A Theoretical and Computational Investigation of AG-groups

By

***Muhammad* Shah**

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2012

A Theoretical and Computational Investigation of AG-groups

By

Muhammad Shah

Supervised by

Dr. Asif Ali

& Co-Supervised By

Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2012

A Theoretical and Computational Investigation of AG-groups

By

Muhammad Shah

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

DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

Supervised by

Dr. Asif Ali

& Co-Supervised By

Dr. Tariq Shah

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan

2012

External Reviewers

1. **Prof. Dr. Kuiyuan Li**
   Co-Director
   Florida-China Linkages Institute
   Professor & Chair
   Department of Mathematics and statistics.
   University of West Florida, Pensacola, FL 32514-5750
   E-mail: kli@uwf.edu

2. **Prof. Dr. Young Bae Jun**
   Department of Mathematics Education.
   Gyeongsang National University,
   Chinju 660-701,
   Korea.
   E-mail: skywine@gmail.com

3. **Dr. Haci Aktas**
   Department of Mathematics, Faculty of Arts and Science
   University of Gaziosmanpasa 60100 Tokat,
   Turkey
   Email: haktas@gop.edu.tr

CERTIFICATE

A Theoretical and Computational Investigation of AG-groups

By

Muhammad Shah

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

We accept this thesis as conforming to the required standard

Prof. Dr. Muhammad Ayub
(Chairman)

Tariq Shah

Dr. Asif Ali
(Supervisor)

Dr. Tariq Shah
(Co-Supervisor)

Karamat

Muhammad Anwar 6/12/2012

Prof. Dr. Karamat H. Dar
(External Examiner)

Prof. Dr. M. Anwar Chaudhry
(External Examiner)

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2012

To my late mother who supported me more than anybody else and whose prayers give me strength in every difficulty.

Declaration

This thesis is the outcome of my own research while enrolled as a student at the Department of Mathematics, Quaid-i-Azam University Islamabad, under the supervision of Dr. Asif Ali. Everything written here is my own work, except where otherwise stated. This work has not been submitted for any other degree or award in any other university or educational establishment. This work emerged as a result of a series of my papers with my collaborators. See [15, 79, 80, 82, 83, 81, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94].

Muhammad Shah
Islamabad, March 2012

Acknowledgements

Thanks to Almighty ALLAH, the Creator of every thing who enabled me to accomplish this task. After that I would like to thank my supervisor Dr. Asif Ali. It was he who introduced me to quasigroups and loops and it was he who got me interested in learning the FINDER and GAP softwares. He has been a continuing source of ideas, inspiration and intellectual energy for me. He always provided a great deal of high-level feedback and insight in response to my queries. Indeed he was the first place I looked whenever I was stuck. I am also very grateful to Dr. Tariq Shah for supervising me in absence of Dr. Asif for some period of time. My thanks also go to all professors of the department and my Ph.D colleagues for creating such an excellent research environment which helped me a lot during my studies. My special thanks must go to Prof. Dr. Qaiser Mushtaq that he taught me the course of theory of LA-semigroups which I am developing in this dissertation. I am especially thankful to my PhD colleagues Inayat-ur-Rehman, Rehan Ahmad, Mohammad Ayub, Noor Rehman, Dr. Ahmer Mehmood, Sufian Munawar, Nazim Tufail and Adnan Saeed also to all the M. Phil students of Dr. Asif for many constructive conversations.

I am deeply indebted to my wife, Zaiboon, for relaxing me of my domestic responsibilities and worries during my doctoral studies. I would like to extend my thanks to my brother Feroz Shah, to my nephew Sher Hassan and to my friends Zahir Ahmad (lecturer in Mathematics Govt College Pabbi), Abdullah (Assistant Professor of Chemistry, Govt College Yakaghond) and Muhammad Ismail (Assistant Professor of Chemistry, Govt College Peshawar) for their moral and financial support.

I am of course very grateful to the Higher Education Commission (HEC) of Pakistan for the financial support during my stay at Birmingham University, UK otherwise this dissertation might not have been become possible. My thanks are due to the School of Computer Science, University of Birmingham, for hosting me, and the Ramsay Research Fund for their kind financial support. 1 want to express my profound gratitude to my collaborators Dr. Volker Sorge and Dr. Charles Gretton(School of Computer Science, University of Birmingham, UK), Dr. Sergey Shpectorov (School of Mathematics, University of Birmingham, UK) and Dr. Andreas Distler (Centro de Algebra, Universidade de Lisboa, Lisboa, Portugal). I really enjoyed their company and learnt lots from them.

Muhammad Shah
Islamabad, March 2012

Abstract

An AG-group (also called LA-group) is an AG-groupoid having left identity and inverses. AG-groups have been originally introduced by M.S. Kamran. This thesis concentrates on the study of AG-groups as a special class of quasigroups and as a general class of abelian groups both from a theoretical and computational point of view. We investigate several properties of abelian groups which can be generalized to the non-associative structure of AG-groups. Similarly several properties of loops are shown to hold in AG-groups. We introduce Bol* quasigroups, a generalization of AG-groups, as well as some interesting subclasses of AG-groups. We present both a computational and an algebraic enumeration of AG-groups. Computationally we can enumerate them up to order 11 but algebraically we are able to count them of any given order.

A further motivation to study AG-groups is that they have two-sided unique inverses and can therefore be seen as a generalization of two-sided loops. Consequently we provide investigation of two such loops (i) C-loops and (ii) Jordan loops. This leads to the enumeration of Jordan loops up to order 10 which is also a part of this thesis. Furthermore, we investigate the application of AG-groups in geometry and exploit AG-groups to map out the general structure of AG-groupoids and further explore cancellativity of AG-groupoids.

In spite of a great deal of investigations of AG-groupoids and their subclasses for nearly four decades no progress had been made in obtaining enumeration results. In fact, not even the exact number of non-associative AG-groupoids for the order 3, the smallest possible order, was known up to now. We are enumerating AG-groupoids up to order 6 for the first time. We then classify our data and give twenty four new classes of AG-groupoids. The relations between them to each other have been established. In the end we have collected all our findings into a GAP package "AGGROUPOIDS" that contain several functions that check various characteristics of a given Cayley table of AG-groupoids and AG-groups.

Contents

Acknowledgements **v**

Abstract **vii**

1 History, Definitions and Notations **1**

1.1 Background 1

1.2 Survey of AG-groupoids 4

1.2.1 Investigation of The Real Pioneer of AG-groupoids 4

1.2.2 Development of The Theory of AG-groupoids 5

1.3 Quasigroups and Loops 7

1.4 Motivation 8

1.5 Notations 8

2 Jordan Loops and C-Loops **11**

2.1 Introduction 11

2.2 On Jordan Loops 12

2.2.1 A Few Properties of Jordan Loops 12

2.2.2 Construction of Jordan Loops 14

2.3 Nuclei and Commutant of C-Loops 18

2.3.1 Commutant of C-Loops 21

3 Enumeration of AG-Groupoids **23**

3.1 Introduction 23

3.2 Constructing AG-groupoids 25

3.2.1 CSP and Minion 25

3.2.2 Symmetry Breaking and GAP 26

3.2.3 Search 28

3.3 Classification of AG-groupoids 29

3.4 Conclusions 31

4 Discovery of New Classes of AG-groupoids **35**
4.1 Introduction 35
4.2 Quasi-cancellativity of AG-groupoids 37
4.3 Anti-commutativity and Transitively Commutativity 41
4.4 Construction of Bol*-groupoid from Semigroups 43
4.5 Paramedial AG-groupoids and
Bol*-AG-groupoids 45
4.6 AG-groupoid Semigroups 48
4.7 Alternative and Flexible AG-groupoids 50
4.8 Self-dual AG-groupoids and Unipotent AG-groupoids 52
4.9 Type 1, Type 2, Type 3 and Type 4 AG-groupoids 53
4.10 Zero-AG-groupoid, Zero-AG-group 58

5 On The Cancellativity of AG-groupoids **61**
5.1 Introduction 61
5.2 Cancellativity of AG-groupoids 61
5.3 Partial Solution to The Open Problem 69

6 Enumerating AG-groups **79**
6.1 Introduction 79
6.2 Counting AG-groups up to Isomorphism 80
6.3 AG-group of Smallest Order 81
6.4 Smarandache AG-groups 82

7 Generalization of Abelian Groups **87**
7.1 Some Structural Properties of AG-groups 87
7.1.1 Basic Properties of AG-groups 88
7.1.2 Duality Between Left AG-groups and Right AG-groups . . 90
7.1.3 Power Associativity of AG-groups 91
7.1.4 General Properties of AG-groups 92
7.2 AG-groups as Generalization of Abelian Groups 93
7.2.1 Complexes 94
7.3 Conjugacy Relations in AG-groups 98
7.3.1 Normality in AG-groups 101
7.3.2 Normalizer of an AG-subgroup of an AG-group 106
7.3.3 Commutators in AG-group 107
7.3.4 Direct Products of AG-groups 113
7.3.5 AG-group Actions 115

8 A Study of AG-groups as Quasigroups 121
8.1 Introduction . . . 121
8.2 AG-groups as Invertible Quasigroups . . . 121
8.2.1 Main Results . . . 122
8.2.2 Constructing a Family of AG-groups via Quasigroup Extension . . . 129
8.2.3 A Word about Applications of AG-groups . . . 132
8.3 Multiplication Group of an AG-group . . . 132

9 AG-groups as Parallelogram Spaces 139
9.1 Introduction . . . 139
9.2 Parallelograms . . . 140

10 Classes of Right Bol Quasigroups 149
10.1 Introduction . . . 149
10.2 Preliminaries . . . 152
10.3 Particular Classes of AG-groups . . . 155
10.4 Some Examples . . . 156
10.5 Re-visiting Multiplication Group of an AG-group . . . 157
10.6 Sharma's Correspondence . . . 159

11 AG-monoids from Commutative Monoids 163

12 AG-GROUPOIDS: A GAP Package 167
12.1 Testing Cayley Tables . . . 167
12.2 Testing Magma . . . 169
12.3 Some Useful Operations . . . 170
12.4 Some Counting Operations . . . 171

13 Conclusion 175

Bibliography 177

Chapter 1

History, Definitions and Notations

In this chapter we give definitions, notations, history and a short survey of AG-groupoids which we will use throughout the thesis. This is partly for fixing terminology, partly to provide a background and partly for setting up notation. Motivation for studying AG-groups is also given here.

1.1 Background

We first give a brief introduction into the mathematical theory of AG-groupoids and especially define some of their existing subclasses we are interested in, for their classification and to which we will add several more subclasses in the thesis.

The structure of AG-groupoid was introduced by Naseeruddin and Kazim in 1972 [27] and was originally called **left almost semigroup** (LA-semigroup). It has also been studied under the names **right modular groupoid** [7] and **left invertive groupoid** [23], before Stevanovic and Protic called the structure Abel-Grassmann groupoid (or AG-groupoid for short) [106], which is the primary name under which it is known today. AG-groupoids generalize the concept of commutative semigroups and have an important application within the theory of flocks [61].

We first recall that a groupoid is defined as a non-empty set S together with a binary operation $\circ : S \times S \to S$. In the sequel we will generally elide the binary operation. We now define an AG-groupoid as follows:

Definition 1. *A groupoid S is called an **AG-groupoid** if for all $a, b, c \in S$ the* *following identity holds:*

$$(ab)c = (cb)a \tag{1.1}$$

The identity (1.1) is called **left invertive law**.

Definition 2. *A groupoid S is called **medial** if S satisfies the **medial law**, that for all $a, b, c, d \in S$ we have*

$$(ab)(cd) = (ac)(bd). \tag{1.2}$$

It has been shown in [7], that every AG-groupoid is medial. Observe that the medial law is a property closely related to commutativity. Consequently, AG-groupoids can also be viewed as a generalization of commutative semigroups.

We now define a number of properties that give rise to interesting subclasses of AG-groupoids, which we will identify in our classification later in the thesis.

