$ (for $g_B^*(\mu), g_B^*(\nu) \in g_B^*$ there exists $g_A^*(\alpha) \in g_A^*$ such that $g_B^*(\mu)(g_A^*(\alpha)g_B^*(\nu)) \in g_B^*$).

Moreover, g_B is called a TRS M-system over g_A if, g_{B*} and g_B^* are soft M-systems over g_{A*} and g_A^* respectively.

Example 4.1.40. Consider the LA-ring $R_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ of Example 4.1.14. Let g_A be a soft set over S_{LA} , where $E = A = R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$. $g_A(\alpha) = \{\beta \in S_{LA} | \alpha.\beta \in \{0, 7\}\}$ for all $\alpha \in A$ Then, $g_A(0) = g_A(3) = g_A(5) = g_A(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $g_A(1) = g_A(2) = g_A(4) = g_A(7) = \{0, 3, 5, 6\}$. Define a set valued mapping $T : R_{LA} \rightarrow P^*(S_{LA})$ such that $T(0) = T(3) = T(4) = T(7) = \{0, 3\}$ and $T(1) = T(2) = T(5) = T(6) = \{2, 7\}$. Then, $g_{A*}(0) = g_{A*}(3) = g_{A*}(5) = g_{A*}(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $g_{A*}(1) = g_{A*}(2) = g_{A*}(4) = g_{A*}(7) = \{0, 3, 4, 7\}$. On the other hand $g_A^*(0) = g_A^*(3) = g_A^*(5) = g_A^*(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and

$g_A^*(1) = g_A^*(2) = g_A^*(4) = g_A^*(7) = \{0, 3, 4, 7\}$, which are all sub LA-rings of R_{LA} and hence g_{A*} and g_A^* are soft LA-rings over R_{LA} implying that g_A is a TRS LA-ring over S_{LA} .

Consider a soft subset g_B of g_A such that $B = \{1, 3, 5, 6, 7\} \subseteq A$ and $g_B(1) = g_B(7) = \{0, 3, 5, 6\}$, $g_B(3) = g_B(5) = g_B(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Now $g_{B*}(\alpha) = \{\beta \in R | T(\beta) \subseteq g_B(\alpha)\}$ and $g_B^*(\alpha) = \{\beta \in R_{LA} | T(\beta) \cap g_B(\alpha) \neq \emptyset\}$. Then, $g_{B*}(1) = g_{B*}(7) = \{0, 3, 4, 7\}$ and $g_{B*}(3) = g_{B*}(5) = g_{B*}(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$. On the other hand, $g_B^*(1) = g_B^*(7) = \{0, 3, 4, 7\}$ and $g_B^*(3) = g_B^*(5) = g_B^*(6) = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Here it can be seen that if $g_{B*}(\mu), g_{B*}(\nu) \in g_B$ then there exists $g_A(\alpha) \in g_{A*}$ such that $g_{B*}(\mu)(g_{A*}(\alpha)g_{B*}(\nu)) \in g_B$. Hence g_{B*} is a soft M-system over g_{A*} .

Similarly it can be seen that g_B^* is a soft M-system over g_{A*} . Hence g_B is a TRS M-system over the TRS LA-ring g_A .

Definition 4.1.41. Let R_{LA} and S_{LA} be two LA-rings and $T : R_{LA} \rightarrow P^*(S_{LA})$ be a set valued mapping, where $P^*(S_{LA})$ denotes the set of all non-empty subsets of S_{LA} . Let g_A be a TRS LA-ring over S_{LA} . A non empty soft set g_C over S_{LA} is said to be lower (upper) a TRS P-system over g_A if,

1. g_C is a soft subset of g_A .
2. $g_{C*}(g_C^*)$ is a soft P-system over $g_{A*}(g_A^*)$ that is, for all $g_{C*}(\mu) \in g_{C*}$ there exists $g_{A*}(\alpha) \in g_{A*}$ such that $g_{C*}(\mu)(g_{A*}(\alpha)g_{C*}(\mu)) \in g_{C*}$ (for $g_C^*(\mu) \in g_C^*$ there exists $g_A^*(\alpha) \in g_A^*$ such that $g_C^*(\mu)(g_A^*(\alpha)g_C^*(\mu)) \in g_C^*$.)

Furthermore, g_C is called a TRS P-system over g_A if, g_{C*} and g_C^* are soft P-systems over g_{A*} and g_A^* respectively.

Example 4.1.42. Let $R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ be an LA-ring taken from [129], with the following additive and multiplicative tables on the next page.

Let g_A be a soft set over S_{LA} , where $E = A = R_{LA} = S_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ and $g_A(0) = g_A(1) = g_A(3) = g_A(4) = \{0, 3, 5, 6\}$ and $g_A(2) = g_A(5) = g_A(6) = g_A(7) = g_A(8) = \{1, 2, 3, 4\}$. Define a set valued mapping $T : R_{LA} \rightarrow P^*(S_{LA})$ such that $T(0) = T(8) = \{0, 5\}$, $T(1) = T(6) = \{1, 2\}$, $T(3) = \{3\}$ and $T(2) = T(4) = T(5) = T(7) = \{7\}$. Then, $g_{A*}(0) = g_{A*}(1) = g_{A*}(3) = g_{A*}(4) = \{0, 3, 8\}$ and $g_{A*}(2) = g_{A*}(5) = g_{A*}(6) = g_{A*}(7) = g_{A*}(8) = \{1, 3, 6\}$. On the other hand, $g_A^*(0) =$

+	0	1	2	3	4	5	6	7	8	·	0	1	2	3	4	5	6	7	8
0	3	4	6	8	7	2	5	1	0	0	3	1	6	3	1	6	6	1	3
1	2	3	7	6	8	4	1	0	5	1	0	3	0	3	8	8	3	0	8
2	1	5	3	4	2	0	8	6	7	2	8	1	5	3	7	2	6	4	0
3	0	1	2	3	4	5	6	7	8	3	3	3	3	3	3	3	3	3	3
4	5	0	4	2	3	1	7	8	6	4	0	6	7	3	5	4	1	2	8
5	4	2	8	7	6	3	0	5	1	5	8	6	4	3	2	7	1	5	0
6	7	6	0	1	5	8	3	2	4	6	8	3	8	3	0	0	3	8	0
7	6	8	1	5	0	7	4	3	2	7	0	1	2	3	4	5	6	7	8
8	8	7	5	0	1	6	2	4	3	8	3	6	1	3	6	1	1	6	3

$g_A^*(1) = g_A^*(3) = g_A^*(4) = \{0, 3, 8\}$ and $g_A^*(2) = g_A^*(5) = g_A^*(6) = g_A^*(7) = g_A^*(8) = \{1, 3, 6\}$, which are sub LA-rings of R_{LA} and hence g_{A*} and g_A^* are soft LA-rings over R_{LA} implying that g_A is a TRS LA-ring over S_{LA} .

Consider a soft subset g_C of g_A such that $C = \{1, 3, 5, 7\} \subseteq A$ and $g_C(1) = g_C(3) = \{0, 3, 5, 6\}$, $g_C(5) = g_C(7) = \{1, 2, 3, 4\}$. Now $g_{C*}(\alpha) = \{\beta \in R_{LA} | T(\beta) \subseteq g_C(\alpha)\}$ and $g_C^*(\alpha) = \{\beta \in R_{LA} | T(\beta) \cap g_C(\alpha) \neq \emptyset\}$. Then, $g_{C*}(1) = g_{C*}(3) = \{0, 3, 8\}$ and $g_{C*}(5) = g_{C*}(7) = \{1, 3, 6\}$. On the other hand, $g_C^*(1) = g_C^*(3) = \{0, 3, 8\}$ and $g_C^*(5) = g_C^*(7) = \{1, 3, 6\}$. Here it can be seen that if $g_{C*}(\mu) \in g_C$ then there exists $g_{A*}(\alpha) \in g_A$ such that $g_{C*}(\mu)(g_{A*}(\alpha)g_{C*}(\mu)) \in g_C$. Hence g_{C*} is a soft P-system over g_{A*} .

Similarly it can be seen that g_C^* is a soft P-system over g_A^* . Hence g_C is a TRS P-system over the TRS LA-ring g_A .

Remark 4.1.43. Since it is clear from Example 3.4 [129], that a soft P-system over a soft LA-ring may not be a soft M-system over it. So, for a TRS LA-ring g_A over S_{LA} , a TRS P-system over g_A may not be a TRS M-system over it.

4.2 Soft Intersection LA-rings

Çağman et al. [27] introduced the notion of soft intersection groups which is based on the inclusion relation and the intersection of sets. They used the operations of soft sets defined by Çağman and Enginoğlu [28]. Several soft intersection algebraic structures have been

defined so far, such as soft intersection rings by Çitak and Çağman [32], soft intersection near rings by Sezgin et al. [120] and soft intersection LA-semigroups by Sezgin [118]. For more soft intersection algebraic structures we recommend: [8, 88, 89, 99, 121–123]. Motivated by [27] and [32], we introduce soft intersection LA-group and soft intersection LA-rings, and explore some of their properties in this section.

Throughout this section, we would use the abbreviations; SI-LA-group, SI-LA-ring, SI-LA-semigroup and SI-ring respectively, for soft intersection LA-group, LA-ring, LA-semigroup and ring.

4.2.1 Soft Intersection LA-groups

This section provides introduction of soft intersection LA-groups. For further details on LA-groups, see [124].

Definition 4.2.1. Let G be an LA-group and $f_G \in S(U)$. Then, f_G is called a soft intersection groupoid over U if $f_G(xy) \supseteq f_G(x) \cap f_G(y)$ for all $x, y \in G$.

f_G is called an SI-LA-group over U if the soft intersection groupoid satisfies $f_g(x^{-1}) = f_G(x)$ for all $x \in G$.

Example 4.2.2. Consider $U = \{0, 1, 2, 3, 4, 5, 6, 7\} \subseteq \mathbb{Z}$ is the universal set and the set of parameters is $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$, the LA-group of order 8, taken from [124] such that:

·	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	3	0	1	2	6	7	5	4
2	2	3	0	1	5	4	7	6
3	1	2	3	0	7	6	4	5
4	6	4	7	5	2	0	1	3
5	7	5	6	4	0	2	3	1
6	4	7	5	6	3	1	2	0
7	5	6	4	7	1	3	0	2

Define a soft set f_G over U by:

$$f_G(x) = \begin{cases} \{x\}, & 0 \leq x \leq 3; \\ \emptyset, & 4 \leq x \leq 7. \end{cases}$$

Then it can be easily shown that,

$f_G = \{(0, \{0\}), (1, \{1\}), (2, \{2\}), (3, \{3\}), (4, \emptyset), (5, \emptyset), (6, \emptyset), (7, \emptyset)\}$ is an SI-LA-Group over U . But the soft set g_G , defined by

$$g_G(x) = \begin{cases} \{x\}, & 0 \leq x \leq 3; \\ \{x, x+1\}, & x = 4, 6; \\ \{x-1, x\}, & x = 5, 7. \end{cases}$$

such that:

$g_G = \{(0, \{0\}), (1, \{1\}), (2, \{2\}), (3, \{3\}), (4, \{4, 5\}), (5, \{4, 5\}), (6, \{6, 7\}), (7, \{6, 7\})\}$ is not an SI-LA-Group over U , since $g_G(4 \cdot 5) \not\supseteq g_G(4) \cap g_G(5)$.

4.2.2 Soft Intersection LA-rings

Definition 4.2.3. Let R_{LA} be an (a special) LA-ring with respect to the two binary operations ‘+’ and ‘·’, and $f_{R_{LA}} \in S(U)$. Then, $f_{R_{LA}}$ is called a soft intersection (special) LA-ring denoted SI-LA-ring (SI-special LA-ring) over U , if for all $\mu, \nu \in R_{LA}$

1. $f_{R_{LA}}(\mu + \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$;
2. $f_{R_{LA}}(-\mu) = f_{R_{LA}}(\mu)$;
3. $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$.

That is $f_{R_{LA}}$ is an SI-LA-group (soft int-group) over U for the binary operation ‘+’ in $S(U)$ induced by ‘+’ in R_{LA} , and $f_{R_{LA}}$ is a soft int-groupoid over U for the binary operation ‘·’ in $S(U)$ induced by ‘·’ in R_{LA} .

Since a special LA-ring is an LA-ring, an SI-special LA-ring is also an SI-LA-ring.

Theorem 4.2.4. Let R_{LA} be an LA-ring and $f_{R_{LA}} \in S(U)$. Then, $f_{R_{LA}}$ is an SI-LA-ring over U iff

1. $f_{R_{LA}}(\mu - \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$;
2. $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$.

Proof. When $f_{R_{LA}}$ is an SI-LA-ring, then we have $f_{R_{LA}}(\mu + \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$ and $f_{R_{LA}}(-\mu) = f_{R_{LA}}(\mu)$. Thus $f_{R_{LA}}(\mu - \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(-\nu) = f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$. Furthermore, as $f_{R_{LA}}$ is a soft int-groupoid over U , we have $f_{R_{LA}}(ab) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$.

Conversely, suppose that $f_{R_{LA}}(\mu - \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$ and $f_{R_{LA}}(ab) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$ for all $\mu, \nu \in R_{LA}$. Now choose $\mu = 0$, then $f_{R_{LA}}(0 - \nu) = f_{R_{LA}}(-\nu) \supseteq f_{R_{LA}}(\nu)$. On the other hand, $f_{R_{LA}}(\nu) = f_{R_{LA}}(0 - (-\nu)) \supseteq f_{R_{LA}}(-\nu)$, for any $\nu \in R_{LA}$. Hence, $f_{R_{LA}}(-\mu) = f_{R_{LA}}(\mu)$ for all $\mu \in R_{LA}$. Moreover, $f_{R_{LA}}(\mu + \nu) = f_{R_{LA}}(\mu - (-\nu)) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(-\nu) = f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$.

Thus, $f_{R_{LA}}$ is an SI-LA-ring over U . ■

Example 4.2.5. Let $R_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\} = U$ be an LA-ring from Example 3.1.2.

Define a soft set $f_{R_{LA}}$ over U by,

$f_{R_{LA}}(0) = f_{R_{LA}}(4) = f_{R_{LA}}(3) = f_{R_{LA}}(7) = R$ and $f_{R_{LA}}(1) = f_{R_{LA}}(2) = f_{R_{LA}}(5) = f_{R_{LA}}(6) = \{0, 3, 4, 7\}$. Then it is easy to check that $f_{R_{LA}}$ is SI-LA-ring over U .

Definition 4.2.6. Let R_{LA} be an LA-ring. Then, an SI-LA-ring $f_{R_{LA}}$ is called a soft intersection left ideal or an SI-left ideal over U , if $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\nu)$ for all $\mu, \nu \in R_{LA}$ and $f_{R_{LA}}$ is called a soft intersection right ideal or an SI-right ideal over U , if $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu)$ for all $\mu, \nu \in R_{LA}$.

If $f_{R_{LA}}$ is an SI-left and SI-right ideal over U , then $f_{R_{LA}}$ is called an SI-ideal over U .

Theorem 4.2.7. Let R_{LA} be an LA-ring and $f_{R_{LA}} \in S(U)$. Then, $f_{R_{LA}}$ is an SI-ideal over U , iff

1. $f_{R_{LA}}(\mu - \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$;
2. $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cup f_{R_{LA}}(\nu)$ for all $\mu, \nu \in R_{LA}$.

Proof. Let $f_{R_{LA}}$ be an SI-ideal over U . Then by definition $f_{R_{LA}}(\mu - \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$. Furthermore, $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu)$ and $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\nu)$, imply that $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cup f_{R_{LA}}(\nu)$.

Conversely, suppose that $f_{R_{LA}}(\mu - \nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$ and $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cup f_{R_{LA}}(\nu)$ for all $\mu, \nu \in R_{LA}$. So that, $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cup f_{R_{LA}}(\nu) \supseteq f_{R_{LA}}(\mu)$ and $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cup f_{R_{LA}}(\nu) \supseteq f_{R_{LA}}(\nu)$. Finally, $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$. Hence, $f_{R_{LA}}$ is an SI-ideal over U . ■

Remark 4.2.8. Since each commutative and associative ring should be an LA-ring so in that case the soft int-ring defined in [32] becomes a particular case of an SI-LA-ring.

Proposition 4.2.9. If $f_{R_{LA}}$ is an SI-LA-ring/ SI-ideal over U , then $f_{R_{LA}}(0) \supseteq f_{R_{LA}}(\mu)$ for all $\mu \in R_{LA}$.

Proof. When $f_{R_{LA}}$ is an SI-LA-ring/ SI-ideal over U , for all $\mu \in R_{LA}$,

$$\begin{aligned} f_{R_{LA}}(0) &= f_{R_{LA}}(\mu - \mu) \\ &\supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\mu) \\ &= f_{R_{LA}}(\mu). \end{aligned}$$

■

Proposition 4.2.10. Let R_{LA} be an LA-ring with left identity ‘ e ’. If $f_{R_{LA}}$ is an SI-ideal over U , then $f_{R_{LA}}(\mu) \supseteq f_{R_{LA}}(e)$ for all $\mu \in R_{LA}$.

Proof. Suppose that $f_{R_{LA}}$ is an SI-ideal over U . Then, for all $\mu \in R_{LA}$,

$$\begin{aligned} f_{R_{LA}}(\mu) &= f_{R_{LA}}(e\mu) \\ &\supseteq f_{R_{LA}}(e). \end{aligned}$$

■

Theorem 4.2.11. Let R_{LA} be an LA-field and $f_{R_{LA}} \in S(U)$. Then $f_{R_{LA}}$ is an SI-ideal over U if and only if $f_{R_{LA}}(\mu) = f_{R_{LA}}(e) \subseteq f_{R_{LA}}(0)$ for all $0 \neq \mu \in R_{LA}$.

Proof. Let $f_{R_{LA}}$ be an SI-ideal over U . As $f_{R_{LA}}(0) \supseteq f_{R_{LA}}(\mu)$, for all $\mu \in R_{LA}$. Then in particular $f_{R_{LA}}(0) \supseteq f_{R_{LA}}(e)$. Now if $0 \neq \mu \in R_{LA}$, then $f_{R_{LA}}(\mu) = f_{R_{LA}}(e\mu) \supseteq f_{R_{LA}}(e)$ and $f_{R_{LA}}(e) = f_{R_{LA}}(\mu^{-1}\mu) \supseteq f_{R_{LA}}(\mu)$. Implying that $f_{R_{LA}}(\mu) = f_{R_{LA}}(e) \subseteq f_{R_{LA}}(0)$.

Conversely, let $\mu, \nu \in R_{LA}$. If $\mu - \nu \neq 0$, then $f_{R_{LA}}(\mu - \nu) = f_{R_{LA}}(e) = f_{R_{LA}}(\mu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$, and if $\mu - \nu = 0$, then $f_{R_{LA}}(\mu - \nu) = f_{R_{LA}}(0) \supseteq f_{R_{LA}}(\mu) \supseteq f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)$.

Let $\mu, \nu \in R_{LA}$. If $\mu \neq 0$ and $\nu = 0$, then $f_{R_{LA}}(\mu\nu) = f_{R_{LA}}(0) \supseteq f_{R_{LA}}(e) = f_{R_{LA}}(\mu)$ and $f_{R_{LA}}(\mu\nu) = f_{R_{LA}}(0) = f_{R_{LA}}(\nu)$. Thus, $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cup f_{R_{LA}}(\nu)$. Now if $\mu \neq 0$ and $\nu \neq 0$, then by the Theorem3.4.2, $\mu\nu \neq 0$. So, $f_{R_{LA}}(\mu\nu) = f_{R_{LA}}(e) = f_{R_{LA}}(\mu)$ and $f_{R_{LA}}(\mu\nu) = f_{R_{LA}}(e) = f_{R_{LA}}(\nu)$. Thus $f_{R_{LA}}(\mu\nu) \supseteq f_{R_{LA}}(\mu) \cup f_{R_{LA}}(\nu)$ implying that $f_{R_{LA}}$ is an SI-ideal over U . ■

Theorem 4.2.12. Let $f_{R_{LA}}$ be an SI-special LA-ring/SI-ideal over U . If $f_{R_{LA}}(\mu - \nu) = f_{R_{LA}}(0)$, for any $\mu, \nu \in R_{LA}$, then $f_{R_{LA}}(\mu) = f_{R_{LA}}(\nu)$.

Proof. Let $f_{R_{LA}}(\mu - \nu) = f_{R_{LA}}(0)$ for any $\mu, \nu \in R_{LA}$. Then

$$\begin{aligned} f_{R_{LA}}(\mu) &= f_{R_{LA}}(\mu - \nu + \nu) \\ &\supseteq f_{R_{LA}}(\mu - \nu) \cap f_{R_{LA}}(\nu) \\ &= f_{R_{LA}}(0) \cap f_{R_{LA}}(\nu) \\ &= f_{R_{LA}}(\nu). \end{aligned}$$

Similarly, since $f_{R_{LA}}(0) = f_{R_{LA}}(\mu - \nu) = f_{R_{LA}}(-(\nu - \mu)) = f_{R_{LA}}(\nu - \mu)$.

So,

$$\begin{aligned} f_{R_{LA}}(\nu) &= f_{R_{LA}}(\nu - \mu + \mu) \\ &\supseteq f_{R_{LA}}(\nu - \mu) \cap f_{R_{LA}}(\mu) \\ &= f_{R_{LA}}(0) \cap f_{R_{LA}}(\mu) \\ &= f_{R_{LA}}(\mu). \end{aligned}$$

Thus $f_{R_{LA}}(\mu) = f_{R_{LA}}(\nu)$. ■

Theorem 4.2.13. Let $f_{R_{LA}}$ and $f_{T_{LA}}$ be two SI-LA-rings over U . Then, $f_{R_{LA}} \wedge f_{T_{LA}}$ is an SI-LA-ring over U .

Proof. Let $(\mu_1, \nu_1), (\mu_2, \nu_2) \in R_{LA} \times T_{LA}$. Then

$$\begin{aligned} (f_{R_{LA}} \wedge f_{T_{LA}})((\mu_1, \nu_1) - (\mu_2, \nu_2)) &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_1 - \mu_2, \nu_1 - \nu_2) \\ &= f_{R_{LA}}(\mu_1 - \mu_2) \cap f_{T_{LA}}(\nu_1 - \nu_2) \\ &\supseteq (f_{R_{LA}}(\mu_1) \cap f_{R_{LA}}(\mu_2)) \cap (f_{T_{LA}}(\nu_1) \cap f_{T_{LA}}(\nu_2)) \\ &= (f_{R_{LA}}(\mu_1) \cap f_{T_{LA}}(\nu_1)) \cap (f_{R_{LA}}(\mu_2) \cap f_{T_{LA}}(\nu_2)) \\ &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_1, \nu_1) \cap (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_2, \nu_2). \end{aligned}$$

and

$$\begin{aligned} (f_{R_{LA}} \wedge f_{T_{LA}})((\mu_1, \nu_1)(\mu_2, \nu_2)) &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_1\mu_2, \nu_1\nu_2) \\ &= f_{R_{LA}}(\mu_1\mu_2) \cap f_{T_{LA}}(\nu_1\nu_2) \\ &\supseteq (f_{R_{LA}}(\mu_1) \cap f_{R_{LA}}(\mu_2)) \cap (f_{T_{LA}}(\nu_1) \cap f_{T_{LA}}(\nu_2)) \\ &= (f_{R_{LA}}(\mu_1) \cap f_{T_{LA}}(\nu_1)) \cap (f_{R_{LA}}(\mu_2) \cap f_{T_{LA}}(\nu_2)) \\ &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_1, \nu_1) \cap (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_2, \nu_2). \end{aligned}$$

Therefore, $f_{R_{LA}} \wedge f_{T_{LA}}$ is an SI-LA-ring over U . ■

Theorem 4.2.14. Let $f_{R_{LA}}$ and $f_{T_{LA}}$ be two SI-ideals over U . Then, $f_{R_{LA}} \wedge f_{T_{LA}}$ is an SI-ideal over U .

Proof. We have seen in Theorem 4.2.13 that if $f_{R_{LA}}$ and $f_{T_{LA}}$ are SI-LA-rings over U , then so is $(f_{R_{LA}} \wedge f_{T_{LA}})$. Let $(\mu_1, \nu_1), (\mu_2, \nu_2) \in R_{LA} \times T_{LA}$. Then

$$\begin{aligned} (f_{R_{LA}} \wedge f_{T_{LA}})((\mu_1, \nu_1)(\mu_2, \nu_2)) &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_1\mu_2, \nu_1\nu_2) \\ &= f_{R_{LA}}(\mu_1\mu_2) \cap f_{T_{LA}}(\nu_1\nu_2) \\ &\supseteq f_{R_{LA}}(\mu_1) \cap f_{T_{LA}}(\nu_1) \\ &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_1, \nu_1) \end{aligned}$$

and

$$\begin{aligned} (f_{R_{LA}} \wedge f_{T_{LA}})((\mu_1, \nu_1)(\mu_2, \nu_2)) &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_1\mu_2, \nu_1\nu_2) \\ &= f_{R_{LA}}(\mu_1\mu_2) \cap f_{T_{LA}}(\nu_1\nu_2) \\ &\supseteq f_{R_{LA}}(\mu_2) \cap f_{T_{LA}}(\nu_2) \\ &= (f_{R_{LA}} \wedge f_{T_{LA}})(\mu_2, \nu_2) \end{aligned}$$

Therefore, $f_{R_{LA}} \wedge f_{T_{LA}}$ is an SI-ideal over U . ■

Definition 4.2.15. Let $f_{R_{LA}}, g_{T_{LA}}$ be SI-LA-rings over U . Then, the product of SI-LA-rings $f_{R_{LA}}$ and $g_{T_{LA}}$ is defined as $f_{R_{LA}} \times g_{T_{LA}} = h_{R_{LA} \times T_{LA}}$, where $h_{R_{LA} \times T_{LA}}(\mu, \nu) = f_{R_{LA}}(\mu) \times g_{T_{LA}}(\nu)$ for all $(\mu, \nu) \in R_{LA} \times T_{LA}$.

