CONDITIONS FOR LA-SEMIGROUPS TO RESEMBLE ASSOCIATIVE STRUCTURES

by

MUHAMMAD SARWAR (KAMRAN)

SUPERVISED BY

DR. QAISER MUSHTAQ

Department of Mathematics
Quaid-i-Azam University
Islamabad

(1993)

CONDITIONS FOR LA-SEMIGROUPS TO RESEMBLE ASSOCIATIVE STRUCTURES

By

MUHAMMAD SARWAR (KAMRAN)

A thesis submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfilment of the requirements for the degree of Doctor of Philosophy in the subject of Mathematics.

TO THE BEST TEACHER OF THE WORLD

SEEK KNOWLEDGE FROM THE CRADLE TO THE GRAVE

SEEK AND YE SHALL FIND
KNOCK IT SHALL BE OPENED
ASK IT SHALL BE GIVEN UNTO YOU

ACKNOWLEDGEMENTS

During my little sojourns in the field of research I realised that at every step the hazards involved in a research work cannot be confronted by a single individual. There are always ideas and persons behind a research that serve as motivating force. These are the supervisor and guide, colleagues, friends, library men, books and research papers, experiences of the past and visions of the future. It is obligatory upon me to extend my gratitude to all aforementioned with an explicit emphasis on a few.

I consider it my first and foremost obligation to express my heartfel gratitude to Dr. **Qasier Mushtaq** – my supervisor, teacher and friend who guided, motivated and inspired me during the course of my research work. Words are insufficient to describe my long intellectual, emotional and mathematical attachment and association with him. He undoubtedly leaves indelible marks of his witty and scholarly intimacy, presence and association upon the people around him.

To quote an observation made by a biographer about Sir Winston Churchil with a slight modification "In short he is a great teacher but still a greater gentleman". But for his cordial attitude, kindness, guidance and persistent interest, I would not have moved further and completed my thesis.

I also wish to thank **Prof. Dr. Asghar Qadir**, *Chairman,* Department of Mathematics, whose presence in the Department has always been a source of encouragement and persuasion to me. In fact he is an emblem of research in the Department.

Last but not least — my special thanks go to my wife, who, very generously kept me free from domestic responsibilities and worries during this uphill task. She has been watching me engrossed in activities with great perseverance and patience and has been looking forward to see my efforts materialized.

I also thank all those who morally, intellectually and physically assisted and helped me in any capacity during the course of my research.

Finally, I am really thankful to my friend *Mr. Muhammad Sharaz* who was willing to spare time to type my manuscript.

May 1993. **MUHAMMAD SARWAR (KAMRAN)**

PREFACE

For an inquisitive mind, life is prickly with why's, what's, if's and but's. This fundamental questionnaire has always urged the human mind to make an unending quest in the realm of the unknown and invisible. The ardent purposefulness has always led to the opening of new vistas of panoramic expanse which has thereby stimulated the quester to go on adding to the depth of his vision and the height of his intuition.

This inquisitiveness led T.S. Frank [10] in 1967 wherein he put forward the question, whether or not can there exist a subtractive group. Obviously operations of substraction and division are non-associative and as such any structure based upon them would be non-associative.

It was much later when Q. Mushtaq and S. Kamran [18] in 1987 succeeded in defining a "non-associative group" which they called an "LA-group" and can be equally manipulated with as a subtractive group. We genuinely acknowledge that much of the spade work has been done by M.A. Kazim and M. Naseerudin, and Q. Mushtaq and S.M. Yusuf, in this field. The introduction of an LA-group is an important offshoot of an LA-semigroup.

In ternary operations the commutative law is given by abc = cba. M.A. Kazim and M. Naseerudin [20] in 1972, introduced braces on the left of this equation to get a new pseudo associative law, that is, (ab)c = (cb)a. This they called the left invertive law. A groupoid is called the left almost semigroup, abbreviated as LA-semigroup, if its elements satisfy the left invertive law. Similarly, a groupoid is called a right almost semigroup, abbreviated as RA-semigroup, if its elements satisfy the right invertive law, that is, a(bc) = c(ba). A groupoid is called an almost semigroup if it is both an LA-semigroup and an RA-semigroup.

An LA-semigroup is an algebraic structure midway between a groupoid and a commutative semigroup. Despite the fact that the structure is non-associative and non-commutative, it nevertheless possesses many interesting properties which we usually find in commutative and associative algebraic structures.

This thesis comprises five chapters. The first chapter contains a brief history of semi group and LA-semigroup, preliminaries of these structures and of those definitions and fundamental results which are directly related to our study of LA-semigroups. We have mentioned in this chapter the results without proofs in order to avoid making the thesis unnecessarily voluminous. We have also avoided giving the definitions (which are available in text books) by presuming that the reader is familiar with these. Nevertheless, one can refer for references to several text books, and one of them is: A.H. Clifford and G.B. Preston, The algebraic theory of semi groups, Amer. Math. Soc., Vols.I, 1961 and II, 1967.

In chapter 2, we have established a condition for an LA-monoid to be a commutative group. It is often important to use the behaviour and character of one algebraic structure and study another for the sake of having more and better informative results. But it is not always conveniently possible. In the beginning the definition of an LA-monoid G is given and later by dropping an element, left zero, from a finite LA-monoid a condition has been investigated, discovered and established to convert it into a commutative group.

In chapter 3, a system known as left pseudo-inverse quasigroup has been defined and the question of the possibility of its closest possible resemblance with an LA-group has been investigated. A left pseudo-inverse quasigroup is a more generalized structure. The technique adopted for the purpose is that of mapping the system homomorphically into an LA-group and then examining the kernel of the homomorphism. Intuitively, the smaller the kernel, the more LA-group like, the system is. A suitable LA-group has been found such that, if the system is mapped homomorphically into it, the kernel is the smallest and hence in our sense the LA-group resembles the system most closely.

Prior to that, in 1967, T.S. Frank [10] defined an inverse quasigorup $(Q,\circ)$. He has given what amounts to an elegant construction of the universal group of $(Q,\circ)$. This implies, in particular, when $(Q,\circ)$ is obtained from a group G by taking $Q = G$ and $a\circ b = a^{-1}b$.

Later P. Singh and N.S. Yadev [42] generalized the definition of an inverse quasigroup and defined a homomorphism of the system, called a pseudo-inverse quasigroup into a group. They exhibited a group that had the smallest kernel when the system is mapped homomorphically into it.

We have generalized the notions discussed in [10] and [42] to the case of left pseudo-inverse quasigroups.

In chapter 4, we have discussed the elements of an LA-monoid with their powers. Q. Mushtaq and S.M. Yusuf in [33] defined a locally associative LA-semigroup G to be an LA-semigroup wherein for every a in G $(aa)a = a(aa)$. They showed that a locally associative LA-semigroup does not necessarily have associative powers. They also put an extra condition on a locally associative LA-semigroup that it should possess a left identity. Thus for a locally associative LA-monoid they proved most of the results contained in this chapter.

The condition for LA-monoid to be locally associative is sufficiently strong. We have dropped this condition and without imposing any extra condition on an LA-monoid have established most of the results, proved by Q. Mushtaq and S.M. Yusuf, in [34] and by Q. Mushtaq and Q. Iqbal in [30]. Of the vital importance is our result that "the left identity becomes right identity for every element with even positive integral index". We have shown that every positive integral index can be added provided the odd positive integral index falls to its left. It has been shown that odd powers commute with odd and even powers with even. During this course, it is worth mentioning that the generalization of results is not quite straight forward, rather sometimes it becomes tedious. A relation ρ has been defined on an an LA-monoid and it is shown that ρ is a congruence relation. We have shown that the relation ρ is separative and that if G is an LA-monoid, then G/ρ is the maximal separative homomorphic image of G. It has also been shown that a subset Q, consisting of even powers of elements, of an LA-monoid G is a commutative semigroup.

Lastly in chapter 5, the concept of a left almost group; abbreviated as LA-group, has been introduced. It is a non-associative structure with interesting properties. It has been shown that if G is an LA-group and H is an LA-subgroup then G/H is an LA-group. The partitioning of an LA-group has been done with the remark that an LA-group can be decomposed into right cosets only and an RA-group can be decomposed into left cosets.

Further, Lagrange's theorem for LA-groups has been proved, that is, if G is a finite LA-group and H is an LA-subgroup of G then the order of H divides the order of G. In the end we have investigated that every finite set G, $n \geq 3$, is an LA-group under a binary operation * and that there is a bijection between this LA-group and the group of cyclic permutations of the elements of G.

The work contained in this thesis has been submitted for publication in the form of five papers in international professional journals.

CONTENTS

CHAPTER ONE

BRIEF HISTORY, PRELIMINARIES AND SOME FUNDAMENTAL RESULTS

As the time rolls on, the idea of *Left Almost Semigroup* is capturing the attention. This is because of its peculiar characteristics and applications, especially in the theory of Polyadic groups and Flocks.

The term 'semigroup' first appeared in mathematical literature on page 8 of J.A. de Seguier's book, Elements de la Theorie des Groupes Abstracts (Paris 1904) and the first paper about semigroups was a brief one by L.E. Dickson [8]. But the theory really began in 1928 with the publication of a paper of fundamental importance by A.K. Suschkewitsch. He showed that every finite semigroup contains a Kernel (a simple ideal) and completely determined the structure of finite simple semigroups. His result was not in a readily usable form. This flaw was removed by D. Rees [40], in 1940 with the introduction of the notion of a matrix over a group with zero and moreover, the domain of validity was extended to infinite simple semigroups containing primitive idempotents.

Since 1940, the number of papers appearing each year has grown fairly steadily to a little more than thirty on the average and now more than that. Mathematical Journals like 'Semigroup Forum' are continually contributing to the subject.

The first book which deals predominantly with the algebraic theory of semigroups is of A.K.Suschkewitsch, "The Theory of Generalized

Groups" (Kharkow, 1937). This is in Russian and is now out of print [6].

Many authors, including most of those writing in French, use the term "demigroup" for an associative groupoid, these authors reserve "semigroup" for what we shall call a cancellative semigroup. Other terms are "monoid" (Bourbaki) and "associative system" (Russian authors). The present terminology is standard in English and German literature [3].

These seminal papers generated enough enthusiasm amongst mathematicians who later developed it as an independent theory. After the advent of the theory of semigroups, mathematicians continued generalizing the algebraic notions and introduced new notions such as quasi-groups, loops, nets, polyadic groups, flocks, Moufang loops, exponential semigroups, weakly exponential groups, duo-semigroups, hypergroups, free semigroups, ordered and biordered semigroups, regular semigroups, orthodox semigroups, fuzzy semigroups, medial semigroups and almost semigrups etc. [1], [4],[13],[34],[35],[37] and [44] can be referred to in this regard.

Some concepts and facts are collected from [20],[22],[33] and [36] and they are stated (without proofs) in this chapter because they are essential for the growth of the subject matter of this thesis. These results flash back in our discussion throughout. Of the immense importance is the medial law, which has been frequently used along with the left invertive law.

It would be interesting to know that during the last five years, that is, from 1988 to 1992 nearly **1283** papers appeared on semigroups, and there were as much as **450** papers exclusively on group generalization.

This state of affairs indicates a fair

tendency of research in the field of semigroups and group generalization.

T.S. Frank [10] in 1967 put forward the question, whether or not can there exist a subtractive group. Plainly speaking, operations of subtraction and division are non-associative and as such any structure based upon them would be non-associative.

It was much later when Q.Mushtaq and S.Kamran [18] in 1987 succeeded in defining a "non-associative group" which they call an "LA-group" and can be equally manipulated with as a subtractive group. They successfully checked the validity of the structure and verified some importnat and known results of group theory. In addition, they also found that some of the group theoretic results are redundant for this structure and that some more or new interesting results appeared as off springs. The definition examples and results of this structure will be given later in this chapter at an appropriate place.

We should genuinely acknowledge that much of the spade work has been done by M.A.Kazim and M. Naseerudin, and Q.Mushtaq and S.M.Yusuf, in this field. The introducton of an LA-group is an important offshoot of an LA-semigroup.

In 1972, M.A.Kazim and M.Naseerudin [20] introduced a new pseudo associative law. In ternary operations, commutative law is given by abc = cba. M.A.Kazim and M.Naseerudin put braces on the left of this equation, that is, (ab)c = (cb)a and thus set aside the associative law. With the help of this new law, they successfully manipulated subtraction and division as binary operations, introduced new non-associative structure and proved several interesting results.

A left almost semigroup, abbreviated as *LA-semigroup*, is an algebraic structure midway between a groupoid and a commutative semigroup. An LA-semigroup is a non-commutative and non-associative algebraic structure. This structure has been defined in [20] and [36] as a groupoid G in which the *left invertive law*:

$$(ab)c = (cb)a \quad \text{for all } a,b,c \text{ in } G \text{ holds.} \qquad (1.1)$$

M.Naseerudin has investigated some basic characteristics of this structure in his doctoral thesis [36]. He has generalized some rudimentary but useful and important results of semigroup theory. Relations between LA-semigroups and quasigroups, semigorups, loops, monoids and groups have been established.

M.A.Kazim and M.Naseerudin, in their paper on almost semigroups [20], have shown that *G is medial*. That is,

$$(ab)(cd) = (ac)(bd) \quad \text{for all } a,b,c,d \text{ in } G. \qquad (1.2)$$

Right almost semigroups can be dually defined.

That is, a groupoid (G,.) is called a right almost semigorup, abbreviated as an *RA-semigroup*, if it satisfies the *right invertive law*:

$$a(bc) = c(ba) \quad \text{for all } a,b,c \text{ in } G.$$

EXAMPLES 1.3

The set $\mathbb{Z}$ of integers, $\mathbb{Q}$ of rationals, $\mathbb{R}$ of reals are LA-semigroups under binary operation '$*$' defined below and RA-semigroups under the binary operation '$\dagger$' defined below. For more examples one can refer to [33]

(i) $(\mathbb{Z},*)$: $a*b = b-a$ for all a,b in $\mathbb{Z}$

$(\mathbb{Z},\dagger)$: $a\dagger b = a-b$ for all a,b in $\mathbb{Z}$

'$-$' being ordinary subtraction.

(ii) $(\mathbb{Q},*)$: $a*b = b-a$ for all a,b in $\mathbb{Q}$

$a*b = b\div a$ for all a,b in $\mathbb{Q}\backslash\{o\}$

$(\mathbb{Q},\dagger)$: $a\dagger b = a-b$ for all a,b in $\mathbb{Q}$

$a\dagger b = a\div b$ for all a,b in $\mathbb{Q}\backslash\{o\}$

'−' and '÷' being ordinary subtraction and division.

(iii) $(\mathbb{R},*)$: $a*b = b-a$ for all a,b in $\mathbb{R}$

$a*b = b \div a$ for all a,b in $\mathbb{R}\setminus\{o\}$

$(\mathbb{R},\dagger)$: $a\dagger b = a-b$ for all a,b in $\mathbb{R}$

$a\dagger b = a \div b$ for all a,b in $\mathbb{R}\setminus\{o\}$.

EXAMPLE 1.4

The set E of even integers is also an LA-semigroup under '$*$' and RA-semigroup under '$\dagger$' defined by $a*b = b-a$ and $a\dagger b = a-b$ for all a,b in E. Where '−' is ordinary subtraction.