Definition 3. *An AG-groupoid S is called **weak associative** if it satisfies the identity $(ab)c = b(ac)$ for all $a, b, c \in S$. We call S an AG*-groupoid.*

Definition 4. *An AG-groupoid S is called an **AG-monoid** if S has a left identity, i.e., there exists an element $e \in S$ such that for all elements $a \in S$ we have $ea = a$.*

Observe that since AG-groupoids are not necessarily associative, the existence of a left identity does not imply the existence of a general identity.

Definition 5. *An AG-groupoid S that satisfies the identity $a(bc) = b(ac)$ for any $a, b, c \in S$ is called a **AG**-groupoid**.*

Definition 6. *A groupoid S is called **paramedial** if S satisfies the **paramedial law**, i.e, for all $a, b, c, d \in S$ we have $(ab)(cd) = (db)(ca)$.*

One can easily verify the following facts that (i) every AG-monoid is an AG**-groupoid, and that (ii) every AG**-groupoid is paramedial. However, the converse is generally not true.

Example 1. *As example structures we consider the four AG-groupoids of order 5 below, where (i) is an AG-monoid, (ii) is an AG*-groupoid (iii) is an AG**-groupoid and therefore also paramedial, while (iv) is a paramedial groupoid which is not an AG**-groupoid.*

(i)

$\circ$	0	1	2	3	4
0	0	0	0	0	0
1	0	0	3	0	1
2	0	1	2	3	4
3	0	0	1	0	3
4	0	3	4	1	2

(ii)

$\circ$	0	1	2	3	4
0	4	1	1	2	4
1	1	1	1	1	1
2	1	1	1	1	1
3	1	1	1	2	1
4	4	1	1	1	4

(iii)

$\circ$	0	1	2	3	4
0	1	0	4	4	3
1	4	3	1	1	0
2	0	1	2	3	4
3	0	1	3	3	4
4	3	4	0	0	1

(iv)

$\circ$	0	1	2	3	4
0	0	0	0	0	0
1	0	0	0	0	0
2	1	0	4	4	1
3	0	1	4	4	0
4	0	0	0	0	0

Definition 7. *Let S be an AG-groupoid. We call S* ***locally associative*** *if for all $a \in S$ the identity $a(aa) = (aa)a$ holds.*

Definition 8. *An AG-groupoid S is called an* ***AG-2-band*** *or simply* ***AG-band*** *if for all $a \in S$ the identity $aa = a$ is satisfied. In other words, in an AG-band S every element is idempotent.*

Definition 9. *An AG-groupoid S is called an* ***AG-3-band*** *if for every $a \in S$ we have $a(aa) = (aa)a = a$.*

Definition 10. *An element a of an AG-groupoid S is called* ***left cancellative*** *if $ax = ay \Rightarrow x = y$ for all $x, y \in S$. Similarly an element a of an AG-groupoid S is called* ***right cancellative*** *if $xa = ya \Rightarrow x = y$ for all $x, y \in S$. An element a of an AG-groupoid S is called* ***cancellative*** *if it is both left and right cancellative. S is called* ***(left,right) cancellative*** *if all of its elements are (left,right) cancellative.*

We define AG-groups, an important subclass of AG-groupoids, which generalizes abelian groups. We will focus on AG-groups in the thesis.

Definition 11. *An AG-groupoid S is called an* ***AG-group*** *if S has a left identity $e \in S$ and inverses with respect to this identity, i.e., for all elements $a \in S$ there exists an element $b \in S$ such that $ab = ba = e$.*

Example 2. *As further example structures we give (i) an AG-band, (ii) an AG-3-band, and (iii) an AG-group below. For the latter we observe that the element 3 is the left identity element and that the structure is indeed not a group as there is no corresponding right identity.*

(i)

$\circ$	0	1	2	3	4
0	0	3	1	4	1
1	4	1	3	0	3
2	3	0	2	1	4
3	1	4	0	3	0
4	3	0	4	1	4

(ii)

$\circ$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	3	4	2
2	0	4	2	1	3
3	0	2	4	3	1
4	0	3	1	2	4

(iii)

$\circ$	0	1	2	3	4
0	3	0	1	4	2
1	4	3	0	2	1
2	2	4	3	1	0
3	0	1	2	3	4
4	1	2	4	0	3

Finally we will need the following definitions in the thesis.

Definition 12. *A non-empty subset H of an AG-groupoid S is called an* ***AG-subgroupoid*** *if $ab \in H$ for all $a, b \in H$.*

Definition 13. *A subset I of an AG-groupoid S is called* ***left ideal (right ideal)*** *if $SI \subseteq I (IS \subseteq I)$. A subset I of an AG-groupoid S is called* ***ideal*** *if it is both left and right ideal.*

Definition 14. *An ideal I of an AG-groupoid S is called* ***maximal ideal (right ideal)*** *if I is not properly contained in any larger ideal of S.*

1.2 Survey of AG-groupoids

Here we take a short survey of the forty years history of AG-groupoids in which a lot of work has been done on this structure. Starting slowly and gradually the last couple of years saw a rapid research in this area and proved to be an interesting and productive field for researchers. Many researchers are giving attention to this field these days. Our survey will provide a guideline to them and will help them to know how much work has already been done and which aspects has already been explored. So we want to take a quick review of the last forty years of the literature. Also there is a bit ambiguity about its name which poses the question that who is the real pioneer of AG-groupoids? We will put some light on this question.

1.2.1 Investigation of The Real Pioneer of AG-groupoids

As mentioned earlier it is believed by the AG-groupoids community that the structure of AG-groupoids was first introduced by Naseeruddin and Kazim in 1972 [27] under the name of left almost semigroup or simply LA-semigroup as can be easily seen from the literature. Thus M. Naseeruddin and Kazim are known as the pioneer of AG-groupoids. But in our opinion the structure of AG-groupoid has existence earlier than prior to their paper. We agree with Stevanovic and Protic that they called it Abel Grassmann groupoids (or shortly AG-groupoids) for the first time by giving reference to a very famous and authentic book [10]. This book was published in 1974. In which very famous identities have been collected on Pages $58-60$. Among them the identity (22) is of Abel Grassmann groupoids, that is, groupoids satisfying $a(bc) = c(ba)$ which in [27, Page 48] has been called a Right Almost semigroup or simply RA-semigroup and which is the dual of LA-semigroup and that is obviously not material. From this can be easily comprehended that AG-groupoid had existence before 1972 in the form of an identity defined by Abel Grassmann. It can be the case that this has also existence by the name of right modular groupoid because in [7], this has not been claimed that they are defining right modular groupoids for the first time. It looks like that perhaps M. Naseeruddin and Kazim were ignorant of it. There is no doubt that researchers took interest in AG-groupoids when they came to know that a new interesting structure has been defined by M. Naseeruddin and Kazim. Indeed the theory of the AG-groupoids began to grow at this very point.

1.2.2 Development of The Theory of AG-groupoids

After [27] Q. Mushtaq was the first who started work on AG-groupoids in his M. Phil at first then with S. M. Yusuf and later on with his students. Q. Mushtaq and S. M. Yusuf [57] started basics and proved results such as: an AG-groupoid with right identity becomes a commutative semigroup, if an element of AG-groupoid with left identity has a left inverse or right inverse then it becomes inverse, a left cancellative is also cancellative. They also proved that an AG-groupoid S can be constructed from a commutative group G via

$$a * b = b \cdot a^{-1} \, \forall a, b \in G.$$

After that they in [58] defined locally associative AG-groupoid S to be an AG-groupoid which satisfies $(aa)a = a(aa)$ for all $a \in S$ and proved in locally associative AG-groupoid S powers are defined. They also defined a relation ρ on locally associative AG-groupoid S as:

$$a\rho b \Longleftrightarrow ab^n = b^{n+1} \text{ and } ba^n = a^{n+1} \text{ for some positive integer } n, \text{ where } a, b \in S.$$

which they proved to be a separative congruence, that is, ρ is reflexive, symmetric, transitive and $ab\rho a^2, ab\rho b^2 \Longrightarrow a\rho b$, in case S has left identity. In [49] it was proved that a locally associative AG-groupoid S with left identity is uniquely expressible as a semilattice Y of archimedean locally associative AG-groupoids $S_\alpha(\alpha \in Y)$ with left identity. Further they in [59] reduced the condition of construction of AG-groupoid S from a commutative group done in [57] into commutative inverse semigroup G. Then using the fact that commutative inverse semigroup is the union of groups, they discussed certain homomorphisms between S and these groups.

Kamran in his thesis extended the notion of AG-groupoid to an AG-group (LA-group). They discussed cosets of an AG-subgroup H of an AG-group G and proved that quotient G/H is defined for every AG-subgroup H. They also proved that Lagrange's Theorem holds for AG-group. Later on the eminent results of [26] appeared in [51].

In [33], S. M. Yusuf further extended the notion to another non-associative structure with respect to both binary operations '+' and '.' namely left almost ring (LA-ring). By a left almost ring we mean a non-empty set R with at least two elements such that $(R, +)$ is an AG-group and $(R, .)$ is an AG-groupoid and both left and right distributive laws hold in R. An LA-ring $(R, +, .)$ with left identity e is called almost field if every nonzero element a of the ring has multiplicative inverse a^{-1} in R.

N. Stevanovic, P. V. Protic [106] introduced the concept of inflations in AG-groupoids and discuss some of their properties. Q. Mushtaq and M. S. Kamran [50] showed that if S is a finite AG-groupoid with left zero then, under certain conditions, without the left zero element S is a commutative semigroup. P. V. Protic, N. Stevanovic [74] introduced a few congruence relations on AG-band and considered decompositions of AG-bands induced by those congruences. They proved that this give rise to the natural partial order on AG-band. N. Stevanovic, P. V. Protic [107] introduced the notions of a 3 potent element of an AG-groupoid of AG–3-band. They devised methods for the construction of AG-3-band. Q. Mushtaq [48] introduced the notions of zeroids and idempoids in AG-groupoids. Q. Mushtaq and K. Mahmood [56] characterized division μ-AG-groupoids by their linear forms as well as by permutations.

From 2006 a new era of AG-groupoids started when Q. Mushtaq and M. Khan [52] defined ideals in AG-groupoid and especially when AG-groupoids were fuzzified. This really attracted the researchers to AG-groupoids whose effect we can see in 2010 and 2011 that numerous papers were submitted for publication and some of them exist on arXiv. Ideals in particular subclasses such as AG-band and AG*-groupoid of AG-groupoids were discussed in [54]. They studied decomposition of a locally associative AG**-groupoid in [53].

The structure of union of groups within the variety of AG-groupoids was explored in [46] and in [47] he further proved that within the variety AG-groupoids the collection of all groupoids whose power groupoid is a band [generalized inflation of a band; a union of groups] determines an inclusion class of AG groupoids. He also proved that any groupoid anti-isomorphic to a finite or countable anti-rectangular AG-band G is isomorphic to G. He further proved that within isomorphism there is only one countable anti-rectangular AG-band and that it is isomorphic to a proper subset of itself. The concept of AG-groupoids was extended to Γ -AG-groupoids in T. Shah and I. Rehman [98] and [97] . T. Shah and I. Rehman started to apply LA-rings in [99]. Ideals in generalized LA-ring were studied in [95] LA-modules were studied in [96]. AG-groupoids were fuzzified in [34] and then different subclasses of AG-groupoids, Γ-AG-groupoids and different types of ideals were characterized by means of fuzzification in [29, 30, 31, 32] and which is still continued.

1.3 Quasigroups and Loops

We will first introduce a number of definitions about loops that are needed in this thesis.

Definition 15. *A set $(Q, \cdot)$ is a quasigroup if and only if in the equation $x \cdot y = z$, any two of the symbols x, y, z are assigned as elements of Q, the third is uniquely determined as an element of Q.*
The following table lists the names of some identities, which we will refer to throughout this thesis.

Definition 16. *A loop is a quasigroup with neutral element. In other words a quasigroup $(Q, \cdot)$ is called loop if there exists an element 1 of Q with the property*

$$x \cdot 1 = 1 \cdot x = x \,\forall x \in Q.$$

Some identities related to quasigroups and loops have been listed in Table 1.1.