Theorem 4.2.16. If $f_{R_{LA}}$ and $g_{T_{LA}}$ are SI-LA-rings over U , then so is $f_{R_{LA}} \times g_{T_{LA}}$ over $U \times U$.

Proof. By the Definition 4.2.15, let $f_{R_{LA}} \times g_{T_{LA}} = h_{R_{LA} \times T_{LA}}$, where $h_{R_{LA} \times T_{LA}}(\mu, \nu) = f_{R_{LA}}(\mu) \times g_{T_{LA}}(\nu)$ for all $(\mu, \nu) \in R_{LA} \times T_{LA}$. Then, for all $(\mu_1, \nu_1), (\mu_2, \nu_2) \in R_{LA} \times T_{LA}$,

$$\begin{aligned} h_{R_{LA} \times T_{LA}}((\mu_1, \nu_1) - (\mu_2, \nu_2)) &= h_{R_{LA} \times T_{LA}}(\mu_1 - \mu_2, \nu_1 - \nu_2) \\ &= f_{R_{LA}}(\mu_1 - \mu_2) \cap g_{T_{LA}}(\nu_1 - \nu_2) \\ &\supseteq (f_{R_{LA}}(\mu_1) \cap f_{R_{LA}}(\mu_2)) \times (g_{T_{LA}}(\nu_1) \cap g_{T_{LA}}(\nu_2)) \\ &= (f_{R_{LA}}(\mu_1) \times g_{T_{LA}}(\nu_1)) \cap (f_{R_{LA}}(\mu_2) \times g_{T_{LA}}(\nu_2)) \\ &= h_{R_{LA} \times T_{LA}}(\mu_1, \nu_1) \cap h_{R_{LA} \times T_{LA}}(\mu_2, \nu_2). \end{aligned}$$

and

$$\begin{aligned}
h_{R_{LA} \times T_{LA}}((\mu_1, \nu_1)(\mu_2, \nu_2)) &= h_{R_{LA} \times T_{LA}}(\mu_1 \mu_2, \nu_1 \nu_2) \\
&= f_{R_{LA}}(\mu_1 \mu_2) \cap g_{T_{LA}}(\nu_1 \nu_2) \\
&\supseteq (f_{R_{LA}}(\mu_1) \cap f_{R_{LA}}(\mu_2)) \times (g_{T_{LA}}(\nu_1) \cap g_{T_{LA}}(\nu_2)) \\
&= (f_{R_{LA}}(\mu_1) \times g_{T_{LA}}(\nu_1)) \cap (f_{R_{LA}}(\mu_2) \times g_{T_{LA}}(\nu_2)) \\
&= h_{R_{LA} \times T_{LA}}(\mu_1, \nu_1) \cap h_{R_{LA} \times T_{LA}}(\mu_2, \nu_2).
\end{aligned}$$

Hence, $f_{R_{LA}} \times g_{T_{LA}} = h_{R_{LA} \times T_{LA}}$ is an SI-LA-ring over $U \times U$. ■

Definition 4.2.17. Let $f_{R_{LA}}$ be an SI-ideal of an LA-ring R_{LA} and $g_{T_{LA}}$ be SI-ideal of an LA-ring T_{LA} over U . Then, the product of SI-ideals $f_{R_{LA}}$ and $g_{T_{LA}}$ is defined as $f_{R_{LA}} \times g_{T_{LA}} = h_{R_{LA} \times T_{LA}}$, where $h_{R_{LA} \times T_{LA}}(\mu, \nu) = f_{R_{LA}}(\mu) \times g_{T_{LA}}(\nu)$ for all $(\mu, \nu) \in R_{LA} \times T_{LA}$.

Theorem 4.2.18. If $f_{R_{LA}}$ is an SI-ideal of an LA-ring R_{LA} and $g_{T_{LA}}$ is an SI-ideal of an LA-ring T_{LA} over U , then $f_{R_{LA}} \times g_{T_{LA}}$ is an SI-ideal of $R_{LA} \times T_{LA}$ over $U \times U$.

Proof. In the Theorem 4.2.16, we have shown that if $f_{R_{LA}}$ and $g_{T_{LA}}$ are SI-LA-rings over $U \times U$. Let $(\mu_1, \nu_1), (\mu_2, \nu_2) \in R_{LA} \times T_{LA}$,

$$\begin{aligned}
h_{R_{LA} \times T_{LA}}((\mu_1, \nu_1)(\mu_2, \nu_2)) &= h_{R_{LA} \times T_{LA}}(\mu_1 \mu_2, \nu_1 \nu_2) \\
&= f_{R_{LA}}(\mu_1 \mu_2) \cap g_{T_{LA}}(\nu_1 \nu_2) \\
&\supseteq f_{R_{LA}}(\mu_1) \times g_{T_{LA}}(\nu_1) \\
&= f_{R_{LA}}(\mu_1) \times g_{T_{LA}}(\nu_1) \\
&= h_{R_{LA} \times T_{LA}}(\mu_1, \nu_1).
\end{aligned}$$

and

$$\begin{aligned}
h_{R_{LA} \times T_{LA}}((\mu_1, \nu_1)(\mu_2, \nu_2)) &= h_{R_{LA} \times T_{LA}}(\mu_1 \mu_2, \nu_1 \nu_2) \\
&= f_{R_{LA}}(\mu_1 \mu_2) \cap g_{T_{LA}}(\nu_1 \nu_2) \\
&\supseteq f_{R_{LA}}(\mu_2) \times g_{T_{LA}}(\nu_2) \\
&= f_{R_{LA}}(\mu_2) \times g_{T_{LA}}(\nu_2) \\
&= h_{R_{LA} \times T_{LA}}(\mu_2, \nu_2).
\end{aligned}$$

Hence, $f_{R_{LA}} \times g_{T_{LA}} = h_{R_{LA} \times T_{LA}}$ is an SI-ideal of $R_{LA} \times T_{LA}$ over $U \times U$. ■

Theorem 4.2.19. Let $f_{R_{LA}}$ and $g_{R_{LA}}$ be two SI-LA-rings over U . Then, $f_{R_{LA}}\tilde{\cap}g_{R_{LA}}$ is an SI-LA-ring over U .

Proof. Let $\mu, \nu \in R_{LA}$. Then,

$$\begin{aligned} (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\mu - \nu) &= f_{R_{LA}}(\mu - \nu) \cap g_{R_{LA}}(\mu - \nu) \\ &\supseteq (f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)) \cap (g_{R_{LA}}(\mu) \cap g_{R_{LA}}(\nu)) \\ &= (f_{R_{LA}}(\mu) \cap g_{R_{LA}}(\mu)) \cap (f_{R_{LA}}(\nu) \cap g_{R_{LA}}(\nu)) \\ &= (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\mu) \cap (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\nu). \end{aligned}$$

and

$$\begin{aligned} (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\mu\nu) &= f_{R_{LA}}(\mu\nu) \cap g_{R_{LA}}(\mu\nu) \\ &\supseteq (f_{R_{LA}}(\mu) \cap f_{R_{LA}}(\nu)) \cap (g_{R_{LA}}(\mu) \cap g_{R_{LA}}(\nu)) \\ &= (f_{R_{LA}}(\mu) \cap g_{R_{LA}}(\mu)) \cap (f_{R_{LA}}(\nu) \cap g_{R_{LA}}(\nu)) \\ &= (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\mu) \cap (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\nu). \end{aligned}$$

Therefore, $f_{R_{LA}}\tilde{\cap}g_{R_{LA}}$ is an SI-LA-ring over U . ■

Theorem 4.2.20. Let $f_{R_{LA}}$ and $g_{R_{LA}}$ be two SI-ideals over U . Then, $f_{R_{LA}}\tilde{\cap}g_{R_{LA}}$ is an SI-ideal over U .

Proof. We have seen in Theorem 4.2.19 that if $f_{R_{LA}}$ and $g_{R_{LA}}$ are SI-LA-rings over U , then so is $f_{R_{LA}}\tilde{\cap}g_{R_{LA}}$. Let $\mu, \nu \in R_{LA}$. Then

$$\begin{aligned} (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\mu\nu) &= f_{R_{LA}}(\mu\nu) \cap g_{R_{LA}}(\mu\nu) \\ &\supseteq f_{R_{LA}}(\mu) \cap g_{R_{LA}}(\mu) \\ &= (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\mu). \end{aligned}$$

and

$$\begin{aligned} (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\mu\nu) &= f_{R_{LA}}(\mu\nu) \cap g_{R_{LA}}(\mu\nu) \\ &\supseteq f_{R_{LA}}(\nu) \cap g_{R_{LA}}(\nu) \\ &= (f_{R_{LA}}\tilde{\cap}g_{R_{LA}})(\nu). \end{aligned}$$

Therefore, $f_{R_{LA}}\tilde{\cap}g_{R_{LA}}$ is an SI-ideal over U . ■

The following example shows that if $f_{R_{LA}}$ and $g_{R_{LA}}$ are two SI-LA-rings(SI-ideals) over U then, $f_{R_{LA}} \tilde{\cup} g_{R_{LA}}$ need not be an SI-LA-ring (SI-ideal) over U .

Example 4.2.21. Assume that the universal set

$$U = S_3 = \{1, (12), (13), (23), (123), (132)\}.$$

Let $R_{LA} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ be the LA-ring from Example 3.1.2. We define an SI-LA-ring (SI-ideal) $f_{R_{LA}}$ over $U = S_3$ by

$$f_{R_{LA}}(0) = f_{R_{LA}}(3) = f_{R_{LA}}(4) = f_{R_{LA}}(7) = \{1, (12), (13), (123)\}$$

$$f_{R_{LA}}(1) = f_{R_{LA}}(2) = \{1, (12), (123)\}$$

$$f_{R_{LA}}(5) = f_{R_{LA}}(6) = \{1, (123)\}$$

and another SI-LA-ring (SI-ideal) $g_{R_{LA}}$ over $U = S_3$ by

$$g_{R_{LA}}(0) = g_{R_{LA}}(3) = g_{R_{LA}}(4) = g_{R_{LA}}(7) = \{1, (12), (23), (132)\}$$

$$g_{R_{LA}}(1) = g_{R_{LA}}(2) = \{1, (23), (132)\}$$

$$g_{R_{LA}}(5) = g_{R_{LA}}(6) = \{1, (132)\}.$$

Then, $f_{R_{LA}} \tilde{\cup} g_{R_{LA}}$ is not an SI-LA-ring (SI-ideal) over $U = S_3$.

Definition 4.2.22. Let R_{LA} be an LA-ring and T_{LA} be a sub LA-ring of R_{LA} . Let $f_{R_{LA}}$ be an SI-LA-ring over U and $f_{T_{LA}}$ be a non-empty soft subset of $f_{R_{LA}}$ over U . If $f_{T_{LA}}$ is itself an SI-LA-ring over U , then $f_{T_{LA}}$ is said to be a SI-sub LA-ring of $f_{R_{LA}}$ over U .

Theorem 4.2.23. Let $f_{R_{LA}}$ be an SI-LA-ring over U , and $f_{T_{LA}}, f_{L_{LA}}$ be two SI-sub LA-rings of $f_{R_{LA}}$ over U . Then, $f_{T_{LA}} \tilde{\cap} f_{L_{LA}}$ is a soft int-sub LA-ring of $f_{R_{LA}}$ over U .

Proof. Let $\mu, \nu \in R_{LA}$. Then,

$$\begin{aligned} (f_{T_{LA}} \tilde{\cap} f_{L_{LA}})(\mu - \nu) &= f_{T_{LA}}(\mu - \nu) \cap f_{L_{LA}}(\mu - \nu) \\ &\supseteq (f_{T_{LA}}(\mu) \cap f_{T_{LA}}(\nu)) \cap (f_{L_{LA}}(\mu) \cap f_{L_{LA}}(\nu)) \\ &= (f_{T_{LA}}(\mu) \cap f_{L_{LA}}(\mu)) \cap (f_{T_{LA}}(\nu) \cap f_{L_{LA}}(\nu)) \\ &= (f_{T_{LA}} \tilde{\cap} f_{L_{LA}})(\mu) \cap (f_{T_{LA}} \tilde{\cap} f_{L_{LA}})(\nu). \end{aligned}$$

and

$$\begin{aligned} (f_{T_{LA}} \tilde{\cap} f_{L_{LA}})(\mu\nu) &= f_{T_{LA}}(\mu\nu) \cap f_{L_{LA}}(\mu\nu) \\ &\supseteq (f_{T_{LA}}(\mu) \cap f_{T_{LA}}(\nu)) \cap (f_{L_{LA}}(\mu) \cap f_{L_{LA}}(\nu)) \\ &= (f_{T_{LA}}(\mu) \cap f_{L_{LA}}(\mu)) \cap (f_{T_{LA}}(\nu) \cap f_{L_{LA}}(\nu)) \\ &= (f_{T_{LA}} \tilde{\cap} f_{L_{LA}})(\mu) \cap (f_{T_{LA}} \tilde{\cap} f_{L_{LA}})(\nu). \end{aligned}$$

Therefore, $f_{T_{LA}} \tilde{\cap} f_{L_{LA}}$ is an SI-LA-ring over U . ■

4.2.3 Construction of SI-special LA-rings and SI-ideals

In this section we study the construction of soft int-special LA-ring and soft int-ideals using the SI-rings [32], SI-LA-semigroups [118] and their soft int-ideals.

Following is the construction of an SI-special LA-ring using an SI-ring.

Proposition 4.2.24. If f_R is a soft int-ring of a commutative and associative ring R then $h_{R[L]}$ is a soft int-special LA-ring of $R[L]$, where for $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$h_{R[L]}(\varphi) = \cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho}). \quad (4.2.1)$$

Proof. Let φ and $\psi \in R[L]$ then $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ and $\psi = \sum_{\varrho \in L} \nu_{\varrho} \varrho$ where $\mu_{\varrho}, \nu_{\varrho} \in R$ for all $\varrho \in L$.

$$\begin{aligned} h_{R[L]}(\varphi - \psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho - \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{\varrho \in L} (\mu_{\varrho} - \nu_{\varrho}) \varrho) \\ &= \cap_{\varrho \in \text{Supp}(\varphi - \psi)} f_R(\mu_{\varrho} - \nu_{\varrho}) \\ &\supseteq \cap_{\varrho \in \text{Supp}(\varphi - \psi)} [f_R(\mu_{\varrho}) \cap f_R(\nu_{\varrho})] \\ &= [\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\psi)} f_R(\nu_{\varrho})] \\ &= h_{R[L]}(\varphi) \cap h_{R[L]}(\psi). \end{aligned}$$

$$\begin{aligned} h_{R[L]}(\varphi \psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{u \in L} c_u u) \text{ (where } c_u = \sum_{\varrho h = u} \mu_{\varrho} \nu_h) \\ &= \cap_{u \in \text{Supp}(\varphi \psi)} f_R(c_u) \\ &= \cap_{u \in \text{Supp}(\varphi \psi)} f_R(\sum_{\varrho h = u} \mu_{\varrho} \nu_h) \\ &\supseteq \cap_{u \in \text{Supp}(\varphi \psi)} [\cap_{u = \varrho h} f_R(\mu_{\varrho} \nu_h)] \\ &\supseteq \cap_{u \in \text{Supp}(\varphi \psi)} [\cap_{u = \varrho h} (f_R(\mu_{\varrho}) \cap f_R(\nu_h))] \\ &= \cap_{u \in \text{Supp}(\varphi \psi)} [(\cap_{u = \varrho h} f_R(\mu_{\varrho})) \cap (\cap_{u = \varrho h} f_R(\nu_h))] \\ &\supseteq [\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\psi)} f_R(\nu_{\varrho})] \\ &= h_{R[L]}(\varphi) \cap h_{R[L]}(\psi). \end{aligned}$$

■

The next proposition gives an application of an SI-LA-semigroup to construct an SI-special LA-ring.

Proposition 4.2.25. If g_L is a soft int-LA-semigroup of an LA-semigroup L then $h_{R[L]}$ is a soft int special LA-ring of $R[L]$, where for $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$h_{R[L]}(\varphi) = \bigcap_{\varrho \in \text{supp}(\varphi)} g_L(\varrho). \quad (4.2.2)$$

Proof. Let φ and $\psi \in R[L]$ then $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ and $\psi = \sum_{\varrho \in L} \nu_{\varrho} \varrho$ where $\mu_{\varrho}, \nu_{\varrho} \in R$ for all $\varrho \in L$.

$$\begin{aligned} h_{R[L]}(\varphi - \psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho - \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{\varrho \in L} (\mu_{\varrho} - \nu_{\varrho}) \varrho) \\ &= \bigcap_{\varrho \in \text{Supp}(\varphi - \psi)} g_L(\varrho) \\ &= \bigcap_{\varrho \in \text{Supp}(\varphi - \psi)} g_L(\varrho) \\ &\supseteq [\bigcap_{\varrho \in \text{Supp}(\varphi)} g_L(\varrho)] \cap [\bigcap_{\varrho \in \text{Supp}(\psi)} g_L(\varrho)] \\ &= h_{R[L]}(\varphi) \cap h_{R[L]}(\psi). \end{aligned}$$

$$\begin{aligned} h_{R[L]}(\varphi \psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{u \in L} c_u u) \text{ (where } c_u = \sum_{\varrho h = u} \mu_{\varrho} \nu_h) \\ &= \bigcap_{u \in \text{Supp}(\varphi \psi)} g_L(u) \\ &= \bigcap_{u = \varrho h \in \text{Supp}(\varphi \psi)} g_L(\varrho h) \\ &\supseteq \bigcap_{\varrho \in \text{Supp}(\varphi) h \in \text{supp}(\psi)} [g_L(\varrho) \cap g_L(h)] \\ &\supseteq \bigcap_{\varrho \in \text{Supp}(\varphi) \cup \text{supp}(\psi)} [g_L(\varrho) \cap g_L(\varrho)] \\ &= \bigcap_{\varrho \in \text{Supp}(\varphi) \cup \text{supp}(\psi)} [g_L(\varrho)] \\ &\supseteq [\bigcap_{\varrho \in \text{Supp}(\varphi)} g_L(\varrho)] \cap [\bigcap_{\varrho \in \text{Supp}(\psi)} g_L(\varrho)] \\ &= h_{R[L]}(\varphi) \cap h_{R[L]}(\psi). \end{aligned}$$

■

The succeeding proposition gives a soft int special LA-ring which is a combination of a soft int ring and a soft int LA-semigroup.

Proposition 4.2.26. If f_R is an SI-ring of a commutative and associative ring R and g_L is an SI-LA-semigroup of an LA-semigroup L then $h_{R[L]}$ is an SI-special LA-ring of $R[L]$, where for $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$h_{R[L]}(\varphi) = (\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})) \cap (\cap_{\varrho \in \text{supp}(\varphi)} g_L(\varrho)). \quad (4.2.3)$$

Proof. Let φ and $\psi \in R[L]$ then $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho$ and $\psi = \sum_{\varrho \in L} \nu_{\varrho} \varrho$ where $\mu_{\varrho}, \nu_{\varrho} \in R$ for all $\varrho \in L$.

$$\begin{aligned} h_{R[L]}(\varphi - \psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho - \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{\varrho \in L} (\mu_{\varrho} - \nu_{\varrho}) \varrho) \\ &= [\cap_{\varrho \in \text{Supp}(\varphi - \psi)} f_R(\mu_{\varrho} - \nu_{\varrho})] \cap [\cap_{\varrho \in \text{supp}(\varphi - \psi)} g_L(\varrho)] \\ &\supseteq [\cap_{\varrho \in \text{Supp}(\varphi - \psi)} f_R(\mu_{\varrho}) \cap f_R(\nu_{\varrho})] \cap [\cap_{\varrho \in \text{supp}(\varphi - \psi)} g_L(\varrho)] \\ &\supseteq [[\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\psi)} f_R(\nu_{\varrho})]] \cap [[\cap_{\varrho \in \text{Supp}(\varphi)} g_L(\varrho)] \cap [\cap_{\varrho \in \text{Supp}(\psi)} g_L(\varrho)]] \\ &= [[\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\varphi)} g_L(\varrho)]] \cap [[\cap_{\varrho \in \text{Supp}(\psi)} f_R(\nu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\psi)} g_L(\varrho)]] \\ &= h_{R[L]}(\varphi) \cap h_{R[L]}(\psi). \end{aligned}$$

$$\begin{aligned} h_{R[L]}(\varphi \psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{\varrho \in L} c_u u) \text{ (where } c_u = \sum_{\varrho h = u} \mu_{\varrho} \nu_h \text{)} \\ &= [\cap_{u \in \text{Supp}(\varphi \psi)} f_R(c_u)] \cap [\cap_{u \in \text{Supp}(\varphi \psi)} g_L(u)] \\ &= [\cap_{u \in \text{Supp}(\varphi \psi)} f_R(\sum_{\varrho h = u} \mu_{\varrho} \nu_h)] \cap [\cap_{u = \varrho h \in \text{Supp}(\varphi \psi)} g_L(\varrho h)] \\ &\supseteq [\cap_{u \in \text{Supp}(\varphi \psi)} [\cap_{u = \varrho h} f_R(\mu_{\varrho} \nu_h)]] \cap \cap_{\varrho \in \text{Supp}(\varphi) h \in \text{supp}(\psi)} [g_L(\varrho) \cap g_L(h)] \\ &\supseteq [\cap_{u \in \text{Supp}(\varphi \psi)} [\cap_{u = \varrho h} (f_R(\mu_{\varrho}) \cap f_R(\nu_h))]] \cap \cap_{\varrho \in \text{Supp}(\varphi) \cup \text{supp}(\psi)} [g_L(\varrho) \cap g_L(\varrho)] \\ &= [\cap_{u \in \text{Supp}(\varphi \psi)} [(\cap_{u = \varrho h} f_R(\mu_{\varrho})) \cap (\cap_{u = \varrho h} f_R(\nu_h))]] \cap \cap_{\varrho \in \text{Supp}(\varphi) \cup \text{supp}(\psi)} [g_L(\varrho)] \\ &\supseteq [\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\psi)} f_R(\nu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\varphi)} g_L(\varrho)] \cap [\cap_{\varrho \in \text{Supp}(\psi)} g_L(\varrho)] \\ &= [[\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\varphi)} g_L(\varrho)]] \cap [[\cap_{\varrho \in \text{Supp}(\psi)} f_R(\nu_{\varrho})] \cap [\cap_{\varrho \in \text{Supp}(\psi)} g_L(\varrho)]] \\ &= h_{R[L]}(\varphi) \cap h_{R[L]}(\psi). \end{aligned}$$

■

Now we establish construction of an SI-ideal.