EXAMPLE 1.5

The set $\mathbb{C}$ of complex numbers is an LA-semigroup under '$*$' and RA-semigroup under '$\dagger$' defined below:

$$a*b = b-a \quad \text{for all } a,b \text{ in } \mathbb{C}$$

$$a \dagger b = a-b \quad \text{for all } a,b \text{ in } \mathbb{C}$$

$$a*b = b \div a \quad \text{for all } a,b \text{ in } \mathbb{C}\backslash\{o\}$$

$$a \dagger b = a \div b \quad \text{for all } a,b \text{ in } \mathbb{C}\backslash\{o\} .$$

Where '-' and '÷' are the ordinary operations of subtraction and division.

This implies that the set of complex numbers is an LA-semigroup under '*' and RA-semigroup under '†' defined above with usual subtraction and division of complex numbers.

EXAMPLE 1.6

The set G = {a,b,c}, under (.), defined below in the form of Cayley's table is an LA-semigroup:

·	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

Further to add that, under (o) G is an RA-semigroup:

o	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

We may point out that it can be easily seen from these examples that the structure LA-semigroup (RA-semigroup) is non-associative.

For instance, in example 1.6

$(cb)a = ca = b$ and

$c(ba) = cc = a$ imply that

$(cb)a \neq c(ba)$.

Example 1.6, is reproduced from [20], because we may need to refer to it later. The non-associativity shown above is different from that shown in

[20], wherein (bb)c ≠ b(bc).

As we have mentioned in the beginning of this chapter that an LA-semigroup is medial. It has been proved in [20] that G is medial, that is, (ab)(cd) = (ac)(bd) for all a,b,c,d in G.

EXAMPLE 1.7

Consider the set G = {a,b,c,d}, which is an LA-semigroup under '.' as shown below:

·	a	b	c	d	f
a	a	b	c	d	f
b	f	a	b	c	d
c	d	f	a	b	c
d	c	d	f	a	b
f	b	c	d	f	a

Then (ab)(cd) = (b)(b) = a

and (ac)(bd) = (c)(c) = a which implies that

(ab)(cd) = (ac)(bd) .

It can be verified that the result holds for all elements in G.

In [20], it has also been proved that in an LA-semigroup G the following conditions are equivalent for all a,b,c in G:

(i) $b(ac) = (ab)c$

(ii) $b(ca) = (ab)c$

The structural properties of LA-semigroups are studied in a number of important papers that have appeared since the introduction of this structure. In one of these papers, M.A.Kazim and M.Naseerudin [20] have tried to find out a *condition* under which an LA-semigroup can be *converted into a group*. They assert that an LA-semigroup G with left identity e, will become a group if for each a in G, there exist b and c in G such that, $a(bc) = e = (ac)b$ holds in G. In [26], Q.Mushtaq has shown that their assertion was defective. He provided a counter example to support his claim.

M.A.Kazim and M.Naseerudin in [20] have extensively used the identity a(a(bc)) = e and (a(bc))a = e, which is not necessarily true as Q.Mushtaq [26], has shown that a(bc) = e does not necessarily imply that

$$a(a(bc)) = e \quad \text{and} \quad (a(bc))a = e .$$

Consider for instance, the following example of an LA-semigroup which satisfies the hypothesis of the theorem by M.A.Kazim and M.Naseerudin but which is not a group.

EXAMPLE 1.8

Let G = {a,b,c,d} be a groupoid and a binary operation (.) be defined in it as shown below:

·	a	b	c	d
a	a	b	c	d
b	d	a	b	c
c	c	d	a	b
d	b	c	d	a

Then (G,.) is an LA-semigroup with left identity a because all the elements of G satisfy the left invertive law and ax = x for all x in G. Moreover, all the elements of G satisfy the identity

$$a(a(bc)) = e \quad \text{and} \quad (a(bc))a = e .$$

Thus, for each x in G, there exist y and z in G, such that, $x(yz) = a = (xz)y$. But (G,.) is not a group. It is not even a semigroup because we find $(bc)d \neq b(cd)$.

Q.Mushtaq and S.M.Yusuf in [23], have defined an LA-semigroup defined by a commutative inverse semigroup. Let (G,.) be a commutative inverse semigroup. Define a binary operation * in G as follows:

$$a*b = b.a^{-1} \quad \text{for every } a,b \text{ in } G.$$

They have proved that (G,*) is an LA-semigroup and referred to this as an 'LA-semigroup defined by a commutative inverse semigorup'. In [31], the authors have described the structure of LA-semigroups defined by commutative inverse semigroups, by means of LA-semigroups defined by commutative groups and certain homomorphisms between them. Specifically, they have shown that if a commutative inverse semigroup G is a semilattice of the inverse semigroup G then the LA-semigroup defined by G is also a semilattice of LA-semigroups. Conversely, they have shown that given a semilattice of LA- semigroups and a family of homomorphisms with certain properties, an LA-semigroup can be defined, which is a union of the given LA-semigroups.

Q.Mushtaq in [25], has shown that conversely, provided that a necessary and sufficient condition is satisfied by an LA-semigroup, it can induce an Abelian group satisfying the condition $a.b = b*a^{-1}$ for all a,b in G. He also observed some additional characteristic of such LA-semigroups. Specifically, the author proved that in (G,.), the following conditions are equivalent:

(i) $a = (cc.ab)b$ for all a,b,c in G,

(ii) there exists an Abelian group (G,*) such that, $a.b = b*a^{-1}$ for all a,b in G,

(iii) (G,.) is cancellative, where G is an LA-monoid with left identity e and $a^2 = e$ for all a in G,

(iv) (G,.) has left identity e and $a^2 = e$ for all a in G.

The notion of a left(right) translative mapping (which is called a left(right) translation in semigroup theory) is natural and very useful. It is well-known [6] that each element of a semigroup induces a left and right translation. These translations play an important role, for example, in the theory of ideal extensions. A system of mappings $T_u : x \longrightarrow T_u(x)$ of a non-empty set G into itself, where u ranges over elements of a set U, is called commutable if $T_uT_v(x) = T_vT_u(x)$ holds for all u,v in U and x in G. A system of mappings $T_u : x \longrightarrow T_u(x)$

is transitive if $T_u(x) = G$ for all x in G, where the set of elements $T_u(x)$ for all u in U, is denoted by $T_u(x)$. A system of mappings $T_u: x \longrightarrow T_u(x)$ of G into itself is called right translative according as $T_u(xy) = x\, T_u(y)$, $T_u(xy) = T_u(x)y$ or $T_u(xy) = x\, T_u(y) = T_u(x)y$ holds for every x,y in G and u in U.

In [27], Q.Mushtaq has defined translative mappings on LA-semigroups, and besides other things, he has shown that if there is a transitive system of translative mappings on an LA-monoid then the structure is necessarily commutative semigroup with identity. It has been shown also that a mapping T_u of a transitive system of mappings over an LA-semigroup G is injective if the right cancellative law holds with respect to every element of $T_u(G)$. Also, every transitive system of transitive mappings over a multiplicative LA-monoid G has the form $x \longrightarrow T_u(x) = x + \vartheta(x)$, where '+' is an Abelian group operation on G and ϑ: U $\longrightarrow$ G is a mapping of U onto G.

Q.Mushtaq and S.Kamran [31], have shown that a cancellative LA-semigroup is a commutative semigroup if a(bc) = (cb)a for all a,b,c in G. Further, it has been shown that an LA-monoid G, is a commutative monoid if and only if (ab)c = b(ca), for all a,b,c in G.

E. Hewitt and H.S. Zuckerman [14], surveyed the field of ternary operations and semigroups giving rise to them. M. Iqbal in [16], has generalized their results to invertive operations and studied the LA-semigroups connected with them. Apart from several interesting results, the main result he has proved is that an LA-semigroup is isomorphic to the direct product of a group, all of whose elements are of order two, and a semigroup under a special binary operation.

Analogous to Vagner-Preston Representation Theorem [6], M.Iqbal in [16], has proved that every inverse LA-semigroup has a faithful representation as an inverse LA-semigroup of partial one-one mappings. M.Iqbal has also shown that the given partial ordering relation is the maximum idempotent-separating congruence of an inverse LA-semigroup.

In [16], a ternary operation on an LA-semigroup was introduced and the author generalized the results of E.Hewitt and H.S.Zukerman [14]. Some useful properties of this structure were studied and a relationship was established between LA-semigroups (S,.) and (S,o), defined on the same set S, such that x.(y.z) = xo(yoz) for all x,y,z in S. If in (S,.) and (S,o), x.(y.z) = xo(yoz) then we say that (S,.) and (S,o) are in relation R with each other. M.Iqbal [16] has shown that if (S,.) and (S,o) are related by R then (S,.) and (S,o) are isomorphic under certain conditions.

M. Khalid in [21] has investigated the division LA-semigroups. He has extensively used medial law of LA-semigroups and has proved some rsults for division μ-LA-semigroups and linear forms of LA-semigroups. He has also shown that under certain conditions an LA-semigroup can be converted into a division μ-LA-semigroup, it has a linear form and it is a commutative group.

M.Khalid in [21], has also considered the left and right translations for LA-semigroups. He has specifically shown that an LA-semigroup becomes a commutative semigroup under certain conditions. He has used the translations to obtain an LA-semigroup from an LA-group. By making use of these translations, he has obtained from an LA-group a commutative monoid and an automorphism of the commutative monoid.

S. Reinhard in [41], has constructed medial semigroups. A semigroup is said to be medial if it satisfies the identity uxyv = uyxv. Let (H,+) be a commutative semigroup and ϕ,ψ endomorphisms of H satisfying (*) $\phi^2 = \phi$, $\psi^2 = \psi$, $\phi\psi = \psi\phi$. Define the product on H by (1) ab = ϕ(a) + ψ(b). The (H,.) is a medial semigroup and satisfies (**) a,b,c,d, x $\in$ H and ab = cd imply axb = cxd. Suppose that a medial semigroup (X,.) is given satisfying (**). Then the a method for constructing a commutative semigroup (H,+) and endomorphisms ϕ,ψ of H satisfying (*) such that, (X,.) is isomorphic to a subsemigroup of the medial semigroup (H,.) obtained from (H,+) by defining the multiplication by (1).

P. Corsini and T. Vougiouklis in [7], have introduced a method for constructing new algebraic structures from old ones, obtaining stronger properties; for example, it is possible to obtain semigroups from groupoids, gaining associativity, or Abelian groups from non-commutative groups.

The method consists of two steps; (a) uniting elements: this means putting together every pair of elements for which a certain property "d" fails; the quotient set becomes a hyperstructure A with the property "d"; (b) making quotients: in a standard way it is possible to obtain from A a strict algebraic structure satisfying property "d".

Q. Iqbal in [17], has described the structure of LA-semigroups by means of LA-semigroups and certain homomorphisms between them. It has been specifically shown that an LA-semigroup G is a semilattice of LA-semigroups. Conversely, it has been shown that given a semilattice of LA-semigroups and a family of homomorphisms, with certain properties, an LA-semigroup can be defined which is a union of the given LA-semigroups.

It has also been shown in [17], that an LA-semigroup G, which has a left regular band of LA-groups as an LA-semigroup of left quotients, is shown to be the LA-semigroup which is a left regular band of right reversible cancellative LA-semigroups. An alternative characterization has been provided by unique spined products. These results have been applied to the case where S is super abundant and where the set of idempotents forms a left normal band.

Translations and transformations play a vital role in the theory of semigroups. In [18], S. Kamran, has shown that under certain conditions the set of left translations on an LA-semigroup forms an LA-semigroup. A parallel result to Cayley's theorem for the set of left translations defined on an LA-semigroup has been proved in [18]. In [18], the concepts of zeroids and idempoids in LA-semigroups are also discussed in detail and some interesting results have been proved.

Q.Mushtaq [28], has proved that if an LA-semigroup contains the left cancellative

LA-subsemigroup such that, the LA-subsemigroup is contained in the centre of the LA-semigroup then it can be embedded in a commutative monoid whose cancellative elements form an Abelian group and the identity element of this group coincides with the identity element of the commutative monoid.

In order to define associative powers in an LA-semigroup G, we impose the condition that

$$b(ac) = (ab)c$$

or $$b(ca) = (ab)c \quad \text{for all } a,b,c \text{ in } G.$$

As already mentioned above that these conditions are equivalent, we call them a weak associative law. Notice that, if $a = b = c$ in the first, then LA-semigroup with weak associative law becomes a locally associative LA-semigroup, that is, an LA-semigroup with the condition $(aa)a = a(aa)$ for all a in G.

In [34], Q.Mushtaq and S.M.Yusuf have defined a locally associative LA-semigroup G and on one hand, have verified the notable results of semigroup theory and on the other hand, have derived some new results of vital importance.

In [44], T. Tamura and T. Nordhal have called the semigroup satisfying the identity $(xy)^m = x^m y^m$ $(m \geq 2)$ as exponential m-semigroup.

It is important to note that an LA-semigroup G with weak associative property is exponential. One can refer to [34] and [31] for more details about this theory.

In [34], it has been proved that locally associative LA-semigroups are exponential. Several structural theorems are proved in this paper.

The following results are fundamental and essential for our subsequent discussion of the subject matter and are frequently referred to, whenever and wherever found imperative. These results are proved in [18],[29] and [31], and here we are enlisting and mentioning them without proofs. To begin with, at this juncture we recall that an LA-semigroup G is a groupoid which satisfies the left invertive law viz: $(ab)c = (bc)a$ for all a,b,c in G and that an LA-monoid G is an LA-semigroup with left identity.

THEOREM 1.9

In an LA-monoid the identity is unique.

THEOREM 1.10

In an LA-semigroup the right identity becomes a two sided identity.

It would not be out of place to mention here that the converse of the above theorem is not necessarily true. That is, the left identity does not become the right identity.

Thereupon as a consequence to the above theorem, we have the following important results.

THEOREM 1.11

An LA-semigroup with right identity is a commutative monoid.

THEOREM 1.12

In an LA-monoid G a(bc) = b(ac), for all a,b,c in G.

THEOREM 1.13

An LA-monoid with left(right) inverses has two sided inverses.

THEOREM 1.14

A left cancellative LA-semigroup is a cancellative LA-semigroup.

THEOREM 1.15

In an LA-monoid G ab = cd implies that ba = dc for all a,b,c,d in G.

THEOREM 1.16

A finite LA-semigroup G is a group provided that a(bc) = (cb)a, for all a,b,c in G.

THEOREM 1.17

If (G,.) is a commutative group then (G,*) is an LA-semigroup under *, where * is defined by:

$$a*b = a'.b = b'.a$$

for every a,b in G, and by a′ we mean the inverse of a.

THEOREM 1.18

A subset containing all the idempotent elements of an LA-monoid is a commutative subsemigroup with identity.

In view of Theorem 2.6, Corollary 2.2 [32], we have the following useful results.

THEOREM 1.19

In a right cancellative LA-semigroup G, every right identity of an idempotent element is its identity.

In Theorems 3.10, 3.11, 3.12, [33] the following significant results have been proved.

THEOREM 1.20

If in an LA-semigroup G, ax = b has a unique solution for every a,b in G, then yc = d has also a unique solution for every c,d in G.