Definition 17. *Let L be a loop. The set*

$$N_\lambda = \{x \in L; x(yz) = (xy)z \,\forall y, z \in L\}$$

is called the left nucleus. Similarly, the set

$$N_\mu = \{x \in L; y(xz) = (yx)z \,\forall y, z \in L\}$$

is called the middle nucleus and the set

$$N_\rho = \{x \in L; y(zx) = (yz)x \, \forall y, z \in L\}$$

is called the right nucleus. The nucleus

$$N = N_\lambda \cap N_\mu \cap N_\rho \textit{of } L \textit{ is a subgroup of } L.$$

Furthermore we define;

Definition 18. *The commutant of a loop L as the set $C(L) = \{c \in L : cx = xc$ for every $x \in L\}$ and the centre of a loop L as $Z(L) = C(L) \cap N$.*

1.4 Motivation

There are several species of loops which have unique inverses. Such loops are called **invertible loops**. C-loops, Jordan loops and Bol loops are examples of invertible loops. Due to the unique inverses these loops have many properties which loops not having unique inverses do not have. That is why invertible loops have been investigated by loop theorists extensively. On the other hand, quasigroups having unique inverses have never received much attention. This motivated us to study such quasigroups. For this purpose we select a special species of quasigroups called AG-groups. We made a choice of AG-groups because since their introduction by Kamran [26], they remained uninvestigated for long.

This class of quasigroups has versatile character and can be studied in many ways. This characteristic of AG-groups motivated us to study them.

1.5 Notations

We will use the following terminology from group theory for AG-groups.

Definition 19. *An arbitrary non-empty subset of a group G is called a **complex** in G.*

We will use these notations in the thesis. By $a \mid b$ we mean a divides b and by $a \nmid b$ we mean a does not divide b. Also to avoid excessive parenthesization, we will use the usual juxtaposition conventions , e.g., $ab \cdot c = (a \cdot b) \cdot c$.

Identity	Name
$x(xy) = (xx)y$	left alternative
$x(yy) = (xy)y,$	right alternative
$x(yx) = (xy)x,$	flexible
$(xx)(yz) = ((xx)y)z$	left nuclear square
$x((yy)z) = (x(yy))z$	middle nuclear square
$x(y(zz)) = (xy)(zz)$	right nuclear square
$x(y(xz)) = (x(yx))z$	left Bol
$x((yz)y) = ((xy)z)y$	right Bol
$(xy)(zx) = (x(yz))x,$	Moufang
$x(y(yz)) = ((xy)y)z$	Central identity or C-identity
$x(y(zx)) = ((xy)z)x$	extra identity
$x^{-1}(xy) = y$	left inverse property
$(yx)x^{-1} = y$	right inverse property
$x(xx) = (xx)x$	$3-$power associativity or local associativity

Table 1.1: Some identities.

Chapter 2

Jordan Loops and C-Loops

2.1 Introduction

As invertible loops motivated us to study AG-groups. So we begin by studying two species of invertible loops namely (1) Jordan loops and (2) C-loops. In Section 1 we study Jordan loops. According to [42], Jordan loops have not received sufficient attention from loop theorists so we decided to study them here a little bit. By doing so we are therefore partly motivated to draw folks to their study. In that spirit we establish a few interesting properties of these loops such as every commutative alternative loop is a Jordan loop and alternative Jordan loops of odd order have no subloop of even order. Thus the nucleus of an alternative Jordan loop is always of odd order Corollary 2. We provide a construction for an infinite family of non-associative Jordan loops. We also provide a count of the isomorphism classes of small Jordan loops by exhaustive enumeration up to order 9, and give a lower bound for order 10.

In Section 2 we study C-loops. C-loops are loops satisfying the identity $x(y(yz)) = ((xy)y)z$. The nature of the identity, where unlike in other Bol-Moufang identities the repeated variable is not separated by either of the other variables, makes them a difficult target of study. Nevertheless they have been investigated in [2, 3, 18, 19, 35, 37, 36, 73, 71, 72, 76].

We extend some results of [73], in particular [73, Proposition 3.1] that states that only even order nonassociative C-loops exist. Investigating this result further using the order of nuclei of C-loops, we prove that (1) all nonassociative C-loops of order $2p$, where p is prime, are Steiner loops, (2) all nonassociative C-loops of order $3n$ are non-simple and non-Steiner, (3) there exists no nonassociative C-loop of order $2 \cdot 3^t, t \geq 1$, and (4) if $C(L)$ is the commutant of a C-loop L and every element of $C(L)$ is of odd order, then $C(L)$ is a subloop of L.

2.2 On Jordan Loops

[39] makes a number of important observations regarding Jordan loops. For example, it introduces the notion of powers of Jordan loops, and give a proof that a non-associative Jordan loop of order n exists if and only if $n \geq 6$ and $n \neq 9$ [39, Theorem 1.1]. It also gives a Cayley table for the smallest non-associative Jordan loop. That loop, of order 6 with a nucleus is of size 1, appears as follows.

Example 3. *Smallest non-associative Jordan loop:*

$\cdot$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	4	5	2
2	2	3	0	5	1	4
3	3	4	5	0	2	1
4	4	5	1	2	0	3
5	5	2	4	1	3	0

2.2.1 A Few Properties of Jordan Loops

We begin by the following simple fact.

Theorem 1. *Every commutative left nuclear square loop is a Jordan loop. Hence, every commutative C-loop is Jordan loop.*

Theorem 2. *Every flexible left alternative loop L satisfies the Jordan identity $x^2(yx) = (x^2y)x$.*

Proof. By applications of flexible law, $(xy)x = x(yx)$, and left alternative laws, $x(xy) = (xx)y$, we have $(x^2y)x = (x(xy))x = x((xy)x) = x^2(yx)$. $\square$

Corollary 1. *Every commutative alternative loop is Jordan loop.*

The converse of the Corollary 1 is not true. The Jordan loop in Example 3 is neither left nor right alternative.

We now prove that [78, Theorem 1] also holds for alternative loops.

Theorem 3. *Let L be any invertible left alternative loop then order of L is even iff L has an element of order 2, i.e. an element a such that $a \neq e$ but $a^2 = e$.*

Proof. The direct part is trivial. We see that the inverse operation is of period 2 so the set of elements of L which are not fixed points must be of even cardinality. If the order of L is even then there must also be an even number of self inverse elements, so e cannot be the only such element. For the converse suppose a is self inverse and distinct from e. Let the operation L_a is defined on L by $L_a(x) = ax$ then L_a is of period 2, as $L_a(L_a(x)) = a(ax) = a^2x = ex = x$, since L is left alternative. Moreover L_a has no fixed point, as if $L_a(x) = x$ then $ax = x$ so $a = e$ contrary to the supposition of the theorem. Therefore L_a partitions into pairs L, so order of L is even. □

Remark 1. It can easily be seen that Theorem 3 also holds for right alternative loop.

Corollary 2. *Alternative Jordan loops of odd order have no subloop of even order and hence have nuclei of odd order always.*

The Square Property

A groupoid has the square property iff $(xy)^2 = x^2y^2$ for all x and y. A group is commutative iff it has square property. This is not true for a Jordan loop. Every Jordan loop is commutative but does not satisfy the square property.

Example 4. *A non-associative Jordan loop of order* 10*:*

$\cdot$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	8	9	6	7
2	2	3	0	1	6	7	4	5	9	8
3	3	2	1	0	8	9	7	6	4	5
4	4	5	6	8	1	0	9	2	7	3
5	5	4	7	9	0	1	2	8	3	6
6	6	8	4	7	9	2	3	0	5	1
7	7	9	5	6	2	8	0	3	1	4
8	8	6	9	4	7	3	5	1	2	0
9	9	7	8	5	3	6	1	4	0	2

This is an example of a Jordan loop in which square property does not hold as $0 = (7 \cdot 8)^2 \neq 7^2 \cdot 8^2 = 1$. So we ask.

Question: On what condition square property will hold in Jordan loops?
A conjecture that might be one answer to this question is given below. It can

easily be observed that for commutative loops and hence for Jordan loops, $N_\lambda = N_\rho$. The following example shows that for Jordan loops, it is not necessary that $N_\lambda = N_\rho = N_\mu$.

Example 5. *A non-associative Jordan loop of order* 8*:*

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	6	1	7	4	5
3	3	2	6	0	7	1	5	4
4	4	5	1	7	0	6	3	2
5	5	4	7	1	6	0	2	3
6	6	7	4	5	3	2	1	0
7	7	6	5	4	2	3	0	1

Here N_λ and N_ρ are of size 1 while N_μ is of size 2.

Conjecture 1. *If a Jordan loop is such that $N_\lambda = N_\rho = N_\mu$ then square property holds.*

2.2.2 Construction of Jordan Loops

We now construct an infinite family of non-associative Jordan loops via extension of loop whose smallest member is a loop of order 12. We adopt the same procedure as done for the construction of non-associative and non-commutative C-loops in [73].

Let G be a multiplicative group with neutral element 1, and A an abelian group written additively with neutral element 0. Any map $\mu : G \times G \to A$ satisfying $\mu(1, g) = \mu(g, 1) = 0\, \forall g \in G$ is called a factor set. When $\mu : G \times G \to A$ is a factor set, we can define multiplication on $G \times A$ by

$$(g, a)(h, b) = (gh, a + b + \mu(g, h)) \qquad (1)$$

The resulting groupoid is clearly a loop with neutral element $(1, 0)$. We denote it by (G, A, μ). Additional properties of (G, A, μ) can be enforced by additional requirements on μ.

Lemma 1. *Let $\mu : G \times G \to A$ be a factor set. Then (G, A, μ) is a Jordan loop iff*

$$\mu(g,h) + \mu(g^2, gh) = \mu(g^2, h) + \mu(g^2h, g) \tag{2}$$

and

$$\mu(g,h) = \mu(h,g) \text{ for every } g, h \in G \tag{3}$$

The loop (G, A, μ) is a Jordan loop iff $[(g,a)(g,a)][(h,b)(g,a)] = [\{(g,a)\ (g,a)\}\ (h,b)](g,a)$ and $(g,a)(h,b) = (h,b)(g,a)$ hold $\forall g, h \in G$ and every $a, b \in A$ straightforward calculation with (1) shows that this happens iff (2) and (3) are satisfied.

We call a factor set μ satisfies (2) and (3) a J-factor set. When G is an elementary abelian 2-group, then equation (2) reduces to equation (3). We now use a particular J-factor set to construct the above-mentioned family of Jordan loops.

Proposition 2.2.1. *Let A be an abelian group of order n where $n > 2$, and $\alpha \in A$ be an element of order greater than 2. Denote by $G = \{1, u, v, w\}$ the Klein group with neutral element 1. Define $\mu : G \times G \to A$ by*

$$\mu(x,y) = \begin{cases} \alpha, & \text{if } (x,y) = (u,v), (v,u); \\ -\alpha, & \text{if } (x,y) = (w,v), (v,w); \\ 0, & \text{otherwise.} \end{cases}$$

Then (G, A, μ) is a non-alternative (hence non-associative) Jordan loop with $N =$

$\{(1,a); a \in A\}$.

Proof. The map μ is clearly a factor set depicted as follows:

μ	1	u	v	w
1	0	0	0	0
u	0	0	α	0
v	0	α	0	$-\alpha$
w	0	0	$-\alpha$	0

To show that $J = (G, A, \mu)$ is a Jordan loop, we have to verify only equation (3). Since μ is a factor set, there is nothing to prove when $g = 1$ or $h = 1$. Assume that $g = u, h = v$ or $g = v, h = u$ then both sides of this equation (3) are equal to α. Assume that $g = w, h = v$ or $g = v, h = w$ then both sides of this equation (3) are equal to $-\alpha$. For all other values of g and h both sides of equation (3) are equal to 0. Hence equation (3) is satisfied and therefore $J = (G, A, \mu)$ is a Jordan loop.