Proposition 4.2.27. If f_R is an SI-left(right) ideal of a commutative and associative ring R then $h_{R[L]}$ is an SI-left(right) ideal of $R[L]$, where for $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$h_{R[L]}(\varphi) = \bigcap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho}). \quad (4.2.4)$$

Proof. By Proposition 4.2.24 $h_{R[L]}$ is a soft int-special LA-ring of $R[L]$ over U .

$$\begin{aligned} h_{R[L]}(\varphi\psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{\varrho \in L} c_u u) \text{ (where } c_u = \sum_{\varrho h = u} \mu_{\varrho} \nu_h) \\ &= \bigcap_{u \in \text{Supp}(\varphi\psi)} f_R(c_u) \\ &= \bigcap_{u \in \text{Supp}(\varphi\psi)} f_R(\sum_{\varrho h = u} \mu_{\varrho} \nu_h) \\ &\supseteq \bigcap_{u \in \text{Supp}(\varphi\psi)} [\bigcap_{u = \varrho h} f_R(\mu_{\varrho} \nu_h)] \\ &\supseteq \bigcap_{u \in \text{Supp}(\varphi\psi)} [\bigcap_{u = \varrho h} f_R(\nu_h)] \\ &= \bigcap_{\varrho \in \text{supp}(\psi)} f_R(\nu_{\varrho}) \\ &= h_{R[L]}(\psi) \end{aligned}$$

■

Proposition 4.2.28. If p_L is an SI-left(right) ideal of an LA-semigroup L then $h_{R[L]}$ is an SI-left(right) ideal of $R[L]$, where for $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$h_{R[L]}(\varphi) = \bigcap_{\varrho \in \text{supp}(\varphi)} g_L(\varrho). \quad (4.2.5)$$

Proof. By Proposition 4.2.25 $h_{R[L]}$ is an SI-special LA-ring of $R[L]$ over U .

$$\begin{aligned} h_{R[L]}(\varphi\psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\varrho \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{\varrho \in L} c_u u) \text{ (where } c_u = \sum_{\varrho h = u} \mu_{\varrho} \nu_h) \\ &= \bigcap_{u \in \text{Supp}(\varphi\psi)} g_L(u) \\ &= \bigcap_{u = \varrho h \in \text{Supp}(\varphi\psi)} g_L(\varrho h) \\ &\supseteq \bigcap_{u = \varrho h \in \text{Supp}(\varphi\psi)} g_L(h) \\ &= \bigcap_{\varrho \in \text{supp}(\psi)} g_L(\varrho) \\ &= h_{R[L]}(\psi) \end{aligned}$$

■

Proposition 4.2.29. If f_R is an SI-left(right) ideal of a commutative and associative ring R and g_L is an SI-left(right) ideal of an LA-semigroup L then $h_{R[L]}$ is an SI-left(right) ideal of $R[L]$, where for $\varphi = \sum_{\varrho \in L} \mu_{\varrho} \varrho \in R[L]$,

$$h_{R[L]}(\varphi) = (\cap_{\varrho \in \text{Supp}(\varphi)} f_R(\mu_{\varrho})) \cap (\cap_{\varrho \in \text{supp}(\varphi)} g_L(\varrho)). \quad (4.2.6)$$

Proof. By Proposition 4.2.26, $h_{R[L]}$ is an SI-special LA-ring of $R[L]$ over U .

$$\begin{aligned} h_{R[L]}(\varphi\psi) &= h_{R[L]}(\sum_{\varrho \in L} \mu_{\varrho} \varrho \sum_{\nu \in L} \nu_{\varrho} \varrho) \\ &= h_{R[L]}(\sum_{\varrho \in L} c_u u) \text{ (where } c_u = \sum_{\varrho h = u} \mu_{\varrho} \nu_h) \\ &= [\cap_{u \in \text{Supp}(\varphi\psi)} f_R(c_u)] \cap [\cap_{u \in \text{Supp}(\varphi\psi)} g_L(u)] \\ &= [\cap_{u \in \text{Supp}(\varphi\psi)} f_R(\sum_{\varrho h = u} \mu_{\varrho} \nu_h)] \cap [\cap_{u = \varrho h \in \text{Supp}(\varphi\psi)} g_L(\varrho h)] \\ &\supseteq [\cap_{u \in \text{Supp}(\varphi\psi)} [\cap_{u = \varrho h} f_R(\mu_{\varrho} \nu_h)]] \cap [\cap_{u = \varrho h \in \text{Supp}(\varphi\psi)} g_L(\varrho h)] \\ &\supseteq [\cap_{u \in \text{Supp}(\varphi\psi)} [\cap_{u = \varrho h} f_R(\nu_{\varrho})]] \cap [\cap_{u = \varrho h \in \text{Supp}(\varphi\psi)} g_L(h)] \\ &= [\cap_{\varrho \in \text{supp}(\psi)} f_R(\nu_{\varrho})] \cap [\cap_{\varrho \in \text{supp}(\psi)} g_L(\varrho)] \\ &= h_{R[L]}(\psi) \end{aligned}$$

■

Every SI-soft int-left(right) ideal is an SI-special LA-ring but the converse is not true. In the following we have an example of a SI-special LA-ring that is neither an SI-left nor an SI-right ideal.

Example 4.2.30. Consider the following LA-semigroup ring $L = \{x, y, z\}$, such that (L, \cdot) is an LA-semigroup such that:

\cdot	x	y	z
x	x	x	x
y	x	x	z
z	x	y	x

with $R = \mathbb{Z}_2 = \{0, 1\}$ $R[L] = \{0, x, y, z, x+y, x+z, y+z, x+y+z\}$ is an LA-semigroup ring with additive and multiplicative tables as:

+	0	x	y	z	x+y	x+z	y+z	x+y+z
0	0	x	y	z	x+y	x+z	y+z	x+y+z
x	x	0	x+y	x+z	y	z	x+y+z	y+z
y	y	x+y	0	y+z	x	x+y+z	z	x+z
z	z	x+z	y+z	0	x+y+z	x	y	x+y
x+y	x+y	y	x	x+y+z	0	y+z	x+z	z
x+z	x+z	z	x+y+z	x	y+z	0	x+y	y
y+z	y+z	x+y+z	z	y	x+z	x+y	0	x
x+y+z	x+y+z	y+z	x+z	x+y	z	y	x	0

and

·	0	x	y	z	x+y	x+z	y+z	x+y+z
0	0	0	0	0	0	0	0	0
x	0	x	x	x	0	0	0	x
y	0	x	x	z	0	x+z	x+z	z
z	0	x	y	x	x+y	0	x+y	y
x+y	0	0	0	x+z	0	x+z	x+z	x+z
x+z	0	0	x+y	0	x+y	0	x+y	x+y
y+z	0	0	x+y	x+z	x+y	x+z	y+z	y+z
x+y+z	0	x	y	z	x+y	x+z	y+z	x+y+z

Now assume that $U = L_3 = \{1, (12), (13), (23), (123), (132)\}$ is the universe set. It is easy to check that $f_{R[L]}$ is a soft int-special LA-ring over $U = L_3$ where

$$f_{R[L]}(0) = L_3$$

$$f_{R[L]}(x) = \{1, (123)\}$$

$$f_{R[L]}(y) = \{1\}$$

$$f_{R[L]}(z) = \{1\}$$

$$f_{R[L]}(x + y) = \{1, (12)\}$$

$$f_{R[L]}(x + z) = \{1, (13)\}$$

$$f_{R[L]}(y + z) = \{1, (23)\}$$

$$f_{R[L]}(x + y + z) = \{1, (132)\}.$$

$f_{R[L]}$ is neither an SI-left nor an SI-right ideal as,

$$f_{R[L]}((x + y)(y + z)) \not\subseteq f_{R[L]}(x + y) \text{ and } f_{R[L]}((x + y)(y + z)) \not\subseteq f_{R[L]}(y + z).$$

Chapter 5

Applications to Coding Theory

DNA computations over associative and commutative rings and fields have attracted many researchers for more than two decades. DNA codes are commonly constructed over a four letter alphabet. In this chapter, we change the trend by introducing DNA codes over a non-commutative and non-associative four-element structure; a special LA-field F_{SLA4} . Linear cyclic codes are established over a special LA-field. In particular, the reversible complement cyclic codes over F_{SLA4} with odd lengths are considered. This is an important class of codes for DNA computing, as these codes satisfy the Hamming constraint and the reversible complement constraint. We establish an algorithm to construct these codes and obtain required codes of lengths 5, 7, 9 and 11. The motivation behind the construction of such codes is taken from an article "Construction of Cyclic Codes over $GF(4)$ for DNA Computing," published in Journal of Franklin Institute, 2006. In this article, T. Abualrub et al. [1] constructed the reversible complement cyclic codes over $GF(4)$ with odd lengths.

5.1 Special LA-Vector Space

Shah and Rehman defined an LA-module in [131]. Similarly, a special LA-vector space can be defined as:

Definition 5.1.1. Let $(F_{SLA}, +, \cdot)$ be a special LA-field with left identity 'e'. An abelian group $(V, +)$ is called a special LA-vector space over F_{SLA} , if the map $F_{SLA} \times V \rightarrow V$, defined as $(a, v) \mapsto av \in V$ (where $a \in F_{SLA}$ and $v \in V$), satisfies:

1. $a(v_1 + v_2) = av_1 + av_2$

2. $(a_1 + a_2)v = a_1v + a_2v$
3. $a_1(a_2v) = a_2(a_1v)$
4. $e.v = v$, for each $a, a_1, a_2 \in F_{SLA}$ and $v, v_1, v_2 \in V$.

We call the elements of a special LA-vector space as special LA-vectors or simply vectors.

- Example 5.1.2.**
1. Every special LA-field F_{SLA} is a special LA-vector space over it self.
 2. Let F_{SLA} be a special LA-field then it is not hard to show that for a positive integer n , $F_{SLA}^n = \{(a_1, a_2, \dots, a_n) : \text{all } a_i \in F_{SLA}\}$ is a special LA-vector space over F_{SLA} . Here the operations are defined component wise.
 3. Let F_{SLA} be a special LA-field and X be a non-empty set then the set $Map(X, F_{SLA}) = \{f : X \rightarrow F_{SLA}\}$ is a special LA-vector space over F_{SLA} .
 4. Let V be the set of all polynomials over a special LA-field F_{SLA} . Then V is a special LA-vector space over F_{SLA} .

Definition 5.1.3. An additive subgroup S of a special LA-vector space V over a special LA-field F_{SLA} is called a special LA-subspace over F_{SLA} , if $F_{SLA}S \subseteq S$, i.e., $as \in S$ for all $a \in F_{SLA}$ and $s \in S$.

The notions of basis and dimension for a special LA-vector space are defined in a way that is similar to that for an ordinary vector space.

5.2 Linear Cyclic Codes over a Special LA-field for DNA Computations

Since, the purpose of our study is to develop cyclic DNA codes over a special LA-field, we first establish some theory for the linear and cyclic codes over special LA-fields.

A code over a special LA-field is a subset of the special LA-vector space F_{SLA}^n . Linear codes over associative fields have many interesting algebraic properties. For the first time, we are defining a linear code over a special LA-field, taking the alphabet of symbol to be a finite special LA-field F_{SLA} .

Definition 5.2.1. Let F_{SLA} be a finite special LA-field and n a positive integer. A special LA-subspace C of the special LA-vector space $V = F_{SLA}^n$ is said to be a linear code over F_{SLA} . If the dimension of C as a special LA-subspace is k , then we say that, C is an $[n, k]$ -code. Moreover, if the code C has minimum hamming distance d , it is called an $[n, k, d]$ -code.

Example 5.2.2. Consider the special LA-field $F_{SLA4} = \{0, 1, 2, 3\}$.

$C_1 = \{000, 120, 230, 310\}$ is a linear $[3, 1, 2]$ -code over F_{SLA4} . But the code $C_2 = \{000, 102, 223\}$ over F_{SLA4} is not linear because $102 + 223 = 321$, but 321 is not a code-word.

A linear code $C \subset F_{SLA}^n$ is called a cyclic code if it is invariant under the mapping $\sigma : F_{SLA}^n \rightarrow F_{SLA}^n$ given by

$$\sigma(\xi_1, \xi_2, \dots, \xi_n) = (\xi_n, \xi_1, \dots, \xi_{n-1}). \quad (5.2.1)$$

σ is called as a cyclic shift. For instance, On the special LA-field F_{SLA4} ,

$C_3 = \{000, 111, 222, 333\}$ and $C_4 = \{000, 123, 231, 312\}$ are cyclic $[3, 1, 3]$ -codes and the linear code C_1 of Example 5.2.2 is not cyclic.

The set

$$F_{SLA}[t]_n = \{a_0 + a_1t + \dots + a_{n-1}t^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F_{SLA}\} \quad (5.2.2)$$

is clearly a special LA-vector space over F_{SLA} with dimension n . As $a \mapsto a(t)$ is an LA-ring isomorphism between the special LA-vector spaces F_{SLA}^n and $F_{SLA}[t]_n$, henceforth we can identify F_{SLA}^n with $F_{SLA}[t]_n$. Thus, corresponding to each codeword $\xi = (\xi_0, \dots, \xi_{n-1})$ we have a polynomial $\xi(t) = \xi_0 + \xi_1t + \dots + \xi_{n-1}t^{n-1}$.

In Section 3.5.3, we established that the set $F_{SLA}[t]$ of all finitely non-zero functions from the set of non-negative integers into a special LA-ring is also a special LA-ring and is called the special LA-ring of Polynomials over F_{SLA} . For any polynomial $\eta(t) \in F_{SLA}[t]$, we can construct the special LA-ring $F_{SLA}[t]/\langle \eta(t) \rangle$ where, $\langle \eta(t) \rangle$ denotes the principal left ideal generated by $\eta(t)$. If $\eta(t)$ has degree n , then $F_{SLA}[t]/\langle \eta(t) \rangle$ can be identified with $F_{SLA}[t]_n$. The multiplication in the special LA-ring $F_{SLA}[t]_n$ is modulo $\eta(t)$.

In particular taking $\eta(t) = t^n - 1$, the quotient special LA-ring $F_{SLA}[t]/(t^n - 1)$ is identified with $F_{SLA}[t]_n$ such that $t^n - 1 = 0$. Thus $F_{SLA}[t]_n$ is turned into a special LA-

ring with relation that $t^n - 1 = 0$. $F_{SLA}[t]_n$ is a special LA-ring as well as a special LA-vector space over F_{SLA} and hence it is a special LA-algebra over F_{SLA} . Let $C \subset F_{SLA}^n$ be a linear code. Since we identify every codeword $\xi = (\xi_0, \dots, \xi_{n-1})$ to a polynomial $\xi(t) \in F_{SLA}[t]_n$, so $C \subset F_{SLA}[t]_n$. The elements of C are now referred to as codewords or code polynomials.

Theorem 5.2.3. Let C be a linear code over F_{SLA} . Then C is cyclic if and only if $t\xi(t) \in C$ for every $\xi(t) \in C$. Where multiplication is performed modulo $(t^n - 1)$.

Proof. In the special LA-ring $F_{SLA}[t]$, where the operation of multiplication is performed in the usual manner,

$$t\xi(t) = t(\xi_0 + \xi_1 t + \dots + \xi_{n-1} t^{n-1}) = \xi_0 t + \xi_1 t^2 + \dots + \xi_{n-1} t^n. \quad (5.2.3)$$

In the special LA-ring $F_{SLA}[t]_n$, where the operation of multiplication is performed modulo $(t^n - 1)$,

$$t\xi(t) = \xi_{n-1} + \xi_0 t + \xi_1 t^2 + \dots + \xi_{n-2} t^{n-1} \in C \quad (5.2.4)$$

■

Thus, it is clear that multiplication by t in the special LA-ring $F_{SLA}[t]_n$ corresponds to cyclic shift σ in F_{SLA}^n .

Following theorem asserts that unlike associative fields and commutative rings, a cyclic code over a special LA-field is a left ideal.

Theorem 5.2.4. Let C be a subset of $F_{SLA}[t]_n$, C is a cyclic code if and only if C is a left ideal of the special LA-ring $F_{SLA}[t]_n$.

Proof. As C is a cyclic code, it is a linear code over F_{SLA} . This implies that for all $\xi(t), \vartheta(t) \in C$ and all $\lambda \in F_{SLA}$, $\xi(t) - \vartheta(t) \in C$ and $\lambda\xi(t) \in C$. Since C is cyclic, by Theorem 5.2.3, $t\xi(t) \in C$ for all $\xi(t) \in C$. Hence, $t^2\xi(t) \in C$, and so on. Therefore, for every $\rho(t) = \rho_0 + \rho_1 t + \dots + \rho_{n-1} t^{n-1} \in F_{SLA}[t]_n$,

$$\rho(t)\xi(t) = \rho_0\xi(t) + \rho_1 t\xi(t) + \dots + \rho_{n-1} t^{n-1}\xi(t) \in C. \quad (5.2.5)$$

Thus, C is proved to be a left ideal in the ring $F_{SLA}[t]_n$.

Conversely, suppose C is a left ideal. Let $\xi(t), \vartheta(t) \in C$ and $\lambda \in F_{SLA}$. Then $\xi(t) - \vartheta(t), \lambda\xi(t) \in C$ since $\lambda \in F_{SLA}[t]_n$. Hence C is a linear code. Further $\rho(t)\xi(t) \in C$ for all $\rho(t) \in F_{SLA}[t]_n$. In particular, $t\xi(t) \in C$ and by Theorem 5.2.3, C is a cyclic code. ■

Following is an example of a cyclic code over a special LA-field that is a left ideal but not a two-sided ideal.

Example 5.2.5. Consider the special LA-field F_{SLA4} . The code $\langle 1 + 3t^2 + t^4 \rangle$ over F_{SLA4} is a left ideal of $F_{SLA}[t]_5$ but, it fails to become a right ideal.

Following two propositions are generalizations of the propositions 8.1 and 8.2, [115].

Proposition 5.2.6. Let C be a cyclic code over F_{SLA} . Then, there exists a unique monic polynomial $\varrho(t)$ such that, for each $\xi(t) \in F_{SLA}[t]_n$, $\xi(t) \in C$ if and only if $\varrho(t)$ divides $\xi(t)$ from right.

Proof. According to the requirements on $\varrho(t)$, it must belong to C (as clearly $\varrho(t)$ divides $\varrho(t)$ from right). Also, it is unique as it divides all other monic polynomials in C from right). Consider $\varrho(t)$ to be a non-zero, monic polynomial of smallest degree in C . For every $\alpha(t) \in F_{SLA}[t]$ we have $\alpha(t)\varrho(t) \bmod (t^n - 1) \in C$. Particularly, if $\alpha(t) \in F_{SLA}[t]_n$, then we have $\alpha(t)\varrho(t) \in C$. Hence, all the multiples of $\varrho(t)$ (from left side) by the polynomials in $F_{SLA}[t]_n$ belong to C .

Conversely, consider $\xi(t)$ to be a codeword in C then, using division algorithm (Theorem 3.5.3), $\xi(t) = \alpha(t)\varrho(t) + \rho(t)$ where $\deg \rho < \deg \varrho$. Now, both $\xi(t)$ and $\alpha(t)\varrho(t)$ are in C , because C is a left ideal of $F_{SLA}[t]_n$ and so is $\rho(t) = \xi(t) - \alpha(t)\varrho(t)$. Since $\varrho(t)$ has least degree in C , we have $\rho(t)$ equal to 0 i.e., $\varrho(t)$ divides $\xi(t)$ from right. ■

From the Proposition 5.2.6, we can write a cyclic code C over F_{SLA} as: $C = \{a(t)\varrho(t) : a(t) \in F_{SLA}[t]_n\}$. Hence C is a principal left ideal of $F_{SLA}[t]_n$ generated by $\varrho(t)$, that is $C = \langle \varrho(t) \rangle$. We call $\varrho(t)$, the generator polynomial of C .

Proposition 5.2.7. Let C be a cyclic code over F_{SLA} with generator $\varrho(t)$. Then, $\varrho(t)$ divides $t^n - 1$ from right.

Proof. Using the division algorithm, we can write $t^n - 1 = \vartheta(t)\varrho(t) + r(t)$, where $\deg r < \deg \varrho$. Now, $\rho(t) = -\vartheta(t)\varrho(t) \bmod (t^n - 1)$ and therefore, from Proposition 5.2.6, we have $\rho(t) \in C$. This indicates that $\rho(t) = 0$, as $\varrho(t)$ is the smallest degree codeword in C . ■

The reciprocal of a polynomial $\xi(t) = \xi_0 + \xi_1 t + \dots + \xi_m t^m$ with $\xi_m \neq 0$, is defined as the polynomial $\xi^*(t) = t^m \xi(1/t) = \xi_r + \xi_{r-1} t + \dots + \xi_1 t^{r-1} + \xi_0 t^r$. Clearly $\deg \xi^*(t) \leq \deg \xi(t)$ with equality when $\xi_0 \neq 0$. $\xi(t)$ is said to be self-reciprocal if and only if $\xi(t) = \xi^*(t)$.

5.3 DNA Cyclic Codes over a Special LA-field

DNA comprises of sequences of letters from the alphabet $\{A, C, G, T\}$. A DNA code of length n is defined to be a set of codewords $(\xi_0, \dots, \xi_{n-1})$ where $\xi_i \in \{A, C, G, T\}$. Because of having a one-one correspondence with the DNA alphabet, Z_4 , $GF(4)$ and $F_2 + uF_2$ are the frequently used rings for DNA computations.

In this section, we shall construct codes over $F_{SLA4} = \{0, 1, 2, 3\}$ and would associate them with codes over $\{A, C, G, T\}$. We map A to 0, G to 3, C to 2 and T to 1. The Watson-Crick complement is: $A^c = T$, $T^c = A$, $C^c = G$ and $G^c = C$. The reverse of a codeword $\xi = (\xi_0, \dots, \xi_{n-1})$ is defined to be $\xi^r = (\xi_{n-1}, \xi_{n-2}, \dots, \xi_0)$, the complement of ξ to be $\xi^c = (\xi_0^c, \xi_1^c, \dots, \xi_{n-1}^c)$ and the reverse complement to be $\xi^{rc} = (\xi_{n-1}^c, \xi_{n-2}^c, \dots, \xi_0^c)$.

Definition 5.3.1. Let C be a linear code over a special LA-field of length n . C is said to be

1. a reversible code, if $\xi^r \in C$ for each $\xi \in C$.
2. a complement code, if $\xi^c \in C$ for each $\xi \in C$.

Definition 5.3.2. We call a cyclic code C of length n and minimum distance d over a special LA-field reversible complement if C is reversible and complement.

Example 5.3.3. The DNA cyclic codes of length 3 over F_{SLA4} are:

$$C_1 = \langle TTT \rangle = \{AAA, TTT, CCC, GGG\},$$

$$C_2 = \langle TCG \rangle = \{AAA, TCG, CGT, GTC\},$$

$$C_3 = \langle TGC \rangle = \{AAA, CTG, TGC, GCT\},$$

$$C_4 = \langle ATT \rangle = \{AAA, CAC, TAT, TTA, ATT, GGA, AGG, GAG, CCA, ACC, CGT, GCT, CTG, GTC, TCG, TGC\},$$

$$C_5 = \langle ATC \rangle = \{AAA, ATC, TCA, CAT, GTA, AGT, TAG, ACG, GAC, CGA, CCC, GGG, CTG, GCT, TTT, TGC\},$$

$$C_6 = \langle ATG \rangle = \{AAA, TAC, ACT, CTA, GTC, CGT, TCG, CCC, GGG, TTT, AGC, CAG, GCA, ATG, GAT, TGA\}.$$

C_1, C_5 and C_6 are complement codes. C_1 and C_4 are reversible codes and C_1 is the only reversible complement code.

Now we categorise the family of reversible complement cyclic codes over F_{SLA4} . These codes have great significance as they satisfy the following constraints [1]:

1. **The Hamming constraint:** $H(\xi, \vartheta) \geq d$, where ξ and ϑ are two different codewords in C . The purpose of this constraint is to limit the undesirable hybridization between the Watson Crick complement of a codeword to a different codeword.
2. **The reverse-complement constraint:** $H(\xi^c, \vartheta^r) \geq d$, where ξ and ϑ are any two codewords in C . The purpose of this constraint is to avoid the undesirable hybridization between a codeword and the reverse of another codeword.

Following theorem provides a criterion for a linear cyclic code over F_{SLA4} to be a reversible code. It is a generalization of Theorem 1, [93].

Theorem 5.3.4. Linear cyclic code $C = \langle \varrho(t) \rangle$ over F_{SLA4} is reversible if and only if $\varrho(t)$ is self reciprocal.

Proof. Let $\xi(t)$ be a codeword from C with corresponding n-tuple $\xi = (\xi_0, \xi_1, \dots, \xi_{n-1})$. The reverse n-tuple $\xi^r = (\xi_{n-1}, \xi_{n-2}, \dots, \xi_0)$ corresponds to the polynomial $\xi^*(t)$ where $\xi^*(t) = t^{n-1}\xi(1/t)$. As $\xi(t) = \eta(t)\varrho(t)$,

$$\begin{aligned}\xi^*(t) &= t^{n-1}[\eta(1/t)\varrho(1/t)] \\ &= [t^{n-r-1}t^r][\eta(1/t)\varrho(1/t)] \\ &= [t^{n-r-1}\eta(1/t)][t^r\varrho(1/t)] \quad (\text{using the medial law}).\end{aligned}$$

The polynomial $t^r\varrho(1/t)$ is the reciprocal polynomial $\varrho^*(t)$ of the polynomial $\varrho(t)$. Now the set of reversed codewords form a cyclic code generated by $\varrho^*(t)$. This is same as the original code generated by $\varrho(t)$ if and only if $\varrho^*(t) = \varrho(t)$. ■

Following Lemma is a reformulation of Lemma 19, [2] in terms of special LA-fields.

Lemma 5.3.5. Let $\eta_1(t)$, $\eta_2(t)$ be any two polynomials in F_{SLA4} , with $\deg\eta_1(t) \geq \deg\eta_2(t)$. Then

1. $[\eta_1(t)\eta_2(t)]^* = \eta_1(t)^*\eta_2(t)^*$; and
2. $[\eta_1(t) + \eta_2(t)]^* = \eta_1(t)^* + t^{\deg\eta_1 - \deg\eta_2}\eta_2(t)^*$.