THEOREM 1.21

If in an LA-monoid G, yc = d has a unique solution for every c,d in G, then ax = b has also a unique solution for every a,b in G.

THEOREM 1.22

If in an LA-semigroup G, ax = b has a unique solution for every a,b in G, then G is a commutative group.

An LA-semigroup may have more than one idempotent which has been reflected by the following example.

EXAMPLE 1.23

Let G = {a,b,c} with binary operation (.) defined in G as follows:

·	a	b	c
a	a	a	a
b	a	a	a
c	a	a	c

Then G is an LA-semigroup with more than one idemptotent. Thus an LA-monoid can have idemptotents other than the identity.

EXAMPLE 1.24

Let $G = \{e,f,a,b,c\}$ and the binary operation (.) be defined as follows:

·	e	f	a	b	c
e	e	f	a	b	c
f	f	f	f	b	c
a	a	f	e	b	c
b	c	c	c	f	b
c	b	b	b	c	f

Then G is an LA-monoid with e as the left identity and f as an idempotent.

Note that $ef = fe = f$ implies that $f \leq e$.

In [29], the following results have been proved.

THEOREM 1.25

An LA-monoid with left identity e contains no idempotent such that $e \leq f$.

THEOREM 1.26

A subset containing all the idempotent elements of an LA-monoid with left identity e, is a commutative subsemigroup with e as its identity.

EXAMPLE 1.27

Let G = {a,b,c} with binary operation (.) in G defined as follows:

·	a	b	c
a	c	c	b
b	b	b	b
c	b	b	b

Then (G,.) is a locally associative LA-semigroup. This example shows that we can not define associative powers in G, as we do in semigroup. Thus in order to define associative powers in a locally associative LA-semigroup, we introduce the left identity.

A brief description about the powers of elements is given here but to a sufficient length we have discussed in chapter 4.

Q.Mushtaq and S.M.Yusuf [34], have proved the following results in this connection.

THEOREM 1.28

Every locally associative LA-monoid has associative powers.

Q.Mushtaq and S.M.Yusuf in [34], have also defined a relation ρ on a locally associative LA-monoid G. It has been proved in [34] that relation ρ is a congruence relation on a locally associative LA-monoid.

Further to that, a relation σ on a locally associative LA-monoid G is separative if and only if

$$ab\sigma a^2 \quad \text{and} \quad ab\sigma b^2 \quad \text{implies} \quad a\sigma b \,.$$

It was also proved in [34] that the relation is separative.

In [32], Q.Mushtaq and S.M.Yusuf have shown that if an LA-semigroup is defined by a commutative inverse semigroup [commutative group], then by defining a binary relation in the LA-semigroup, we can recover the commutative inverse semigroup [commutative group].

In [18] S.Kamran, has defined a left almost group abbreviated as an LA-group

A groupoid (G,.) is called an LA-group, if

(i) (G,.) is a left almost semigroup,

(ii) e.a = a, for all a in G and left identity e in G,

(iii) a′.a = e for all a,a′ in G, where a′ denotes the left inverse of a.

Recall that a′ is two sided.

EXAMPLE 1.29

Let G = {e,a,b,c,d} and (.) be the binary operation in G deifned as follows:

·	e	a	b	c	d
e	e	a	b	c	d
a	d	e	a	b	c
b	c	d	e	a	b
c	b	c	d	e	a
d	a	b	c	d	e

The structure is non-associative as

$$(bc)d \neq b(cd) .$$

Then G is an LA-group with left identity e and each element of G has a left inverse and the elements satisfy the left invertive law. Incidently in this example every element is self inversive, that is, its own inverse, since, a.a = e, for every a in G. It is to be pointed out here that despite a.a = e for every a in G, the structure is neither commutative nor associative — as remarked earlier.

The structure LA-group contains certain

peculiar characteristics. In [18], homomorphisms for an LA-group have been defined and the well known ismorphism theorems have been proved. Cosets play an important role in the theory of groups and similarly in the case of LA-groups, one can see in chapter five that their role is no less significant.

Much of the spade work done by Q.Mushtaq and S.M.Yusuf [25],[26],[29],[32],[33] and by M.A.Kazim and M.Naseerudin [19],[20],[36] has been utilized in [18] and some of the results have been reproduced with a different mode of proof. We are mentioning few of these without proofs as we may need to use them later.

THEOREM 1.30

An LA-group with right identity is an Abelian group. (One may also refer to [33])

THEOREM 1.31

An LA-group is cancellative.

(One may also refer to [33]) .

REMARK 1.32

An RA-group can be defined on a parallel track to that of an LA-group, that is, a groupoid (G,.) is an RA-group if:

(i) a.e = a , for every a in G and right identity e in G,

(ii) a.a′ = e for every a in G,

(iii) a(bc) = c(ba) , for all a,b,c in G.

EXAMPLE 1.33

Let G = {e,a,b,c} and (.) be the binary operation defined as follows:

·	e	a	b	c
e	e	c	b	a
a	a	e	c	b
b	b	a	e	c
c	c	b	a	e

The structure is non-associative as $a(bc) \neq (ab)c$. It can be verified that for all a,b,c in G, we have $a(bc) = c(ba)$. Then G is an RA-group with right identity e and each element has a right inverse and the elements satisfy right invertive law.

THEOREM 1.34

An LA-group can be decomposed into right cosets and an RA-group into left cosets.

THEOREM 1.35

If H is an LA-subgroup of an LA-group G then

$$(aH)(bH) = (ab)H \quad \text{and} \quad (Ha)(Hb) = H(ab) \ ,$$

for all a,b in G.

COROLLARIES 1.36

If H is an LA-subgroup of an LA-group G then for every a,b in G and left identity e in G:

(i) $GG = G$

(ii) $eG = Ge = G$

(iii) $(ab)H = H(ba)$.

LEMMA 1.37

(i) $(ab)' = a'b'$,

(ii) $(abc)' = a'b'c'$,

for all a,b,c in an LA-group G and primes denote the inverses of elements.

REMARK 1.38

It is important to note that there is no concept of group theoretic normality in an LA-group. We can factor an LA-group by any of its LA-subgroups. We know that if G is a group and H is its subgroup then $(aH)(bH) \neq (ab)H$, unless H is normal in G. Here we have no such condition because of the medial property, that is, if aH, bH belong to G/H, then (aH)(bH) = (ab)H, without having an extra condition on H.

In chapter 2, we have established a condition for an LA-monoid to be a commutative group. For commutativity, the condition proved in [31] has been utilized. In this regard various results proved in [20],[29],[31] and [33] have been frequently used. As the structure is non-associative and new in semigroup theory (rather "LA-semigroup" theory), the condition so established is not straight forward in manipulating with algebraic craftsmanship. Anyhow tediousness is a necessary evil for mathematical products.

In chapter 3, a system (Q,o) called left-inverse quasigroup has been defined. The left pseudo-inverse a' of an element a of Q has also been defined. This structure is a generalization of the concept of pseudo-inverse quasigroup defined in [42]. It has been shown that Q is right cancellative and that for a,b in Q, there exists a unique d in Q, such that, doa = b.

A homomorphism f from Q to a given LA-group (G,.) and the kernel K_f of f have been defined. It has been proved that (K_f,o) is a left pseudo-inverse sub-quasigroup of (Q,o). The nucleus N(Q) of Q and an element x called invertor for an ordered triple (a,b,c) and denoted by <abc>, have also been defined. The set A(Q) of all invertors in Q has been defined and it is shown that $N(Q) \cup A(Q) \subseteq K_f$. A condition for a subset S of Q to partition (Q,o) has been proposed and it is shown that K_f partitions (Q,o). The set (H,o) intersection of all left pseudo-inverse sub-quasigroups of (Q,o) which partition (Q,o) and containing $N(Q) \cup A(Q)$ has been defined and shown as left pseudo-inverse sub-quasigroup of Q. It has been proved that there is a homomorphism F from a left pseudo-inverse quasigroup (Q,o) to the LA-group (G,*), where G = {Hoa:a ∈ Q}, defined by F(a) = Hoa with kernel K_f = H. Finally it is shown that H is the smallest kernel of the homomorphism F and so (G,*) is the most closely resembling LA-group to the left pseudo-inverse quasigroup (Q,o).

In chapter 4, the powers of elements of an LA-monoid have been defined and discussed in detail. Some important and interesting results have been established. In [43], T.Tamura and N.Kimura proved that any commutative semigroup G is uniquely expressible as a semilattice of archimedean semigroups. Later in [14], E.Hewitt and H.S.Zuckerman, proved that the following conditions are mutually equivalent: (i) G is separative, (ii) the archimedean components of G are cancellative, (iii) G can be embedded in a union of groups. In [34], Q. Mushtaq, and S.M. Yusuf extended their results to a locally associative LA-semigroup G, which is not an associative structure. They defined a locally associative LA-semigroup G to be an LA-semigroup wherein for every a in G, (aa)a = a(aa). Q.Mushtaq, and S.M.Yusuf in [34], put an extra condition on a locally associative LA-semigroup. They showed that a locally associative LA-semigroup does not necessarily have associative powers. Later Q.Mushtaq and Q.Iqbal in [30] and Q.Iqbal in [17] discussed the decomposition of a locally associative LA-semigroup. Most of our results heavily hinge upon the results deduced and established in [17],[34] and [40]. We have abolished the condition of local associativity on an LA-semigroup with left identity. The results proved in chapter 4, are independent of this condition and have been proved for an LA-monoid. During this course, we came across with the problem of odd and even powers. To establish our main results we had to overcome this difficulty and some basic results have been proved in different cases, considering the even and odd powers separately. A very important result stating that "the left identity becomes the right identity for every element with even positive integral index", has been proved and using another important result from [33], it has been shown that if G is an LA-monoid, then a subset Q of G, consisting of elements of G with even powers, is a commutative monoid.

A relation ρ such that, $a\rho b$ if and only if $b^n a = b^{n+1}$ and $a^n b = a^{n+1}$, for all a,b in an LA-monoid G, has been defined and it is proved that ρ is a congruence relation. Later it has been shown that ρ is separative and that G/ρ is the maximal separative homomorphic image of G. Few more related results have also been proved in the end of chapter 4.

Several authors, for example, B.M. Henry [13], M.A. Kazim and F. Hussain [19] and D.C. Murdock [24] have generalized the concept of a group and have investigated the structural properties of these generalizations. In chapter 5, we have introduced the concept of a left almost group, which is a non-associative structure with interesting properties. Here specifically, it is shown that if G is a left almost group and H is a left almost subgroup then G/H is a left almost group. Further, we have proved Lagrange's theorem for left almost groups, that is, if G is a finite left almost group and H is a left almost subgroup of G then the order of H divides the order of G.

In the end, we have discussed a finite set as how to become an LA-group. It has been shown that every finite set G, $n \geq 3$, under a binary operation * is an LA-group. It has been discovered that there is a bijection between the group of cyclic permutations of elements of G and such an LA-group.

CHAPTER TWO

A CONDITION FOR AN LA-MONOID TO BE A COMMUTATIVE GROUP

We recall that a left almost semigroup [20], abbreviated as LA-semigroup, is a groupoid G whose elements satisfy the left invertive law: (ab)c = (cb)a. It is a non-associative structure midway between a groupoid and a commutative semigroup. The structure is medial [20], that is, (ab)(cd) = (ac)(bd) for all a,b,c,d in G. It has been shown in [32] that if an LA-semigroup contains a left identity, it is unique. It has been proved also in [33] that an LA-semigroup with right identity is a commutative monoid. An element a_o of an LA-semigroup G is called a left (right) zero if $a_o a = a_o$ ($aa_o = a_o$) for all a in G.

We call an LA-semigroup with left identity an *LA-monoid*. Let a,b,c and d belong to an LA-monoid and ab = cd. Then it has been shown in [33] that ba = dc. An element a of an LA-monoid, with left identity e, is called an involution if $a^2 = e$.

An element a^{-1} of an LA-monoid is called a left inverse if $a^{-1}a = e$, where e is the left identity. It has been shown in [32] that if a^{-1} is a left inverse of a then it is unique and is also the right inverse of a. It has been proved in [33] that every left cancellative LA-semigroup is right cancellative and every right cancellative LA-semigroup is left cancellative only if it is an LA-monoid.

It is often important to use the behaviour and character of one algebraic structure and study another for the sake of having more and better informative results. But it is not always conveniently possible. Then the question arises under what circumstances can it be achieved? K. Verma in a paper [45] has established a sufficient condition for a monoid to be a group. He has considered a monoid and converted it into a group under certain conditions whereas we have generalized his result by converting a non-associative algebraic structure, namely an LA-monoid, into a commutative group under weaker conditions.

For sake of convenience, we reproduce here a simple but useful result, namely Theorem 2.1 from [31].

THEOREM 2.1

A cancellative LA-semigroup G is a commutative semigroup if $a(bc) = (cb)a$ for all a,b,c in G.

PROOF

Since G is an LA-semigroup, therefore by left invertive law,

$$(cb)a = (ab)c$$
$$= a(bc) .$$

Thus $(ab)c = a(bc)$ and hence LA-semigroup is a semigroup.

Further, if a,b,c,d belong to G, then by the medial law:

$$(ab)(cd) = (ac)(bd) .$$

This implies that $((ab)c)d = ((ac)b)d$; so $(ab)c = (ac)b$ because G is cancellative. Thus $a(bc) = a(cb)$ because G has been shown associative. This implies that $bc = cb$ as G is cancellative. This proves that G is a commutative semigroup.

COROLLARY 2.2

A finite, cancellative LA-semigroup G, wherein $a(bc) = (cb)a$ for all a,b,c in G is a commutative group.

THEOREM 2.3

If (G,o) is a finite LA-monoid with a left zero a_o, then $G^o = G\backslash\{a_o\}$ is a commutative group under o provided there is binary operation * such that:

(i) $(G,*)$ is an LA-monoid with left inverses;

(ii) $a_o * a = a$, for all a in G;

(iii) $(a*b)oc = (aoc)*(boc)$, for all a,b,c in G;

(iv) $aob = a_o$ implies that either $a = a_o$ or $b = a_o$ for all a,b in G and

(v) $ao(boc) = (cob)oa$ for all a,b,c in G.

PROOF

Let us suppose tht (G,o) is a finite LA-monoid and $G = \{a_o,a_1,a_2,...,a_m\}$, where m is a positive integer and all elements of G are distinct and further let us suppose that one of the elements of G is the identity element of G under the operation o. Let it be denoted by e. It is certainly different from a_o because of (ii) and because a_o is the left zero under o. It can be seen that a_o is also the right zero because

$$a_o o a = a_o = e o a_o \text{ implies that } a o a_o = a_o o e = a_o$$

Thus, in LA-monoid,

$$a_o o a = a o a_o = a_o \ . \qquad (1)$$

Let us now consider the subset G^o of G which is obtained from it by deleting a_o, so that $G^o = \{a_i : i=1,2,...,m\}$. In view of the facts that a_o is a zero under o and it is left identity under * and that (G,o) is a finite LA-monoid, (G^o,o) is also a finite LA-monoid having the same e as the left identity in which all elements are distinct.