Let $a \in A$, since $\alpha \neq -\alpha$, we have $(u,a)((w,a)(w,a)) = (u,3a) \neq (u,3a-\alpha) = ((u,a)(w,a))(w,a)$. This shows that: (i) J is not alternative and thus not associative (ii) $(u,a),(w,a) \notin N_\lambda$. Similarly $(v,a)((w,a)(w,a)) = (v,3a) \neq (v,3a-\alpha) = ((v,a)(w,a))(w,a)$ shows that$(v,a) \notin N_\lambda$. Finally, for $(g,h) \in G$ and $b,c \in A$ we have $((1,a)(g,b))(h,c) = (g, a+b+\mu(1,g))(h,c) = (gh, a+b+c+\mu(g,h))$ and $(1,a)((g,b)(h,c)) = (1,a)(gh, b+c+\mu(g,h)) = (gh, a+b+c+\mu(g,h)+\mu(1,\mu(g,h)))$ $= (gh, a+b+c+\mu(g,h))$ and thus $((1,a)(g,b))(h,c) = (1,a)((g,b)(h,c))$. Similarly it can be shown that $(g,b)((1,a)(h,c)) = ((g,b)(1,a))(h,c)$ and $((g,b)(h,c))(1,a) = (g,b)((h,c)(1,a)) \Longrightarrow (1,a) \in N$. Hence the result follows. $\square$

Corollary 3. *For every natural number n there exists a non-associative Jordan loop having nucleus of order n.*

Proof. It remains to prove that there are non-associative Jordan loops with nuclei of orders 1 and 2. But this is true by Example 3 and by Example 2.2.2. $\square$

Example 2.2.2. *A non-associative Jordan loop of order 8:*

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	1	0	6	7	4	5
3	3	2	0	1	7	6	5	4
4	4	5	6	7	1	0	3	2
5	5	4	7	6	0	1	2	3
6	6	7	4	5	3	2	1	0
7	7	6	5	4	2	3	0	1

Here nucleus is 2.

Example 2.2.3. *The* 3*-element cyclic group* $\{0,1,2\}$ *is the smallest group A which satisfies the assumptions of Proposition 2.2.1. The construction given in Proposition 2.2.1 with* $\alpha = 2$ *yields the following non-associative Jordan loop of order* 12.

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	0	4	5	3	7	8	6	10	11	9
2	2	0	1	5	3	4	8	6	7	11	9	10
3	3	4	5	0	1	2	11	9	10	6	7	8
4	4	5	3	1	2	0	9	10	11	7	8	6
5	5	3	1	2	0	9	10	11	9	8	6	7
6	6	7	8	11	9	10	0	1	2	4	5	3
7	7	8	6	9	10	11	1	2	0	5	3	4
8	8	6	7	10	11	9	2	0	1	3	4	5
9	9	10	11	6	7	8	4	5	3	0	1	2
10	10	11	9	7	8	6	5	3	4	1	2	0
11	11	9	10	8	6	7	3	4	5	2	0	1

We enumerated Jordan loops in Chapter 6. Our enumeration yields all Cayley tables explicitly. We can therefore validate the generated Jordan loops, and test support for conjectures in that data using the GAP [20] computer algebra system. Because there was no functionality present in the GAP *loops* package [60] to test whether a Cayley table is a Jordan loop or not, we have implemented our own function that performs this test. A listing for that function is given in Algorithm 1. The results of our enumeration were validated using that GAP function. Using GAP, we also verified that our data supports the following conjecture.

Conjecture 2. *A Jordan loop is nilpotent if and only if it is strongly nilpotent.*

One should note that the definition of nilpotency for a loop is the same as in group theory. A loop L is said to be strongly nilpotent if its multiplication group is nilpotent. GAP commands for testing the nilpotency of Cayley tables are: `IsNilpotent(` L `)` and `IsStronglyNilpotent(` L `)`. Using those GAP procedures we have verified that all the tables generated for our enumeration satisfy the condition of Conjecture 2.

Algorithm 1. *GAP function for testing if L is a Jordan loop*

```
InstallMethod( IsJordanLoop, "for Loop",
  [IsLoop],
  function( L )
  local x, y;
  if not IsCommutative(L) then
     return false;
```

```
fi;
for x in L do
   for y in L do
     if not (x * x) * (y * x) = ((x * x) * y) * x then
        return false;
     fi;
   od;
od;
return true;
end );
```

2.3 Nuclei and Commutant of C-Loops

We start our considerations with a corollary to [73, Proposition 3.1].

Corollary 4. *Let L be a nonassociative C-loop of order n with nucleus N of order m. Then*

(i) $n/m \equiv 1(\text{mod}3)$ *or* $n/m \equiv 2(\text{mod}3)$*,*

(ii) $(n/2)/m$ *is an integer of the form* $3k-1$ *or* $3k+1$*,*

(iii) $(n/m)^2 \equiv 4(\text{mod}6)$ *or* $n/m \equiv 4(\text{mod}6)$*,*

(iv) n/m *is of the form* $2(3k-1)$ *or* $(n/m)^2$ *is of the form* $2(3k-1)$*.*

Proof. (i) and (iii) are straightforward.
(ii) We have

$$n/m \equiv 2(\text{mod}6) \text{ or } n/m \equiv 4(\text{mod}6)$$
$$n/m = 6k+2 \text{ or } n/m = 6k+4 \text{ for some positive integer } k$$
$$n/m = 2(3k+1) \text{ or } n/m = 2(3k+2)$$
$$n/2m = 3k+1 \text{ or } n/2m = 3k+2$$
$$(n/2)/m = 3k+1 \text{ or } (n/2)/m = 3k+2. \text{ But every integer of the form } 3k+2 \text{ is also of the form } 3k-1.$$

Thus $(n/2)/m = 3k+1$ or $(n/2)/m = 3k-1$.

(iv) By part (iii), we have

$$
\begin{aligned}
(n/m)^2 &\equiv 4(\text{mod}6) \text{ or } n/m \equiv 4(\text{mod}6)\\
(n/m)^2 &= 6k+4 \text{ or } n/m = 6k+4 \text{ for some positive integer } k\\
(n/m)^2 &= 2(3k+2) \text{ or } n/m = 2(3k+2)\\
(n/m)^2 &= 2(3k-1) \text{ or } n/m = 2(3k-1).
\end{aligned}
$$

□

Proposition 1. *A nonassociative C-loop L of order $3n$ is non-simple and non-Steiner.*

Proof. $L/N(L)$ is Steiner, hence $3n/m$ is congruent to 2 or 4 mod 6. So $3n/m$ is not divisible by 3, thus m is divisible by 3. Therefore, $N(L)$ is a group containing an element of order 3 and hence L is not Steiner. Since $N(L)$ is nontrivial and since $N(L)$ is normal in L by [73], it follows that L is not simple. □

The following example illustrates the above proposition.

Example 6. *A nonassociative, noncommutative, non-Steiner non-simple C-loop of order 12 (size of nucleus = 3) is given in table 2.1.*

·	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	0	4	5	3	7	8	6	10	11	9
2	2	0	1	5	3	4	8	6	7	11	9	10
3	3	4	5	0	1	2	9	10	11	6	7	8
4	4	5	3	1	2	0	10	11	9	7	8	6
5	5	3	4	2	0	1	11	9	10	8	6	7
6	6	7	8	10	11	9	0	1	2	5	3	4
7	7	8	6	11	9	10	1	2	0	3	4	5
8	8	6	7	9	10	11	2	0	1	4	5	3
9	9	10	11	8	6	7	3	4	5	2	0	1
10	10	11	9	6	7	8	4	5	3	0	1	2
11	11	9	10	7	8	6	5	3	4	1	2	0

Table 2.1: Example 38.

·	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	5	4	9	8	7	6
2	2	3	0	1	6	8	4	9	5	7
3	3	2	1	0	7	9	8	4	6	5
4	4	5	6	7	0	1	2	3	9	8
5	5	4	8	9	1	0	7	6	2	3
6	6	9	4	8	2	7	0	5	3	1
7	7	8	9	4	3	6	5	0	1	2
8	8	7	5	6	9	2	3	1	0	4
9	9	6	7	5	8	3	1	2	4	0

Table 2.2: Example 39.

Corollary 5. *Let L be a nonassociative C-loop of order n with nucleus N of order m, then if for some positive integer t, 3^t divides n, then 3^t also divides m.*

The next proposition confirms that there are indeed some even orders for which no nonassociative C-loop exists.

Proposition 2. *There is no nonassociative C-loop of order* $2 \cdot 3^t$ *for* $t \geq 1$.

Proof. n/m is not divisible by 3, hence $L/N(L)$ is of index at most 2, which is impossible by [73]. □

The following proposition states that there exist orders for which all nonassociative C-loops will be Steiner.

Proposition 3. *A nonassociative C-loop* L *of order* $2p$ *with* p *prime, is Steiner.*

Proof. Since L is nonassociative, $p > 2$. Let m be the order of $N(L)$. Since $N(L)$ is normal in L by [73], m divides $2p$. If $m = 2p$, $L = N(L)$ is a group. If $m = p$ then $N(L)$ is of index 2 in L, which is impossible by [73]. Similarly, by [73] $L/N(L)$ is Steiner. If $m = 2$ then $L/N(L)$ is Steiner of order p, which again is impossible. Thus $m = 1$ and L is Steiner. □

Example 7. *The smallest nonassociative C-loop (size of nucleus* $= 1$*) is given in table 2.2. Since its order is* $n = 10 = 2 \cdot 5$, *it is also Steiner.*

It is well known that there are two nonassociative C-loops of order 14. Being of order of the form $2p$ both are Steiner with nucleus of order 1.

Remark 2. *Exploiting the results of propositions 1,2, and 3 can speed up automatic enumeration of C-loops. For example, we know by 1 that there is no nonassociative C-loop of order* 18 *, by 3 that C-loops of order* 24 *are all non-Steiner and by 2 that C-loops of order* 22 *are all Steiner.*

Next we give the general forms of the nuclei of the nonassociative C-loops. Here p is an odd prime other than 3.

Order of C-loop	Admissible order of nucleus
$2 \cdot 3^k p, k \geq 1$	3^k
$2p$	1
$2^l, l \geq 4$	$1, 2, 2^2, ..2^{l-2}$
$2^l \cdot 3^k, l \geq 1, k \geq 1$	$2^h \cdot 3^k, 0 \leq h \leq l-2$
$2^2 p$	$1, 2, p$
$2p^2$	$1, p$
$2^k p, k > 2$	$2^h, 2^l p, 0 \leq h \leq k-1, 0 \leq l \leq k-2$
$2p^k, k > 2$	$p^l, 0 \leq l \leq k-1$
$2^2 p^2$	$1, 2, p, p^2, 2p$
$2^2 \cdot 3 \cdot p$	$3, 6, 3p$

As application of the above table we can give the orders of C-loops and the admissible orders of their corresponding nuclei in the following table.