Proof. 1.

$$\begin{aligned}
\eta_1(t)^* \eta_2(t)^* &= [t^{\deg \eta_1} \eta_1(1/t)] [t^{\deg \eta_2} \eta_2(1/t)] \\
&= [t^{\deg \eta_1} t^{\deg \eta_2}] [\eta_1(1/t) \eta_2(1/t)] \text{ (by medial law)} \\
&= t^{\deg \eta_1 + \deg \eta_2} \eta_1(1/t) \eta_2(1/t) \\
&= [\eta_1(t) \eta_2(t)]^*.
\end{aligned}$$

2.

$$\begin{aligned}
[\eta_1(t) + \eta_2(t)]^* &= t^{\deg(\eta_1 + \eta_2)} [\eta_1(1/t) + \eta_2(1/t)] \\
&= t^{\deg(\eta_1 + \eta_2)} [\eta_1(1/t) + \eta_2(1/t)] \\
&= t^{\deg \eta_1} [\eta_1(1/t) + \eta_2(1/t)] \\
&= t^{\deg \eta_1} \eta_1(1/t) + t^{\deg \eta_1} \eta_2(1/t) \\
&= t^{\deg \eta_1} \eta_1(1/t) + t^{\deg \eta_1 - \deg \eta_2} t^{\deg \eta_2} \eta_2(1/t) \\
&= \eta_1(t)^* + t^{\deg \eta_1 - \deg \eta_2} \eta_2(t)^*.
\end{aligned}$$

■

Lemma 5.3.6. Let $t^n - 1 = \eta(t)\beta(t)\rho(t)$, where $\eta(t)$ and $\beta(t)$ are nontrivial polynomials that divide $t^n - 1$ in $F_{SLA_4}[t]_n$. Then

1. if $\eta(t)$ and $\beta(t)$ are self-reciprocal then $\eta(t)\beta(t)$ is self reciprocal,
2. if either $\eta(t)$ or $\beta(t)$ (but not both) is not self-reciprocal then $\eta(t)\beta(t)$ is not self-reciprocal,

Proof. The proof is an analog of the proof of Lemma 5, [1]. ■

Following proposition is a generalization of Lemma 8, [1].

Proposition 5.3.7. A linear cyclic code $C = \langle \varrho(t) \rangle$ of length n (odd) over F_{SLA_4} is complement $\Leftrightarrow t - 1$ does not divide $\varrho(t)$.

Proof. Let $C = \langle \varrho(t) \rangle$ to be cyclic code over F_{SLA_4} . Take a codeword $\xi_0 + \xi_1 t + \dots + \xi_{n-1} t^{n-1}$ from C (where n is odd). $\xi^c(t) = \xi_0^c + \xi_1^c t + \dots + \xi_{n-1}^c t^{n-1}$. Notice that, for any x in F_{SLA_4} , $x + x^c = 1$. Thus, $\xi(t) + \xi^c(t) = 1 + t + \dots + t^{n-1} \in C \Leftrightarrow t^n - 1/t - 1 \in C \Leftrightarrow t^n - 1/t - 1 = p(t)\varrho(t) \Leftrightarrow t^n - 1 = (p(t)\varrho(t))(t - 1)$ (for some polynomial $p(t)$). Since n is odd, by Remark 3.5.11 $t^n - 1$ has unique distinct irreducible factors. So, $\xi^c(t) \in C$ if and only if $t - 1$ does not divide $\varrho(t)$. ■

Algorithm for the Construction of Reversible Complement Cyclic Codes of Odd Lengths over F_{SLA4}

We used the theory developed above and formulated the following algorithm to construct reversible complement cyclic codes over F_{SLA4} of length n , where $n = 5, 7, 9$ and 11 .

Input: A non-associative special LA-field $F_{SLA4} = \{0, 1, 2, 3\}$.

Step 1: Generate all the elements $\varrho(t)$ of the special LA-ring $F_{SLA4}[t]_n$.

Step 2: Iterate over the elements in step 1, accept if; $\varrho(t) = \varrho^*(t)$ (i.e., $\varrho(t)$ is self reciprocal).

Step 3: Iterate over the elements in step 2, accept if; $t - 1$ doesn't divide $\varrho(t)$.

Step 4: Generate a left principal ideal C of $F_{SLA4}[t]_n$ from each element in step 3.

Step 5: Store unique ideals C from step 4 as reversible complement cyclic codes over F_{SLA4} .

Using the above algorithm and found the following codes:

- Length 5: There are two codes given by:

$$C_1 = \langle t^2 + 2t + 1 \rangle .$$

$$C_2 = \langle t^4 + t^3 + t^2 + t + 1 \rangle .$$

- Length 7: There is only one code given by:

$$C = \langle t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \rangle .$$

- Length 9: We get three codes as:

$$C_1 = \langle t^2 + t + 1 \rangle .$$

$$C_2 = \langle t^6 + t^3 + 1 \rangle .$$

$$C_3 = \langle t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \rangle .$$

- Length 11: The only code we obtained is given :

$$C = \langle t^{10} + t^9 + t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \rangle .$$

Remarks on Running Times

We used a computer system with processor: *Intel® Core™ i5-2410M CPU @ 2.30GHz* × 4, RAM: 6 GB and python version 3.6 for the computation process. The processing times for $n=5, 7, 9$ and 11 are given in the following table:

n	T	E	G	P
5	0.33 sec	1024	48	0.019 sec
7	29 sec	16384	192	0.45 sec
9	45 min	262144	768	10 sec
11	3 days	4194304	3072	4 min

where T = Total processing time, E = No. of elements in $F_{SLA_4}[t]_n$, G = number of generators with required constraints, and P = processing time for a single generator.

Chapter 6

Applications to Cryptography

Cryptology deals with the secure storage and communication of data. It has two subdivisions; cryptography and cryptanalysis. Cryptography is the way of keeping the information confidentiality using mathematical approaches, while cryptanalysis is the art of cracking encrypted information using mathematical and computational devices without accessing the cryptographic key. Though, both cryptography and cryptanalysis aim at the same target, however cryptanalysis has transformed the techniques and methods radically throughout the history of cryptography. There are many of techniques have been used for cryptanalysis. Differential cryptanalysis is widely used for block ciphers. Differential cryptanalysis is a study in which we analyze the concern of specific difference in plaintext pairs on the difference of the consequent cipher text pairs. These differences are used to allocate probabilities to the practicable keys and to find the nearly all possible keys [22]. Literature review concludes that differential attack is the only attack which applies on such S-boxes that are constructed by finite Galois field extension of binary field \mathbb{Z}_2 . The S-boxes are typically constructed over Galois field and some other commutative and associative structures. In this chapter, we construct S-boxes of different orders over special LA-rings. In wake of the non-associative and non-commutative behavior of the ring structure, these S-boxes have increased resilience.

6.1 Cryptosystem Design over a Special LA-field

In this section, small S-boxes are designed over a special LA-field of order 16. The purpose of these S-boxes designing is to increase the robustness due to non-commutative and non-

associative behaviour of the LA-rings. We used the Majority Logic Criterion (MLC) to determine the strength of these S-boxes in image encryption. A watermarking application of these S-boxes is given along with their comparison in the context.

6.1.1 S-box Construction over a Non-associative LA-field of Order 16

We used MACE4 [95] to find the following example of a special LA- field F_{SLA} of order 16. Let $F_{SLA} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ be an LA-field with the operations of addition and multiplication defined by Table 6.1 and Table 6.2 respectively.

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	3	2	6	7	4	5	11	13	15	8	14	9	12	10
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3	2	1	0	7	6	5	4	14	15	13	12	11	10	8	9
3	2	3	0	1	5	4	7	6	12	10	9	14	8	15	11	13
4	6	4	7	5	1	3	0	2	9	8	12	13	10	11	15	14
5	7	5	6	4	3	1	2	0	10	12	8	15	9	14	13	11
6	4	6	5	7	0	2	1	3	13	11	14	9	15	8	10	12
7	5	7	4	6	2	0	3	1	15	14	11	10	13	12	9	8
8	11	8	14	12	9	10	13	15	1	4	5	0	3	6	2	7
9	13	9	15	10	8	12	11	14	4	1	3	6	5	0	7	2
10	15	10	13	9	12	8	14	11	5	3	1	7	4	2	6	0
11	8	11	12	14	13	15	9	10	0	6	7	1	2	4	3	5
12	14	12	11	8	10	9	15	13	3	5	4	2	1	7	0	6
13	9	13	10	15	11	14	8	12	6	0	2	4	7	1	5	3
14	12	14	8	11	15	13	10	9	2	7	6	3	0	5	1	4
15	10	15	9	13	14	11	12	8	7	2	0	5	6	3	4	1

Table 6.1: Addition table for LA-field F_{SLA}

·	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	1	3	5	8	10	9	12	15	7	0	14	11	2	13	6
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	6	1	0	4	9	8	11	13	7	14	15	3	2	10	5	12
4	9	1	4	8	7	15	14	2	12	13	6	5	3	0	10	11
5	11	1	6	9	14	7	3	10	13	5	12	4	0	15	8	2
6	8	1	5	10	15	0	7	11	6	12	4	13	14	3	2	9
7	13	1	7	12	2	11	10	4	3	0	14	15	8	9	6	5
8	14	1	9	7	13	12	5	0	2	10	11	8	4	6	15	3
9	7	1	8	15	12	6	13	3	11	2	9	10	5	4	0	14
10	3	1	11	14	5	13	4	15	10	8	2	9	6	12	7	0
11	15	1	10	0	6	4	12	14	9	11	8	2	13	5	3	7
12	10	1	13	2	0	3	15	9	4	6	5	12	7	14	11	8
13	2	1	12	11	3	14	0	8	5	4	13	6	15	7	9	10
14	12	1	15	6	11	9	2	5	14	3	7	0	10	8	4	13
15	5	1	14	13	10	2	8	6	0	15	3	7	9	11	12	4

Table 6.2: Multiplication table for LA-field F_{SLA}

4×4 S-box over Galois Field $GF(2^4)$

The elements of Galois extension field $GF(2^4)$ of order 16 are given in the Table 6.3:

Exp	Polynomial	Nibble	Exp	Polynomial	Nibble	Exp	Polynomial	Nibble
$-\infty$	0	0000	5	$x + x^2$	0110	11	$1 + x^3$	1001
0	1	1000	6	$x + x^3$	0101	12	x^3	0001
1	$1 + x$	1100	7	$1 + x^2 + x^3$	1011	13	$1 + x + x^3$	1101
2	$1 + x^2$	1010	8	x^2	0010	14	$x + x^2 + x^3$	0111
3	$1 + x + x^2 + x^3$	1111	9	$x^2 + x^3$	0011			
4	x	0100	10	$1 + x + x^2$	1110			

Table 6.3: Galois extension field $GF(2^4)$

Now, let us construct a typical S-box on the Galois field extension $GF(2^4)$. It could be seen in Table 6.4, the most basic 4×4 S-box and it satisfies all the fundamental properties being an S-box.

0	11	12	6
0000	1011	1100	0110
3	8	4	2
0011	1000	0100	0010
1	9	13	15
0001	1001	1001	1111
14	7	10	5
1110	0111	1100	0101

Table 6.4: S-box on $GF(2^4)$

Construction Steps of 4×4 S-box over LA-field of Order 16

1. Table F_{SLA} , LA-field of order 16.
2. Define an inversion map $f : F_{SLA} - \{1\} \rightarrow F_{SLA} - \{1\}$.
3. Define an Affine transformation $g : F_{SLA} \rightarrow F_{SLA}$ as: $g(a) = 3a + 10$.
4. Compose the two functions f and g .
5. Construct a 4×4 S-box by arranging the step 4 row wise.

Define the invertive map $f : F_{SLA} - \{1\} \rightarrow F_{SLA} - \{1\}$ as: $f(a) = a^{-1}$.

a	0	2	4	5	6	7	8	9	10	11	12	13	14	15	4
a^{-1}	13	2	7	15	14	4	8	9	10	11	3	0	6	5	7

Table 6.5: The multiplicative inverses chart of elements of F_{SLA}

a	0	2	4	5	6	7	8	9	10	11	12	13	14	15	4
$f(a)$	13	2	7	15	14	4	8	9	10	11	3	0	6	5	7

Table 6.6: The function f

Now define the Affine function $g : F_{SLA} \rightarrow F_{SLA}$ as: $g(a) = 3a + 10$.

a	0	1	2	4	5	6	7	8	9	10	11	12	13	14	15	4
$g(a)$	14	10	15	12	3	5	7	2	11	6	0	9	13	1	8	4

Table 6.7: The function g

Thus, the composition $g \circ f : F_{SLA} - \{1\} \rightarrow F_{SLA}$ is given in the Table 6.8.

a	0	2	4	5	6	7	8	9	10	11	12	13	14	15	4
$g \circ f(a)$	1	15	13	2	4	8	3	11	6	0	9	12	14	7	5

Table 6.8: The Table for function $g \circ f$

1	10	15	13
1	1010	1111	1101
2	4	8	3
10	100	1000	11
11	6	0	9
1011	110	0	1001
12	14	7	7
1100	1110	111	111

Table 6.9: The 4×4 S-box over LA-field F_{SLA} of order 16

The XOR operation for F_{SLA} and $GF(16)$ are given in Table 6.10 and Table 6.11.

a	b	a XOR b	a XOR b	a	b	a XOR b	a XOR b	a	b	a XOR b	a XOR b	a	b	a XOR b	a XOR b
		F_{SLA}	$GF(16)$			F_{SLA}	$GF(16)$			F_{SLA}	$GF(16)$			F_{SLA}	$GF(16)$
0	0	0	0	2	0	2	2	4	0	4	4	6	0	6	6
0	1	1	1	2	1	3	5	4	1	5	15	6	1	7	11
0	2	2	2	2	2	0	0	4	2	6	10	6	2	4	3
0	3	3	3	2	3	1	6	4	3	7	7	6	3	5	2
0	4	4	4	2	4	6	10	4	4	0	0	6	4	2	12
0	5	5	5	2	5	7	1	4	5	1	8	6	5	3	9
0	6	6	6	2	6	4	3	4	6	2	12	6	6	0	0
0	7	7	7	2	7	5	12	4	7	3	3	6	7	1	10
0	8	8	8	2	8	10	15	4	8	12	5	6	8	14	14
0	9	9	9	2	9	11	11	4	9	13	14	6	9	15	5
0	10	10	10	2	10	8	4	4	10	14	2	6	10	12	7
0	11	11	11	2	11	9	9	4	11	15	13	6	11	13	1
0	12	12	12	2	12	14	7	4	12	8	6	6	12	10	4
0	13	13	13	2	13	15	14	4	13	9	11	6	13	11	15
0	14	14	14	2	14	12	13	4	14	10	9	6	14	8	8
0	15	15	15	2	15	13	8	4	15	11	1	6	15	9	13
1	0	1	1	3	0	3	3	5	0	5	5	7	0	7	7
1	1	0	0	3	1	2	9	5	1	4	2	7	1	6	14
1	2	3	5	3	2	1	6	5	2	7	1	7	2	5	12
1	3	2	9	3	3	0	0	5	3	6	11	7	3	4	4
1	4	5	15	3	4	7	7	5	4	1	8	7	4	3	3
1	5	4	2	3	5	6	11	5	5	0	0	7	5	2	13
1	6	7	11	3	6	5	2	5	6	3	9	7	6	1	10
1	7	6	14	3	7	4	4	5	7	2	13	7	7	0	0
1	8	9	10	3	8	11	13	5	8	13	4	7	8	15	11
1	9	8	3	3	9	10	1	5	9	12	6	7	9	14	15
1	10	11	8	3	10	9	12	5	10	15	15	7	10	13	6
1	11	10	6	3	11	8	5	5	11	14	3	7	11	12	8
1	12	13	13	3	12	15	10	5	12	9	14	7	12	11	2
1	13	12	12	3	13	14	8	5	13	8	7	7	13	10	5
1	14	15	7	3	14	13	15	5	14	11	12	7	14	9	1
1	15	14	4	3	15	12	14	5	15	10	10	7	15	8	9

Table 6.10: The XOR operations in LA-field F_{SLA} and Galois field $GF(2^4)$ of orders 16

a	b	a XOR b	a XOR b	a	b	a XOR b	a XOR b	a	b	a XOR b	a XOR b	a	b	a XOR b	a XOR b
		F_{SLA}	$GF(16)$			F_{SLA}	$GF(16)$			F_{SLA}	$GF(16)$			F_{SLA}	$GF(16)$
8	0	8	8	10	0	10	10	12	0	12	12	14	0	14	14
8	1	9	10	10	1	11	8	12	1	13	13	14	1	15	7
8	2	10	15	10	2	8	4	12	2	14	7	14	2	12	13
8	3	11	13	10	3	9	12	12	3	15	10	14	3	13	15
8	4	12	5	10	4	14	2	12	4	8	6	14	4	10	9
8	5	13	4	10	5	15	15	12	5	9	14	14	5	11	12
8	6	14	14	10	6	12	7	12	6	10	4	14	6	8	8
8	7	15	11	10	7	13	6	12	7	11	2	14	7	9	1
8	8	0	0	10	8	2	1	12	8	4	9	14	8	6	6
8	9	1	12	10	9	3	13	12	9	5	8	14	9	7	4
8	10	2	1	10	10	0	0	12	10	6	3	14	10	4	11
8	11	3	7	10	11	1	14	12	11	7	15	14	11	5	10
8	12	4	9	10	12	6	3	12	12	0	0	14	12	2	5
8	13	5	3	10	13	7	9	12	13	1	1	14	13	3	2
8	14	6	6	10	14	4	11	12	14	2	5	14	14	0	0
8	15	7	2	10	15	5	5	12	15	3	11	14	15	1	3
9	0	9	9	11	0	11	11	13	0	13	13	15	0	15	15
9	1	8	3	11	1	10	6	13	1	12	12	15	1	14	4
9	2	11	11	11	2	9	9	13	2	15	14	15	2	13	8
9	3	10	1	11	3	8	5	13	3	14	8	15	3	12	14
9	4	13	14	11	4	15	13	13	4	9	11	15	4	11	1
9	5	12	6	11	5	14	3	13	5	8	7	15	5	10	10
9	6	15	5	11	6	13	1	13	6	11	15	15	6	9	13
9	7	14	15	11	7	12	8	13	7	10	5	15	7	8	9
9	8	1	12	11	8	3	7	13	8	5	3	15	8	7	2
9	9	0	0	11	9	2	2	13	9	4	10	15	9	6	7
9	10	3	13	11	10	1	14	13	10	7	9	15	10	5	5
9	11	2	2	11	11	0	0	13	11	6	4	15	11	4	12
9	12	5	8	11	12	7	15	13	12	1	1	15	12	3	11
9	13	4	10	11	13	6	4	13	13	0	0	15	13	2	6
9	14	7	4	11	14	5	10	13	14	3	2	15	14	1	3
9	15	6	7	11	15	4	12	13	15	2	6	15	15	0	0

Table 6.11: The XOR operations in LA-field F_{SLA} and Galois field $GF(2^4)$ of orders 16

6.1.2 Majority Logic Criterion for the Analysis of S-Boxes

In [64, 126], a majority logic criterion (MLC) has been provided. The purpose of MLC is the analysis of the statistical strength of the S-box, used in image encryption. Encryption produces distortions in the image, and the type of these distortions determines the strong composition of the algorithm. The entropy gauges the measure of randomness in a system. The degree of entropy in an image is connected to the positioning of pieces, which enables the human eye to recognise the image. Contrast licenses the watcher to identify the stuffs in an image. Because of the technique used to encrypt the image, the amount of randomness upsurges ends up in the altitude of contrast level to a very tall value. The higher level of contrast in the encrypted image reflects a robust encryption. Correlation is an investigation that calculates the correlation of a pixel to its neighbor by ownership into account the texture of the entire image. The closeness of the distribution of components in the grey level co-occurrence matrix (GLCM) to GLCM diagonal is dealt by the homogeneity analysis. The statistics of combinations of pixel brightness values or grey levels in tabular form are displayed by the GLCM. For analysis, we measure the energy of the encrypted images as conserved by several S-boxes. This measure offers the sum of square elements in GLCM. The results of MLC, arranged in Table 6.12, display that the proposed S-boxes fulfill all the criteria as much as the standard and can be utilized for safe communication.

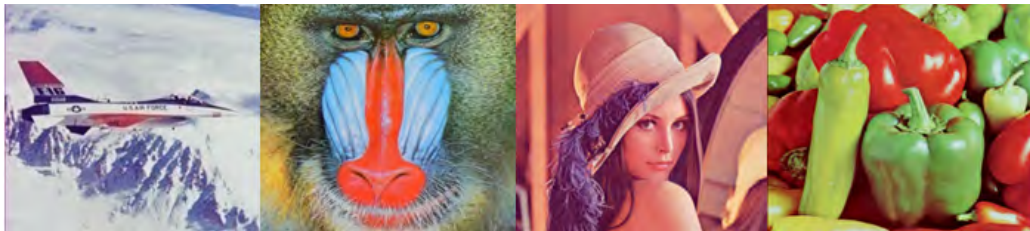


Figure 6.1: Four 512×512 plain images of Airplane; Baboon; Lena; Pepper

6.1.3 Differential Cryptanalysis on LA-field F_{SLA} based S-box

In [54], it is demarcated that differential cryptanalysis constructs the high probability in the differences of precise outcomes of plaintext and differences into the final round of the cipher. Such as, observe a procedure with two inputs A' and A'' and resulting outputs B'

LSB Image→ MLC↓	Airplane	Baboon	Lena	Pepper	LSB Image→ MLC↓	Airplane	Baboon	Lena	Pepper
Contrast	0.275	0.5381	0.2491	0.2944	Contrast	0.311	0.6646	0.2763	0.3391
Correlation	0.939	0.9281	0.9778	0.9763	Correlation	0.9401	0.9401	0.9779	0.9756
Energy	0.2712	0.1513	0.1689	0.1721	Energy	0.3413	<u>0.3413</u>	0.1625	0.1925
Homogeneity	0.9302	0.838	0.9181	0.9222	Homogeneity	0.9245	0.9245	0.914	0.9113
Entropy	5.5133	5.9673	5.9698	5.9901	Entropy	5.5077	5.5077	5.9538	5.9911

Table 6.12: MLC of LSB's of four 512×512 images by S-boxes on Galois field $GF(2^4)$ and LA-field F_{SLA}

and B'' correspondingly. $\Delta A = A' + A''$ and is known as input difference where signify an addition defined in addition Table 6.1 and therefore,

$$\Delta A = [\Delta A_1, \Delta A_2, \dots, \Delta A_n] \quad (6.1.1)$$

whereas $\Delta A = A' + A''$ by A' and A'' on behalf of the i^{th} bit of A' and A'' , correspondingly. Similarly, $\Delta B = B' + B''$ is the output difference and given as;

$$\Delta B = [\Delta B_1, \Delta B_2, \dots, \Delta B_n]. \quad (6.1.2)$$

Calculation of Difference Distribution Table of S-box

By taking the S-box of our cipher, for every input pair as $(\Delta A = A' + A'')$, the resulting values of ΔB were derived. We calculate the difference distribution tables of LA field like differential attack on Mini-AES by using addition of LA field, instead of bitwise XOR [50]. For an S-box we summarize the data in a "difference distribution table" in which ΔA values (in decimal) arranged in rows and ΔB (in decimal) are in columns. These tables for the S-boxes of Table 6.9 and Table 6.4 are given in Table 6.13 and Table 6.14 respectively.

Difference Distribution Tables of S-boxes

Inputs (A)	Outputs (B)															
	2	10	8	13	9	0	5	1	12	4	11	15	3	7	14	6
0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	2	0	1	1	1	1	1	1	1	1	1	1
3	1	1	1	2	1	0	1	1	1	1	1	1	1	1	1	1
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	2	0	1	1	1	1	1	1	1	1
12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 6.13: Difference Distribution Table of S-box over LA-field F_{SLA}

Inputs (A)	Outputs (B)															
	0	11	12	6	3	8	4	2	1	9	13	15	14	7	10	5
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	2	0	0	0	2	0	2	2	2	4	0	0	0	2
2	0	0	2	0	2	0	2	2	0	0	2	0	4	2	0	0
3	0	2	0	0	2	0	2	2	0	0	0	2	2	2	2	0
4	0	0	0	4	2	0	0	2	2	0	2	0	0	0	2	2
5	0	0	2	0	0	2	2	2	6	0	0	0	0	0	2	0
6	0	0	0	2	2	0	0	0	2	2	0	2	2	0	2	2
7	0	2	2	2	4	2	0	0	0	0	2	0	0	0	0	2
8	0	4	2	0	0	0	0	2	0	2	0	0	0	2	2	2
9	0	2	0	2	2	0	2	0	2	2	2	2	0	0	0	0
10	0	0	0	0	2	2	0	0	0	2	2	0	0	6	0	2
11	0	0	2	2	0	2	4	2	0	0	0	0	2	0	0	2
12	0	2	2	2	0	0	2	0	0	2	0	0	2	2	2	0
13	0	0	0	0	0	2	0	2	0	4	2	2	2	0	0	2
14	0	2	2	0	0	2	0	2	0	0	2	2	0	0	4	0
15	0	2	0	2	0	4	0	0	2	0	0	2	2	2	0	0

Table 6.14: Difference Distribution Table of S-box over Galois field $GF(2^4)$

In this difference distribution tables, each element illustrates quantity of results of the relating output difference ΔB value given the input difference ΔA , except for the exceptional case $\Delta A = 0, \Delta B = 0$. In Table 6.13, the highest value of $(\Delta A, \Delta B)$ is 2. For instance, we have talked about that there is a considerable measure of properties of the difference distribution table that must be revealed. Initially, all elements sum in a row is $2^n = 16$. Similarly, all column sum is $2^n = 16$. Also, in Table 6.13 the all elements sum in rows and columns is $2^n = 16$, but all values are not even seen in Table 6.13 and it also contained some odd values. Might be one consider that for occurrence of these odd values be the

due to the S-box which are used here for calculating the difference distribution table are constructed over different structure. By way of, lowest difference value in this Table 6.13, because 0 means there is no change occur.