Let us examine whether an element a of G^o has an inverse in G^o under o or not. Let us form a set $H = \{a_k o a_1, a_k o a_2, ..., a_k o a_m\}$, where $a_k \neq a_o$. If

$a_k = a_o$ then because a_o is a zero in G under o and the left identity under *, the ultimate form of the set H will be $\{a_o\}$. Therefore it has been supposed that $a_k \neq a_o$.

We assert that all the elements of H are distinct. Suppose otherwise and let

$$a_k \text{ o } a_r = a_k \text{ o } a_s \qquad (2)$$

for $r,s = 1,2,\ldots,m$ and $r \neq s$. Since H is an LA-monoid under o, therefore (2) implies that

$$a_r \text{ o } a_k = a_s \text{ o } a_k \qquad (3)$$

(in an LA-monoid ab = cd implies that ba = dc)

for $r,s = 1,2,\ldots,m$ and $r \neq s$. Consider now the element $(a_s * a_r^{-1})\text{o}a_k$, which is certainly an element of the set G, where a_r^{-1} is the left inverse of a_r in G with respect to * (because (G,*) is an LA-monoid with left inverses. Now,

$$\begin{aligned}(a_s*a_r^{-1})\text{o}a_k &= (a_s\text{o}a_k)*(a_r^{-1}\text{o}a_k)\\ &= (a_r\text{o}a_k)*(a_r^{-1}\text{o}a_k), \text{ because of 3.}\end{aligned}$$

Thus $(a_s * a_r^{-1}) o a_k = (a_r * a_r^{-1}) o a_k$

$$= a_o o a_k$$

$$= a_o ,$$

because of (iii) and the facts that a_r^{-1} is the inverse of a_r under * and a_o is a left zero under o. Thus,

$$(a_s * a_r^{-1}) o a_k = a_o .$$

Since $a_k \neq a_o$, therefore because of (iv)

$$a_s * a_r^{-1} = a_o .$$

Next, $(a_s * a_r^{-1}) * a_r = a_o * a_r$ implies that

$(a_s * a_r^{-1}) * a_r = a_r$ because a_o is the left identity in G under *. Hence by the left invertive law,

$$a_r = (a_s * a_r^{-1}) * a_r$$

$$= (a_s * a_r^{-1}) * a_s$$

$$= a_o * a_s$$

$$= a_s .$$

This proves that $a_r = a_s$.

But since $a_o, a_1, \ldots, a_m$ are distinct elements of the set G and so $a_1, \ldots, a_m$ are also the distinct elements of the set G^o. In no case any element of the set G^o will be equal to the other. Therefore the result $a_r = a_s$ contradicts our assumption; this proves our assertion that H contains distinct elements.

Next since H contains distinct elements and the number of elements of the set H is equal to the number of the elements of the set G^o and each element of H is an element of G^o, therefore $H = G^o$.

Also, since G^o is an LA-monoid under o with the left identity e, so is H and hence H contains the left identity e. So e will be of the form $a_i o a_j$, so $e = a_i o a_j$ showing that a_i is left inverse of a_j under o. But in an LA-monoid (if it contains left inverses) every left inverse is a right inverse. Thus a_j is the right inverse of a_i under o.

It can similarly be shown that each element of G^o has unique inverse under o by constructing different sets just like H, by choosing other elements of the set G^o instead of a_k. Thus, we have shown so far, that G^o is an LA-monoid with inverses under o. Meaning thereby that G^o is an LA-group under o.

If a_i, a_j, a_k belong to G^o such that:

$a_i o\ a_k = a_j\ oa_k$, then using the left invertive law

$$(a_i oa_k)oa_k^{-1} = (a_j oa_k)oa_k^{-1}$$

implies that $(a_k^{-1}oa_k)oa_i = (a_k^{-1}oa_k)oa_j$.

This implies that $a_i = a_j$.

Thus G^o is right cancellative under o. But G^o being right cancellative LA-monoid under o, is a left cancellative LA-monoid also, therefore G^o is a cancellative LA-monoid. Since G^o is a cancellative LA-monoid whose elements satisfy condition (v), therefore by applying Theorem 2.1, we conclude that G^o is a commutative group under o.

COROLLARY 2.4

If (G,o) is a finite LA-monoid with a left zero a_o, then $(G\setminus\{a_o\},o)$ is a cancellative LA-monoid with inverses provided there is another binary operation * such that:

(i) (G,*) is an LA-monoid with left inverses

(ii) $a_o * a = a$ for all a in G

(iii) (a*b)oc = (aoc)*(boc) for all a,b,c in G,

and

(iv) aob = a_o implies that either a = a_o or b = a_o for all a,b in G.

PROOF

The proof is analogous to the proof of theorem 2.3.

CHAPTER THREE

LA-GROUPS AS HOMOMORPHIC IMAGES OF LEFT INVERSE QUASIGROUPS

In [12], U.C. Guha and T.K. Hoo have defined a CA-element of a quasigroup Q. They call an element x of a quasigroup Q a CA-element if x satisfies the two conditions

(1) $a(xb) = b(ax)$ and

(2) $(ax)b = (xb)a$, where a,b are any two elements of Q. Further, they call Q a CA-Quasigroup (or CA-loop) if it has at least one CA-element. If Q has at least one CA-element, then Q is a loop and is called a CA-loop. Let A(a) denote the subset

containing all the CA-elements of Q. Then Guha and Hoo have proved a CA-loop Q may be decomposed into mutually exclusive cosets of A(Q).

In 1967, T.S. Frank [10] has defined an inverse quasigroup (Q,o). He has given what amounts to an elegant construction of the universal group of (Q,o). This applies, in particular, when (Q,o) is obtained from a group G by taking Q = G and $aob = a^{-1}b$.

Later, P. Singh and N.S. Yadev [42] have generalized the definition of an inverse quasigroup and defined a homomorphism of the system, called a pseudo-inverse quasigroup into a group. They have exhibited a group that has the smallest kernel when the system is mapped homomorphically into it.

M.A. Kazim and M. Naseeurdin [20] have defined a non-associative structure, called an LA-semigroup, which is midway between a groupoid and a commutative semigroup. They have established the conditions under which the structure is a commutative semigroup, a quasigroup, a loop or a group. The structure was later studied by Q. Mushtaq and S.M. Yusuf [32], Q. Mushtaq and S. Kamran [31] and Q. Mushtaq and Q. Iqbal [30].

In this chapter, a system known as a left pseudo-inverse quasigroup has been defined and the question of the possibility of its closest possible resemblance with an LA-group has been investigated. A left pseudo-inverse quasigroup is a more generalized structure than those considered in [10],[12] and [43].

The technique adopted for the purpose is that of mapping the system homomorphically into an LA-group and then examining the kernel of the homomorphism. Intuitively, the smaller the kernel, the more LA-group like the system is. A suitable LA-group has been found such that, if the system is mapped homomorphically into it, the kernel is the smallest and hence in our sense the LA-group resembles the system most closely.

Recall that LA-semigroup [20], is a groupoid whose elements satisfy the left invertive law.

$$(ab)c = (cb)a \tag{1}$$

An LA-semigroup is medial, that is,

$$(ab)(cd) = (ac)(bd) \tag{2}$$

and, if it possesses left identity then

$$ab = cd \text{ implies that } ba = dc \tag{3}$$

it is left cancellative, if ab = ac implies that

$$b = c \tag{4}$$

and right cancellative if ba = ca implies that

$$b = c \tag{5}$$

A subset H of an LA-group G is called an LA-subgroup if H is an LA-group under the same binary operation. Notice that (aH)(bH) = (ab)H for all a,b in G implies that we do not need the concept of 'normality' as we do in group theory, to obtain a factor LA-group G/H [18].

If a^{-1} is the inverse of a in an LA-group G, then for all a in G, it is easy to check that

$$(a^{-1})^{-1} = a \tag{6}$$

and for all a,b in G,

$$(ab)^{-1} = a^{-1}b^{-1} . \tag{7}$$

It is important to note that because of the left invertive law during the course of discussion hereafter the braces essentially fall to the left wherever occur. Further to that, S. Kamran in [18] has proved that an LA-group can be decomposed into right cosets only and RA-group into left cosets only.

3. PSEUDO-INVERSE QUASIGROUPS AND LA-GROUPS

Let Q be a non empty set and 'o' a binary operation defined in it. The system (Q,o) is called a left pseudo-inverse quasigroup if for any a in Q, their exists an element a′ in Q such that

$$(boa)oa' = b \qquad (8)$$

for every b in Q. The element a′ is called a left pseudo-inverse of a. It is a generalization of the concept of pseudo-inverse defined in [43].

Let us have an example of a left pseudo-inverse quasi-group.

EXAMPLE 3.1

Let (G,.) be an LA-group. Define a binary operation 'o' in G as follows. For every a,b in G, let boa = b.a′, where $a' = a^{-1}$. Then (G,o) is a left pseudo-inverse quasigroup, because

(boa)oa′ = (b.a′)oa′ = (b.a′).a″ (by virtue of (6)) it is (b.a′).a = (a.a′).b = e.b = b, by the fact that e is left identity in (G,.).

We shall need the following results for our main result, namely, Theorem 3.9.

THEOREM 3.2

In a left pseudo-inverse quasigroup (Q,o), the right cancellative law holds.

PROOF

For every a,b,c in Q, boa = coa implies that (boa)oa′ = (coa)oa′ and so by (8), b = c.

THEOREM 3.3

If a′ is a left pseudo-inverse for a, then a is also a left pseudo-inverse for a′.

PROOF

By (8) and (5),

{(boa′)oa}oa′ = boa′   implies that

(boa′)oa = b = (boa)oa′ .

Thus, if a′ is a left pseudo-inverse for a, then a is also a left pseudo-inverse for a′.

THEOREM 3.4

If (Q,o) is left pseudo-inverse quasigroup, then for every a,b in Q, their exists a unique d in Q such that doa = b.

PROOF

By (8) and theorem 3.2, (boa′)oa = b implies that doa = b where d = boa′.

For uniqueness, let doa = b and $d_1$oa = b. Then by Theorem 3.2, doa = $d_1$oa implies that d = d_1.

THEOREM 3.5

If (Q,o) is a left pseudo-inverse quasigroup and a′,a″ are left pseudo-inverses of a belonging to Q, then boa′ = boa″ for every b in Q.

PROOF

Since (boa′)oa = b = (boa″)oa therefore by

Theorem 3.2, $(boa')oa = (boa'')oa$ implies that $boa' = boa''$.

A homomorphism f from a left pseudo-inverse quasigroup (Q,o) to a given LA-group (G,.) is a mapping from Q to G such that, $f(aob) = f(a).f(b)$ for all a,b in Q.

It is important to mention here that if a' is a pseudo-inverse of a in (Q,o) then,

$$f(a') = (f(a))^{-1} \qquad (9)$$

because $(boa)oa' = b$ implies that

$$\begin{aligned} f(b) &= f((boa)oa') \\ &= (f(b).f(a)).f(a') \\ &= (f(a').f(a)).f(b), \text{ by left invertive law .} \end{aligned}$$

Since (G,.) contains the left identity and it is right cancellative,

$$e = f(a').f(a),$$

that is

$$f(a') = (f(a))^{-1} .$$

The kernel K_f of f is defined as:
{x ∈ Q: f(x) = e, where e is the left identity of (G,.)}.

THEOREM 3.6

In the above notation (K_f,o) is a left pseudo-inverse sub-quasigroup of (Q,o).

PROOF

Let k be in K_f. Then there exists k′ in Q such that, (aok′)ok = a for a in k. Now operating f on it we get f((aok′)ok) = f(a) and because k belongs to K_f and because of (1) and e is left identity of (G,.),

$$(f(a).f(k')).f(k) = (f(a).f(k')).e$$
$$= (e.f(k')).f(a) = f(k').f(a).$$

This implies that

$$f(k').f(a) = f(a) .$$

Thus $f(k').f(a) = e.f(a)$ and so $f(k') = e$ because e is the left identity in (G,.) and because of (5). Hence k' belongs to Q and so $(aok')ok = a$ implies that K_f is a left pseudo-inverse sub-quasigroup.

The nucleus N(Q) of (Q,o) is the set $\{xox': x \in Q\}$. It is obvious from Theorem 3.3 that $N(Q) = \{x'ox: x \in Q\}$.

If (a,b,c) is any ordered triple of elements of Q, then by Theorem 3.4 there exists an element x in Q such that, $(aob)oc = xo\{(cob)oa\}$.

We call x an invertor and will denote it by <abc>. Let A(Q) be the set of all invertors in (Q,o).

THEOREM 3.7

In the above notation, $N(Q) \cup A(Q) \subseteq K_f$.

PROOF

Recall that N(Q) consists of the elements of the form xox' or $x'ox$ and $A(Q)$ contains the elements $x = \langle abc \rangle$ where $(aob)oc = \langle abc \rangle((cob)oa)$.

Now $a = (aox')ox$ implies that

$$
\begin{aligned}
f(a) &= f((aox')ox) \\
&= (f(a).f(x')).f(x) \\
&= (f(x).f(x')).f(a), \quad \text{by virtue of (8) and (1)} .
\end{aligned}
$$

Thus because of (5),

$$e.f(a) = (f(x).f(x')).f(a) \quad \text{implies that}$$

$$e = f(x).f(x')$$

$$e = f(xox').$$ Hence xox' belongs to K_f ,

that is, $N(Q) \subseteq K_f$.

Since $(aob)oc = \langle abc \rangle o((cob)oa)$, therefore $f((aob)oc) = f(\langle abc \rangle o((cob)oa))$. Then by (1),

$$
\begin{aligned}
((f(a).f(b)).f(c) &= f(\langle abc \rangle).((f(c).f(b)).f(a)) \\
&= f(\langle abc \rangle).((f(a).f(b))).f(c)) .
\end{aligned}
$$

Now, by (5), we get

$$e = f(\langle abc \rangle),$$

which implies that $\langle abc \rangle$ belongs to K_f. That is,

$A(Q) \subseteq K_f$. Hence $N(Q) \cup A(Q) \subseteq K_f$.

A subset S of Q is said to partition (Q,o) if and only if:

(i) for any a,b in Q, the sets Soa and Sob are either identical or disjoint.

(ii) if $x \in Soa$ and $y \in Sob$, then $xoy \in So(aob)$.

THEOREM 3.8

The kernel K_f partitions (Q,o).

PROOF

Let $K_f oa \cap K_f ob \neq \phi$, for some a,b in Q. Then we show that $K_f oa = K_f ob$. Let $k_1, k_2 \in K_f$ such that $k_1 oa = k_2 ob$. Then $f(k_1 oa) = f(k_2 ob)$ implies that $f(k_1).f(a) = f(k_2).f(b)$ or $f(a) = f(b)$.

$$\begin{aligned} \text{Now } f((K_f ob)oa') &= (f(K_f).f(b)).f(a') \\ &= (f(a').f(b)).f(K_f) \\ &= e.f(K_f) \\ &= e \end{aligned}$$

implying that $(K_f ob) oa' \subseteq K_f$. Thus $((K_f ob) oa') oa \subseteq K_f oa$ implies that $K_f ob \subseteq K_f oa$ as $((K_f ob) oa') oa = K_f ob$. Similarly $K_f ob \subseteq K_f oa$ and so $K_f oa = K_f ob$. Further, let $x \in K_f oa$ and $y \in K_f ob$.