C-loop	Nucleus	C-loop	Nucleus	C-loop	Nucleus
10	1	42	3	74	1
12	3	44	1, 2, 11	76	1, 2, 19
14	1	46	1	78	3
16	1, 2, 4	48	3, 6, 12	80	1, 2, 4, 5, 8, 10, 20
20	1, 2, 5	50	1, 5	82	1
22	1	52	1, 2, 13	84	3, 6, 21
24	3, 6	56	1, 2, 4, 7, 14	86	1
26	1	58	1	88	1, 2, 4, 11
28	1, 2, 7	60	3, 6, 15	90	9, 18, 45
30	3	62	1	92	1, 2, 23
32	1, 2, 4, 8	64	1, 2, 4, 8, 16	94	1
34	1	66	3	96	3, 6, 12
36	9	68	1, 2, 7	98	1, 7
38	1	70	1, 5, 7	100	1, 2, 5
40	1, 2, 4, 5, 10	72	9, 18		

2.3.1 Commutant of C-Loops

The commutant of a loop is also known as the centrum, Moufang center or semi-center [38]. As discussed in [38], in a group, or even a Moufang loop, the commutant is a subloop, but this does not need to be the case in general. In [38], it has been proved that the commutant of a Bol loop of odd order is a subloop. In the following we discuss a special case for the commutant of C-loops, which is not necessarily a subloop as the following example demonstrates:

Example 8. *Consider the following nonassociative flexible C-loop of order* 20*, whose commutant is* $\{0, 1, 2, 3, 4, 5\}$ *that is not a subloop.*

·	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14	17	16	19	18
2	2	3	1	0	6	7	5	4	10	11	9	8	18	19	16	17	15	14	13	12
3	3	2	0	1	7	6	4	5	11	10	8	9	19	18	17	16	14	15	12	13
4	4	5	6	7	1	0	3	2	12	13	16	17	9	8	18	19	11	10	15	14
5	5	4	7	6	0	1	2	3	13	12	17	16	8	9	19	18	10	11	14	15
6	6	7	5	4	3	2	0	1	14	15	18	19	16	17	8	9	12	13	10	11
7	7	6	4	5	2	3	1	0	15	14	19	18	17	16	9	8	13	12	11	10
8	8	9	10	11	12	13	15	14	0	1	2	3	4	5	7	6	18	19	16	17
9	9	8	11	10	13	12	14	15	1	0	3	2	5	4	6	7	19	18	17	16
10	10	11	9	8	16	17	19	18	2	3	1	0	15	14	12	13	5	4	6	7
11	11	10	8	9	17	16	18	19	3	2	0	1	14	15	13	12	4	5	7	6
12	12	13	18	19	9	8	17	16	4	5	14	15	1	0	11	10	6	7	3	2
13	13	12	19	18	8	9	16	17	5	4	15	14	0	1	10	11	7	6	2	3
14	14	15	16	17	18	19	9	8	6	7	13	12	10	11	1	0	3	2	5	4
15	15	14	17	16	19	18	8	9	7	6	12	13	11	10	0	1	2	3	4	5
16	16	17	15	14	11	10	13	12	18	19	5	4	7	6	3	2	0	1	8	9
17	17	16	14	15	10	11	12	13	19	18	4	5	6	7	2	3	1	0	9	8
18	18	19	13	12	15	14	11	10	16	17	7	6	3	2	5	4	8	9	0	1
19	19	18	12	13	14	15	10	11	17	16	6	7	2	3	4	5	9	8	1	0

We now investigate a condition under which the commutant of C-loop will be a subloop.

Proposition 4. *Let $C(L)$ be the commutator of a C-loop L. If every element in $C(L)$ has odd order then $C(L)$ is a subloop of L.*

Proof. Since $C(L)$ is has odd order by [73], then in fact, C(L) = Z(L). By [73] L is power-alternative, thus $C(L)$ is closed under powers. Now, let $a, b \in C(L)$ with $|a| = 2k + 1$. Then $a = a^{2k+2}$ is a square, hence in $N(L)$ again by [73]. The rest of the proof is clear from this observation. $\square$

Chapter 3

Enumeration of AG-Groupoids

3.1 Introduction

Enumeration and classification of mathematical entities is an important part of mathematical research in particular in finite algebra. For algebraic structures that are more general than groups this task is often only feasible by use of computers due to the sheer number of structures that have to be considered. The classification of mathematical structures is an important branch of research in pure mathematics. In particular, in abstract algebra the classification of algebraic structures is an important pre-requisite for their goal-directed construction to make them amenable in practical applications. For example, the classification of finite simple groups — which was described as one of the major intellectual achievements of the twentieth century [24] — not only allows to immediately compute the number of non-isomorphic, simple groups of a particular finite order but also gives a concrete recipe how to construct a representant for each class.

While full classification of structures is usually the goal, an important first step towards this goal is often the enumeration of structures with particular properties. Enumeration results can be obtained by a variety of means, depending on the domain, for example by combinatorial or algebraic considerations. However, in algebraic domains where the objects under consideration exhibit little in way of internal structure, exhaustive generation is often the most reliable means of obtaining useful enumeration results. As a consequence, a number of projects have been concerned with automatic enumeration of algebraic structures that are more general than groups.

Quasigroups and loops — two types of non-associative structures with Latin square property — have been enumerated up to size 11 using a mixture of combinatorial considerations and bespoke exhaustive generation software [45, 44]. In other approaches general purpose automated reasoning technology has been employed. For instance the model generator FINDER (Finite Domain Enumerator) [101] has been used for obtaining novel enumeration results, most recently for IP-loops up to size 13 [1], but also has been successfully employed to solve open questions in quasigroup theory. Going beyond pure enumeration is the generation of classification theorems that provide discriminating algebraic properties for different isomorphism and isotopism classes of quasigroups and loops up to size 7 using a combination of theorem proving, model generation, satisfiability solving and computer algebra [105]. For the case of associative structures, more general than groups, the number of semigroups and monoids have been counted up to order 9 and 10, respectively, using a combination of constraint satisfaction techniques implemented in the Minion constraint solver with bespoke symmetry breaking provided by the computer algebra system GAP [11, 12, 13].

Here we consider the algebraic structures of finite Abel Grassmann Groupoids (AG-groupoids for short). AG-groupoids were first introduced by Naseeruddin and Kazim in 1972 [27] and have applications for example in the physics theory of flocks. They are generally considered midway between a groupoid and a commutative semigroup, that is, every commutative semigroup is an AG-groupoid but not vice versa. Thus AG-groupoids can also be non-associative, however they do not necessarily have the Latin square property. As a consequence neither of the enumeration techniques developed for quasigroups and loops or for semigroups and monoids can be employed directly. Our approach is based on the constraint solving technique developed for the enumeration of monoids and semigroups presented in [13]. However, since the original work explicitly exploited the associativity property for symmetry breaking we now present its novel adaptation to deal with our domain. Furthermore, we go beyond simple enumeration of the structures by the constraint solver and obtain a further division of the domain into interesting subclasses of AG-groupoids using the computer algebra system GAP. We have currently obtained enumeration results for AG-groupoids up to size 6 together with enumeration of some of the relevant subclasses. In addition, unlike in enumeration approaches using combinatorial techniques or algebraic counting, our enumeration also produces all multiplication tables for the structures found. These can be used both for further, more specialised, classification as well as be included into a library for GAP system in the future.

As no enumeration of AG-groupoids had been attempted before we present novel mathematical results, which are important as they give a first indication on the domain size of AG-groupoids as well as on the growth rate for the classes for increasing size of structures. This information can potentially be exploited when developing applications involving AG-groupoids. Our results also help to chart further the landscape of algebraic structures more general than groups.

The work is organised as follows: in the next section we give an introduction to the mathematical theory of AG-groupoids. We then present an overview of the constraint solving techniques that we have used to enumerate AG-groupoids in Sec. 3.2, with a particular emphasis on their adaptations to the new domain and how symmetries are broken using the computer algebra system GAP. We then discuss the classification results in Sec. 3.3 before concluding in Sec. 3.4.

3.2 Constructing AG-groupoids

To obtain all AG-groupoids up to isomorphism we adapt a method which was introduced in [12] and [13] in the search for monoids. The idea is to combine the advantages of a constraint solver for a fast search with that of a computer algebra system to efficiently rule out isomorphic copies. We will give a brief overview of the used technique. More detailed explanations and applications for various subclasses of semigroups can also be found in [11, Chapters 4, 5].

There are a number of important differences in the approach presented here to the one developed for enumerating semigroups and monoids. Instead of one search for each order, several independent searches were performed in [12, 11, 13], and for many of them it became far easier to avoid isomorphic solutions. These case splits were often based on structural knowledge about monoids and semigroups which also lead to a more efficient search in the remaining difficult, but more specific, cases. The enumeration of monoids and semigroups also benefit hugely from the fact that not all such objects needed to be counted. For semigroups there exists a formula for the majority of such objects [11, Section 2.3], while most monoids were constructed using semigroups and groups of lower order. For AG-groupoids we performed only one search for each order, as attempts to accelerate the search using a case split were not successful. This might change in the future, when the mathematical understanding of AG-groupoids has deepened further.

3.2.1 CSP and Minion

Constraint Programming is a powerful technique for solving large-scale combinatorial problems. To get an overview of this area the reader might want to start with [77]. Here we provide just basic definitions meeting our needs.

Definition 20. *A* constraint satisfaction problem (CSP) *is a triple* (V, D, C)*, consisting of a finite set* V *of* variables*, a finite set* D*, called the* domain*, of* values*, and a set* C *containing subsets of* D^V *(that is, all functions from* V *to* D*) called* constraints.

In practice, constraints, instead of being subsets of D^V, are usually formulated as conditions uniquely defining such subsets. Intuitively it is clear that one is looking for assignments of values in the domain of a CSP to all variables such that no constraint is violated. This is formalised in the next definition.

Definition 21. *Let* $L = (V, D, C)$ *be a CSP. A partial function* $f : V \to D$ *is an* instantiation*. An instantiation* f satisfies *a constraint if there exists a function* F *in the constraint, such that* $F(x) = f(x)$ *for all* $x \in V$ *on which* f *is defined. An instantiation is* valid *if it satisfies all the constraints in* C*. An instantiation defined on all variables is a* total *instantiation. A valid, total instantiation is a* solution *to* L*.*

The class of CSPs is a generalization of propositional satisfiability (SAT), and is therefore NP-complete. Solving problems using CSPs proceeds in two steps: modeling and solving. Solvers typically proceed by building a search tree, in which the nodes are assignments of values to variables and the edges lead to assignment choices for the next variable. If at any node a constraint is violated, then search backtracks. If a leaf is reached, then no constraints are violated, and the assignments provide a solution.

For our purposes we rely on Minion [21] as solver which offers fast, scalable constraint solving. A major feature of modern SAT solvers is their optimised use of modern computer architecture. Using this approach, Minion has been designed to minimise memory usage.

3.2.2 Symmetry Breaking and GAP

CSPs are often highly symmetric. Given any solution, there can be others which are equivalent in terms of the underlying problem. Symmetries may be inherent in the problem, or be created in the process of representing the problem as a CSP. Without symmetry breaking (henceforth SB), many symmetrically equivalent solutions may be found and, often more importantly, many symmetrically equivalent parts of the search tree will be explored by the solver. An SB method aims to avoid both of these problems.

Definition 22. *Let $L = (V, D, C)$ be a CSP.*

(i) Elements in the set $V \times D$ are called literals. *Literals are denoted in the form $(x = k)$ with $x \in V$ and $k \in D$.*

(ii) Let χ denote the set of all literals of L. A permutation $\pi \in S_\chi$ is a symmetry *of L if, under the induced action on subsets of χ, instantiations are mapped to instantiations and solutions to solutions.*

(iii) A variable-value symmetry *is a symmetry $\pi \in S_\chi$ such that there exists an element (τ, δ) in $S_V \times S_D$ with $(x = k)^\pi = (x^\tau = k^\delta)$ for all $(x = k) \in \chi$.*

The given definition of symmetry of a CSP is relatively strong. On the other hand all symmetries are variable-value symmetries in our case and as such will always send instantiations to instantiations. For more information on symmetries in CSPs, including different definitions see [77, Chapter 10].

There is a general technique, called lex-leader, for generating constraints that break symmetries [8]. The idea of lex-leader is to order solutions by defining an order on the literals of the CSP. This allows one to define the canonical representative in each set of symmetric solutions to be the solution which is smallest (or largest) with respect to the order. To define an order on solutions of a CSP L, first fix an ordering $(\chi_1, \chi_2, \ldots, \chi_{|V||D|})$ of the literals $\chi = V \times D$. Given the fixed ordering of the literals, an instantiation can be represented as a bit vector of length $|V||D|$. The bit in the i-th position is 1 if χ_i is contained in the instantiation and otherwise the bit is 0. The bit vector for the instantiation $I \subseteq \chi$ corresponding to the ordering of the literals $(\chi_1, \chi_2, \ldots, \chi_{|V||D|})$ will be denoted by $(\chi_1, \chi_2, \ldots, \chi_{|V||D|})_{|I}$. Of all bit vectors corresponding to a set of symmetric solutions of L, one is the lexicographic maximal, which shall be the property identifying the canonical solution. If $\geq_{\text{lex}}$ denotes the standard lexicographic order on vectors, extend L by adding for all symmetries π the constraint

$$(\chi_1, \chi_2, \ldots, \chi_{|V||D|})_{|I} \geq_{\text{lex}} (\chi_1^\pi, \chi_2^\pi, \ldots, \chi_{|V||D|}^\pi)_{|I}. \tag{3.1}$$

Then, from each set of symmetric solutions in L, exactly those with lexicographic greatest bit vector are solutions of the extended CSP.