6.1.4 Propagation Ratio

Propagation ratio is also known as the probability. The highest and lowest probability of S-boxes over LA-field F_{SLA} and Galois field $GF(2^4)$ are given in Table 6.15.

S-box over	Highest probability	Lowest probability
F_{LA}	$2/16 = 0.125$	$1/16 = 0.0625$
$GF(2^4)$	$4/16 = 0.25$	$2/16 = 0.125$

Table 6.15: Highest and Lowest probability of S-boxes over LA-field F_{SLA} and $GF(2^4)$

6.1.5 Watermarking Applications

With development in medium of information, digital media is now used extensively all over the world. Digital libraries comprising enormous volume of information have been molded. These libraries cover digital data (Books, images, magazines even video and audio information) that can be get into by anyone in the world at any place. To prevent ill use of this information, its holders and inventers use concealed digital signatures and other practices. One of these techniques is the watermarking of an image. It is conceivable to watermark an image using the S-box formed through the technique described in [138]. A novel digital watermarking algorithm based on the chaotic map is given in [71] by which the data is hidden in images using LSBs - a new digital watermarking algorithm based on the chaotic map. This distinct type of watermark not only hides information in the image nonetheless it also changes the shade of each pixel, altering the entire image as an outcome. It also makes it impossible for a person to find the hidden information short of the original image. Thus, in order to copy the image or use it, a person would have to ask for the original image itself from the possessor. A considerable tender of newly constructed S-boxes is that they could be cast off in watermarking of an image. One of the key features of watermarking is that it does not condense the quality of the image. Therefore, keeping this point in mind, the S-boxes transformations have been useful to the least significant

bits (LSBs) of each pixel of an image, which will not change the quality of the image. In Figure 6.2, the algorithm is explained.

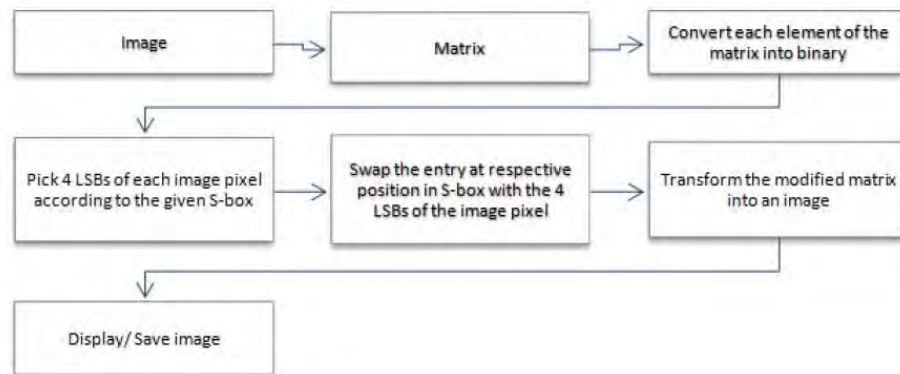


Figure 6.2: Water Marking Algorithm

The changeless of histogram of a water marked image than the plain image is premium feature for calculating the strength of an image water marking scheme. We give analysis of the the color airplane, baboon, Lena and pepper images with dimension 512×512 , which have different contents along with their histograms. The histograms of water marked pictures with respect to the proposed algorithm are correspondingly similar to the original images. In Figures, 6.3 (i-xxiv), we have drawn 3-D histograms of the original and water marked pictures to investigate the changelessness in water marked images. The histogram of an image shows frequency of pixels intensity values. A flawless water marked image should have a histogram same as to the histogram of the plain image.

6.2 LA-ring Based Construction of 8×8 S-boxes with an Image Encryption Application

In this section, using a non-associative ring of order 512 obtained by using computational techniques given in section 3.2, a triplet of 8×8 S-boxes is designed. The motivation behind this study was the article "Steps towards redesigning cryptosystems by a non-associative algebra of IP-loops," published in the journal Wireless Personal Communications, in the year 2019. In this article, Naseer et al. [102] introduced a novel design of S-boxes over the elements of inverse property loop. The attractive features of the structure are; it is non-associativity and the existence of the inverse of zero elements. These prop-



Figure 6.3: (i-xxiv): RGB image (3-dimensional matrix of pixels having intensities between 0 and 255) comparison of original image and watermarked image by 4×4 S-boxes from the 16 order structures of Galois field $GF(2^4)$ and LA-field F_{SLA} . The images of airplane, baboon, Lena and pepper contain watermark in the four LSBs of each pixel of the each original image by the transformation of 3 dimensional two 4×4 S-boxes.

erties increase the availability of the number of structures of IP-Loops. The purpose of S-boxes constructed in this section is to increase the robustness due to non-associative and non-commutative behavior of the LA-rings and increase 65,536 times the key space. Thus, the obtained S-boxes having significant level of resistance against existing crypt analyses attack.

In last two decades, the notion of chaos has found several applications in various sciences. In Cryptography 8×8 S-boxes are also been produced by using chaotic maps [65, 80]. Because of its low non-linearity, they do not get much significance like S-boxes constructed through algebraic structures. Cryptography, which might be supposed to be a branch of arithmetic and technology, has clutched a tremendous deal of consideration and an oversize variety of analysis work, is devoted to the experience of chaos-based cryptologic algorithms [70, 80]. The qualities of chaotic maps stand after their use within the smartness of such algorithms. These main options comprise highly sensitive dependence on initial conditions and controlling parameter, ergodicity, randomness, mixing, etc., that are alike the confusion and diffusion properties of Claude Shannon [136]. Precisely, the random-like behavior of the outputs of chaotic maps brands them suitable bases to be used in cryptographs. A lot of image encryption algorithms are built on chaotic systems, for instance [42, 63, 141]. Whereas Liu et al. [85], anticipated a chaos-based color image block encryption scheme using S-box. A novel color image encryption application is foreseen in which primarily newly obtained 3 S-boxes are being castoff to crop confusion in three layers of a standard RGB image. Though, for diffusion 3D Arnold chaotic map is used in the proposed encryption scheme. A comparison with some of current chaos and S-box reliant color image encryption schemes spectacles the performance results of the estimated RGB image encryption and pragmatic as approaching the standard principal level.

6.2.1 Generating Algorithm for Pair of S-boxes

Consider the special LA-ring with identity $R_{SLA8} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ from Example 3.2.3. Here the zero element is '2' and the left identity element is '4'. Units in R_{SLA8} are: 0, 1, 3, and 4. The set $\mathcal{R} = R_{SLA8} + uR_{SLA8} + u^2R_{SLA8}$ (with $u^3 = 0$) is a special LA-ring with 512 elements. The left identity element in \mathcal{R} is '422'. An element $a + bu + cu^2$ is a unit in $\mathcal{R} = R_{SLA8} + uR_{SLA8} + u^2R_{SLA8}$ if and only if a is a unit in R_{SLA8} . So, there are 256 units in $\mathcal{R} = R_{SLA8} + uR_{SLA8} + u^2R_{SLA8}$. The list of units of the ring \mathcal{R} is given in

Table 6.16.

The scheme of the S-boxes triplets is based on a sub LA-module M of the special LA-ring \mathcal{R} and a multiplicative LA-group $U(\mathcal{R})$ consisting of units in \mathcal{R} . Where the sub LA-module

$$M = \{200, 201, \dots, 277, 500, 501, \dots, 577, 600, 601, \dots, 677, 700, 701, \dots, 777\},$$

is decimal equivalent to $\{128, 129, \dots, 191, 320, 321, \dots, 511\}$ and the multiplicative LA-group

$$U(\mathcal{R}) = \{000, 001, \dots, 077, 100, 101, \dots, 177, 300, 301, \dots, 377, 400, 401, \dots, 477\}$$

is expressed in decimal notation as: $\{0, 1, \dots, 127, 192, 193, \dots, 319\}$. The sub LA-module M holds two operations; namely addition and scalar multiplication, but the LA-group $U(\mathcal{R})$ is facilitated only with only one operation that is the operation of multiplication. The actions of $PGL(2, GF(2^8))$, the projective general linear group to the Galois field $GF(2^8)$ gives the ultimate S-boxes.

CASE I: Generating S-boxes over Sub-LA-module of R-LA-module \mathcal{R}

As M is \mathcal{R} -sub LA-module of \mathcal{R} -module \mathcal{R} , we can define an affine mapping $\theta : M \rightarrow M$, $\theta(s) = rs + m$, where $r = 342$ and $m = 653$ are fixed elements in $U(\mathcal{R})$ and M respectively. As the elements of M are 9 binary bits representation, so we define a bijection $\sigma : M \rightarrow GF(2^8)$ by

$$\sigma(x) = \begin{cases} x + 64, & \text{if } 128 \leq x \leq 191; \\ x - 320, & \text{if } 320 \leq x \leq 511. \end{cases} \quad (6.2.1)$$

Finally, the linear fractional transformation is given as; $\psi : PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8)$ defined as: $\psi(x) = \frac{ax+b}{cx+d}$, where $a = 158$, $b = 54$, $c = 20$, $d = 92$ in $GF(2^8)$ such that $ad - bc \neq 0$. To construct this S-box, our algorithm starts using the sub LA-module M of a special LA-ring \mathcal{R} and $GF(2^8)$. Eventually, the map ψ purposes the S-box with the action of $PGL(2, GF(2^8))$ on $GF(2^8)$. The newly constructed S-box, using the suggested algorithm is a 16×16 look up table which can be used to process eight binary bits of data. The S-box is given in Table 6.17.

Sr.	Units	Sr.	Units	Sr.	Units	Sr.	Units	Sr.	Units	Sr.	Units	Sr.	Units	Sr.	Units
1	000	33	040	65	100	97	140	129	300	161	340	193	400	225	440
2	001	34	041	66	101	98	141	130	301	162	341	194	401	226	441
3	002	35	042	67	102	99	142	131	302	163	342	195	402	227	442
4	003	36	043	68	103	100	143	132	303	164	343	196	403	228	443
5	004	37	044	69	104	101	144	133	304	165	344	197	404	229	444
6	005	38	045	70	105	102	145	134	305	166	345	198	405	230	445
7	006	39	046	71	106	103	146	135	306	167	346	199	406	231	446
8	007	40	047	72	107	104	147	136	307	168	347	200	407	232	447
9	010	41	050	73	110	105	150	137	310	169	350	201	410	233	450
10	011	42	051	74	111	106	151	138	311	170	351	202	411	234	451
11	012	43	052	75	112	107	152	139	312	171	352	203	412	235	452
12	013	44	053	76	113	108	153	140	313	172	353	204	413	236	453
13	014	45	054	77	114	109	154	141	314	173	354	205	414	237	454
14	015	46	055	78	115	110	155	142	315	174	355	206	415	238	455
15	016	47	056	79	116	111	156	143	316	175	356	207	416	239	456
16	017	48	057	80	117	112	157	144	317	176	357	208	417	240	457
17	020	49	060	81	120	113	160	145	320	177	360	209	420	241	460
18	021	50	061	82	121	114	161	146	321	178	361	210	421	242	461
19	022	51	062	83	122	115	162	147	322	179	362	211	422	243	462
20	023	52	063	84	123	116	163	148	323	180	363	212	423	244	463
21	024	53	064	85	124	117	164	149	324	181	364	213	424	245	464
22	025	54	065	86	125	118	165	150	325	182	365	214	425	246	465
23	026	55	066	87	126	119	166	151	326	183	366	215	426	247	466
24	027	56	067	88	127	120	167	152	327	184	367	216	427	248	467
25	030	57	070	89	130	121	170	153	330	185	370	217	430	249	470
26	031	58	071	90	131	122	171	154	331	186	371	218	431	250	471
27	032	59	072	91	132	123	172	155	332	187	372	219	432	251	472
28	033	60	073	92	133	124	173	156	333	188	373	220	433	252	473
29	034	61	074	93	134	125	174	157	334	189	374	221	434	253	474
30	035	62	075	94	135	126	175	158	335	190	375	222	435	254	475
31	036	63	076	95	136	127	176	159	336	191	376	223	436	255	476
32	037	64	077	96	137	128	177	160	337	192	377	224	437	256	477

Table 6.16: Units $U(\mathcal{R})$ in the ring $\mathcal{R} = R_{SLA_8} + uR_{SLA_8} + u^2R_{SLA_8}$

CASE II: Generating S-boxes over $U(\mathcal{R})$

We define the inverse and affine linear mappings $\varphi', \theta' : U(\mathcal{R}) \rightarrow U(\mathcal{R})$ by $\varphi'(t) = t^{-1}$ and $\theta'(t) = r't + m'$, where $r' = 436$ and $m' = 275$ are fixed elements in $U(\mathcal{R})$ and M respectively. Accordingly the composition $\theta' \circ \varphi' : U(\mathcal{R}) \rightarrow U(\mathcal{R})$ of mappings is defined by $\theta' \circ \varphi'(t) = (r't + m')^{-1}$. As the elements of $U(\mathcal{R})$ are 9 binary bits representation, so we define a bijection $\sigma' : U(\mathcal{R}) \rightarrow GF(2^8)$ by

$$\sigma'(z) = \begin{cases} z, & \text{if } 0 \leq z \leq 255; \\ R_m + 128, & \text{if } 320 \leq z \leq 511. \end{cases} \quad (6.2.2)$$

R_m denotes the remainder after division by 256. So, in the end, the linear fractional transformation is given as; $\psi' : PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8)$, $\psi'(z) = \frac{(a'z+b')}{(c'z+d')}$, where $a' = 210, b' = 17, c' = 84, d' = 60$ in $GF(2^8)$ such that $a'd' - b'c' \neq 0$. To construct this S-box, the algorithm activates using the LA-group $U(R_{SLA})$ of units or invertible elements in the special LA-ring R_{SLA} and $GF(2^8)$. Ultimately, the map ψ' generates the S-box with the action of $PGL(2, GF(2^8))$ on $GF(2^8)$. Table 6.18 shows the new S-box constructed with the suggested algorithm, a 16×16 look up table that can be used to process eight binary bits of data.

136	12	95	103	137	169	92	101	158	198	128	6	44	195	171	152
247	162	217	253	255	78	133	86	14	49	161	105	225	214	130	182
165	237	254	164	246	151	102	199	93	230	150	190	179	70	176	94
219	229	117	18	50	143	157	248	146	184	45	30	224	110	228	159
187	173	239	96	118	73	116	25	31	41	227	232	201	226	8	91
178	156	154	3	56	68	7	9	209	43	180	125	106	17	62	191
39	244	54	84	10	149	40	11	81	218	66	99	177	203	27	71
170	202	135	55	167	147	207	129	109	189	13	181	186	126	47	172
245	0	175	5	61	76	82	72	75	85	231	64	144	174	107	213
249	32	240	132	33	153	215	204	139	205	148	193	210	252	212	24
236	221	97	15	59	134	200	74	155	192	98	100	20	19	123	197
16	35	194	120	242	108	28	113	34	79	38	36	211	58	42	46
60	67	89	222	90	111	216	168	69	208	88	104	238	22	52	185
140	183	234	141	1	2	220	29	142	87	163	114	206	166	112	138
48	223	124	21	23	188	37	26	251	65	122	121	241	63	77	4
80	233	51	235	160	127	115	196	243	250	57	131	119	53	145	83

Table 6.17: S-box 1 designed over LA-sub-module of LA-ring \mathcal{R}

To synthesize another S-box, we compose the above generated S-boxes and get an S-box given in Table 6.19.

The flow chart for the algorithm is illustrated in Figure 6.4

234	242	36	111	151	240	12	171	129	125	78	19	9	43	255	98
220	70	116	69	73	92	61	65	208	181	7	22	155	83	143	138
101	25	249	13	8	4	123	246	68	33	159	152	26	190	117	168
31	58	245	212	149	164	174	85	235	247	100	178	127	74	50	44
52	56	229	137	134	204	239	27	102	10	142	28	87	172	96	57
91	97	195	38	150	66	105	41	194	218	49	154	199	227	132	86
81	53	55	148	51	23	145	109	210	237	17	48	147	191	182	223
11	252	193	238	62	29	236	185	128	217	82	5	179	250	71	133
167	202	216	79	197	94	241	251	136	214	157	226	206	131	201	75
126	76	139	60	120	144	1	118	224	254	183	122	93	243	90	80
88	107	184	231	166	54	219	112	30	192	209	124	230	104	14	162
198	188	2	15	59	42	3	228	46	156	253	158	205	37	146	119
163	89	21	203	20	34	211	215	108	106	207	140	24	161	72	95
18	114	222	169	244	121	176	170	160	200	130	77	35	99	39	232
248	135	221	141	165	45	153	225	177	40	180	103	6	189	187	16
115	64	213	84	0	47	233	67	173	110	175	196	113	186	32	63

Table 6.18: S-box 2 designed over LA-group of units in LA-ring \mathcal{R}

144	247	250	195	18	215	217	105	187	228	196	92	78	188	211	177
254	47	126	226	136	185	63	87	100	171	84	227	205	167	32	24
213	88	206	115	122	141	66	3	133	253	135	77	95	182	161	82
120	119	81	208	111	222	189	131	165	39	19	85	158	154	156	16
130	89	231	97	53	238	145	212	174	255	46	112	192	146	178	128
106	6	180	73	246	147	116	127	251	98	207	56	194	83	25	200
168	80	234	142	50	248	43	235	96	118	17	150	72	124	58	223
203	209	186	151	233	45	162	113	199	35	44	140	160	52	129	34
93	70	20	61	101	11	10	62	252	28	37	210	225	163	49	202
201	68	90	110	33	40	197	230	244	104	153	15	79	157	94	149
219	1	91	74	4	175	30	29	103	59	41	38	138	7	239	2
143	152	42	229	224	86	31	55	159	236	117	26	241	8	125	9
123	48	179	144	71	218	76	21	191	216	5	132	107	22	240	99
169	108	166	176	220	65	60	245	121	102	64	51	14	67	109	170
36	139	204	155	181	232	190	164	75	237	137	27	243	13	193	69
172	184	12	54	0	134	23	198	183	214	249	173	148	242	221	57

Table 6.19: S-box 3 (the composition of S-boxes 1, 2)

6.2.2 Key Space Analysis

In case when we consider the special LA-ring $\mathcal{R} = R_{SLA8} + uRR_{SLA8} + u^2R_{SLA8}$, the affine map $g : U(\mathcal{R}) \rightarrow U(\mathcal{R})$ such that $g(x) = ax + b$ for all $x \in U(\mathcal{R})$ results 256 possible choices of the fixed unit element a in $U(\mathcal{R})$ and 256 choices of the element b in M . Hence, we obtained $256 \times 256 = 65,536$ possible affine mappings. Accordingly, we get 65,536 number of 9×9 pseudo S-boxes of dimension 16×16 . These 9×9 pseudo S-boxes are transforming into byte based 65,536 vague random sequences by using the bijective maps σ . Thus we are able to get a huge figure of 8×8 S-boxes with their diversified strength.

The total number of unlike keys cast-off in the encryption or decryption process is called the key space. A sufficiently large key space ensures an efficient cryptosystem to

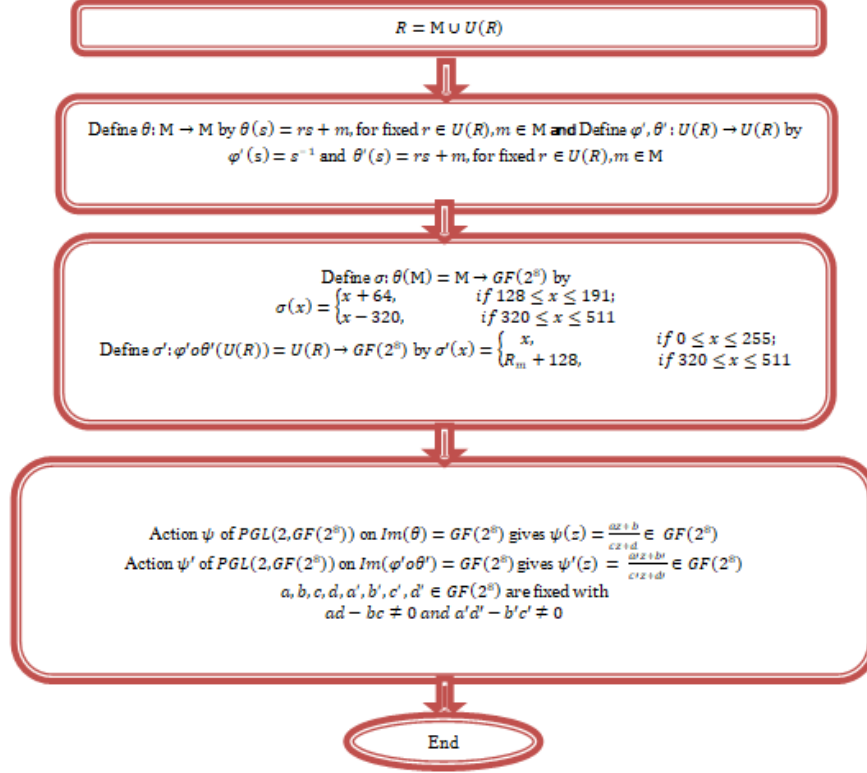


Figure 6.4: Flow chart for the generation of S-boxes pairs over the special LA-ring \mathcal{R}

repel brute-force attacks. In the first case of suggested algorithm, $256!$ Number of choices for affine function and from the action of $PGL(2, GF(2^8))$ on $\sigma(U(\mathcal{R})) = GF(2^8)$, we could design 16776960 number of S-boxes [17]. Though due to step 2 of the algorithm 256 choices for affine functions could be considered and thus $256 \times (16776960)$ will be the possible choices in computing 8×8 S-boxes. Consequently, considering all possibilities together, we have large enough key space to armor contrary to brute force attack.

6.2.3 Performance analysis of S-boxes

An efficient S-box should satisfy some specific cryptographic criteria; bijectiveness, non-linearity, outputs bit independence, strict avalanche and linear approximation probability. We gadget diverse analyses for the proposed S-box to test their strong suit and standing with respect to few other well-known S-boxes.

Nonlinearity

The nonlinearity of a Boolean function f is the measures of the gap between f and the collection of all affine linear functions. In other words, it indicates the count of bits in the truth table of f that are changed to approach the nearby affine function. The nonlinearity value (NL) [81] is its upper bound and is given by:

$$NL = 2^{n-1} - 2^{\frac{n}{2}-1}, \quad (6.2.3)$$

thus, the highest value of nonlinearity for $n = 8$, is 120. It is also observed from Table 6.20 that average nonlinearity of the suggested S-boxes 1 and 2 is 103.25 and 104.75 which are better than Prime S-box.

Strict Avalanche Criteria

Webster and Tavares [144] were the first to familiarize the SAC in 1985. The concepts of completeness and avalanche develop the SAC. It is satisfied if an alteration of a single bit of input causes output bits to change with a probability of 1/2. In other words, while single bit of input is altered, fifty percent of its respective output bits will change. It could be verified from Table 6.20 that the suggested S-box successfully satisfied SAC.

Bit Independent Criterion

Webster and Tavares [144] were the pioneers to introduce BIC. This is one more essential property for any cryptographic schemes. The outcomes of BIC analysis of the suggested S-box are presented in the Table 6.20. The suggested S-box holds adequate BIC in the sense of encryption strength. In Table 6.21, comparing the rank of our suggest S-box to S-boxes from literature, we noticed that the our S-box satisfied BIC close to the optimal value.

Linear Approximation Probability

The linear approximation probability is the highest value of the imbalance of an event. The parity of the input bits selected by the mask G_x is equal to the parity of the output bits selected by the mask G_y . Congruent to Matsui's original definition [94], linear approximation probability of a given S-box is given by:

$$LP = \max_{G_x, G_y \neq 0} \frac{|\{x \in X | x \cdot G_x = S(x) \cdot G_y\}|}{2^n} - \frac{1}{2}, \quad (6.2.4)$$

where G_x and G_y are input and output covers, respectively, ‘ X ’ the set of all possible inputs; and 2^n is the number of elements of X . It is evident from Table 6.20 that the average value of LP of the suggested S-boxes is 0.132813 that is strong enough against linear attacks and of better from Xyi S-box and S-box constructed on residue of prime numbers.

Differential Approximation Probability

The differential approximation probability (DP) of S-box is a measure for differential uniformity and is defined as:

$$DP(\Delta a \rightarrow \Delta b) = \frac{|\{a \in X | S(a) \oplus S(a \oplus \delta a) = \Delta b\}|}{2^m}. \quad (6.2.5)$$

This implies, an input differential Δa_i , should uniquely map to an output differential Δb_i , thus ensuring a uniform mapping probability for each i . The average value of differential approximation probability for proposed S-boxes are 0.140625 and (see Table 6.20), whereas the Table 6.21 shows the comparison of differential approximation probability of proposed S-box with AES, APA, Gray, S_8 AES, Skipjack, Xyi and residue prime S-boxes and we observed that the results of DP of proposed box are relatively better from skip jack Xyi S-box residue of prime and Lui S-boxes.