Then $x = k_1 oa$ and $y = k_2 ob$ for k_1, k_2 in K_f. Then $f(x) = f(k_1 oa) = f(k_1).f(a) = e.f(a) = f(a)$ and similarly $f(y) = f(b)$. Thus

$$f(x).f(y) = f(a).f(b)$$

or $$f(xoy) = f(aob).$$

Thus, because of (9) and the fact that f is a homomorphism,

$$\begin{aligned} e &= f(xoy).(f(aob))^{-1} \\ &= f(xoy).f((aob)') \\ &= f((xoy)o(aob)') . \end{aligned}$$

This shows that $(xoy)o(aob)'$ belongs to K_f. Hence $((xoy)o(aob)')o(aob)$ belongs to $K_f o(aob)$, that is, (xoy) belongs to $K_f o(aob)$ by virtue of (1). Thus K_f partitions (Q,o).

Let H denote the intersection of all left pseudo-inverse sub-quasigroups of (Q,o) which partition (Q,o) and contain N(Q) ∪ A(Q). Then, one can check easily that (H,o) is left pseudo-inverse sub-quasigroup of (Q,o). Also, the kernel of any homomorphism from (Q,o) into any LA-group must contain (H,o).

In the next two theorems, we shall show that there is a homomorphism from (Q,o) to a suitable LA-group constructed with the help of H as the kernel of the homomorphism.

THEOREM 3.9

The collection {Hoa: a ∈ Q} forms an LA-group under the binary operation * defined b (Hoa)*(Hob)= Ho(aob), where H is the intersection of all left pseudo-inverse sub-quasigroups of the left pseudo-inverse quasigroup (Q,o).

PROOF

Let $Hoa_1 = Hoa_2$ and $Hob_1 = Hob_2$. Let $a_1 \in H$. Then $a_1oa'_1 \in H$, because $N(Q) \subseteq H$. Also, $(a_1oa'_1)oa_1 \in Hoa_1$ implies that $a_1 \in Hoa_1$ or $a_1 \in Hoa_2$ as H partitions (Q,o). Similarly, $b_1 \in Hob_2$ and So, again because of the fact that H partitions (Q,o), $Ho(a_1ob_1) = Ho(a_2ob_2)$. Hence $Hoa_1 = Hoa_2$ and $Hob_1 = Hob_2$ imply that $Ho(a_1ob_1) = Ho(a_2ob_2)$. Thus the operation * is well-defined. Now,

$$\begin{aligned} H*(Hoa) &= Ho(aoa')*(Hoa) \\ &= Ho((aoa')oa) \\ &= Hoa \qquad \text{because } aoa' \in H. \end{aligned}$$

$N(Q) \subseteq H$ and $Ho(aoa') = H$. Thus, $H*Hoa = Hoa$, that is, H is the left identity of Hoa under *.

Since $A(Q) \subseteq H$, we have $H = Ho\langle abc\rangle$ and so

$$\begin{aligned} H*((Hoc*Hob)*Hoa)) &= Ho\langle abc\rangle*((Hoc*Hob)*Hoa) \\ &= Ho\langle abc\rangle*((Ho(cob))*Hoa) \end{aligned}$$

$$= Ho\langle abc\rangle * (Ho((cob)oa))$$

$$= Ho\langle abc\rangle o((cob)oa)$$

$$= Ho((aob)oc)$$

$$= (Ho(aob)) * Hoc$$

$$= (Hoa * Hob) * Hoc \ .$$

Hence, $\{Hoa: a \in Q\}$ is an LA-semigroup with left identity, which one can show easily, is unique.

Since $aoa' \in H$. Therefore $(Hoa)o(Hoa') = Ho(aoa') = H$. Also, $(Hoa')o(Hoa) = Ho(a'oa) = H$ as $aoa' \in H$ and $N(Q) \subseteq H$. Thus, the collection $\{Hoa: a \in Q\}$ is an LA-group under the binary operation $*$ defined by $(Hoa)*(Hob) = Ho(aob)$.

THEOREM 3.10

There is a homomorphism F from a left pseudo-inverse quasigroup (Q,o) to the LA-group $(G,*)$ where $G = \{Hoa: a \in Q\}$, defined by $F(a) = Hoa$ with kernel $K_F = H$.

PROOF

Since $F(a) = Hoa$ for all $a \in (Q,o)$, therefore

$$F(aob) = Ho(aob)$$
$$= (Hoa)*(Hob)$$
$$= F(a)*F(b)$$

implies that F is a homomorphism.

Let $a \in K_F$. As $K_F \subseteq Q$ and H is the left identity of $(G,*)$, therefore, $F(a) = H$. But $F(a) = Hoa$ and so $Hoa = H$ implies that $a \in H$. Thus $K_F \subseteq H$.

Conversely, let $a \in H$. Then $H = Hoa = F(a)$ implies that $a \in K_F$. Hence $H \subseteq K_F$. Combining the two inclusions, we conclude that $K_F = H$.

Thus H is the smallest kernel of the homomorphism F and so $(G,*)$ is the most closely resembling LA-group to the left pseudo-inverse quasigroup (Q,o).

We may point out that H can be regarded as the measure of the degree to which (Q,o) is like an LA-group.

CHAPTER FOUR

LA-MONOID WITH ELEMENTS AND THEIR POWERS

T. Tamura and N. Kimura in [43], proved that any commutative semigroup G is uniquely expressible as a semilattice of archimedean semigroups. Later E. Hewitt and H.S. Zuckerman in [14], proved that the following conditions are mutually equivalent:

(i) G is separative, (ii) the archimedean components of G are cancellative, (iii) G can be embedded in a union of groups.

Q. Mushtaq and S.M. Yusuf in [34], have extended their results to a locally associative LA-semigroup G, which we know, is not an associative structure.

They defined a locally associative LA-semigroup G to be an LA-semigroup wherein for every a in G, (aa)a = a(aa). They have also shown that a locally associative LA-semigroup does not necessarily have associative powers.

EXAMPLE 4.1

For example, in a locally associative LA-semigroup G = {a,b,c}, defined by the table:

.	a	b	c
a	c	c	b
b	b	b	b
c	b	b	b

$$a(a(aa)) = c \neq b = (a(aa))a$$

Q. Mushtaq and S.M. Yusuf in [34], put an extra condition on a locally associative LA-semigroup that it should possess a left identity. Thus for a locally associative LA-monoid they proved most of the results contained in this chapter.

Q. Mushtaq and Q. Iqbal in [30] and Q. Iqbal in [17] have discussed the decomposition of a locally associative LA-semigroup. They have defined a relation η on a locally associative LA-semigroup G such that, for a,b in G, $a\eta b$ if and only if each of the elements a and b divides some power of the other. Then they have proved that the relation η on G is the least semilattice congurence on G and that G/η is a maximal semilattice homomorphic image of G.

They have also shown that G with left idenity is separative if and only if its archimedean components are cancellative and that the G can be embedded in a semigroup which is a union of groups if and only if G is separative.

The condition for an LA-monoid to be locally associative is sufficiently strong. In this chapter we have dropped this condition and without imposing any extra condition on an LA-monoid have established most of the results, proved by Q. Mushtaq, and S.M. Yusuf, in [34] and by Q. Mushtaq, and Q. Iqbal in [30]. The results proved independently in this chapter heavily hinge upon some fundamental results and pre-requisites, proved and deduced in the earlier section of this chapter. These pre-requisites have provided a strong foundation for our subsequent discussion of theorems. Of the vital importance is our result that "the left identity becomes the right identity for every element with even positive integral index". We have shown that every positive integral index can be added, provided the odd positive integral index falls to its right and the even positive integral index falls to its left. It has been shown that the odd powers commute with odd and even with even. During this course, it is worth mentioning that the generalization of results in not quite straight forward, rather sometimes it becomes tedious. There are enormous results which one would like to prove and continue the study in this thesis, but we have restricted ourselves to a few results. Nevertheless, the study is interesting and gives enough insight for further study. To start with, we are giving the definition of a positive integral index of an element of an LA- monoid and shall gradually go on deducting the minor and major results.

DEFINITION 4.1

If G is an LA-monoid and a belongs to G, then we define a^m for every positive integer m as follows:

(i) $a^m = (((aa)a)a)a \ldots$ m times. It implies that $a^2a = a^3$, $a^3a = a^4$, ...

(ii) $a^{m-1}a = a^m$, $a^ma = a^{m+1}$.

LEMMA 4.2

If G is an LA-monoid then for positive integer m and for every a in G, $a^2a^m = a^{m+2}$.

PROOF

$a^2a^m = (aa)a^m$ by definition and by left invertive law $= (a^ma)a = (a^{m+1})a = a^{m+1+1} = a^{m+2}$ by definition given above.

LEMMA 4.3

If G is an LA-monoid and a belongs to G, then for every positive integer m,

(A) $a^m = a^{m-1}a = a^{m-3}a^3 = a^{m-5}a^5 = a^{m-7}a^7 = \dots$

(B) $a^m = a^2a^{m-2} = a^4a^{m-4} = a^6a^{m-6} = \dots$

PROOF

By definition 4.1(ii) and by left invertive law we have,

$$a^m = a^{m-1}a$$
$$= (a^{m-2}a)a.$$
$$= (aa)a^{m-2} \quad = a^2a^{m-2} \qquad \text{(i)}$$

Since G is an LA-monoid, it possesses left identity e, therefore, $a^2a^{m-2} = (ea^2)(a^{m-2}) = (ea^2)(a^{m-3}a)$, which by definition, by medial law and since e is the left identity $= (ea^{m-3})(a^2a) = a^{m-3}a^3$. Thus

$$a^2a^{m-2} = a^{m-3}a^3 \qquad \text{(ii)}$$

Now, by definition and by left invertive law

$$a^{m-3}a^3 = (a^{m-4}a)a^3 = (a^3a)a^{m-4} = a^4a^{m-4} \qquad \text{(iii)}$$

Further, by left invertive law and since e is the left identity, $a^4a^{m-4} = (ea^4)a^{m-4} = (ea^4)(a^{m-5}a) = (ea^{m-5})a = a^{m-5}a^5$ (iv)

Repeating the above process, we conclude the results given in Lemma 4.3.

REMARK 4.4

If anywhere occurs a^o, it will be considered as left identity e.

THEOREM 4.5

If G is an LA-monoid and a belongs to G, then for every positive integer n,

$$a^{2n} = a^{2n-1}a = aa^{2n-1} .$$

PROOF

By Lemma 4.3, we have $a^m = a^{m-1}a = a^{m-3}a^3 = a^{m-5}a^5 = \ldots$ Generalization of the results gives $a^m = a^{m-1}a = \ldots = a^{m-2n+1}a^{2n-1}$, where $m \geq 2n$, m and n being positive integers. Now for m = 2n, it implies that

$$a^{2n} = a^{2n-1}a = aa^{2n-1} .$$

COROLLARY 4.6

For m = 2n+1, $a^{2n+1} = a^{2n}a = a^2a^{2n-1}$.

THEOREM 4.7

If G is an LA-monoid and a belongs to G, then for every positive integr m and n,

$$a^m a^{2n-1} = a^{m+2n-1} .$$

PROOF

By induction, the theorem is true for m = 1, Now, because of theorem 4.5, that is,

$$aa^{2n-1} = a^{2n} .$$

Therefore, by definition, by left invertive law, by theorem 4.5 and by induction

$$a^{m+1}a^{2n-1} = (a^m a)(a^{2n-1}) = (a^{2n-1}a)(a^m)$$
$$= (aa^{2n-1})(a^m) = (a^m a^{2n-1})a$$
$$= a^{m+2n-1}a = a^{m+2n-1+1} = a^{m+1+2n-1} .$$

Thus $a^{m+1}a^{2n-1} = a^{m+1+2n-1}$.

LEMMA 4.8

If G is an LA-monoid and a belongs to G, then for every positive integer m and n,

$$a^{2n}a^{m} = a^{2n+m} .$$

PROOF

Also follows by induction [34]. But we are giving here a simpler proof. We have by theorem 4.7 $a^{m}a^{2n-1} = a^{m+2n-1}$ therefore, it implies that $(a^{m}a^{2n-1})a = (a^{m+2n-1})a$ which by left invertive law to the L.H.S. and by definition to the R.H.S. yields $(aa^{2n-1})(a^{m}) = a^{m+2n-1+1}$. By lemma 4.5 it implies that, $a^{2n}a^{m} = a^{m+2n} = a^{2n+m}$.

REMARK 4.9

The odd powers with odd and even powers with even of an element of an LA-monoid commute for all positive integral powers, that is, $a^{2k-1}a^{2n-1} = a^{2n-1}a^{2k-1}$ by virtue of theorem 4.7 and by virtue of lemma 4.8, $a^{2n}a^{2k} = a^{2k}a^{2n}$ where k and n are positive integers.

REMARK 4.10

$a^{2n-1}a^{m} \neq a^{2n-1+m}$, when m is a positive even integer. The result does not hold true for m = 2. The even powers can only be added when they fall to the left, by lemma 4.8. Hence the *odd and even* powers of an element *do not commute*.

COROLLARY 4.11

If m is positive even intger, then in an LA-monoid G for all a in G and for every positive integer n, $(a^{2n-1}a^{m})e = a^{2n-1+m}$, where e is the left identity of G.

PROOF

Now by left invertive law and the theorem 4.7

$(a^{2n-1}a^{m})e = (ea^{m})(a^{2n-1}) = a^{m}a^{2n-1} = a^{m+2n-1} =$

a^{2n-1+m}.

LEMMA 4.12

If G is an LA-monoid and a belongs to G, then for every positive integer m and n,

$$a^m a^{2n-1} = a^{m+2n-1} = a^{2n-2}a^{m+1} = a^{m+2}a^{2n-3} = a^{2n-4}a^{m+3} = \ldots$$

PROOF

By theorem 4.7, $a^m a^{2n-1} = a^{m+2n-1}$, so it implies that $(a^m a^{2n-1})e = (a^{m+2n-1})e$. Therefore, by left invertive law to the L.H.S. we have $(ea^{2n-1})a^m = (a^{m+2n-1})e$. Since e is the left identity in G so $a^{2n-1}a^m = (a^{m+2n-1})e$ and thus $(a^{2n-2}a)a^m = (a^{m+2n-1})e$ which due to left invertive law renders $(a^m a)a^{2n-2} = (a^{m+2n-1})e$ and so by definition $a^{m+1}a^{2n-2} = (a^{m+2n-1})e$, therefore we easily have $(a^{2n-2}a^{m+1})e = (a^{m+2n-1})e$. Thus by right cancellation, $a^{2n-2}a^{m+1} = a^{m+2n-1} = a^m a^{2n-1}$ (i)

Further, $a^{2n-2}a^{m+1} = a^m a^{2n-1}$, it implies that $(a^{2n-3}a)a^{m+1} = a^m a^{2n-1}$ which by left invertive law to the L.H.S. gives $(a^{m+1}a)a^{2n-3} = a^m a^{2n-1}$ and thus

$a^{m+2}a^{2n-3} = a^m a^{2n-1}$ (ii)

The other results follow similarly.