To generate the constraints for symmetry breaking we use specialist software that provides robust, efficient and extensive implementations of algorithms in abstract algebra. GAP [20] (Groups, Algorithms and Programming) is a system for computational discrete algebra with particular emphasis on, but not restricted to, computational group theory. GAP provides a large library of functions that implement algebraic algorithms.

3.2.3 Search

We first formulate a CSP to search for all different AG-groupoids on the set $\{1, 2, \ldots, n\}$ for a positive integer n, and will subsequently add symmetry breaking to it.

CSP 1. *For a positive integer n define a CSP $L_n = (V_n, D_n, C_n)$. The set V_n consists of n^2 variables $\{A_{i,j} \mid 1 \leq i, j \leq n\}$, one for each position in an $(n \times n)$-multiplication table, having domain $D_n = \{1, 2, \ldots, n\}$. The constraints in C_n are*

$$A_{A_{i,j},k} = A_{A_{k,j},i} \text{ for all } i, j, k \in \{1, 2, \ldots, n\}, \tag{3.2}$$

reflecting the left-invertive law.

In Minion the constraint (3.2) is enforced using element constraints. The constraint $element(vector, i, val)$ specifies that, in any solution, $vector[i] = val$. We add a new variable $T_{a,b,c}$ for each triple (a, b, c). The pair of constraints

$$element(column(c), A_{a,b}, T_{a,b,c}) \text{ and } element(column(a), A_{c,b}, T_{a,b,c})$$

then enforces (3.2) for the triple.

As mentioned in Section 3.2.2, modeling a problem often introduces symmetries. In our case this happens by introducing identifiers, 1 up to n, for the n elements, even though we want them to be initially indistinguishable. The symmetries are the isomorphism between AG-groupoids, hence elements in S_n. To find a single representative from every equivalence class we have to break these introduced symmetries. We want to use the lex-leader method described in Section 3.2.2 and therefore define an ordering of the literals. We use

$$(A_{1,1}, A_{1,2}, \ldots, A_{1,n}, A_{2,1}, \ldots, A_{2,n}, \ldots, A_{n,1}, \ldots, A_{n,n}) \tag{3.3}$$

as variable order and define for the literals $(A_{i,j} = k) \leq_{\text{lex}} (A_{r,s} = t)$ if either $A_{i,j}$ comes earlier than $A_{r,s}$ in (3.3) or $k \leq t$. The canonical table in every isomorphism class is then defined by having the lex-largest bit vector with respect to this ordering of literals, which corresponds to the lex-smallest table with respect to standard row-by-row ordering. By adding for each $\pi \in S_n$ constraint (3.1) to L_n we obtain a CSP $\overline{L}_n$ which has AG-groupoids of order n up to isomorphism as solutions.

The data from running the instances L_n and $\overline{L}_n$ for $1 \leq n \leq 6$ is summarised in Table 3.1. Further classification for non-isomorphic AG-groupoids is presented

Table 3.1: Solutions and timings for L_n and $\overline{L}_n$

Order n	1	2	3	4	5	6
L_n, solutions	1	6	105	7 336	3 756 645	28 812 382 776
–, solve time	ϵ	ϵ	ϵ	ϵ	25 s	104 245 s
$\overline{L}_n$, solutions	1	3	20	331	31 913	40 104 513
–, solve time	ϵ	ϵ	ϵ	ϵ	ϵ	121 s

The times are rounded to seconds. They were obtained using version 0.11 of Minion on a machine with 2.80 GHz Intel X-5560 processor. The symbol ϵ stands for a time less than 0.5 s.

in the following section. A computation solving $\overline{L}_7$ to enumerate AG-groupoids of order 7 up to isomorphism is currently running and counted already more than $3 \cdot 10^{11}$ solutions in two weeks.

3.3 Classification of AG-groupoids

To obtain our classification results we have used Minion as discussed in the previous section to enumerate the entire space of non-isomorphic AG-groupoids as well as to produce the multiplication tables for all structures. This data is then further exploited to perform more fine-grained division into subclasses of AG-groupoids with respect to the properties presented in Sec. 1.1. This classification task is performed in GAP using functionality built on top of GAP's Loops library [60]. Although for large data sets (e.g, in the case of the classification of AG-groupoids of order 6) we use some parallelisation, this is fairly trivial and we will not present details here.

Table 3.2 presents our main result, the enumeration of the total number of

Order	3	4	5	6
Total	20	331	31913	40104513
Associative & commutative	12	58	325	2143
Associative & non-commutative	0	4	121	5367
Non-associative & non-commutative	8	269	31467	40097003

Table 3.2: General classification result for AG-groupoids of orders 3–6.

Order	3	4	5	6
Total	8	269	31467	40097003
AG-monoids	1	6	29	188
AG*-groupoid	0	0	0	9
AG**-groupoid	4	39	526	13497
Locally Associative	3	78	4482	1818828
AG-band	0	1	3	8
AG-3-band	0	1	3	10
Paramedial	8	264	31006	39963244
Cancellative	1	4	4	1
AG-groups	1	2	1	1

Table 3.3: Classification of non-associative AG-groupoids.

AG-groupoids of orders 3 to 6, which have not been known to date. These numbers are further broken down with respect to associativity and commutativity properties of the AG-groupoids. Observe that we only consider three classes here as it can be easily shown that every AG-groupoid that is non-associative is also non-commutative.

Tables 3.3, 3.4 and 3.5 then present the results of our further classification into subclasses. Observe that the structures in Table 3.5 are all commutative semigroups, which is the type of structure generalized by the notion of AG-groupoid. As a consequence some of the classification results are expected to be trivial as it is known that some of the properties are exhibited by all structures in that class. For example, every associative structure is also locally associative, and every semigroup is paramedial.

Similarly, in Table 3.4 it was to be expected that some of the rows would be empty or contain all structures in the class. However, it should be pointed out that it was assumed that all semigroups would also be AG*- and AG**-groupoids. Yet the result of our classification clearly shows that for order 6 there has to exist a further class of non-commutative semigroups that are neither AG*- nor AG**-groupoids. This is a novel, non-trivial result from our classification which will lead to a new class of structures to be investigated in the future.

A further minimal example, which was not known before, appears in Table 3.3. We see that there are two non-associative AG-3-bands of order 6 which are not AG-bands. This is of particular interest since it concerns AG-groupoids which are not semigroups.

Regarding the correctness of our results we are very confident that there are no errors. We only utilized established and well-tested functionality in GAP and Minion, and a more involved version of our approach has successfully been used before [11, 12, 13]. Moreover, most of the results were verified using other means. For AG-monoids we compared the numbers with a purely algebraic way of counting which we will give in chapter 11. In the case of associative AG-groupoids, that is for all results presented in Tables 3.4 and 3.5, we obtained identical numbers from experiments with the GAP package Smallsemi [14], which contains a database of all semigroups up to order 8. Finally, all numbers less than one million in Tables 3.2 to 3.5 were verified by one of the reviewers using Mace4 and Isofilter (parts of the Prover9/LADR package) [43].

3.4 Conclusions

We have presented novel classification results for the algebraic domain of AG-groupoids. We have produced both enumeration results for orders up to 6 and a partial classification of the domain using additional algebraic properties. To obtain these results we have employed a combination of the constraint solver Minion and the computer algebra system GAP. Thereby GAP is used on the one hand to perform symmetry breaking during the constraint solving process and on the other hand to perform the subsequent subclassification. While Minion has been previously applied in the classification of Semigroups and Monoids, the adaptation to our new application domain as discussed in Sec. 3.2 are both novel and non-trivial.

One of the advantages of our classification approach over techniques that use combinatorial or algebraic considerations for enumeration, is that it allows us to produce the multiplication tables of the structures under consideration. These can be further used to produce more fine-grained subclassifications as we have done in the case of AG-groupoids via a two step approach: firstly separating with respect to associativity and commutativity properties followed by a second refinement step using more specialised properties. While these were primarily motivated by mathematical considerations, the obtained results have already stimulated further investigations into other properties that could help to further subdivide the domain and lead to interesting, distinct classes of algebraic structures. For example our classification results of order 6 AG-groupoids have already yielded a heretofore unknown subclass of non-commutative semigroups that are neither AG*- nor AG**-groupoids as well as a new subclass of non-associative AG-groupoids that are AG-3-bands but not AG-bands. We hope to obtain more evidence on these new classes once our classification of order 7 has concluded and will then start its theoretical investigation.

In general, we see the work presented here as an important stepping stone for a further more fine-grained charting for algebraic structures that are more general than groups. Having the computational means to obtain reliable, non-trivial classification results will play a crucial role in this endeavour. As a consequence we intend to collate both our data and the functionality we have implemented in the process of our investigations into a GAP package to be published shortly. For more details about the package see chapter 12.

Order	3	4	5	6
Total	0	4	121	5367
AG-monoids	0	0	0	0
AG*-groupoid	0	4	121	5360
AG**-groupoid	0	4	121	5360
Locally Associative	0	4	121	5367
AG-band	0	0	0	0
AG-3-band	0	0	0	0
Paramedial	0	4	121	5367
Cancellative	0	0	0	0
AG-groups	0	0	0	0

Table 3.4: Classification of associative, non-commutative AG-groupoids.

Order	3	4	5	6
Total	12	58	325	2143
AG-monoids	5	19	78	421
AG*-groupoid	12	58	325	2143
AG**-groupoid	12	58	325	2143
Locally Associative	12	58	325	2143
AG-band	2	5	15	53
AG-3-band	4	13	41	162
Paramedial	12	58	325	2143
Cancellative	1	2	1	1
AG-groups	1	2	1	1

Table 3.5: Classification of associative, commutative AG-groupoids.

Chapter 4

Discovery of New Classes of AG-groupoids

4.1 Introduction

We presented enumeration of AG-groupoids up to order 6 in Chapter 3 and also we are constructing a GAP package AGGROUPOIDS for working with AG-groupoids see Chapter 12 for more details about the package. Using AG-GROUPOIDS and the Cayley tables obtained in enumeration we partially classified AG-groupoids in Chapter 3. We further investigated those Cayley tables and thus we came across twenty new and interesting subclasses of AG-groupoids, one new class of groupoid and one new class which is AG-groupoid as well as semigroup. We are presenting all this new stuff in this chapter.

We prove the existence of a new class of groupoids which we call Bol*-groupoid. A groupoid is called **Bol*-groupoid** if it satisfies the identity $(ab \cdot c)d = a \cdot (bc \cdot d)$. We call it Bol star groupoid because by taking $d = b$ it becomes the famous right Bol Identity. By a construction we prove that Bol star groupoids are obtainable from semigroups through endomorphisms of semigroups. Due to the unavailability of all the endomorphisms of semigroups we are unable to confirm that we get all Bol*-groupoids from semigroups. We found a new class of semigroups and AG-groupoids which we call AG-groupoid semigroup, that is a groupoid which satisfies left invertive law as well as associative law. This class contain all commutative semigroups. However we study non-commutative AG-groupoid semigroups because they are more interesting. This class has quite different properties from the already known famous subclasses of semigroups.

We add the following nineteen new subclasses of AG-groupoids to the above mentioned classes of AG-groupoids: paramedial AG-groupoid, anti-commutative AG-groupoid, transitively commutative AG-groupoid, self-dual AG-groupoid, Bol*-AG-groupoid, unipotent AG-groupoid, left alternative AG-groupoid, right alternative AG-groupoid, alternative AG-groupoid, flexible AG-groupoid, quasi-cancellative AG-groupoid, T^1-AG-groupoid, T^2-AG-groupoid, T_l^3-AG-groupoid, T_r^3-AG-groupoid, T^3-AG-groupoid, T_f^4-AG-groupoid, T_f^4-AG-groupoid, T^4-AG-groupoid.