As there are 256×16776960 possible S-boxes depending on the choice of defined parameters, so after variety of options one can obtain the best S-boxes having optimal strength against statistical attacks.

6.2.4 RGB Image Encryption

The Arnold map is one the most important 2D Chaotic map [30, 31], specifically in image encryption algorithms. The following equation signifies the 2D Arnold caotic map. For x_i, y_i in the interval $[0, 1)$,

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \text{ mod } 1, \quad (6.2.6)$$

Of course, the determinant of the matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ on the right-hand side of equation 6.2.6 is 1. Thus the map is area preserving. The eigen values $\lambda_1 = \ln -(\frac{3+\sqrt{5}}{2})$ and

Analysis for S-box 1 and S-box 2	Max.	Min.	Average	Square Deviation	Differential approximation probability (DP)	Linear approximation probability (LP)
Nonlinearity	106 106	100 100	103.25 104.75			
SAC	0.625 0.59375	0.40625 0.375	0.504883 0.498047	0.0218748 0.0216392		
BIC		98 96	103.571 102.714	2.79577 3.08055		
BIC- SAC	0.476563 0.464844		0.500558 0.498535	0.0139369 0.0155518		
DP			0.0390625 0.0390625			
LP	164 160				0.140625	0.132813

Table 6.20: Performance Indexes for proposed S-box

$\lambda_2 = \ln -\left(\frac{3-\sqrt{5}}{2}\right)$ of the matrix A represents the two Lyapunov exponents. The positive Lyapunov exponent spectacles the chaotic behavior in equation 6.2.6 and hence its exponential sensitivity to its initial conditions is observed. In [31], the generalized form of equation 6.2.6 is given, i.e.,

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \text{ mod } 1. \quad (6.2.7)$$

Furthermore, the map of equation 6.2.7 is transformed to a 3D caotic map described as:

$$X_{i+1} = \begin{pmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} \text{ mod } 1. \quad (6.2.8)$$

Where the matrix A is answerable for producing chaotic behavior, here

$$A = \begin{pmatrix} 3 & 1 & 4 \\ 8 & 3 & 11 \\ 6 & 2 & 9 \end{pmatrix} \quad (6.2.9)$$

S-boxes	Nonlinearity	SAC	BIC-SAC	BIC	DP	LP
AES S-box	112	0.5058	0.504	112	0.0156	0.062
APA S-box	112	0.4987	0.499	112	0.0156	0.062
Gray S-box	112	0.5058	0.502	112	0.0156	0.062
Skipjack S-box	105.7	0.498	0.499	104.1	0.0468	0.109
Xyi S-box	105	0.5048	0.503	103.7	0.0468	0.156
Residue Prime	99.5	0.5012	0.502	101.7	0.281	0.132
LuiS-box	105	0.499756	0.500698	104.071	0.0390625	0.128906
Proposed S-box 1	103.25	0.504883	0.500558	103.571	0.0390625	0.140625
Proposed S-box 2	104.75	0.498047	0.498535	102.714	0.0390625	0.132813

Table 6.21: Comparison of Performance indices of suggested S-box

The general form of matrix A is

$$A = \begin{pmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y b_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{pmatrix} \quad (6.2.10)$$

In matrix A all $a_x, a_y, a_z, b_x, b_y, b_z$ are considered to be the positive integers. It is trivial to verify that matrix A is area preserving, that is $|A| = 1$. The Eigen values of A are $\lambda_1 = 14.3789$, $\lambda_2 = 0.4745$ and $\lambda_3 = 0.1466$. As the larger Eigen value is greater than 1, so equation 6.2.8 shows chaotic behavior and thus holds all the characteristics of chaos.

To generate the chaotic sequence X_{i+1} , the initial values used in this work are $x_0 = 0.9557$, $y_0 = 0.3494$ and $z_0 = 0.6789$.

S-boxes are considered as a main part of a block cipher, the only component of a cipher that produces non-linearity and hence guarantee the resistance against linear and differential attacks. Currently, by advancement in techniques of cryptanalysis and in computer technology, which enhances correspondingly support, generating S-boxes of good quality is the subject of core attention. Due to uncertainty in communication and in storage of RGB images, a need for the encryption is preferred. One of the basic aims of this work is to encrypt RGB images using 3 S-boxes originated by a non-associative structure of LA-ring. For the requirement of the RGB image encryption each layer is passed through the different 8×8 S-box. In the subsequent step, the 3D Arnold caotic map is functional not to correlate the adjacent pixel of the image. The procedure of this image encryption scheme

is illustrated below.

Following are the steps for encrypting the image:

Substitute the S-boxes S_1 , S_2 and S_3 in Red, Green and Blue channels of the color image. Thus, instead of a single S-box used for encryption our proposed scheme provides three different S-boxes S_1 , S_2 and S_3 . Use the 3D Arnold chaotic map to produce non-correlated behavior between adjacent pixels of the image.

Figure 6.5 is the flow chart of the proposed color image encryption.

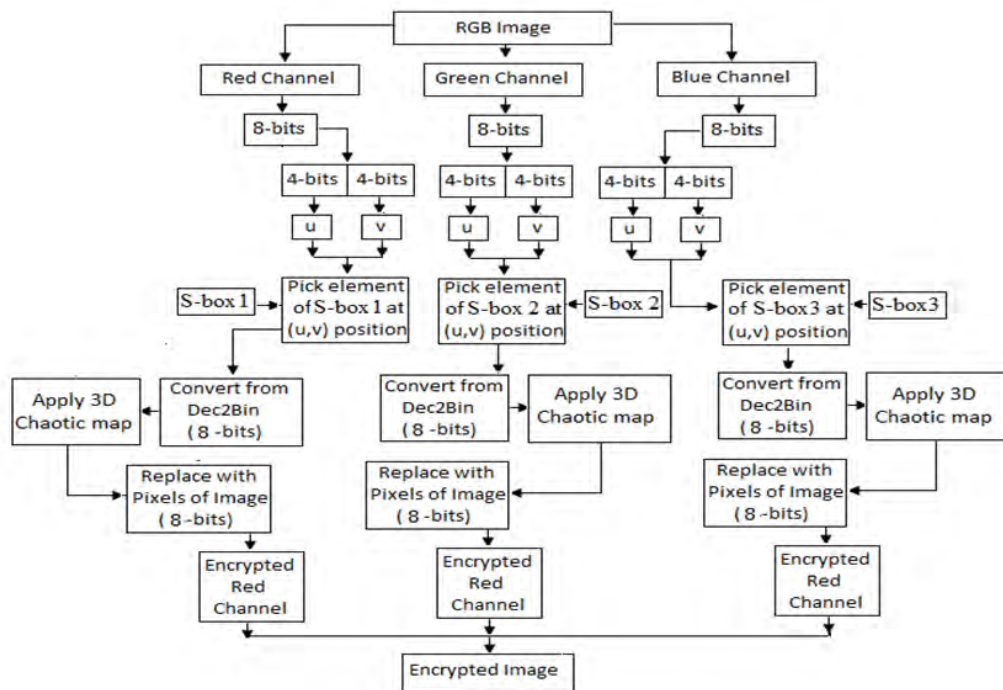


Figure 6.5: RGB image encryption scheme using S-boxes designed over LA-submodule and LA-group of units of \mathcal{R}

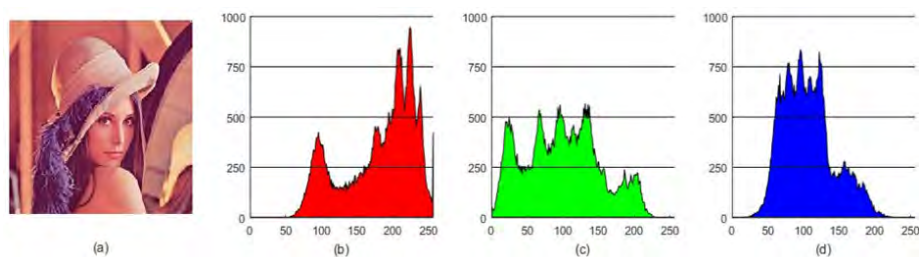


Figure 6.6: (a) Lena Original image. (b), (c) and (d) represent the histogram of red(R), green(G) and blue(B) layer of (a).

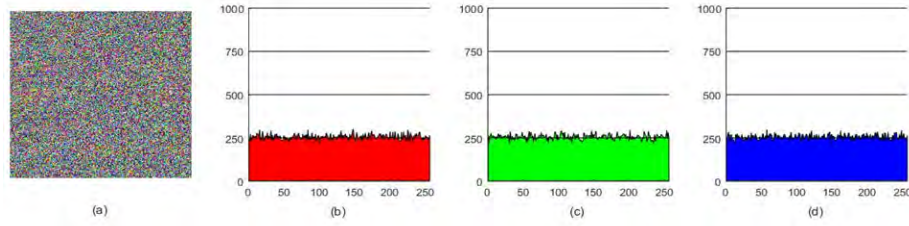


Figure 6.7: (a) Encrypted Lena image. (b), (c) and (d) show the histogram layers of R, G and B channel of the encrypted image (a).

6.2.5 Texture Analysis of Image Encryption

Texture is among the further most significant parameters of a material that enlightens the physical presentation of a material surface except its chromatic character. Texture may be analyzed in diverse approaches but Fourier methodology among these techniques is the most operative. A fascinating analysis, however, is intriguing as it relates to how the human visual system realizes the texture, the first line of the texture, and is extensively used in the segmentation of photograph. Over and done with this method we can calculate 5 diverse characteristics of image which are: Energy, Contrast, Entropy Homogeneity and Correlation to elucidate texture.

Energy

Energy analysis measures the energy an encrypted image that discards the gray-level co-occurrence matrix (GLCM), where energy is the sum of squared components in GLCM and is given by:

$$E = \sum_{m_1} \sum_{m_2} p^2(m_1, m_2), \quad (6.2.11)$$

where m_1 and m_2 are the image pixels. Note that for constant image the energy value is unity.

Entropy

The measure of level of disorder and randomness in a system is called its entropy. The maximal amount of randomness makes it difficult to recognize the image and the randomness of an image can be amplified by considering its non-linear components which is

defined as

$$H = \sum_{i=0}^n f(x_i) \log_b f(x_i), \quad (6.2.12)$$

where x_i defines the Histogram calculations.

Contrast

To differentiate the objects of an image, the observer has to contrast it is used. Owing to image encryption process, a robust encryption can be realized from the high level of contrast. This factor has a direct relation with the confusion created by the S-box. Mathematically, the formula for contrast is given by:

$$C = \sum_{m_1} \sum_{m_2} (m_1 - m_2)^2 f(m_1, m_2). \quad (6.2.13)$$

Homogeneity

The closeness of distributed pixels of Gray Level Co-occurrence Matrix (GLCM) to GLCM is measured in the Homogeneity analysis. It is also documented as gray tone spatial dependency matrix. Mathematically, the look for homogeneity analyses is represented by the equation:

$$H^* = \sum_{m_1} \sum_{m_2} \frac{f(m_1, m_2)}{1 - |m_1 - m_2|}. \quad (6.2.14)$$

Correlation

The purpose of correlation analysis is to analyze the adjacent pixel correlation of an image. Normally, three different types of analyses are carried out to ensure the strength of the encrypted image. These are: the horizontal, the vertical and the diagonal correlation. The following equation shows how to calculate the correlation:

$$K = \frac{(m_1 - \alpha m_1)(m_2 - \alpha m_2) f(m_1, m_2)}{\sigma_{m_1} \sigma_{m_2}}. \quad (6.2.15)$$

For a healthier correlation value we need to achieve the number 1 or -1. Whereas for uncorrelated data, this figure is round about 0. It can be observed from the results in Table 6.22 that the suggested encyphering algorithm has strong enough for a successful encryption. Table 6.23 signifies the entropy of 256×256 Lena color image. Obviously, the proposed encryption procedure displays opposition to all the well-known attacks. Analyses reveal that our proposed scheme has the entropy score close to the optimal values. In analogy,

	Original color components of image			Encrypted color components of image		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.445343	0.659896	0.483655	9.96034	10.0962	10.2181
Homogeneity	0.857543	0.831937	0.845328	0.411186	0.404886	0.403524
Entropy	7.27958	7.63153	6.98912	7.99712	7.99725	7.99744
Correlation	0.910667	0.887815	0.804591	0.0516558	0.0379861	0.0239547
Energy	0.135318	0.0838048	0.156122	0.0157684	0.0157087	0.0157107

Table 6.22: Second order texture analyses for original and encrypted Lena image

Images	Red	Green	Blue	RGB Image
Proposed	7.99712	7.99725	7.99744	7.999
Ref.[85]	7.9901	7.9898	7.9899	7.9899
Ref.[86]	7.9913	7.9914	7.9916	7.9914
Ref.[84]	7.9808	7.9811	7.9914	7.9844
Ref.[145]	7.9901	7.9912	7.9921	7.9113
Ref.[98]	7.9949	7.9953	7.9942	7.9948

Table 6.23: Entropy comparison for Lena (256×256) image

the comparison with chaos-based encryption scheme is also provided. Entropy of the proposed scheme is finer than the rest. In Table 6.24, the result for correlation coefficient of Lena 256×256 color image is presented. Results ensure the potency of the suggested encryption technique. The analyses suggest that the correlation results are up to the mark and can be matched with other chaos-based encryption techniques. Information images transmitting via digital communicating media have good similarity amongst their neighboring pixels. For an incredibly well-connected image the estimated correlation coefficient is ± 1 , while for an extra ordinary non-correlated image its values move toward 0. The pixels correlation among original and encrypted Lena image is displayed in Table 6.24. The correlation score shows that the pixels are good non-correlated as its value are more equally 0. Hence, the proposed algorithm gives extra ordinarily de connections the nearby pixels of the encrypted image and meet on hopes of an effective encryption structure.

Image	Horizontal			Vertical			Diagonal		
	R	G	B	R	G	B	R	G	B
Plain image	0.9491	0.9175	0.8561	0.9602	0.9528	0.8962	0.9025	0.8984	0.8715
Cipher image	0.0569	0.0658	-0.0014	0.0036	-0.0180	0.0132	-0.0499	0.0123	-0.0210

Table 6.24: Horizontal, Vertical and Diagonal Correlations among different layers of Plain and Cipher images

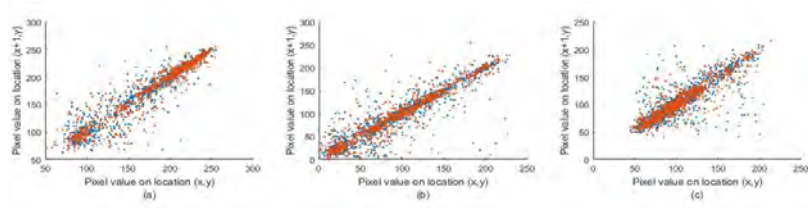


Figure 6.8: (a-c):represent Horizontal Correlation pixels for R, G and B layers of original 256×256 Lena image respectively

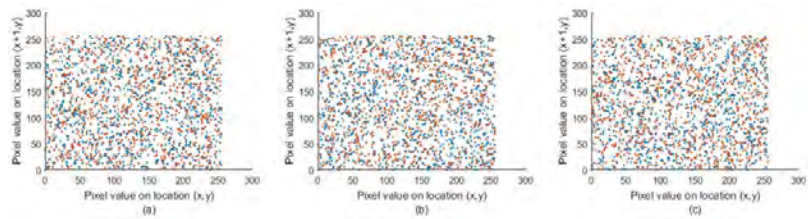


Figure 6.9: (a-c):shows the horizontal Correlation pixels for R, G and B layers of encrypted Lena image

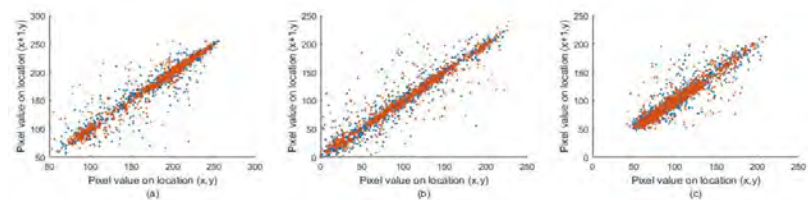


Figure 6.10: (a-c):represent vertical Correlation pixels for R, G and B layers of original 256×256 Lena image respectively

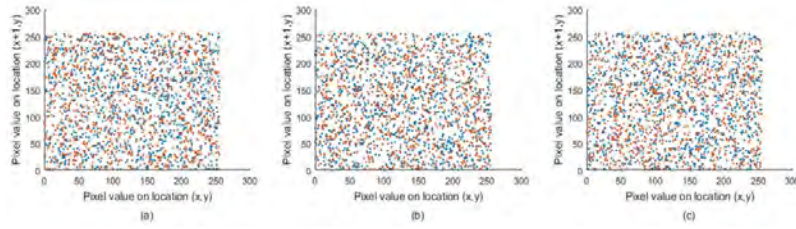


Figure 6.11: (a-c):shows the vertical Correlation pixels for R, G and B layers of encrypted Lena image

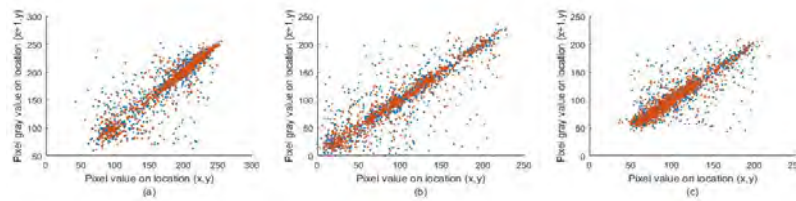


Figure 6.12: (a-c):represent diagonal Correlation pixels for R, G and B layers of original 256×256 Lena image respectively

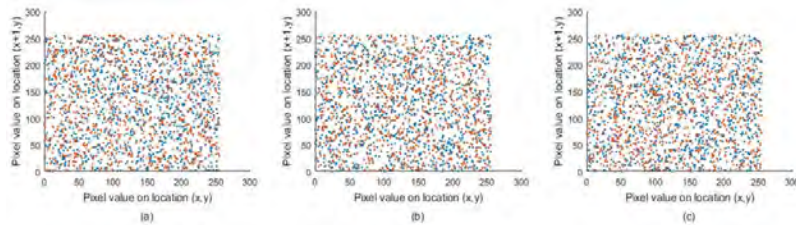


Figure 6.13: (a-c):shows the diagonal Correlation pixels for R, G and B layers of encrypted Lena image

Figure 6.8 to Figure 6.13 show the correlation distribution of horizontally, vertically and diagonally adjacent pixels of a color image. Figure 6.8, Figure 6.10, Figure 6.12 (a,b,c) signify the correlation of the adjacent pixels of Lena original image whereas Figure 6.9, Figure 6.11, Figure 6.13 (a,b,c) look from the nearby pixels of Lena encrypted image. Obviously, it is clear from the figures that there is a great dispassion between nearby pixels of the encrypted image which is intended to be one of the successes of the proposed scheme. The approving correlation coefficient is computed for Lena original and encrypted images and are shown in Table 6.24.

6.2.6 Analyses of Experimental Work

Now we give the experimental analyses of the suggested technique for image encryption. A standard $256 \times 256 \times 3$ Lena image is chosen for encryption as shown in Figure 6.6. Where Figure 6.7 represents the encrypted Lena image. Histogram of RGB layers of the original and encrypted image are also displayed in parallel. Table 6.25 enlists the image quality measures of the encrypted and original image using one round encryption by 3 S-boxes and 3D Arnold Cat map. The modest performance of the proposed notion is displayed in Table 6.25.

Mean Square Error (MSE)

The mean square error (MSE) or mean square deviation (MSD) of an image measures the common of the squares of the errors. This means the arithmetic mean square distinction between the calculable values and what's estimated. MSE is a risk function, comparable to the mean of the squared error loss. Followed [31], it judges the standard of an encrypted image. It is given by the formula:

$$MSE = \frac{1}{M_1 \times M_2} \sum_{y=1}^{M_1} \sum_{x=1}^{M_2} [P(x, y) - E(x, y)]^2, \quad (6.2.16)$$

where $P(x, y)$ and $E(x, y)$ are respectively the plain and encrypted images with respective dimensions M_1 and M_2 . A greater amount of MSE may be acknowledged as the better first-rate.

Peak Signal-To-Noise Ratio (PSNR)

Signal representation dependability can be affected by corrupting noise [68]. Thus the ratio of the power of a signal to the power of corrupting noise is designated as Peak signal-to-noise ratio (PSNR). It is expressed in terms of the logarithmic decibel gauge due to the diverse dynamic range of signals. Occasionally, the PSNR is used to evaluate the quality of restoration of the encrypted image. In this study, signal is characterized by original image and noise is the distortion created by encryption. The PSNR value is directly proportional to the rate of rebuilding of an image. It is defined as

$$PSNR = 10 \log_{10} \frac{MAX_1^2}{\sqrt{MSE}}. \quad (6.2.17)$$

Normalized Cross-Correlation (NK)

The correlation function also gives the idea that how much two digital images are closed to each other as shown in [139]. The normalized cross-correlation (NK) determines the resemblance amongst two images and is computed by:

$$NK = \sum_{y=1}^{M_1} \sum_{x=1}^{M_2} \frac{P(x, y) \times E(x, y)}{\sum_{y=1}^{M_1} \sum_{x=1}^{M_2} [P(x, y)]^2}, \quad (6.2.18)$$

where $P(x, y)$ is the original image, $E(x, y)$ is the encrypted version and M_1, M_2 are respectively the dimensions of the images.

Average Difference

The difference between reference signal and test image is given the name of Average difference (AD) [68]. AD is calculated by the formula:

$$AD = \frac{\sum_{y=1}^{M_1} \sum_{x=1}^{M_2} [P(x, y) - E(x, y)]}{M_1 \times M_2}, \quad (6.2.19)$$

where $P(x, y)$ is the original picture, $E(x, y)$ is the encrypted form and M_1, M_2 are the dimensions of the pictures.

Structural Content

One of the correlation based measure is the structural content (SC) [68] and it computes the resemblance among two images. SC is premeditated as

$$SC = \frac{\sum_{y=1}^{M_1} \sum_{x=1}^{M_2} [P(x, y)]^2}{\sum_{y=1}^{M_1} \sum_{x=1}^{M_2} [E(x, y)]^2}, \quad (6.2.20)$$

where $P(x, y)$ is the original image, $E(x, y)$ is the encrypted version and M_1, M_2 are respectively the dimensions of the images.

Maximum Difference (MD)

Scheming maximum of the error signals gives what we call maximum difference (MD) (difference between the test image and reference signal) (see [7]) and it is attained by

$$MD = \max -|P(x, y) - E(x, y)|, \quad (6.2.21)$$

where $P(x, y)$ is the original image, $E(x, y)$ is the encrypted version.

Normalized Absolute Error

By [98], the Normalized absolute error betwixt the original and encrypted image is computed as:

$$NAE = \frac{\sum_{y=1}^{M_1} \sum_{x=1}^{M_2} |P(x, y) - E(x, y)|}{\sum_{y=1}^{M_1} \sum_{x=1}^{M_2} |P(x, y)|}, \quad (6.2.22)$$

where $P(x, y)$ is the original image, $E(x, y)$ is the encrypted version and M_1, M_2 are the dimensions of the images.

Root Mean Square Error (RMSE)

RMSE is the square root of the mean of the square of all the errors [98]. The root-mean-square error (RMSE) is a regularly times used method to measure the variations between original image and the cipher image.

$$RMSE = \sqrt{\frac{\sum_{y=1}^{M_1} \sum_{x=1}^{M_2} [P(x, y) - E(x, y)]^2}{M_1 \times M_2}}, \quad (6.2.23)$$

where $P(x, y)$ represents the original image, $E(x, y)$ is the encrypted version and M_1, M_2 are respectively the dimensions of the images.

Universal Quality Index (UQI)

According to [140], the UQI breaks the comparison between original and distorted image into three comparisons: Contrast, luminance and structural comparisons. The UQI for original image ‘ P ’ and encrypted image ‘ E ’ might be defined as:

$$UQI(P, E) = \frac{4\mu_P\mu_E\mu_{PE}}{(\mu_P^2 - \mu_E^2)(\sigma_P^2 - \sigma_E^2)}, \quad (6.2.24)$$

where μ_P, μ_E represent the mean values of original and distorted images and σ_P, σ_E denote the standard deviation of plain and distorted images.

Mutual Information (MI)

To obtain the amount of information from encrypted image for the agreeing plain image is termed as mutual information given in [140]. The mutual information of two images ‘ P ’ and ‘ E ’ can be defined as:

$$MI(P, E) = \sum_{y \in E} \sum_{y \in P} p(x, y) \log_2 \frac{p(x, y)}{p(x)p(y)}, \quad (6.2.25)$$

where $p(x, y)$ is the joint probability function of P and E , further $p(x)$ and $p(y)$ are the marginal probability distribution functions of P and E respectively.