LEMMA 4.13

If G is an LA-monoid and a belongs to G, then for every positive integer m and n,

$$a^{2n}a^m = a^{m+2n} = a^{m+1}a^{2n-1} = a^{2n-2}a^{m+2} = a^{m+3}a^{2n-3} = \ldots$$

PROOF

Now, by lemma 4.8, $a^{2n}a^m = a^{m+2n}$ implies that $(a^{2n-1}a)a^m = a^{m+2n}$ which due to left invertive law gives $(a^m a)a^{2n-1} = a^{m+2n}$ and thus,

$$a^{m+1}a^{2n-1} = a^{m+2n} = a^{2n}a^m \qquad \text{(i)}$$

Further, $a^{m+1}a^{2n-1} = a^{2n}a^{m}$ implies that $(a^{m+1}a^{2n-1})e = (a^{2n}a^{m})e$ which due to left invertive law to the L.H.S. renders $(ea^{2n-1})a^{m+1} = (a^{2n}a^{m})e$ and since e is the left identity in G so $a^{2n-1}a^{m+1} = (a^{2n}a^{m})e$ which by definition gives $(a^{2n-2}a)a^{m+1} = (a^{2n}a^{m})e$. Then by left invertive law to the L.H.S. $(a^{m+1}a)a^{2n-2} = (a^{2n}a^{m})e$ which by definition yields $a^{m+2}a^{2n-2} = (a^{2n}a^{m})e$ which enables us to have $(a^{2n-2}a^{m+2})e = (a^{2n}a^{m})e$ and thus by right cancellation $a^{2n-2}a^{m+2} = a^{2n}a^{m}$. Hence $a^{2n}a^{m} = a^{2n-2}a^{m+2}$. (ii)

The other results follow similarly.

We now come across with a very important and crucial result of LA-semigroup theory which is a key note for our subsequent theorems in general and for our theorem 4.14 in particular.

THEOREM 4.14

If G is an LA-monoid with left identity e and a belongs to G, then for every positive integer n, $a^{2n} = a^{2n}e$.

PROOF

We have from theorem 4.5 $a^{2n} = a^{2n-1}a = aa^{2n-1}$, which implies that $a^{2n}e = (a^{2n-1}a)e = (aa^{2n-1})e$. Then by left invertive law, by theorem 4.5 and since e is the left identity $(ea)a^{2n-1} = (ea^{2n-1})a = aa^{2n-1} = a^{2n-1}a$. Hence $a^{2n}e = a^{2n}$.

THEOREM 4.15

A necessary and sufficient condition for a subset Q of an LA-monoid G with left identity e to become a commutative monoid is, that each of its elements should consist of even powers of some element of G.

PROOF

The condition is necessary. Suppose each b in Q is an even power of some a in G. Then Q is non-empty for $e^2 = ee = e$ belongs to Q. Further every b in Q is of the form $b = a^{2n}$ and $a^{2n} = a^{2n}e$ by theorem 4.14. Thus every b in Q implies that b = be which implies that e is also the right identity of Q. Hence by [33], Q is a commutative monoid.

Conversely, if Q is a commutative monoid of an LA-monoid G with left identity e then Q consists of even powers of elements of G. Since Q is a commutative monoid it contains two sided identity. Thus for every b in Q we have b = eb = be. As Q is a subset of G therefore, each b in Q is an element of LA-monoid G. Hence each b in G wherein b = eb = be, by virtue of theorem 4.14 implies that $b = a^{2n}$ for some a in G and positive integer n.

COROLLARY 4.16

The subset Q defined in theorem 4.15 being commutative monoid satisfies every result and property of a semigroup or a commutative semigroup.

REMARK 4.17

If G is an LA-monoid, then for every a,b,c in G and positive integers k,m and n, we have the following immediate results:

$$a^2b^2 = b^2a^2 \quad (1)$$

$$a^{2k}b^{2k} = b^{2k}a^{2k} \quad (2)$$

$$a^{2k}(b^{2k}c^{2k}) = (a^{2k}b^{2k})c^{2k} \quad (3)$$

$$a^{2m}b^{2n} = b^{2n}a^{2m} \quad (4)$$

$$a^{2m}(b^{2n}c^{2k}) = (a^{2m}b^{2n})c^{2k} \quad (5)$$

THEOREM 4.18

If G is an LA-monoid then for every a,b in G and positive integer n, $(ab)^n = a^nb^n$.

PROOF

The result can be proved by induction [29]. But we are giving here another mode of proof based on successive application of medial law.

Now by medial law $(ab)^2 = (ab)(ab) = (aa)(bb) = a^2b^2$. Also by medial law again and by defintion $(ab)^3 = (ab)^2(ab) = (a^2b^2)(ab) = (a^2a)(b^2b) = a^3b^3$. Further more, by medial law and by definition again $(ab)^4 = (ab)^3(ab) = (a^3b^3)(ab) = (a^3a)(b^3b) = a^4b^4$. Hence the generalization culminates at the required result, namely, $(ab)^n = a^nb^n$.

THEOREM 4.19

If G is an LA-monoid and a belongs to G, then $(a^k)^m = a^{km}$ for every positive integer k and m. (A straight forward proof based on induction is given in [34].)

PROOF

Here two cases arise so we discuss them separately.

<u>CASE I</u>

When k is odd say $k = 2n-1$. Then $(a^k)^m = a^{km}$ implies that $(a^{2n-1})^m = a^{(2n-1)m}$. By induction the result is true for $m = 1$.

Now, by induction and by theorem 4.7 $(a^{2n-1})^{m+1} = (a^{2n-1})^m \ a^{2n-1} = a^{(2n-1)m} \ a^{2n-1} = a^{(2n-1)m+2n-1} = a^{(2n-1)(m+1)}$.

<u>CASE II</u>

When k is even say $k = 2n$. Then $(a^k)^m = a^{km}$ implies that $(a^{2n})^m = a^{(2n)m}$. By induction the result is true for $m = 1$.

Now, by induction and by lemma 4.8 $(a^{2n})^{m+1} = (a^{2n})^m \ a^{2n} = a^{(2n)m} \ a^{2n} = = a^{(2n)m+2n} = a^{(2n)(m+1)}$.

Thus $(a^k)^m = a^{km}$ whether k is odd or k is even.

DEFINITION 4.20

Let G be an LA-monoid. Define a relation ρ on G as follows:

$a\rho b$ if and only if $b^n a = b^{n+1}$ and $a^n b = a^{n+1}$.

THEOREM 4.21

If G is an LA-monoid and there exist positive integers m and n such that $b^m a = b^{m+1}$ and $a^n b = a^{n+1}$ then $a\rho b$.

PROOF

Here again two cases arise and we deal with them separetely.

<u>CASE I</u>

When the positive integers m and n simultaneously both are odd or both are even. For definiteness we assume that $m < n$, then it implies that n-m is even. We can multiply $b^m a = b^{m+1}$ by b^{n-m} and thus we have by lemma 4.8 $b^{n-m}(b^m a) = b^{n-m}b^{m+1} = b^{n-m+m+1} = b^{n+1}$. Also, by theorem 4.14, $b^{n-m}(b^m a) = (b^{n-m}e)(b^m a) = b^{n+1}$. Then by medial law $(b^{n-m}b^m)(ea) = b^{n+1}$. Since e is the left identity, therefore $(b^{n-m}b^m)a = b^{n+1}$. Hence by lemma 4.8 $b^{n-m+m}a = b^{n+1}$. Thus $b^n a = b^{n+1}$. Hence $b^m a = b^{m+1}$ implies that $b^n a = b^{n+1}$. Since $b^n a = b^{n+1}$ which implies that $a\rho b$.

CASE II

When one of the m and n is even the other is odd. To be definite let m be even and n be odd and that $m < n$, then it implies that n-m is odd. We can multiply $b^m a = b^{m+1}$ by b^{n-m} and thus by theorem 4.7 and as m+1 is odd we have $b^{n-m}(b^m a) = b^{n-m}(b^{m+1}) = b^{n-m+m+1} = b^{n+1}$. Also, since e is the left identity $b^{n-m}(b^m a) = b^{n+1}$ implies that $(eb^{n-m})(b^m a) = b^{n+1}$. Then by medial law $(eb^m)(b^{n-m}a) = b^m(b^{n-m}a) = b^{n+1}$.

Now, by theorem 4.14 and since m is even $(b^m e)(b^{n-m} a) = b^{n+1}$, which due to medial law gives $(b^m b^{n-m})(ea) = b^{n+1}$. Then by lemma 4.8 $(b^{m+n-m})(a) = b^{n+1}$ which implies that $b^n a = b^{n+1}$. Hence $b^m a = b^{m+1}$ implies that $b^n a = b^{n+1}$. Since $a^n b = a^{n+1}$ which implies that $a \rho b$.

Thus in all the cases whether m and n are both odd, both even or one is odd other is even we have $a \rho b$.

THEOREM 4.22

The relation ρ defined above on an LA-monoid is a congruence relation.

PROOF

Now $a \rho b$ implies that $b^k a = b^{k+1}$, $a^k b = a^{k+1}$. Clearly ρ is reflexive and symmetric.

For transitivity we have to examine the

situation in two cases, namely, when k is odd and when k is even.

CASE I

When k is odd, let $a\rho b$ and $b\rho c$ so that there exist positive integers n and m such that,

$$b^{2n-1}a = b^{2n}, \quad a^{2n-1}b = a^{2n} \qquad (i,ii)$$

$$c^{2m-1}b = c^{2m}, \quad b^{2m-1}c = b^{2m} \qquad (iii,iv)$$

Suppose that ℓ is odd, so that, $\ell = (2n)(2m)-1 = (2n-1)(2m) + (2m-1)$. Therefore we have $c^{\ell}a = \{c^{(2n-1)(2m)+(2m-1)}\}a$. Now, by theorem 4.7 and by theorem 4.14 $c^{\ell}a = \{c^{(2n-1)(2m)}c^{2m-1}\}a = \{(c^{(2n-1)(2m)}e)c^{2m-1}\}a$. Then repeatedly by left invertive law $c^{\ell}a = \{(c^{2m-1}e)c^{(2n-1)(2m)}\}a = \{ac^{(2n-1)(2m)}\}(c^{2m-1}e)$. Thus by theorem 4.19, by (iii) and by theorem 4.18 $c^{\ell}a = \{a(c^{2m})^{2n-1}\}(c^{2m-1}e) = \{a(c^{2m-1}b)^{2n-1}\}(c^{2m-1}e) = \{a(c^{(2m-1)(2n-1)}b^{2n-1})\}(c^{2m-1}e)$. Since e is the left identity and also by medial law $c^{\ell}a$ = $\{(ea)(c^{(2m-1)(2n-1)}b^{2n-1})\}(c^{2m-1}e)$ = $\{(ec^{(2m-1)(2n-1)}(ab^{2n-1})\}(c^{2m-1}e)$ = $\{c^{(2m-1)(2n-1)}((b^{2n-1}a)e)\}(c^{2m-1}e)$. Now, by (i) and because of theorem 4.14

$c^{\ell}a = \{c^{(2m-1)(2n-1)}((b^{2n})e)\}(c^{2m-1}e)$

$= \{c^{(2m-1)(2n-1)}b^{2n}\}(c^{2m-1}e)$. Then by medial law, theorem 4.7 and theorem 4.14

$c^{\ell}a = \{c^{(2m-1)(2n-1)}c^{2m-1}\}(b^{2n}e)$

$= \{c^{(2m-1)(2n-1)+2m-1}\}(b^{2n}e)$.

$= \{c^{(2m-1)(2n-1)+2m-1}\}b^{2n}$. Then by theorem 4.18 and because of (iii) we have,

$c^{\ell}a = c^{(2m-1)(2n)}b^{2n} = (c^{2m-1}b)^{2n} = (c^{2m})^{2n}$. Hence by our supposition in the beginning $c^{\ell}a$ = $c^{2n(2m)-1+1} = c^{\ell+1}$.

CASE II

When k is even, let $a\rho b$ and $b\rho c$ so that there exist positive integers n and m such that,

$$b^{2n}a = b^{2n+1} \quad , \quad a^{2n}b = a^{2n+1} \qquad (v,vi)$$

$$c^{2m}b = c^{2m+1} \quad , \quad b^{2m}c = b^{2m+1} \qquad (vii,viii).$$

suppose that ℓ is even, so that $\ell = 2n(2m+1)+2m$. Therefore, we have, $c^{\ell}a = \{c^{2n(2m+1)+2m}\}a$. Now by lemma 4.8, theorem 4.19 and by (vii) we have, $c^{\ell}a = \{c^{2n(2m+1)}c^{2m}\}a = \{c^{2m+1})^{2n}c^{2m}\}a = \{(c^{2m}b)^{2n}c^{2m}\}a$. Then by theorems 4.18, 4.19 and 4.14 $c^{\ell}a = \{((c^{2m})^{2n}b^{2n})c^{2m}\}a = \{(c^{2m(2n)}b^{2n})(c^{2m}e)\}a$. Therefore by medial law, by theorem 4.14 and by lemma 4.8, $c^{\ell}a = \{(c^{2m(2n)}c^{2m})(b^{2n}e)\}a = \{(c^{2m(2n)}c^{2m})b^{2n}\}a = (c^{2m(2n)+2m}b^{2n})a$. Further since e is the left identity, by medial law and by theorem 4.14, we have $c^{\ell}a = \{c^{(2n+1)2m}b^{2n}\}(ea) = (c^{(2n+1)2m}e)(b^{2n}a) = c^{(2n+1)2m}(b^{2n}a)$. Again by (v), by theorem 4.18 and by (vii) $c^{\ell}a = c^{(2n+1)2m}(b^{2n+1}) = (c^{2m}b)^{2n+1} = (c^{2m+1})^{(2n+1)}$. Thus by theorem 4.19 $c^{\ell}a = c^{(2m+1)(2n+1)}$. Hence by our supposition in the beginning $c^{\ell}a = c^{2n(2m+1)+2m+1} = c^{\ell+1}$. Hence whether k is odd or even, the transitivity of relation holds. Thus $a\rho b$ implying $b^k a = b^{k+1}$, $a^k b = a^{k+1}$ implies ρ is an equivalence relation.

We define the compatibility of ρ as follows. Assume that $a\rho b$ is such that for some positive integer k, $b^k a = b^{k+1}$ and $a^k b = a^{k+1}$. Let c belong to LA-monoid G. Then we show that (i) $bc\rho ac$ and (ii) $cb\rho ca$. Now, by theorem 4.18 and by medial law $(bc)^k(ac) = (b^k c^k)(ac) = (b^k a)(c^k c)$. Again by definition and by theorem 4.18 $(bc)^k(ac) = b^{k+1}c^{k+1} = (bc)^{k+1}$. Similarly by theorem 4.18, by medial law and by definition, $(ac)^k(bc) = (a^k c^k)(bc) = (a^k b)(c^k c) = a^{k+1}c^{k+1} = (ac)^{k+1}$.

This implies that $bc\rho ac$ (A)

Also by theorem 4.18 and by medial law $(cb)^k(ca) = (c^k b^k)(ca) = (c^k c)(b^k a)$, which by definition and by theorem 4.18 renders $(cb)^k(ca) = c^{k+1}b^{k+1} = (cb)^{k+1}$. In the same way, by theorem 4.18 and by medial law

$(ca)^k(cb) = (c^k a^k)(cb) = (c^k c)(a^k b)$. Again by definition and by theorem 4.18 $(ca)^k(cb) = (c^{k+1})(a^{k+1}) = (ca)^{k+1}$.