We prove the existence of the above classes by providing their Cayley tables. All our examples are non-associative except if otherwise necessary as in case of AG-groupoid semigroup. We give their counting up to order 6. Relations between them and to other classes are also discussed. Further we prove the existence of zero-AG-groupoid, zero-AG-group. The chapter consists of a table and ten sections. Table 1 provides the counting of the new found classes of AG-groupoids for the non-associative AG-groupoids. In Section 4.2 we discuss quasi-cancellative AG-groupoids. Here we prove that every AG-band is quasi-cancellative and also prove the famous Burmistrovich's theorem for AG-groupoids. It states that "an AG**-groupoid S is a quasi-cancellative iff S is a semilattice of cancellative AG**-groupoids". Section 4.3 is about anti-commutative AG-groupoids and transitively commutative AG-groupoids. Here we prove that every anti-commutative AG-groupoid and every cancellative AG**-groupoid S is transitively commutative. Also the equivalence of AG-band locally associativity is proved for anti-commutative AG-groupoid. In Section 4.4 we construct Bol*-groupoids from semigroups through endomorphisms of semigroups. The main results of Section 4.5 are of proving that Bol*-AG-groupoid is the generalization of AG**-groupoid and a special kind of paramedial AG-groupoid and proving the in-existence of non-associative paramedial AG-3-band. We emphasis on non-commutative AG-groupoid semigroup in Section 4.6 that it does not lie in the known classes of semigroups and provides an example of such semigroups in which the product of idempotents is always an idempotent. It cannot contain left identity as well as right identity and always satisfies paramedial property. In Section 4.7 we introduce the concept of alternativity and flexibility from loop theory into AG-groupoids. Here we prove two basic facts that every AG-3-band is flexible and that in a right alternative AG-groupoid, square of every element commute with every element. Section 4.8 is about the existence of self-dual AG-groupoid and unipotent AG-groupoids. Here we prove that a self-dual AG-groupoid with left identity becomes commutative monoid and also that in a left alternative self dual AG-groupoid, square of every element commutes with every element. In Section 4.9

we introduce 8 more AG-groupoids which we call types and are mentioned above. Thus we prove that Every AG-3-band, T^1-AG-groupoid and T^2-AG-groupoid is T^3-AG-groupoid and every T^2-AG-groupoid is Bol*-AG-groupoid. For T^1-AG-groupoid we prove that square of every element is idempotent and if it has left identity also then it becomes a unitary AG-group.

As in semigroup theory the concept of zero-semigroup and zero-group exists, we find a similar concept for zero-AG-groupoid and zero-AG-group in Section 4.10.

Table 4.1 presents the counting of the new subclasses of AG-groupoids. Note that except from non-commutative AG-groupiod Semigroup only the number of non-associative AG-groupoids is shown.

4.2 Quasi-cancellativity of AG-groupoids

In this section we introduce the notion of quasi-cancellativity from semigroup into AG-groupoids. Quasi-cancellativity is the generalization of cancellativity. We will consider cancellativity of AG-groupoids in Chapter 5.

Definition 23. *An AG-groupoid S is **quasi-cancellative** if for any $x, y \in S$,*

(i) $x^2 = xy$ and $y^2 = yx$ imply that $x = y$,

(ii) $x^2 = yx$ and $y^2 = xy$ imply that $x = y$.

Using our under construction package AGGROUPOIDS the two parts of the above definition are equivalent for AG-groupoids up to order 6. Thus:

Conjecture 3. *Conditions (i) and (ii) of Definition 23 are equivalent for AG-groupoids.*

Order	3	4	5	6
Total	20	331	31913	40104513
Paramedial AG-groupoids	8	264	31006	39963244
Anti-commutative AG-groupoids	1	2	4	0
Transitively commutative AG-groupoids	3	61	2937	1239717
Self-dual AG-groupoids	0	8	133	4396
Bol*-AG-groupoids	4	58	2706	1357494
Quasi-cancellative AG-groupoids	1	6	18	66
Non-commutative AG-groupiod semigroup	0	4	121	5367
Left alternative AG-groupoids	0	5	171	12029
Right alternative AG-groupoids	2	33	997	139225
Alternative AG-groupoids	0	2	59	4447
Flexible AG-groupoids	1	19	447	32770
T^1-AG-groupoids	2	14	101	783
T^2-AG-groupoids	1	3	8	16
T_l^3-AG-groupoids	2	17	135	1272
T_r^3-AG-groupoids	3	36	374	5150
T^3-AG-groupoids	2	16	111	870
T_f^4-AG-groupoids	1	13	90	784
T_b^4-AG-groupoids	0	1	6	11
T^4-AG-groupoids	0	1	3	7
Unipotent AG-groupoids	5	74	3946	1739186
Left nuclear square AG-groupoids	8	265	31127	40009235
Right nuclear square AG-groupoids	2	32	1083	169152
Middle nuclear square AG-groupoids	3	56	3131	1494920
Nuclear square AG-groupoids	2	32	1077	168431

Table 4.1: Classification and enumeration results for new subclasses of AG-groupoids of orders 3–6.

Example 9. *A quasi-cancellative AG^{**}-groupoid of order* 5.

$\cdot$	1	2	3	4	5
1	1	1	1	1	1
2	1	2	2	4	5
3	1	2	3	4	5
4	1	5	5	2	4
5	1	4	4	5	2

Proposition 5. *Every AG-band is quasi-cancellative.*

Proof. Let S, be an AG-band such that for any $x, y \in S$ we have

(i) $x^2 = xy$ and $y^2 = yx$ which by definition of AG-band become $x = xy$ and $y = yx$. Now $x = xy = xy \cdot y = y^2x = yx = y$.

(ii) $x^2 = yx$ and $y^2 = xy$ which by definition of AG-band become $x = yx$ and $y = xy$. Now $x = yx = y^2x = xy \cdot y = y^2 = y$. Hence S is quasi-cancellative.

□

Conjecture 4. *Every AG-3-band is quasi-cancellative.*

Lemma 2. *In a quasi-cancellative paramedial AG-groupoid S, for any $x, y, a, b \in S$ the following statements hold*

(i) $xa = xb$ *iff* $ax = bx$*;*

(ii) $x^2a = x^2b$ *implies that* $xa = xb$*;*

(iii) $(xy)a = (xy)b$ *implies that*$(yx)a = (yx)b$.

Proof. (i) if $xa = xb$, then $(xa)(xa) = (xb)(xa)$ and $(xa)(xb) = (xb)(xb)$ so that $(ax)^2 = (ax)(bx)$ and $(bx)^2 = (bx)(ax)$ which by Definition 23 implies that $ax = bx$. The opposite implication follows by symmetry.

(ii) If $x^2a = x^2b$, then $(x^2a)a = (x^2b)a$ and $(x^2a)b = (x^2b)b$ which implies that

$$a^2x^2 = (ab)x^2 \text{ or } (ax)^2 = (ax)(bx) \tag{1}$$

and

$$(ba)x^2 = b^2x^2 \text{ or } (bx)^2 = (bx)(ax) \tag{2}$$

Thus from (1) and (2) by Definition 23(i) we have $ax = bx$. But then by (i), also $xa = xb$

(iii)

$$\begin{aligned}
\text{Let } (xy)a &= (xy)b \text{ then} \\
a^2(xy) &= (ab)(xy) \\
(xy)^2a^2 &= (xy)^2(ab) \\
(yx)^2a^2 &= (yx)^2(ab)
\end{aligned}$$

Thus

$$[a(yx)]^2 = [b(yx)][a(yx)] \tag{3}$$

$$\begin{aligned}
\text{similarly } (xy)a &= (xy)b \text{ then} \\
(ba)(xy) &= b^2(xy) \\
(xy)^2(ba) &= (xy)^2b^2 \\
(yx)^2b^2 &= (yx)^2(ba) \\
[b(yx)]^2 &= (ab)(yx)^2
\end{aligned}$$

This implies that

$$[b(yx)]^2 = [a(yx)][b(yx)] \tag{4}$$

from (3) and (4) by Definition 23(ii) we have $a(yx) = (yx)b$.

□

Burmistrovich's theorem for AG-groupoids:

Here We prove the version of the famous Burmistrovich's theorem of semigroups [4] for AG-groupoids. For AG-groupoids it will become as follows.

Theorem 4. *An AG^{**}-groupoid S is quasi-cancellative iff S is a semilattice of cancellative AG^{**}-groupoids.*

Proof. Necessity: On S define the relation σ by $x\sigma y$ if for any $a, b \in S$,$xa = xb$ if and only if $ya = yb$. It is clear that σ is an equivalence relation. Let $x\sigma y$ and $z \in S$. If

$$\begin{aligned}
(xz)a &= (xz)b \\
&\Longrightarrow (az)x = (bz)x \text{ by left invertible law} \\
&\Longrightarrow x(az) = x(bz) \text{ by Lemma } 2(i) \\
&\Longrightarrow y(az) = y(bz) \text{ by hypothesis} \\
&\Longrightarrow a(yz) = b(yz) \text{ by definition of AG}^{**}\text{-groupoid} \\
&\Longrightarrow (yz)a = (yz)b \text{ by Lemma 2 } (i)
\end{aligned}$$

By symmetry $(yz)a = (yz)b$ implies that $(xz)a = (xz)b$ thus it follows that $xz\sigma yz$. Now if

$$\begin{aligned} (zx)a &= (zx)b \\ &\Rightarrow (xz)a = (xz)b \text{ by Lemma 2 } (iii) \\ &\Rightarrow (yz)a = (yz)b \text{ as above} \\ &\Rightarrow (zy)a = (zy)b \text{ by Lemma 2 } (iii) \end{aligned}$$

By symmetry $(zy)a = (zy)b$ implies that $(zx)a = (zx)b$. Thus it follows that $zx\sigma zy$ and hence σ is congruence. Further, Lemma 2(i) & Lemma 2(ii) imply that S/σ is an AG-band and while Lemma 2(iii) implies that S/σ is commutative. Therefore σ is a semilattice congruence. Suppose that $zx = zy$ and $x\sigma z$ and $y\sigma z$. Since $x\sigma z$, $zx = zy$ implies that $x^2 = xy$ and since $y\sigma z$, it implies that $yx = y^2$. But then Definition 23(i) yields $x = y$. If $xz = yz$ with $x\sigma z$ and $y\sigma z$ then by Lemma 2(i) $zx = zy$, and this reduces to the case just considered. Hence each σ-class is cancellative.

Sufficiency : Suppose S is a semilattice of cancellative AG**-groupoids. Let x and y be elements such that $x^2 = xy$ and $y^2 = yx$. Let β be the component of S that contains xy. Since S is commutative being semilattice we have $yx \in \beta$ as well. Thus $x^2, y^2 \in \beta$. Since β is an AG**-groupoid so by the closure property in β, we have $x, y \in \beta$. But β is cancellative, and therefore the equality $xx = xy$ implies $x = y$. A similar argument applies if $x^2 = yx$ and $y^2 = xy$. □

Let us verify this by an example. Consider the Example 9. Since $S = \{1, 2, 3, 4, 5\}$ is quasi-cancellative AG**-groupoid. So we can write $S = \{A = \{1\}, B = \{3\}, C = \{2, 4, 5\}\}$. Here A, B and C are cancellative AG**-groupoids such that they commute with each other and $A^2 = A, B^2 = B, C^2 = C$. We remark that there are $1, 4, 12$ non-associative quasi-cancellative AG**-groupoids of order $3, 4, 5$ respectively and we have verified them all manually for this theorem.

4.3 Anti-commutativity and Transitively Commutativity of AG-groupoids

Actually the notion of anti-commutativity and transitively commutativity had been defined for AG-bands in [74] which is a very small class of AG-groupoids. We make these definitions global for the whole AG-groupoids and prove their existence in Examples 10 and 11.