Structural Similarity (SSIM)

By [146], the structural similarity index is an enhanced edition of the universal quality index. Through this technique we determine the similarity between two images. The structural similarity index is calculated on various frames of an image. The measure between two frames X and Y of common size $M \times M$ is:

$$SSIM(X, Y) = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_X\sigma_Y + c_2)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)}, \quad (6.2.26)$$

where average of Y and X is represented by μ_Y and μ_X the variance of Y and X by σ_Y^2 and σ_X^2 respectively. Whereas σ_{XY} is the covariance of X and Y , $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are the variables to soothe the division with weak denominator. L is the range of the pixel values and $(k_1, k_2) = (0.01, 0.03)$ by default. The SSIM index lies between -1 and 1 . For similar images this value is 1 .

Quality measure	Encryption by 3 S-boxes and 3D Arnold chaotic map			Optimal values		
	Red	Blue	Green	Red	Blue	Green
MSE	10626.4	9224.93	bf 7162.78	10057.2	9898.89	6948.19
PSNR	7.86695	8.48117	9.57999	8.106	8.1749	9.712
NCC	0.66015	0.993966	1.09709	0.6725	1.0031	1.0923
AD	52.1404	-28.6657	-22.7034	50.0448	-31.4276	-19.7989
SC	1.59967	0.582213	0.562247	1.5787	0.5582	0.5711
MD	250	234	216	236	210	210
NAE	0.467414	0.796259	0.671177	0.4537	0.831	0.6628
RMSE	103.084	96.0465	84.6332	100.286	99.4932	83.3558
UQI	-0.00013497	-0.000714523	-0.0011433	-0.005	-0.0077	0.0107
MI	0.491086	0.689748	0.394636	5.6534	7.2283	6.0723
SSIM	0.00982045	0.0084672	0.00937046	0.0078	0.0053	0.0187

Table 6.25: Image Quality Measures for proposed RGB Image Encryption of Lena image

Table 6.25 shows that through our proposed RGB image encryption scheme the optimal values of Image Quality Measures can be achieved.

6.2.7 Security Measurement

Histograms

A uniform histogram for an image is the calmest and supreme approach to measure the security strength of an encryption procedure against various attacks. Here, we analyze an RGB Lena image of size $256 \times 256 \times 3$. The histogram of the three channels of ciphered image under the proposed scheme is likewise matching though for plain Lena image they are dissimilar. Figure 6.6 and Figure 6.7 show histograms of different layers of plain image and encrypted image respectively. A perfect encrypted image comprises of uniform histogram trickles to sphere the opposing of separating any supportive data from the rocky histogram. Subsequently, no statistical attack can die out this proposed encryption scheme.

Differential Analyses

To exploit the strong suit of differential analyses on an image encryption arrangement the NPCR (Number of Pixels Change Rate) and UACI (unified average changing intensity) analyses are implemented. It measures the normal power of contrast between the two images i.e. original and encrypted image. To compare the encrypted images cryptanalysts realize the bond among the plain image and ciphered image. Attack of this kind is famous for differential attack. The NPCR and UACI are the two typically used tests to ensure the strength of the encrypted scheme against differential analysis. For more details, see [62, 140, 146].

- **Number of Pixels Change Rate (NPCR)** From [146], the impact of single pixel change on the entire image ciphered using the suggested algorithm has been verified by NPCR. It computes the number of pixels change rate of encrypted image when a single pixel of the plain image is changed. Take an encrypted image " Img_1 " of dimension $M_1 \times M_2$, whose respective plain image " Img_2 " has difference of only one-pixel. The NPCR of these two images is defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M_1 \times M_2}, \quad (6.2.27)$$

where

$$D(i,j) = \begin{cases} 0, & \text{if } Img_1(i,j) = Img_2(i,j); \\ 1, & \text{if } Img_1(i,j) \neq Img_2(i,j). \end{cases} \quad (6.2.28)$$

- **Unified Average Changing Intensity (UACI)** By [146], the unified average changing intensity of the given two (plain and ciphered) images estimates the average intensity of the images. Take two enciphered images Img_1 and Img_2 of dimension $M_1 \times M_2$. The UACI is defined by:

$$UACI = \frac{1}{M_1 \times M_2} \sum_{i,j} \left[\frac{|Img_1(i,j) - Img_2(i,j)|}{255} \right]. \quad (6.2.29)$$

Schemes	NPCR			UACI		
	Red	Blue	Green	Red	Blue	Green
Proposed	0.995819	0.9961	0.995926	0.339945	0.338623	0.336869
Ref. [28]	0.996	99.5895	0.9961	0.3343	0.335	0.3343
Ref. [32]	0.9964	0.9962	0.9959	0.3353	0.3327	0.3343
Ref. [37]	0.9468	0.9568	0.9868	0.3346	0.345	0.3549
Ref. [38]	0.985	0.985	0.985	0.321	0.321	0.321
Ref. [39]	0.996	0.9963	0.9959	0.3343	0.3346	0.3347

Table 6.26: Comparing Differential analyses Proposed Image Encryption scheme and existing encryption schemes for 256×256 Lena image

Table 6.26 gives the NPCR and UACI measures of different channels of the color Lena encrypted image. The comparison is taken with encryption schemes based on Chaos and S-box. It verifies the robustness of the suggested Image encryption scheme via S-boxes 1, 2 and 3. Clearly, analyses show that the NPCR and UACI values of our novel encryption technique give optimal values.

6.2.8 Randomness of Test for Cipher

The security strength of a cryptosystem is judged on the basis of some important properties such as: uniform distribution, Long period and high complexity of the output. By a definitive objective to attain such prerequisites, we used NIST SP 800-22 [105] to test the randomness of digital images. A portion of these tests counts in copious subclasses. The distorted Lena digital image is cast-off to clasp all NIST tests. The encrypted data is produced by the proposed RGB image encryption scheme of a colored Lena plain image of dimension $256 \times 256 \times 3$ and 3D a chaotic map. Table 6.27 displays the outcomes of the tests.

Noticeably our suggested digital image encryption tool proficiently passes the NIST tests. Thus, as a result of proficient outcomes, the designed random cryptosystem used for RGB Image encryption constructed via S-boxes from a non-commutative and non-associative finite ring and 3D chaotic map might be professed that are very irregular in its crop.

Test			P - values for color encryptions			Results
Red	Green	Blue	of ciphered image			
Frequency			0.32694	0.80028	0.82481	Pass
Block frequency			0.74131	0.54713	0.97235	Pass
Rank			0.29191	0.29191	0.29191	Pass
Runs (M=10,000)			0.084845	0.09393	0.52759	Pass
Long runs of ones			0.67514	0.7127	0.7127	Pass
Overlapping templates			0.85988	0.85988	0.85988	Pass
No overlapping templates			1	0.9994	0.24017	Pass
Spectral DFT			0.77167	0.56166	0.38399	Pass
Approximate entropy			0.84462	0.85692	0.11867	Pass
Universal			0.99437	0.99976	0.99498	Pass
Serial		p values 1	0.0083409	0.13423	0.34362	Pass
Serial		p values 2	0.12342	0.5943	0.15727	Pass
Cumulative sums forward			0.14445	0.24644	0.24227	Pass
Cumulative sums reverse			0.89099	1.16	0.79042	Pass
Random excursions		X = -4	0.79553	0.98021	0.66539	Pass
		X = -3	0.37236	0.88823	0.16569	Pass
		X = -2	0.57859	0.9465	0.41097	Pass
		X = -1	0.22905	0.9464	0.78375	Pass
		X = 1	0.48349	0.8282	0.44466	Pass
		X = 2	0.13673	0.32154	0.33772	Pass
		X = 3	0.6194	0.020103	0.39284	Pass
		X = 4	0.70227	0.34143	0.62245	Pass
Random excursions variants		X = -5	0.39287	0.0016344	0.46138	Pass
		X = -4	0.66407	0.026809	0.59298	Pass
		X = -3	0.96847	0.12819	0.52709	Pass
		X = -2	0.44399	0.10171	0.91871	Pass
		X = -1	0.33092	0.18588	0.92957	Pass
		X = 1	0.65853	1	0.25054	Pass
		X = 2	0.54029	1	0.30743	Pass
		X = 3	0.81252	0.6726	0.40648	Pass
		X = 4	0.50404	0.31731	0.59298	Pass
		X = 5	1	0.37782	0.76828	Pass

Table 6.27: NIST test results for proposed encrypted image

Chapter 7

Conclusions

This thesis is a compilation of three phases of research work. The first phase comprises of a detailed survey on the developments in the class of non-associative rings known as LA-rings to date and it is included in chapter 2. The second phase focuses on the contributions of our work to the developments in classical LA-ring theory and application of soft set theory to LA-rings. These conceptual ideas are elaborated in chapter 3 and 4. In our third phase, we dealt with the applications of LA-ring theory to coding theory and cryptography and these applications are given in chapters 5 and 6.

A left almost rings (acronym for LA-ring), is in real a generalization of commutative ring. In spite of the reality that this structure is non-associative and non-commutative, it entails properties which usually are valid in associative and commutative algebraic structures. To have a comprehensive study of LA-rings we direct our readers to see [58, 110, 125, 128, 132, 134].

In the first phase of our study, we performed a survey on the maximum work done on LA-rings and their generalizations to date and it is a source of inspiration and motivation for the researchers to make advancements in the development of LA-ring theory. It is observed that, LA-ring theory develops parallel to the commutative ring theory. Although many concepts for commutative rings are generalized for LA-rings, using good techniques, but still there is a lot to dig out. This motivated us to get into our next phase, that is to explore this class of non-associative rings in detail and to find its applications in different areas. During our literature survey, we found the definition of a special LA-ring which is an LA-ring satisfying the definition of an additive abelian group. We made a comparison of LA-rings and special LA-rings and provided several criterion for an LA-ring to

become a special LA-ring. To work further in this area, different examples of LA-rings were required, but we observed that the softwares used by the researchers to find examples are slow and they exhaust after a certain order. This compelled us to construct an algorithm, which generated higher order extensions of LA-rings and special LA-rings. We also constructed LA-semigroup ring as a generalization of a commutative semigroup ring. The newly formed structure carries many properties of LA-semigroup as well as a commutative associative ring.

The study of the concept of divisibility was previously restricted to commutative and associative rings only. We introduced this idea for LA-rings and defined the notions of prime elements, irreducible elements, prime and maximal left ideals etc. Many results regarding these concepts were subject to the constraint of idempotency that holds in special LA-rings but not in LA-rings. Furthermore, we established polynomial formation over a special LA-ring. Our main goal was to define LA-field extension but it was partially achieved due to requirement of a weak associativity. Since field extension theory is based on irreducible polynomials, it was mandatory to study factorization of polynomials over special LA-rings. But due to non associativity and non-commutativity of LA-rings, the factorization of such polynomial was not that smooth. We proved Division algorithm, Remainder theorem and Factorization theorem for this case, which have little similarity to their classical versions. We also included the definition of Euclidean LA-domain.

Molodtsov [97], was the pioneer of the classical soft set theory. Soft set theory is a relatively new approach to handle uncertainties. A soft set is a collection of approximate description of an object. Applications of soft set theory to algebraic structures grabbed the interest of many researchers throughout the world. Following Molodtsov's definition for soft sets, Shah et al. [130] introduced the basic notions of soft LA-rings, which are actually a parameterized family of sub LA-rings of an LA-ring, over an LA-ring. Çağman and Enginoğlu [28] used a more practical approach and redefined the soft sets along with their operations. Using their definitions, we redefined soft LA-rings and worked for some more developments in soft LA-ring theory. Rough soft sets defined in [153], are based on upper and lower approximations of soft sets with respect to some equivalence relation. Since it's not always possible to define an equivalence relation on a set, we approximated soft sets using a set valued mapping T and introduced T -rough soft sets. Since a set valued map gives rise to an equivalence relation, T -rough soft sets are generalizations of the

existing rough soft sets. T-rough soft set theory is a new useful tool for the solution of many problems that contain uncertainties and vagueness. In particular, we constructed a decision making algorithm based on T-rough soft sets. Getting back to our goal, we defined T-rough LA-rings and T-rough soft LA-rings and studied the properties of their ideals using set valued and strong set valued homomorphisms. Further we established idealistic T-rough soft LA-rings (idealistic TRS-LA-rings), T-rough soft M-systems (TRS-M-systems) and T-rough soft P-systems (TRS-P-systems) in T-rough soft LA-rings (TRS-LA-rings). The article "Soft Int-Rings and its Algebraic Applications" by Çitak and Çağman, [32] published in the "Journal of fuzzy and intelligent systems" in the year 2015, motivated us to present the idea of soft intersection LA-rings (SI-LA-rings). This new notion is very practical for obtaining results by means of LA-rings. We introduced the notions of soft intersection sub LA-rings and soft intersection ideals of an LA-ring. We constructed SI-special LA-rings using SI-LA-semigroups [118] and SI-rings (associative) [32].

The third phase of our research comprises of applications of LA-rings in the field of coding theory and cryptography. Coding was previously restricted to associative algebraic structures only. The construction of Codes over finite (associative) fields motivated us to establish codes over finite LA-fields. We studied Linear cyclic codes over special LA-fields which are in fact special LA-vector spaces. We formulated an algorithm for the construction of reversible complement cyclic codes of odd lengths over a special LA-field F_{SLA_4} of order 4. This technique doesn't take much time and generates a set of codewords which are not likely to make undesired bonds with one another during the process of hybridization. The inspiration behind this codes construction was taken from an article "Construction of Cyclic Codes over $GF(4)$ for DNA Computing," published in Journal of Franklin Institute, 2006. In this article, T. Abualrub et al. [1] constructed the reversible complement cyclic codes over F_{LA_4} with odd lengths over $GF(4)$.

An S-box is the main component of the symmetric key cryptosystem. We designed S-boxes over special LA-rings, while classically, the most S-boxes were constructed over commutative and associative structures of Galois field and local rings. The main resolution of these S-boxes designing was to increase the resilience due to non-associative and non-commutative conduct of special LA-rings. We constructed small S-boxes over a special LA-field having order 16. The image encryption capacity of these newly constructed S-boxes was judged through the MLC. In literature, differential cryptanalysis is just ap-

plied on binary Galois field extensions. However, we shift it on S-boxes designed over a special LA-field of order 16. The difference distribution tables have exhibited differential probability which is better than that of the S-boxes depending on the 16 order Galois field. A watermarking application of these S-boxes has been specified to go in conjunction with their comparison in the framework. Furthermore, we constructed S-boxes through a special LA-ring having order 512. The purpose of these S-boxes designing was to produce 256 times more 8×8 S-boxes created through linear fractional transformations having excellent robustness. This study provides $256 \times (16776960)$ choices in constructing 8×8 S-boxes of diverse strength. Thus, uniting all the possible cases, we get a sufficiently large key space to guard brute force attack. A new color image encryption usage is estimated in which firstly these 3 S-boxes were used in producing confusion in each layer of a standard RGB color image. Nevertheless, for the purpose of diffusion 3D Arnold chaotic map is utilized in the newly introduced encryption scheme. A comparison with some of existing chaos and S-box dependent color image encryption schemes were given and the performance outcomes of the estimated RGB image encryption and noted as approaching the standard main level.

Future work

The future prospects relating this study hold a lot of void still to be filled. Some areas are listed hereunder.

1. Construction of LA-field extension free of constraints.
2. Investigation of the generalized rough soft ideal structure in the generalized soft LA-rings and generalized rough soft LA-modules.
3. Defining SI-Quasi ideals, SI-Bi-ideals and SI-Interior ideals. Further different applications of soft intersection like α -inclusion and soft intersection product can be studied for SI-LA-rings.
4. The approach that we used for the construction of DNA codes over F_{SLA_4} can be applied to similar LA-rings.
5. Our search was restricted to the case of odd length for the sake of computational

convenience. Conducting a search for even lengths is promising to yeild more new codes over F_{SLA4} .

6. Due to the most usefulness of light weight cryptography, our small S-boxes could replace the position of small S-boxes used in Mini AES.
7. A successful development in constructing 256 elements LA-field will be more helpful in designing 8×8 S-boxes over it.

Bibliography

- [1] T. Abualrub, A. Ghrayeb and X.N. Zeng, “Construction of Cyclic Codes over $GF(4)$ for DNA Computing,” *J. Franklin Inst.*, Vol. 343, pp. 448–457, 2006.
- [2] T. Abualrub and R. Oehmke, “On the Generators of \mathbb{Z}_4 Cyclic Codes of Length 2^e ,” *IEEE Trans. Inf. Theory*, Vol. 49, No. 9, pp. 2126–2133, 2003.
- [3] U. Acar, F. Koyuncu and Tanay, B., “Soft Set and Soft Rings,” *Comput. Math. Appl.*, Vol. 59, No. 11, pp. 3458–3463, 2010.
- [4] C. Adams, S. Tavares, “Good S-boxes are Easy to Find,” In: *Adv. Cryptol. Proc. CRYPTO-89, Lect. Notes Comput. Sci.*, Springer, NY, USA, pp. 612–615, 1989.
- [5] L. Adleman, “Molecular Computation of the Solution to Combinatorial Problems,” *Sci.*, Vol. 266, pp. 1021–1024, 1994.
- [6] M.H. Ahmed, “LA-Noetherian in a Generalized LA-ring”, *Int. J. Math. Trends Tech.*, Vol. 49, pp. 285–290, 2017.
- [7] M.E. Ahmet and S.F. Paul, Image Quality Measures and their Performance. *IEEE Trans. Commun.*, Vol. 43, pp. 2959—2965, 1995.
- [8] M. Akram and F. Feng, “Soft Intersection Lie Algebras,” *Quasigroups and Related Systems*, Vol. 21, pp. 11–18, 2013.
- [9] H. Aktaş, and N. Çağman, “Soft Set and Soft groups,” *Inform. Sci.* Vol. 177, No 13, pp. 2726–2735, 2007.
- [10] A.A. Albert, “Quasigroups I”, *Trans. Amer. Math. Soc.*, Vol. 54, pp. 507–519, 1943.
- [11] A.A. Albert, “Quasigroups II”, *Trans. Amer. Math. Soc.*, Vol. 55, pp. 401–409, 1944.

- [12] A.M. Alghamdi and F. Sahraoui, “Tensor Product of LA-modules,” *Int. Math. Forum*, Vol. 9, pp. 1309–1319, 2014.
- [13] M.I. Ali, B. Davvaz and M. Shabir, “Some Properties of Generalized Rough Sets,” *Inform. Sci.*, Vol. 224, pp. 170–179, 2013.
- [14] M.I. Ali, F. Feng, X. Liu, W.K. Min and M. Shabir, “On Some New Operations in Soft Set Theory,” *Comput. Math. Appl.*, Vol. 57, pp. 1547–1553, 2009.
- [15] K.M. Ali and M. Khan, “Application based construction and optimization of substitution boxes over 2D mixed chaotic maps,” *Int. J. Theor. Phys.*, Vol. 58, No. 9, pp. 3091–3117, 2019.
- [16] M.I. Ali, M. Shabir and M. Naz, “Algebraic Structures of Soft Sets Associated with New Operations,” *Comput. Math. Appl.*, Vol. 61 No. 9, pp. 2647–2654, 2011.
- [17] A. Altaleb, S.M. Saeed, I. Hussain and M. Aslam, “An Algorithm for the Construction of Substitution Boxes for Block Ciphers Based on Projective General Linear Group,” *AIP Adv.*, 2017, Vol. 710.1063/1.4978264.
- [18] M. Aslam, M. Shabir, and A. Mehmood, “Some Studies in Soft LA-Semigroups,” *J. Adv. Research Pure Math.*, Vol. 3, No. 4, pp. 128–150, 2011.
- [19] K.V. Babitha, and J.J. Sunil, “Soft Set Relations and Functions,” *Comput. Math. Appl.*, Vol. 60, No. 7, pp. 1840–1849, 2010.
- [20] A. Bayram, E.S. Oztas and I. Siap, “Codes over $F_4 + vF_4$ and Some DNA applications,” *Des. Codes Cryptogr.*, Vol. 80, pp. 379–393, 2016.
- [21] N. Bennenni, K. Guenda and S. Mesnager, “New DNA Cyclic Codes over Rings,” *Adv. Math. Commun.*, Vol. 11, No. 1, 2015.
- [22] E. Biham and A. Shamir, “Differential Cryptanalysis of DES like Cryptosystems,” *J. Cryptology*, 4 No. 1, pp. 3–72, 1991.
- [23] R.H. Bruck, “Some Results in the Theory of Quasigroups,” *Trans. Amer. Math. Soc.*, Vol. 56, pp. 19–52, 1944.

- [24] R.H. Bruck, “Some Results in the Theory of Linear Non-Associative algebras, *Trans. Amer. Math. Soc.*, Vol. 56, pp. 414–199, 1944.
- [25] R.H. Bruck, “Contributions to the Theory of Loops,” *Trans. Amer. Math. Soc.*, Vol. 60, pp. 245–354, 1946.
- [26] D.M. Burton, “A First Course in Rings and Ideals,” *Adison-Wesely Publishing Co.*, pp. 121–122, 1970.
- [27] N. Çağman, F. Çitak and H. Aktaş, “Soft Int-group and its Applications to Group Theory,” *Neural Comput. Applic.* Vol. 21, (Suppl 1): pp. S151–S158, 2012.
- [28] N. Çağman and S. Enginoğlu, “Soft Set Theory and Uni-int-Decision Making,” *Eur. J. Oper. Res.* Vol. 207, pp. 848–855, 2010.
- [29] N. Çağman and S. Enginoğlu, “Soft Matrix Theory and its Decision making,” *Comput. Math. Appl.*, Vol. 59, No. 10, pp. 3308–3314, 2010.
- [30] G. Chen and X. Dong, “From Chaos to Order: Methodologies, Perspectives and Applications,” *Singapore: World Scientific*, 1998.
- [31] G. Chen, Y. Mao and C. Chui, “A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps,” *Chaos Solitons Fract*, Vol. 21, pp. 749-761, 2004.
- [32] F. Çitak and N. Çağman, “Soft Int-Rings and its Algebraic Aapplications,” *J. Intell. Fuzzy Systems*, Vol. 28, No. 3, pp. 1225–1233, 2015.
- [33] I. Couso and D. Dubois, “Rough Set, Coverings and Incomplete Information,” *Fundam. Inform.*, Vol. 108, pp. 223–247, 2011.
- [34] L. Cui and Y. Cao, “A new S-box structure named Affine-Power-Affine,” *Int. J. Innov. Comput. Inform. Control*, Vol.3, No. 3, pp. 751-759, 2007.
- [35] T.W. Cusick and P. Stanica, “Cryptographic Boolean functions and applications,” Elsevier/Academic Press, Amsterdam, 2009.
- [36] J. Daemen and V. Rijmen, “The design of Rijndael-AES: the advanced encryption standard.,” Springer, Berlin, 2002.

- [37] B. Davvaz, "A Short Note on Algebraic T-rough Sets," *Inform. Sci.*, Vol. 178, No. 16, pp. 3247–3252, 2008.
- [38] A. Dertli and Y. Cengellenmis, "On the Cyclic DNA Codes over the Finite Rings $\mathbb{Z}_4 + w\mathbb{Z}_4$ and $\mathbb{Z}_4 + w\mathbb{Z}_4 + v\mathbb{Z}_4 + wv\mathbb{Z}_4$," *Biomath*, DOI: 10.11145/j.biomath.2017.12.167.
- [39] D.E. Dobbs, "The Remainder Theorem and Factor Theorem for Polynomials over Noncommutative Coefficient Rings," *Int. J. Math. Edu. Sci. Tech.* Vol. 38, No. 2, pp. 268–273, 2007.
- [40] R. Dubisch and S. Perlis, "On the Radical of a Non-Associative Algebra," *Amer. J. Math.*, Vol. 70, pp. 540–546, 1948.
- [41] D. Dubois and H. Prade, "Rough Fuzzy Sets and Fuzzy Rough Sets," *Int. J. Gen. Syst.*, Vol. 17, No. 2, pp. 191–209, 1990.
- [42] A.K. Farhan, N.M.G. Al-Saidi, A.T. Maolood and F. Nazarimehr, "Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder," *Entropy*, Vol. 21, doi:10.3390/e21100958, 2019.
- [43] B. Feng, S.S. Bai, B.Y. Chen and X.N. Zohu, "The Constructions of DNA Codes from Linear Self-dual Codes over \mathbb{Z}_4 ," *International Conference on Computer information systems and industrial applications*, CISIA, 2015.
- [44] F. Feng, Y.B. Jun, X. Liu and L. Li, "An Adjustable Approach to Fuzzy Soft Set Based Decision Making," *J. Comput. Appl. Math.*, Vol. 234, No. 1, pp. 10–20, 2010.
- [45] F. Feng, Y.B. Jun and X. Zhao, "Soft Semirings," *Comput. Math. Appl.*, Vol. 56 No. 10, pp. 2621–2628, 2008.
- [46] F. Feng, C. Li, B. Davvaz and M.I. Ali, "Soft Sets Combined with Fuzzy Sets and Rough Sets: A Tentative Approach," *Soft Comput.*, Vol. 14, No. 9, pp. 899–911, 2010.
- [47] P. Gaborit and O.D. King, "Linear Constructions for DNA Codes," *Comput. Sci.*, Vol. 334, No. 1, pp. 99–113, 2005.
- [48] T. Gaketem, "Quasi-ideals of a p-regular Near Left Almost Rings," *Int. J. Pure Appl. Math.*, Vol. 87, pp. 219–227, 2013.