This implies that $cb\rho ca$. (B)

From (A) and (B) we conclude that ρ is compatible. Thus ρ is a congruence relation on G.

DEFINITION 4.23

A relation σ on an LA-monoid G is called "separative" if and only if $a^2\sigma ab$ and $b^2\sigma ab$ implies that $a\sigma b$.

REMARK 4.24

It is to be noted that the definition of a separative relation in an LA-monoid has the following implication. That is, $a^2\sigma ab$ and $b^2\sigma ab$ implies that $a\sigma b$, can be restated as $a^2e\sigma(ab)e$ and $b^2e\sigma(ab)e$, which means that $a^2\sigma ba$ and $b^2\sigma ba$, implying that $b\sigma a$ by virtue of the fact that e is the left identity in an LA-monoid, left invertive law and theorem 4.14.

THEOREM 4.25

The relation ρ is separative.

PROOF

Let a,b belong to an LA-monoid G with left identity e. Then by definition of ρ, there exist positive integers m and n such that,

$$(a^2)^m(ab) = (a^2)^{m+1} \quad , \quad (ab)^m a^2 = (ab)^{m+1}$$

$$(b^2)^n(ab) = (b^2)^{n+1} \quad , \quad (ab)^n b^2 = (ab)^{n+1} .$$

Now, by theorem 4.19 and 4.14, by medial law and by the fact that e is the left identity, $(a^2)^m(ab) = (a^{2m}e)(ab) = (a^{2m}a)(eb) = a^{2m+1}b$. Thus by definition of ρ and by theorem 4.19, $(a^2)^m(ab) = a^{2m+1}b = a^{2m+2} = (a^2)^{m+1}$.

Similarly, by theorem 4.19, by the fact that e is the left identity and by medial law $(b^2)^n(ab) = (b^{2n})(ab) = (eb^{2n})(ab) = (ea)(b^{2n}b) = ab^{2n+1}$. Again since e is the left identity and by definition we have $(b^2)^n(ab) = (ab^{2n+1}) = (b^{2n+1}a)e$, which by definition of ρ and by theorem 4.14, yields $(b^2)^n(ab) = (b^{2n+2})e = b^{2n+2}$. Thus $(b^2)^n(ab) = b^{2n+2}$, whence by theorem 4.19 $(b^2)^n(ab) = b^{2n+2} = (b^2)^{n+1}$. Hence by theorem 4.21, $a\rho b$ and therefore ρ is separative.

THEOREM 4.26

If G is an LA-monoid, then G/ρ is the maximal separative homomorphic image of G.

PROOF

We know that ρ is separative. Hence G/ρ is separative. We now show that ρ is contained in every separative congruence relation σ on G.

Let $a\rho b$ so that there exists positive integer n such that

$$b^n a = b^{n+1} \quad \text{and} \quad a^n b = a^{n+1} .$$

We have to show that $a\sigma b$, where σ is separative congruence on G. Let k be any positive integer such that $b^k a \sigma b^{k+1}$, $a^k b \sigma a^{k+1}$ (i)

Suppose now $k \geq 2$, then by theorems 4.18 and 4.19 $(b^{k-1}a)^2 = (b^{k-1})^2 a^2 = b^{2k-2}a^2 = b^{2k-2}(aa) = (b^k b^{k-2})(aa)$, whether k is odd or even and if k = 2, b^o will denote e the left identity of G. Thus by medial law $(b^{k-1}a)^2 = (b^k a)(b^{k-2}a)$, which implies that $(b^{k-1}a)^2 = (b^k a)(b^{k-2}a)$. But $(b^k a)(b^{k-2}a)\sigma(b^{k+1})(b^{k-2}a)$. Now two cases arise, that is, k is even or odd.

<u>CASE I</u>

Let k be odd. Then because k+1 is even, by theorem 4.14 and because of medial law;

$(b^{k+1})(b^{k-2}a) = (b^{k+1}e)(b^{k-2}a) = (b^{k+1}b^{k-2})(ea)$.

Again by theorem 4.7, by lemma 4.8 and by medial law $(b^{k+1})(b^{k-2}a) = (b^{k+1+k-2})(a) = (b^{2k-1})a = (b^{k-1}b^{k})(ea) = (b^{k-1}e)(b^{k}a)$. Then by theorem 4.14, we have, $(b^{k+1})(b^{k-2}a) = b^{k-1}(b^{k}a)$. (ii)

Further by medial law and since e is the left identity $(b^{k+1})(b^{k-2}a)=(eb^{k-1})(b^{k}a) =(eb^{k})(b^{k-1}a) = b^{k}(b^{k-1}a)$. (iii)

Hence $(b^{k-1}a)^{2}\sigma b^{k}(b^{k-1}a)$ (iv)

Now, $b^{k+1}\sigma b^{k}a$, implies that $(b^{k-1})(b^{k+1})\sigma b^{k-1}(b^{k}a)$ which because of k-1 is even and because of lemma 4.8 means $b^{(k-1)+(k+1)}\sigma b^{k-1}(b^{k}a)$ or $b^{2k}\sigma(b^{k-1})(b^{k}a)$. Therefore, by theorem 4.19, $(b^{k})^{2}\sigma(b^{k-1})(b^{k}a)$. But $b^{k-1}(b^{k}a) = b^{k}(b^{k-1}a)$ from (ii) and (iii) and this implies that $(b^{k})^{2}\sigma b^{k}(b^{k-1}a)$ (v)

Thus from (iv) and (v) we conclude that

$$(b^{k})^{2}\sigma(b^{k})(b^{k-1}a) \text{ and } (b^{k-1}a)^{2}\sigma b^{k}(b^{k-1}a) .$$

CASE II

Let k be even. Then because e is the left identity and because of medial law we have,

$(b^{k+1})(b^{k-2}a) = (eb^{k+1})(b^{k-2}a) = (eb^{k-2})(b^{k+1}a) = b^{k-2}(b^{k+1}a)$. Now since k-2 is even so by theorem 4.14 and by medial law, $(b^{k+1})(b^{k-2}a) = (b^{k-2}e)(b^{k+1}a) = (b^{k-2}b^{k+1})(ea)$. Further, by lemma 4.8 and since k-2 is even, we have, $(b^{k+1})(b^{k-2}a) = (b^{(k-2)+(k+1)})(ea) = (b^{2k-1})(ea) = (b^k b^{k-1})(ea)$. Again by medial law and by theorem 4.14, $(b^{k+1})(b^{k-2}a) = (b^k b^{k-1})(ea) = (b^k e)(b^{k-1}a) = b^k(b^{k-1}a)$. (i)

Now by medial law and since e is the left identity $(b^{k+1})(b^{k-2}a) = (eb^k)(b^{k-1}a) = (eb^{k-1})(b^k a) = b^{k-1}(b^k a)$ (ii)

Hence by virtue of (i) we have,

$(b^{k-1}a)^2 \sigma b^k(b^{k-1}a)$ (iii)

Now $b^{k+1}\sigma b^k a$ implies that $(b^{k-1})(b^{k+1})\sigma b^{k-1}(b^k a)$, which means $b^{(k-1)+(k+1)}\sigma b^{k-1}(b^k a)$. Again because $k+1$ is odd and because of theorem 4.7 it implies that $b^{2k}\sigma b^{k-1}(b^k a)$. Then by theorem 4.19 $(b^k)^2\sigma b^{k-1}(b^k a)$. But $b^{k-1}(b^k a) = b^k(b^{k-1})$ from (i) and (ii), and this implies that

$$(b^k)^2\sigma b^k(b^{k-1}a) \qquad \text{(iv)}$$

Thus we conclude from (iii) and (iv) that

$$(b^k)^2\sigma(b^k)(b^{k-1}a) \quad \text{and} \quad (b^{k-1}a)^2\sigma b^k(b^{k-1}a)$$

Hence the relation is true whether k is odd or even.

Let $x = b^k$ and $y = b^{k-1}a$, then from

$$(b^k)^2\sigma b^k(b^{k-1}) \quad \text{and} \quad (b^{k-1}a)^2\sigma b^k(b^{k-1}a)$$

we have $x^2\sigma xy$ and $y^2\sigma xy$. Since σ is separative therefore, by virtue of remark 4.24, $b^{k-1}a\sigma b^k$. It can be similarly shown that $a^{k-1}b\sigma a^k$. Therefore if

$$b^k a\sigma b^{k+1}\ ,\ a^k b\sigma a^{k+1} \qquad \text{(A)}$$

holds for k, it holds for (k-1). By induction down from k, it follows that (A) holds for k = 1. Therefore, by use of left identity a straight forward implication of (A) yields $ba\sigma b^2$, $ab\sigma a^2$. Since σ is separative $a\sigma b$. Thus $\rho \subseteq \sigma$ and G/ρ is the maximal separative homomorphic image of G by virtue of [6, Proposition 1.7, p-18].

THEOREM 4.27

Let ρ and σ be separative congruences on an LA-monoid G. If $\rho \cap (GxG) \subseteq \sigma \cap (GxG)$, then $\rho \subseteq \sigma$.

PROOF

Let $a\rho b$, then since ρ is separative

$$[a^2(ab)]^2 \ \rho \ [a^2(ab)](a^2b^2) \ \rho \ (a^2b^2)^2$$

obviously $[a^2(ab)]^2$, $(a^2b^2)^2 \in G$ and by medial law, by left invertive law and by the fact the e is the left identity, $[a^2(ab)](a^2b^2) = (a^2a^2)[(ab)b^2] = a^4[(b^2b)a] = a^4(b^3a) = (ea^4)(b^3a) = b^3(a^4a) = b^3a^5 \in G$. Also σ is separative, therefore, $[a^2(ab)]^2 \ \sigma \ [a^2(ab)](a^2b^2) \ \sigma \ (a^2b^2)^2$ implies that $a^2(ab)\sigma(a^2b^2)$ because $x^2\sigma xy\sigma y^2$ implies that $x\sigma y$. Since ρ is separative $a^4\rho a^2b^2$, $b^4\rho a^2b^2$. Obviously a^2b^2, a^4, b^4 belong to G, we have therefore $a^4\sigma a^2b^2$. Since by theorem 4.18 $a^2b^2 = (ab)^2$, therefore $(a^2)^2\sigma a^2(ab)\sigma(ab)^2$. Thus we have $a^2\sigma ab$, because $x^2\sigma xy\sigma y^2$ implies that $x\sigma y$.

Finally, $a^2\rho b^2$ and a^2, b^2 belong to G, we obtain $a^2\sigma ab\sigma b^2$ and therefore $a\sigma b$. Thus $\rho \le \sigma$.

COROLLARY 4.28

The subset Q defined in theorem 4.15 is separative.

PROOF

Self evident —— as Q is a commutative monoid by theorem 4.15, hence it is separative.

CHAPTER FIVE

LEFT ALMOST GROUPS

Several authors, for example, B.M. Henry [13], M.A. Kazim and F. Hussain [19] and D.C. Murdock [24] have generalized the concept of a group and have investigated the structural properties of these generalizations. A left almost group which though is a non-associative structure has interesting resemblance with a commutative group. Here specifically, it is shown that if G is a left almost group and H is a left almost subgroup then G/H is a left almost group. Further, we have proved that if G is a finite left almost group and H is a left almost subgroup of G then the order of H divides the order of G.

In this chapter we have also investigated as to how a finite set G under a binary operation * becomes an LA-group. It has been shown that there is a bijection between the group of cyclic permutations of elements of G and this LA-group.

DEFINITIONS AND EXAMPLES 5.1

Let us recall here the definition of an LA-group. A groupoid G is called a left almost group, abbreviated as LA-group, if

(i) there exists $e \in G$ such that $ea = a$ for every $a \in G$,

(ii) for every $a \in G$ there exists $a' \in G$ such that $a'a = e$

(iii) $(ab)c = (cb)a$ for every $a,b,c \in G$.

Throughout this chapter, by e we shall mean the left identity. It is not very hard to see that the left identity e and the left inverses are unique. The condition (iii) is known as the left invertive law. For details of this law see [20], [25], [32], [33] and [34]. It is important to note that if a′ is the left inverse of a then aa′ = (ea)a′ = (a′a)e = e implies that a′ is the right inverse of a.

Suppose (G, .) is a commutative group. Then it is easy to see that (G, *), where * is defined as: $a*b = b.a^{-1}$ for all $a,b \in G$, is an example of an LA-group.

RESULTS 5.2

Now we prove some results concerning an LA-group G. By a′ we shall mean the inverse of $a \in G$.

THEOREM 5.3

An LA-group is cancellative.

PROOF

Let G be an LA-group and a,b,c be arbitrary elements of G such that ba = ca. Then, by left invertive law, (ba)a′ = (ca)a′ implies that (a′a)b = (a′a)c. This shows that b = c as a′a = e and e is the left identity. Thus G is right cancellative.

Now let ab = ac. Then (ab)e = (ac)e implies that (eb)a = (ec)a. This shows that ba = ca. Since G is right cancellative, therefore b = c. This shows that G is left cancellative as well; thus implying that G is cancellative.

It is important to note that if G is an LA-group and a′, a″ are the left inverses of a and a′ respectively then a″ = (a′)′ = a. Also if $a,b \in G$ then (ab)′ = a′b′. Another important fact is that G is medial, that is, (ab)(cd) = (ac)(bd) for every $a,b,c,d \in G$.

A non-empty subset H of an LA-group G is said to be an LA-subgroup of G if H is itself an LA-group under the same operation as defined in G. We denote this fact by $H \leq G$.

THEOREM 5.4

If G is an LA-group, then

(i) $GG = G$,

(ii) $eG = Ge = G$.

PROOF

(i) If $a \in G$ then $a = ea$ implies that $a \in GG$. Thus $G \subseteq GG$. Conversely, if $a \in G$ then $a = bc$ where $b, c \in G$. Since G is a groupoid therefore $bc \in G$. Hence $a \in G$ implies that $GG \subseteq G$. Thus $G = GG$.

(ii) $Ge = (GG)e = (eG)G = GG$. This implies that $Ge = GG = G = eG$. Hence $eG = Ge = G$.

THEOREM 5.5

If H is a non-empty subset of an LA-group G then $H \leq G$ iff $ab' \in H$, for all $a, b \in H$.

PROOF

Suppose $H \leq G$. Then $a, b \in H$ implies that $a, b' \in H$ and so $ab' \in H$.

Conversely, suppose for every $a, b \in H$, $ab' \in H$. Since $H \subseteq G$ therefore for every $a, b, c \in H$, $(ab)c = (cb)a$. If we let $a = b$ then $aa' = a'a = e$ implies that $e \in H$. Also if we let $a = e$ then $eb' \in H$ implies that $b' \in H$. Moreover, a, $b' \in H$ implies that $a(b')' \in H$. Hence $ab \in H$ as $(b')' = b$. Thus $H \leq G$.

LEMMA 5.6

If G is an LA-group and $H \leq G$, then

(i) $aH = (Ha)e$ and

(ii) $(ab)H = H(ba)$.

PROOF

(i) $aH = (Ha)e$ is trivially true because $ah = (ea)h = (ha)e$ for all $h \in H$.

(ii) If $x \in (ab)H$ then $x = (ab)h$ for some h in H. This means that $x = (hb)a = (hb)(ea) = (he)(ba)$ because H is medial. But $he \in H$ because $h,e \in H$. Thus $x \in Hba$ and so $(ab)H \subseteq H(ba)$. Conversely, let $x \in H(ba)$. Then $x = h(ba)$ for some $h \in H$. Since $ba = (ab)e$, $x = h((ab)e) = (eh)((ab)e) = (e(ab))(he) = (ab)(he)$. As $e, h \in H$, $he \in H$ and so $(ab)(he) = x \in (ab)H$. This shows that $H(ba) \subseteq (ab)H$. Combining the two inclusions we conclude that $(ab)H = H(ba)$.

Let G be an LA-group and $H \leq G$. Then for $a,b \in G$, we say that a is congruent to b mod H if and only if $ab' \in H$. We denote this fact by $a \equiv b \pmod{H}$.

LEMMA 5.7

The relation $a \equiv b \pmod{H}$ is an equivalence relation.

PROOF

As $H \leq G$, $aa' = e \in H$ implies that $a \equiv a \pmod{H}$. Therefore the relation '$\equiv$' is reflexive.

Suppose $a \equiv b \pmod{H}$. This implies that $ab' \in H$. Since $H \leq G$ therefore $(ab')' \in H$. But $(ab')' = a'b'' = a'b$ implies that $a'b \in H$ and so $ba' = (eb)a' = (a'b)e \in H$. This shows that $b \equiv a \pmod{H}$. Thus the relation is symmetric.

Lastly, let $a \equiv b \pmod{H}$ and $b \equiv c \pmod{H}$. These relations imply that ab' and bc' belong to H. Now since the relation is symmetric $ba' \in H$. As H is an LA-subgroup $(ba')' \in H$ and so $b'a \in H$. Further $ac' = e(ac') = (b'b)(ac')$. By the medial law $(b'b)(ac') = (b'a)(bc')$ and so $b'a \in H$, $bc' \in H$ implies that $ac' = (b'a)(bc') \in H$. That is $a \equiv c \pmod{H}$. This proves that the relation is transitive.

By Lemma 5.7, the relation $a \equiv b \pmod{H}$ is an equivalence relation and so it partitions G into non-empty and disjoint classes. Let C_a denote the equivalence class $\{x: x \equiv a \pmod{H}\}$. A right coset H in G is defined as the set $Ha = \{x: x \equiv ha$ for $h \in H\}$.

LEMMA 5.8

In the above notation $C_a = Ha$ for all $a \in G$.

PROOF

If $x \in C_a$ then $x \equiv a \pmod{H}$ and so $xa' \in H$. This implies that $xa' = h$ where $h \in H$. Now $(xa')a = ha$ implies that $(aa')x = ha$. That is $ex = x = ha$ and this implies that $x \in Ha$. Thus for every $x \in C_a$, we have $x \in Ha$. That is $C_a \subseteq Ha$.

Conversely, if $x \in Ha$, then $x = ha$ for some $h \in H$. This implies that $xa' = (ha)a' = (a'a)h = h$

and hence $xa' \in H$. Consequently, $x \equiv a \pmod{H}$ and so $x \in C_a$. Thus every $x \in Ha$ implies that $x \in C_a$. That is, $Ha \subseteq C_a$. Combining the two inclusions we conclude that $C_a = Ha$.

REMARK 5.9

An LA-group can be partitioned into right cosets only and an RA-group into left cosets only, as such we do not require two sided decomposition in case of LA-groups (RA-groups). For details in this connection, we can refer to [18].

THEOREM 5.10

If H is an LA-subgroup of a finite LA-group G then the order of H divides the order of G.

PROOF

Using lemma 5.8 and following the group theoretic technique it is easy to prove the theorem.

It is interesting to note that we can factor an LA-group G by any of its LA-subgroups. We know that if G is a group and H is a subgroup then $H(ab) \neq (Ha)(Hb)$ unless H is normal in G. Here, in the case of LA-groups, there is no such requirement. Hence we have the following theorem.

THEOREM 5.11

If G is an LA-group and $H \leq G$ then

$$G/H = \{Ha: a \in G\} \text{ is an LA-group.}$$

PROOF

Let $x \in (Ha)(Hb)$. Then $x = (h_1a)(h_2b)$ for some $h_1, h_2 \in H$. By the medial law $x = (h_1h_2)(ab)$ and so $x \in H(ab)$. This implies that $(Ha)(Hb) \subseteq H(ab)$.

Conversely, if $x \in H(ab)$ then $x = h(ab)$, for some $h \in H$. Since H contains the left identity, we can write $x = (eh)(ab)$ and so $x = (ea)(hb)$ by medial law. Because $ea \in Ha$ and $hb \in Hb$, therefore $x = (ea)(hb) \in (Ha)(Hb)$. Hence $H(ab) \subseteq (Ha)(Hb)$ and the two inclusions imply that $H(ab) = (Ha)(Hb)$. Thus G/H is closed under the multiplication of right cosets of H in G.

Rest, it is easy to show that $eH = H = He$ is the left identity in G/H, Ha' is the left inverse of Ha and the left invertive law holds in G/H.

REMARK 5.12

The isomorphism theorems with a careful manipulation have been proved in [18]. It is to be pointed out that we do not need the concept of group theoretic normality and we can factor every LA-group G with its LA-subgroup H. We know that if G is a group and H is its subgroup then $(aH)(bH) \neq (ab)H$, unless H is normal in G. Here there is no such condition because of the medial property. That is if aH, bH belong to G/H, where G is an LA-group and H is an LA-subgroup, then (aH)(bH) = (ab)H without having extra condition on H.

THEOREM 5.13

Every finite set G, $n \geq 3$ forms an LA-group under the binary operation * where

$$a_i * a_j = a_k \quad \text{and} \quad k \equiv (j+1)-i \pmod{n} .$$

PROOF

The set G is non-associative because

$$\begin{aligned}(a_i * a_j) * a_\ell &= a_{j+1-i} * a_\ell \\ &= a_{\ell+1-j-1+i} = a_{\ell+i-j}\end{aligned}$$

and

$$\begin{aligned}a_i * (a_j * a_\ell) &= a_i * (a_{\ell+1-j}) \\ &= a_{\ell+1-j+1-i} = a_{\ell-i-j+2}\end{aligned}$$

which implies that $(a_i * a_j) * a_\ell \neq a_i * (a_j * a_\ell)$. On the other hand G is an LA-semigroup as $(a_\ell * a_j) * a_i = a_{j+1-\ell} * a_i = a_{i+1-j-1+\ell} = a_{i+\ell-j}$. Thus $(a_i * a_j) * a_\ell = (a_\ell * a_j) * a_i$.

G possesses the left identity a_1 as we can see that $a_1 * a_i = a_{i+1-1} = a_i$ and $a_i * a_1 = a_{1+1-i} = a_{2-i}$. Hence a_1 is the left identity in G. Also G contains inverses because for every i, $a_i * a_i = a_{i+1-i} = a_1$ which implies that every a_i in G is its own inverse. So G is an LA-group.

THEOREM 5.14

There exists a bijection between the LA-group G, defined in theorem 5.13 and the group of cyclic permutations of the elements of G.

PROOF

Since both the structures are finite, it is sufficient to show that mapping between the two structures is one-one.

Now $G = \{a_1, a_2, \ldots, a_n\}$ and

$T = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ where each α_i in T is a cyclic permutation of the elements of G and $\alpha_1 = I$. Define a mapping $\phi: G \longrightarrow T$ such that $\phi(a_i) = \alpha_i$. Where

$$\alpha_i = \begin{pmatrix} a_1 & a_2 & a_3 & & & & a_n \\ a_i & a_{i+1} & a_{i+2} & a_n & a_i & \dots & a_{i-1} \end{pmatrix}.$$

Then $\phi(a_i) = \phi(a_j)$ implies that $\alpha_i = \alpha_j$ which implies that

$$\alpha_i = \begin{pmatrix} a_1 & a_2 & a_3 & & & & a_n \\ a_i & a_{i+2} & a_{i+2} & a_n & a_1 & \dots & a_{i-1} \end{pmatrix} =$$

$$\begin{pmatrix} a_1 & a_2 & a_3 & & & & a_n \\ a_j & a_{j+1} & a_{j+2} & a_n & a_1 & \dots & a_{j-1} \end{pmatrix}$$

and thus in particular $a_i = a_j$. So ϕ is a one to one mapping.

REMARK 5.14

Thus the above theorem establishes a bijection between the cyclic group of permutations and an LA-group.

EXAMPLE 5.15

Let $S = \{a_1, a_2, a_3, a_4, a_5\}$, then under binary operation * defined in theorem 5.13, (G,*) is an LA-group. Completing Caley's table for (G,*)

*	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	a_3	a_4	a_5
a_2	a_5	a_1	a_2	a_3	a_4
a_3	a_4	a_5	a_1	a_2	a_3
a_4	a_3	a_4	a_5	a_1	a_2
a_5	a_2	a_3	a_4	a_5	a_1

It is to be noted that the group of cyclic permutations is displayed with mathematical symmetry in the form of rows in Caley's table. The result of table can easily be generalized to n elements.

REFERENCES

1. Albert, A.A., Quasi groups I, Trans. Amer. Math. Soc. 54(1943), 507-519.

2. Bailes, G., Right inverse semigroups, J. Algebra, 26(1973), 492-507.

3. Bruck, R.H., "A survey of binary systems", Springer-Verlag, Berlin, 1958.

4. Chaudhry, A.C., Quasi-groups and non associative systems I, Bull. Calcutta Math. Soc., 40(1948), 187-194.

5. Clifford, A.H., and D.D. Miller, Semigroups having zeroid elements, Amer. J. Math. 70 (1948), 117-125 (MR 9.330).

6. Clifford, A.H., and G.B. Preston, Algebraic theory of semigroups, Amer. Math. Soc. Math. Surveys, 7, Vols. I,II, 1961 and 1967.

7. Corsini, P., and T. Vougiouklis, From groupoids to groups through hypergroups, Rend. Mat. Appl., (7)9 (1989) no.2, 173-181.

8. Dickson, L.E., Definitions of a group and field by independent postulates, Trans. Amer. Math. Soc., 6(1905), 198-204.

9. Dawson, D.F., "Semigroups having left or right zeroid elements", Acta Scienntiorum Mathematicarum Tommus XXVII, 1966.

10. Frank, T.S., On groups, quasi and otherwise, Amer. Math. Monthly., 7(1965), 1-7.

11. Gould, V., Clifford, Semigroups of left quotients, Glas. Math., J. 28(1986), 181-191.

12. Guha, U.C., and T.H. Hoo, On a class of quasigroups, Ind. Jour. Math., 7(1965), 1-7.

13. Henry, B.M., On certain systems which are almost groups, Bull. Amer. Math. Soc., 50 (1944), 879-881.

14. Hewitt, E. and H.S. Zuckerman, The irreducible representation of semigroup related to the semigroup, Ill. J. Math., 1(1957), 188-213.

15. Howie, J.M., "An introduction to semigroup theory", Academic Press, New York, 1976.

16. Iqbal, M., Some studies in LA-semigroup, M.Phil. Dissertation, Quaid-i-Azam University, 1988.

17. Iqbal, Q., Some studies in left almost semigroups, Ph.D. Thesis, Quaid-i-Azam University, 1992.

18. Kamran, S., Structural properties of LA-semigroups, M.Phil. Dissertation, Quaid-i-Azam University, 1987.

19. Kazim, M.A., and F. Hussain, On postulates defining a substractive group, Math. Student, 31(1963), 95-107.

20. Kazim, M.A., and M. Naseeruddin, On almost semigroups, The Aligarh Bull. Math., 2(1972), 1-7.

21. Khalid, M., On the medial properties of LA-semigroups, M.Phil. Dissertation, Quaid-i-Azam University, 1990.

22. Levi, F.W., On semigroups, Bull. of Calcutta Math. Soc. I,II, 36(1944), 141-146; 38(1946), 123-124.

23. Mcalister, D.B., One-to-one partial right translations of a right cancellative semi-groups, J. Algebra, 43(1976), 231-251.

24. Murdock, D.C., Quasi groups which satisfy certain generalized associative laws, Amer. J. Math. 61(1939), 509-522.

25. Mushtaq, Q., Abelian groups defined by LA-semigroups, Studia Sci. Math. Hungar., 18 (1983), 427-428.

26. Mushtaq, Q., A note on almost semigroups, Bull. Malaysian Math. Soc., (Second Ser.), 11 (1988), 29-31.

27. Mushtaq, Q., A note on translative mappings on LA-semigroups, Bull. Malaysian Math. Soc., (Second Ser.), 11(1988), 39-42.

28. Mushtaq, Q., Embedding of an LA-semigroup in a commutative monoid, Pak. Acad. Sci., 26, 4 (1989), 319-324.

29. Mushtaq, Q., Left almost semigroups, M.Phil. Dissertation, Quaid-i-Azam University, 1978.

30. Mushtaq, Q., and Q. Iqbal, Decomposition of a locally associative LA-semigroup, Semigroup Forum, 41(1991), 155-164.

31. Mushtaq, Q., and S. Kamran, On LA-semigroups with weak associative law, Sci. Khyber, 2,1 (1989), 69-71.

32. Mushtaq, Q., and S.M. Yusuf, LA-semigroup defined by a commutative inverse semigroup, Math., Bech., 40(1988), 59-62.

33. Mushtaq Q., and S.M. Yusuf, On LA-semigroups, The Aligarh Bull. Math., 8(1978), 65-70.

34. Mushtaq Q., and S.M. Yusuf, On locally associative LA-semigroups, J. Nat. Sci. Math., 1, 19 (1979), 57-62.

35. Nagy, A., Weakly exponential semigroups, Semigroup Forum, 28(1984), 291-302.

36. Naseerudin, M., Some studies on almost semigroups and flocks, Ph.D. Thesis. The Aligarh Muslim University, India, 1970.

37. Nordhal, T., Semigroup satisfying $(xy)^m = x^m y^m$, Semigroup Forum 8(1974), 332-346.

38. Pastijn. F., A representation of a semigroup by a semigroup of matrices over a group with zero, Semigroup Forum, 10(1975), 238-249.

39. Pondeticek, B., On weakly commutative semigroups, Czech. Math. J., 25(100), (1975).

40. Rees, D., On semigroups, Proc. Cambridge Soc., 36(1940), 387-400.

41. Reinhard, S., Construction of medial semigroups, Comment. Math. Univ. Carolin. 25(1984), no.4, 689-697.

42. Singh, P., and N.S. Yadev, A note on inverse quasigroups, The Alig. Bull. Math., 2(1972), 15-20.

43. Tamura, T., and N. Kimura, On decomposition of a commutative semigroup, Kodai Math. Sem. Rep., 1954, 102-112.

44. Tamura, T., and T. Nordahl, On exponential semigroups II, Proc. Japan Acad., 48(1972), 474-478.

45. Verma, K., A sufficient condition for a monoid to be a group, Comm. Algebra, 15, 6(1987), 1187-1193.