- [49] T. Gaketem, “Some Applications of Prime Ideals of AG-rings,” *Int. J. Pure Appl. Math.*, Vol. 97, pp. 195–200, 2014.
- [50] A.D.A. Gemellia and S. Indarjani, “Differential Attack on Mini AES,” *The 5th International Conference on Reaserch and Education in Mathematics*, 2012.
- [51] J. Ghosh and T.K. Samanta, “Rough Soft Sets and Rough Soft Groups,” *J. of Hyperstructures*, Vol. 2, No. 1, pp. 18–29, 2013.
- [52] R. Gilmer, “Commutative Semigroup Rings,” The University of Chicago Press, Chicago 1984.
- [53] K. Guenda and T.A. Gulliver, “Construction of Cyclic Codes over $F_2 + uF_2$ for DNA cComputing,” *AAECC*, Vol. 24, No. 6, pp. 445–459, 2013.
- [54] H.M. Heys, “A Tutorial on Linear and Differential Cryptanalysis,” *Electrical and Computer Engineering Faculty of Engineering and Applied Science Memorial University of Newfoundland*.
- [55] F. Hussain and S. Firdous, “Direct Product of Left Almost Rings,” *Int. J. Sci. Basic Appl. Research*, Vol. 28, pp. 113–127, 2016.
- [56] F. Hussain, S. Firdous and N. Sadiq, “Congruences on Near Left Almost Rings,” *Appl. Math. Inform. Sci. Letters*, Vol. 6, No. 2, pp. 69–74, 2018).
- [57] F. Hussain, Z. Jadoon, S. Abdullah and N. Sadiq, “Some Properties of Near Left Almost Rings by using Ideals,” *Italian J. Pure Appl. Math.*, Vol. 38, pp. 390–401, 2017.
- [58] F. Hussain and W. Khan, “Congruences on Left Almost Rings,” *Int. J. Algebra Stats.*, Vol. 4, pp. 1–6, 2015.
- [59] F. Hussain, W. Khan, M.S. Khan and S. Abdullah, “Quasi and Bi Ideals in Left Almost Rings,” *Honam Mathematical J.*, Vol. 41, No. 3, pp. 449–461, 2019.
- [60] F. Hussain, M.S.A. Khan, K. Rahman and M. Khan, “Congruences and External Direct Sum of LA-Modules,” *Indain J. Sci. Tech.*, DOI: 10.17485/ijst/2015/v8i28/54260.

- [61] I. Hussain and T. Shah, “Literature Survey on Nonlinear Components and Chaotic Nonlinear Components of Block Cipher,” *Nonlinear dyn.*, Vol. 74, pp. 869-904, 2013.
- [62] I. Hussain, T. Shah and M.A. Gondal, “Image Encryption Algorithm Based on $PGL(2, GF(2^8))$ S-boxes and TD-ERCS Chaotic Sequence” *Nonlinear Dyn.*, Vol. 70, pp. 181-187, 2012.
- [63] I. Hussain, T. Shah and M. A. Gondal, “A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm,” *Nonlinear Dynamics*, Vol. 70, No. 3, pp. 1791-1794, 2012.
- [64] I. Hussain, T. Shah, M.A. Gondal and H. Mahmood, “Generalized Majority Logic Criterion to Analyze the Statistical Strength of S-boxes, *Z. Naturforsch*, Vol. 67, No. 5, pp. 282—288, 2012.
- [65] I. Hussain, T. Shah, M. A. Gondal and H. Mahmood, “An efficient approach for the construction of LFT s-boxes using chaotic logistic map,” *Nonlinear Dynamics*, Vol. 71, No. 1, pp. 133-140, 2013.
- [66] I. Hussain, T. Shah and H. Mahmood, “A Group Theoretic Approach to Construct Cryptographically Strong Substitution Boxes,” *Neural Comput. Appl.*, doi:10.1007/s00521-012-0914-5, 2012.
- [67] I. Hussain, T. Shah, H. Mahmood, M.A. Gondal and U.Y. Bhatti, “Some Analysis of S-box Based on Residue of Prime number,” *Proc. Pak. Acad. Sci.*, Vol. 48 No. 2, pp. 111-115, 2011.
- [68] Q. Huynh-Thu, M. Ghanbari, “Scope of Validity of PSNR in Image/Video Quality Assessment,” *Electron. Lett.*, Vol. 44, pp. 800–801, 2008.
- [69] N. Jacobson, “Cayley Numbers and Normal Simple Lie Algebras of type G,” *Duke Math. J.*, Vol. 5, pp. 775–783, 1939.
- [70] G. Jakimoski and L. Kocarev, “Chaos and cryptography: block encryption ciphers based on chaotic maps,” *IEEE Transactions on Circuits and Systems I: Fundament Theory and Applications*, Vol. 48, No. 2, pp. 163-169, 2001.

- [71] S.S. Jamal, T. Shah and I. Hussain, “An Efficient Scheme for Digital Watermarking Using Chaotic Map,” *Nonlinear dyn.*, Vol. 73 No. 3, pp. 1469-1474, 2013.
- [72] Y.B. Jun, “Soft BCK/BCI-Algebras,” *Comput. Math. Appl.*, Vol. 56, No. 5, pp. 1408–1413, 2008.
- [73] N. Kausar, “Direct Product of Finite Intuitionistic Fuzzy Normal Subrings over Non-associative Rings,” *Eur. J. Pure Appl. Math.*, Vol. 12, No. 2, pp. 622–648, 2019.
- [74] N. Kausar, B. Islam, M. Javaid, S. Amjad and U. Ijaz, “Characterizations of Non-associative Rings by the Properties of their Fuzzy Ideals,” *J. Taibah Uni. Sci.*, Vol. 13, No. 1, pp. 820–833, 2019.
- [75] N. Kausar, M. Munir, M. Gulzar, G.M. Addis and M. Gulistan, “Study on Left Almost-rings by Anti Fuzzy Bi-ideals,” *Int. J. Nonlinear Anal. Appl.*, Vol. 11, pp. 483–498, 2020.
- [76] N. Kausar and M. Waqar, “Characterizations of Non-associative Rings by their Intuitionistic Fuzzy Bi-ideals,” *Eur. J. Pure Appl. Math.*, Vol. 12, No. 1, pp. 226–250, 2019.
- [77] M.K. Kazim and M. Naseeruddin, “On Almost Semigroups,” *The Aligarh Bulliten. Math.*, Vol. 2, pp. 1–7, 1972.
- [78] R. Kellil, “On Inverses of Left Almost Semirings and Strong Left Almost Semirings,” *J. Math. Sci. Adv. Appl.*, Vol. 26, pp. 29–39, 2014.
- [79] P. Khachorncharoenkul, K. Laipaporn and S. Wananiyakul, “Left Almost Seminearings,” *Lobachevskii J. Math.*, Vol. 41, No. 3, pp. 349–361, 2020.
- [80] M. Khan, T. Shah, H. Mahmood and M. A. Gondal, “An efficient method for the construction of block cipher with multi-chaotic systems,” *Nonlinear Dynamics*, Vol. 71, No. 3, pp. 489-492, 2013.
- [81] J. Kim and R.C.W. Phan, “Advanced Differential-Style Crypt-Analysis of the NSA’s Skipjack Block Cipher,” *Cryptologia*, Vol. 33, No. 3, pp. 246–270, 2009.
- [82] J. Liang and L. Wang, “On Cyclic DNA Codes over $F_2 + uF_2$,” *J. Comput. Appl. Math.*, Vol. 51, pp. 81–91, 2016.

- [83] D. Limbachiya, K.G. Banerjee, B. Rao and M.K. Gupta, “On DNA Codes using the Ring $\mathbb{Z}_4 + w\mathbb{Z}_4$,” *IEEE International Symposium on Information Theory (ISIT)*, pp. 2401–2405, 2018.
- [84] H. Liu, A. Kadir, and P. Gong, “A Fast Color Image Encryption Scheme using One-Time S-Boxes based on Complex Chaotic System and Random Noise,” *Opt. Commun.*, Vol. 338, pp. 340-347, 2015.
- [85] H. Liu, A. Kadir and Y. Niu, “Chaos-Based Color Image Block Encryption Scheme using S-Box,” *AEU-int. J. Electron. Commun.*, Vol. 68, pp. 676-686, 2014.
- [86] H. Liu, A. Kadir, X. Sun and Y. Li, “Chaos Based Adaptive Double-Image Encryption Scheme using Hash Function and S-Boxes,” *Multimed. Tools Apps.*, Vol. 77, pp. 1391-1407, 2018.
- [87] X. Liu, D. Xiang and J. Zhan, et al., “Isomorphism Theorems for Soft Rings,” *Algebra Colloq.*, Vol. 19, pp. 649–656, 2012.
- [88] X. Ma, J. Zhan and B. Davvaz, “Applications of Soft Intersection Sets to Hemirings via SI-h-Bi-Ideals and SI-h-Quasi Ideals,” *Filomat* Vol. 30, No. 8, pp. 2295–2313, 2016.
- [89] T. Mahmood, A. Waqas and M.A. Rana, “Soft Intersectional Ideal in Ternary Semirings,” *Sci. Int.*, Vol. 27, No. 5, pp. 3929–3934, 2015.
- [90] P.K. Maji, R. Biswas and A.R. Roy, “Soft Set Theory,” *Comput. Math. Appl.*, Vol. 45, pp. 555–525, 2003.
- [91] P.K. Maji, R. Biswas and A. R. Roy, “Fuzzy Soft Sets,” *J. Fuzzy Math.*, Vol. 9, pp. 589–602, 2011.
- [92] A. Marathe, A.E. Condon and R.M. Corn, “On Combinatorial DNA Word Design,” *J. Comput. Biol.*, Vol. 8, pp. 201–220, 2001.
- [93] J.L. Massey, “Reversible codes,” *Inf. Control*, Vol. 7, pp. 369–380, 1964.
- [94] M. Matsui, “Linear Cryptanalysis Method for DES Cipher,” *Adv. Cryptol. —EURO-CRYPT’93, Lect. Notes Comput. Sci.*, Vol. 765, ed. T. Helleseth. Springer-Verlag, Berlin, pp. 386–397, 1993.

- [95] W. McCune, Prover9 and MACE4,
<http://www.cs.unm.edu/mccune/mace4/>.
- [96] C.P. Milies and S. Sehgal, “An Introduction to Group Rings,” Springer, Netherlands, 2002.
- [97] D. Molodtsov, “Soft Set Theory- First Results,” *Comput. Math. Appl.* Vol. 37, pp. 19–31, 1999.
- [98] M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez and O.A. Del Campo, “A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos,” *Signal Process.*, Vol. 109, pp. 119-131, 2015.
- [99] P. Murugadas and M.R. Thirumagal, “Soft Intersection Ideals of Semirings,” *Ann. Pure Appl. Math.* Vol. 13, No. 2, pp. 273–292, 2017.
- [100] Q. Mushtaq and S. Kamran, “On Left Almost Groups,” *Proc. Pak. Acad. Sci.*, Vol. 33, pp. 1–2, 1996.
- [101] S.R. Nagpal and S.K. Jain, “Topics in Applied Abstract Algebra,” *Thomsan, Brooks/Cole*, 2005.
- [102] Y. Naseer, T. Shah, S. Hussain and A. Ali, “Steps towards redesigning cryptosystems by a non- associative algebra of IP-loops,” *Wireless Personal Communications*, Vol. 108, pp. 1–14, 2019.
- [103] J.L.P. Omayao, “On k-Ideals and Full k-Ideals of Near Left Almost Rings,” *JP J. Algebra Number Theory Appl.* Vol. 42, No. 2, pp. 239–253, 2019.
- [104] W. Pan and J. Zhan, “Rough Fuzzy Groups and Rough Soft Groups,” *Italian J. Pure Appl. Math.*, Vol. 36, pp. 617–628, 2016.
- [105] F. Pareschi, R. Rovatti and G. Setti, “On Statistical Tests for Randomness Included in the NIST SP800-22 Test Suite and based on the Binomial Distribution,” *IEEE Trans. Inf. Forensics Secur.*, Vol. 7, pp. 491–505, 2012.
- [106] Z. Pawlak, “Rough sets,” *Int. J. Comput. Inform. Sci.*, Vol. 11, pp. 341–356, 1982.

- [107] H. O. Pflugfelder, “Historical Notes on Loop Theory,” *Comment. Math. Univ. Carolinae*, Vol. 41, pp. 359–370, 2000.
- [108] K. Rahman, F. Hussain, S. Abdullah and M.S.A. Khan, “On Left Almost Semirings,” *Int. J. Comp. Sci. Inform. Security*, Vol. 14, pp. 201–216, 2016.
- [109] A. Razzaque and I. Rehman, “On Soft LA-modules and Exact Sequences,” *Italian J. Pure Appl. Math.*, Vol. 38, pp. 797–814, 2017.
- [110] I. Rehman, “On Generalized Commutative Rings and Related Structures,” PhD thesis, Quaid-i-Azam University, Islamabad, Pakistan, 2011.
- [111] I. Rehman, M. Gulistan, M.A. Gondal and S. Nawaz, “Structures of Generalized Fuzzy Sets in Non-Associative Rings,” *Int. J. Pure Appl. Math.*, Vol. 113, pp. 299–325, 2016.
- [112] I. Rehman and A. Razzaque, “Generalized Projective and Injective Modules,” *Seventh International Conference on Modeling, Simulation and Applied Optimization*, April 4-6, 2017. American University of Sharjah, UAE.
- [113] I. Rehman, M. Shah, T. Shah and A. Razzaque, “On Existence of Non-Associative LA-ring,” *An. S_{t.} Univ. Ovidius Constant_a*, Vol. 21, No. 3, pp. 223–228, 2013.
- [114] I. Rehman, N. Yaqoob and S. Nawaz, “Hyperideals and Hypersystems in LA-Hyperring,” *Songklanakarin J. Sci. Technol.*, Vol. 39, pp. 651–657, 2017.
- [115] R.M. Roth, “Introduction to Coding Theory,” Cambridge University Press, 2006, pp. 244–246.
- [116] A. R. Roy and P.K. Maji, “A Fuzzy Soft Set Theoretic Approach to Decision Making Problems,” *J. Comput. Appl. Math.*, Vol. 203, No. 1, pp. 412–418, 2007.
- [117] V.V. Rykov, A.J. Macula, D.C. Torney and P.S. White, “DNA Sequences and Quaternary Cyclic Codes,” in *Information Theory*, Proceedings. 2001 IEEE International Symposium on. IEEE, pp. 248, 2001.
- [118] A. Sezgin, “A New Approach to LA-Semigroup Theory via the Soft Sets,” *J. Intell. Fuzzy System*, Vol. 26, No. 5, pp. 2483–2495, 2014.

- [119] A. Sezgin and A.O. Atagün, “On Operations of Soft Sets,” *Comput. Math. Appl.* Vol. 61, No. 5, pp. 1457–1467, 2011.
- [120] A. Sezgin, A.O. Atagün and N. Çağman, “Soft Int-Near Ring and its Applications,” *Neural Comp. App.* Vol. 21, (Suppl 1), pp. 221–229, 2012.
- [121] A. Sezgin, N. Çağman and A.O. Atagün, “Soft Intersection Interior Ideals, Quasi-Ideals and Generalized Bi-ideals; a New Approach to Semigroup Theory II,” *J. Multi-valued Logic Soft Comput.*, Vol. 23, pp. 161–207, 2014.
- [122] A. Sezgin, N. Çağman and A.O. Atagün, “A Completely New View to Soft Intersection Rings Via Soft-Uni-Int Product,” *Appl. Soft Comput.* Vol. 54, pp. 366–392, 2017.
- [123] A. Sezgin, N. Çağman, A.O. Atagün, M.I. Ali and E. Turkmen, “Soft Intersection Semi Groups, Ideals and Bi-ideals; a New Application on Semigroup Theory I,” *Filomat*, Vol. 29, No. 5, pp. 917–946, 2015.
- [124] M. Shah and A. Ali, “Some Structural Properties of AG-group,” *Int. Math. Forum*, Vol. 6, No. 34, pp. 1661–1667, 2011.
- [125] T. Shah, G. Ali and F. Rehman, “Direct Sum of Ideals in a Generalized LA-Ring,” *Int. Math. Forum*, Vol. 6, No. 22, pp. 1095–1101, 2011.
- [126] T. Shah, I. Hussain, I., M.A. Gondal and H. Mahmood, “Statistical Analysis of S-Boxes Based on Image Encryption,” *Int. J. Phys. Sci.*, Vol. 6, No. 16, pp. 4110–4127, 2011.
- [127] T. Shah, N. Kausar and I. Rehman, “Intuitionistics Fuzzy Normal Subring over a Non-Associative Ring,” *An. Şt. Univ. Ovidius Constanta*, Vol. 20, No. 1, pp. 369–386, 2012S.
- [128] T. Shah, M. Raees and G. Ali, “On LA-Modules,” *Int. J. Contemp. Math. Sci.*, Vol. 6, No. 21, pp. 999–1006, 2011.
- [129] T. Shah and A. Razzaque, “Soft M-systems in a Class of Soft Non-Associative Rings,” *U.P.B. Sci. Bull. Series A*, Vol. 77, No. 3, pp. 131–142, 2015.

- [130] T. Shah, A. Razzaque and I. Rehman, “Applications of Soft Sets to Non-Associative Rings,” *J. Intell. Fuzzy Syst.*, Vol. 30, No. 3, pp. 1537–1546, 2016.
- [131] T. Shah and I. Rehman, “On LA-rings of Finitely Nonzero Functions,” *Int. J. Contemp. Math. Sci.*, Vol. 5, No. 5, pp. 209–222, 2010.
- [132] T. Shah and I. Rehman, “On Characterizations of LA-Rings through some Properties of thier Ideals,” *Southeast Asian Bull. Math.*, Vol. 36, pp. 695–705, 2012.
- [133] T. Shah, F. Rehman and M. Raees, “On Near Left Almost Rings,” *Int. Math. Forum*, Vol. 6, pp. 1103–1111, 2011.
- [134] M. Shah and T. Shah, “Some basic Properties of LA-Rings,” *Int. Math. Forum*, Vol. 6, No. 44, pp. 2195–2199, 2011.
- [135] T. Shah and K. Yousaf, “Topological LA-groups and LA-rings,” *Quasigroups Related Systems*, Vol. 18, pp. 95–104, 2010.
- [136] C. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, Vol. 28, No. 4, pp. 656-715, 1949.
- [137] T. Todorov and Z. Varbanov, “DNA Codes based on Additive Self-Dual Codes over $GF(4)$,” *7th Int. workshop on optimal codes and related topics*, Albena, Bulgaria, Sep. 2013.
- [138] M.T. Tran, D.K. Bui and A.D. Doung, “Gray S-Box for Advanced Encryption Standard,” *International Conference on Computational Intelligence and Security*, Vol. 1, pp. 253-256, 2008.
- [139] Z. Wang, “A Universal Image Quality Index,” *IEEE Signal Process. Lett.*, Vol. 9, pp. 81–84, 2002.
- [140] Z. Wang, A.C. Bovik, H.R. Sheikh and E.P. Simoncelli, “Image Quality Assessment: from Error Visibility to Structural Similarity,” *IEEE Trans. Image Process*, Vol. 13, pp. 600–612, 2004.
- [141] X. Wang and Q. Wang, “A novel image encryption algorithm based on dynamic s-boxes constructed by chaos,” *Nonlinear Dynamics*, Vol. 75, No. 3, pp. 567-576, 2014.

- [142] Q. Wang and J. Zhan, “A Novel View of Rough Soft Semigroups based on Fuzzy Ideals,” *Italian J. of pure and applied Math.*, Vol. 37 pp. 673–686, 2017.
- [143] Q. Wang, J. Zhan and R. A. Borzooei, “A Study on Soft Rough Semigroups and Corresponding Decision Making Applications,” *Open Math*, Vol. 15, pp. 1400–1413, 2017.
- [144] A.F. Webster and S. Tavares, “On the Design of S-Boxes,” In: *Adv. Cryptol.—CRYPTO ’85 Proc., Lect. Notes Comput. Sci.*, pp. 523–534, 1986.
- [145] J.H. Wu, X.F. Liao and B. Yang, “Color Image Encryption based on Chaotic Systems and Elliptic Curve ElGamal Scheme,” *Signal Process.*, Vol. 141, pp. 109–124, 2017.
- [146] Y. Wu, J.P. Noonan and S. Aghaian, “NPCR and UACI Randomness Tests for Image Encryption,” *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, pp. 31–38, 2011.
- [147] S. Yamak, O. Kazanci and B. Davvaz, “Generalized Lower and Upper Approximations in a Ring,” *Inform. Sci.*, Vol. 180, No. 9, pp. 1759–1768, 2010.
- [148] X. Yi, S.X. Cheng, X.H. You, and K.Y. Lam, “A Method for Obtaining Cryptographically Strong 8×8 S-Boxes,” *Int. Conf. Infor. Network Appl.*, Vol. 2, No. 3, pp. 14-20, 2002.
- [149] P. Yiarayong, “On Left Primary and Weakly Left Primary Ideals in LA-Rings,” *Asian J. Appl. Sci.*, Vol. 2, No. 4, pp. 457–463, 2014.
- [150] P. Yiarayong, S. Webchasad and W. Dorchana, “The Bi-ideals in Left Almost Rings,” *Asian J. Appl. Sci.*, Vol. 4, pp. 1200-1208, 2016.
- [151] B. Yildiz and I. Siap, “Cyclic Codes over $F_2[u]/(u^4 - 1)$ and Applications to DNA codes,” *Comput. Math. Appl.*, Vol. 63, No. 7, pp. 1169–1176, 2012.
- [152] L.A. Zadeh, Fuzzy sets, *Inform. Control*, Vol. 8, No. 3, pp. 338–353, 1965.
- [153] J. Zhan and B. Davvaz, “A Kind of New Rough Set: Rough Soft Set and Rough Soft Rings,” *J. Intell. Fuzzy Syst.*, Vol. 30 No. 1, pp. 475–483, 2015.

- [154] J. Zhan and Y. B. Jun, “Soft BL-algebras based on Fuzzy Sets,” *Comput. Math. Appl.*, Vol. 59, No. 6, pp. 2037–2046, 2010.
- [155] J. Zhan, Q. Liu and B. Davvaz, “A New Rough Set Theory: Rough Soft Hemirings,” *J. Intell. Fuzzy Syst.*, Vol. 28, No. 4, pp. 1687–1697, 2015.
- [156] J. Zhan and K. Zhu, “Reviews on Decision Making Methods based on (Fuzzy) Soft Sets and Rough Soft Sets,” *J. Intell. Fuzzy Syst.*, Vol. 29, pp. 1169–1176, 2015.
- [157] M. Zorn, “Theorie Der Alternativen Ringe,” *Abh. Math. Semin. Univ. Hambg.*, Vol. 8, pp. 123–147, 1930.
- [158] M. Zorn, “Alternativkörper Per Und Quadratische Systeme,” *Abh. Math. Semin. Univ. Hambg.*, Vol. 9, pp. 395–402, 1933.
- [159] M. Zorn, “The Automorphisms of Cayley’s Non-Associative Algebra,” *Proc. Natl. Acad. Sci. USA*, Vol. 21, pp. 355–358, 1935.
- [160] M. Zorn, “Alternative Rings and Related Questions I: Existence of the Radical,” *Ann. of Math.*, Vol. 42, pp. 676–686, 1941.
- [161] S. Zhu and X. Chen, “Cyclic DNA Codes over $F_2 + uF_2 + vF_2 + uvF_2$ and their Applications,” *J. Appl. Math. Comput.*, Vol. 55, pp. 479–493, 2017.

Turnitin Originality Report

Development of a Class of Non-Associative Algebras: Applications in Cryptography and Coding Theory by Nazli Sanam .



From DRSM (DRSM L)

- Processed on 07-Jun-2021 11:08 PKT
- ID: 1601930993
- Word Count: 53124

Handwritten signature

Handwritten signature

Similarity Index

17%

Similarity by Source

Internet Sources:

9%

Publications:

11%

Student Papers:

4%

Palun
Focal Person (Turnitin)
Quaid-i-Azam University
Islamabad

sources:

1 1% match (student papers from 24-Jun-2016)
[Submitted to Higher Education Commission Pakistan on 2016-06-24](#)

2 1% match (publications)
[Basic Modern Algebra with Applications, 2014.](#)

3 1% match (publications)
[Tariq Shah, Asima Razzaque, Inayat ur Rehman. "Application of soft sets to non-associative rings". Journal of Intelligent & Fuzzy Systems, 2016](#)

4 1% match (Internet from 14-Mar-2021)
<https://techscience.com/cm/v67n1/41192>

5 < 1% match (student papers from 19-Mar-2012)
[Submitted to Higher Education Commission Pakistan on 2012-03-19](#)

6 < 1% match (student papers from 12-Jul-2018)
[Submitted to Higher Education Commission Pakistan on 2018-07-12](#)

7 < 1% match (student papers from 12-Jul-2018)
[Submitted to Higher Education Commission Pakistan on 2018-07-12](#)

8 < 1% match (student papers from 26-Nov-2015)
[Submitted to Higher Education Commission Pakistan on 2015-11-26](#)