Definition 24. *An AG-groupoid S is called* ***anti-commutative*** *if for all $a, b \in S$, $ab = ba$ implies that $a = b$.*

Definition 25. *An AG-groupoid S is called* ***transitively commutative*** *if for all $a, b, c \in S$, $ab = ba$ and $bc = cb$ implies that $ac = ca$.*

Example 10. *An anti-commutative AG-groupoid*

·	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

Example 11. *A transitively commutative AG-groupoid (a non-anti-commutative AG-groupoid)*

·	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	2	2	2	1

Theorem 5. *Every cancellative AG^{**}-groupoid S is transitively commutative.*

Proof. Let $a, b, c \in S$ such that $ab = ba, bc = cb$. Then consider

$$b(ac) = a(bc) = a(cb) = c(ab) = c(ba) = b(ca)$$

which by left cancellativity implies that $ac = ca$. □

Corollary 6. *Every AG-group is transitively commutative.*

Theorem 6. *Every anti-commutative AG-groupoid S is transitively commutative.*

Proof. Let S be an anti-commutative AG-groupoid and let $a, b, c \in S$ such that $ab = ba, bc = cb$. Then by definition of anti-commutativity, this implies that $a = b, b = c$. But this implies that $a = c$ and which further implies that $ac = ca$. Hence S is transitively commutative. □

Conjecture 5. *Every anti-commutative AG-groupoid S is cancellative but converse is not true.*

Theorem 7. *Let S be an anti-commutative AG-groupoid. Then the following are equivalent.*

(i) S is AG-band;

(ii) S is locally associative.

Proof. $(i) \Longrightarrow (ii)$ is always true.
$(ii) \Longrightarrow (i)$. By definition of locally associativity and anti-commutativity, for every $a \in S$ we have

$$aa^2 = a^2a \Longrightarrow a^2 = a$$

□

4.4 Construction of Bol*-groupoid from Semigroups

In the following we prove that from a given Bol*-groupoid $(S, \cdot)$ we can obtain a semigroup and from a semigroup we can obtain a Bol*-groupoid by defining a new operation $*$ on S by

$$x * y = (xp)y \, \forall x, y \in S.$$

Proposition 6. *Let $(S, \cdot)$ be a Bol*-groupoid Define $* : S \times S \to S$ via $(x, y) \mapsto xp \cdot y$ where p is any fixed element. Then $(S, *)$ is a semigroup.*

Proof. Let $x, y, z \in S$. The set $(S, *)$ is closed since $xp \cdot y$ is an element of S. To check associativity
$(x * y) * z = (((xp)y)p)z = (xp)((yp)z) = x * (y * z)$.
That is, $(x * y) * z = x * (y * z) \, \forall x, y, z \in S$.
Thus $(S, *)$ is a semigroup. □

Example 12. *A Bol*-groupoid which is not Bol*-AG-groupoid.*

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	1	1	3	4

For illustration of the Proposition 6 the following example is provided.

Example 13.

Given the above Bol*-groupoid $(S,\cdot)$ in Example 12 then using Proposition 6 and taking $p=1$ fixed, we get the semigroup $(S,*)$ as in the following table.

$*$	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	1	1	1	1

Theorem 8. *Let $(S,\circ)$ be a semigroup. Let $\alpha,\beta\in End(S)$ such that $\alpha^3=\alpha,\alpha^2\beta=\beta\alpha^2,\beta\alpha\beta=\alpha\beta,\beta^2=\beta$. Define $x\cdot y=\alpha(x)\circ\beta(y)\,\forall x,y\in S$ then $(S,\cdot)$ is a Bol*-groupoid.*

Proof. Let $a,b,c,d\in S$. Then by definition, we have

$$((a\cdot b)\cdot c))\cdot d=\alpha(\alpha(\alpha(a)\circ\beta(b))\circ\beta(c))\circ\beta(d)=\alpha^3(a)\circ\alpha^2\beta(b))\circ\alpha\beta(c))\circ\beta(d) \quad (5)$$

On the other hand, by definition and by using associativity, we have

$$a\cdot((b\cdot c)\cdot d)=\alpha(a)\circ((\beta\alpha^2(b)\circ\beta\alpha\beta(c))\circ\beta^2(d)=((\alpha(a)\circ\beta\alpha^2(b))\circ\beta\alpha\beta(c))\circ\beta^2(d) \quad (6)$$

From (5) and (6), we can say that $(S,\cdot)$ is a Bol*-groupoid if $\alpha^3=\alpha,\alpha^2\beta=\beta\alpha^2,\beta\alpha\beta=\alpha\beta,\beta^2=\beta$. □

Remark 3. Note that if β is identity endomorphism I then $(S,\cdot)$ is a Bol*-groupoid if $\alpha^3=\alpha$ *and if* α is identity endomorphism I then $(S,\cdot)$ is a Bol*-groupoid if $\beta^2=\beta$.

Unfortunately since all the endomorphisms are not available so we cannot confirm that whether this construction will give us all the Bol*-groupoids from a semigroup. As a special case of this in [89] all Bol*-quasigroups have been obtained from groups through involutive automorphisms because groups of large orders are available along with their automorphisms. We have implemented this in AGGROUPOIDS which gives all Bol*- quasigroups of order n. We have also implemented the method for Bol*-groupoids through involutive automorphisms of semigroups which gives many examples of Bol*-groupoids up to order 8 but obviously not all.

4.5 Paramedial AG-groupoids and Bol*-AG-groupoids

Some immediate observations from the definition of paramedial AG-groupoid S are (i) Square of elements commute with each other and therefore an AG-band which is also paramedial AG-groupoid must be commutative semigroup (ii) The identity $(ab)^2 = (ba)^2$ holds (iii) The identity $(ab)(cd) = (dc)(ba)$ holds (iv) Every paramedial groupoid with left identity becomes an AG-groupoid.

Example 14. *A Paramedial AG-groupoid.*

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	2
4	1	1	1	4

Example 15. *A Bol*-AG-groupoid.*

$\cdot$	1	2	3
1	1	1	1
2	1	1	1
3	1	2	2

Theorem 9. *Non-associative paramedial AG-3-band does not exist.*

Proof. Let S be a paramedial AG-3-band. Let $a, b \in S$. Now $ab = a^3b^3 = (ab)(a^2b^2) = (b^2a^2)(ba) = b^3a^3 = ba$. Thus commutative semigroup . $\square$

Definition 26. *An AG-groupoid S satisfying the identity*

$$a(bc \cdot d) = (ab \cdot c)d \tag{7}$$

*is called **Bol*-AG-groupoid**.*

Lemma 3. *Every AG**-groupoid S is Bol*-AG-groupoid.*

Proof. Let $a, b, c, d \in S$.

$$\begin{aligned} (ab \cdot c)d &= (dc)(ab) \text{ by left invertive law} \\ &= a(dc \cdot b) \text{ by } a(bc) = b(ac) \\ &= a(bc \cdot d) \end{aligned}$$

Thus S is an Bol*-AG-groupoid. $\square$

Lemma 4. *Every Bol*-AG-groupoid is paramedial AG-groupoid.*

Proof. Let $a, b, c, d \in S$.

$$\begin{aligned} ab \cdot cd &= (cd \cdot b)a \text{ by left invertive law} \\ &= (bd \cdot c)a \text{ by left invertive law} \\ &= b(dc \cdot a) \text{ by (7)} \\ &= b(ac \cdot d) \text{ by left invertive law} \\ &= (ba \cdot c)d \text{ by (7)} \\ &= (ca \cdot b)d \text{ by left invertive law} \\ &= db \cdot ca \text{ by left invertive law} \end{aligned}$$

Hence S is paramedial AG-groupoid. □

By the above two lemmas Bol*-AG-groupoid is the generalization of AG**-groupoid and a special kind of paramedial AG-groupoid.

Lemma 5. *Every Bol*-groupoid G with right identity e is a semigroup.*

Proof. Take $d = e$ in (7). □

As Example 12 shows a Bol*-groupoid not necessarily has left identity. But it can have it without becoming semigroup as the following shows:

Example 16. *A non-associative Bol*-groupoid of order* 5.

$\cdot$	1	2	3	4	5
1	1	1	1	1	1
2	1	1	1	1	1
3	1	1	1	1	4
4	1	1	1	1	3
5	1	2	3	4	5

Lemma 6. *Let S be a Bol*-groupoid having left identity e. Then,*

(i) $a(bc) = (ae \cdot b)c$;

(ii) $(ab \cdot e)c = a(be \cdot c)$.

Proof. (i) Taking $b = e$ in (7) and re-naming.

(ii) Taking $c = e$ in (7) and re-naming.

□

A left identity is left cancellative by its definition but not necessarily right cancellative as Example 16 shows. But if the left identity is also right cancellative as in the following example then it can enjoy more properties as in the lemma following the example.

Example 17.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	3	4
3	4	3	3	4
4	3	4	3	4

Lemma 7. *Let S be a Bol*-groupoid having left identity e such that e is cancellative. Then,*

(i) $xe \cdot e = x \, \forall x \in S$, *where e is left identity in S;*

(ii) $(ae \cdot be)e = ab$;

(iii) $(ab)e = (ae)(be)$.

Proof. (i) Taking $b = c = e$ in Lemma 6 Part (i) and then using right cancellativity of e.

(ii) Taking $b = be$ and $c = e$ in Lemma 6 Part (i) and then using (i).

(iii) Taking $a = ae$ and $b = be$ in Lemma 6 Part (ii) and then using (i).

□

Remark 4. In Example 17, 1 and 2 are both cancellative so here one might guess that a right cancellative might be cancellative as in the case of AG-groupoids [88]. The following example shows that this is not so.

Example 18. *A Bol*-groupoid of order* 4.

$\cdot$	1	2	3	4
1	1	2	1	1
2	2	1	2	2
3	1	2	4	4
4	1	2	3	3

Here 4 is right cancellative but not left cancellative.

4.6 AG-groupoid Semigroups

This class can be considered as a subclass of both semigroups and AG-groupoids. Further this class trivially contains all commutative semigroups because they satisfy both associative law and invertive law. Also this is easy to see that this class is contained in the class of Bol*-AG-groupoids. The interesting subclass of this is the non-commutative AG-groupoid semigroups. Thus this class lies between commutative semigroups and Bol*-AG-groupoids. This new class of semigroups is different from the other well-known subclasses of semigroups altogether as we will prove. So we consider only the non-trivial case, that is, non-commutative AG-groupoid semigroups. The existence of this class has been shown in Example 19. We emphasis that this class is very interesting and useful as every member of this class enjoy at the same time the characteristics of semigroups as well as AG-groupoids and thus can produce many new results. Also since the structure of semigroups is very well-known and well studied at one hand and on the other hand the structure of AG-groupoids is relatively a new structure and now researchers have taken interest in that so they are bringing different notions from semigroups into AG-groupoids. So this class can be used as a criterion for those concepts. The new notion should be defined in a way that when those new notions are applied to this class should not conflict with each other rather those should coincide when come to this class. So this class can be used as tools for the correctness of such definitions. The previously produced such work and the upcoming both should be checked by researchers for the justification of new definitions. We check some quick and interesting results in the following. We also give some conjectures whose counterexamples do not exist at least up to order 6 and suggest the detailed study of this class as a future work.

Example 19. *A non-commutative AG-groupoid Semigroup.*

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	2
4	1	1	1	2

Recall that an AG-groupoid with right identity is a commutative monoid which we do not consider here but can contain left identity as in Example 1 (i), 2 is left identity and hence is an AG-monoid. Also a semigroup can contain both left identity and right identity but the class we are considering can contain neither as the following simple result shows.

Theorem 10. *An AG-groupoid semigroup with left identity becomes commutative monoid.*

Proof. Let S be an AG-groupoid semigroup with left identity e. Let x be an arbitrary element in S. Then

$$x = ex = (ee)x = (xe)e = x(ee) = xe.$$

Thus e is also the right identity and hence S is a commutative monoid. □

Recall that a band in semigroups is called an AG-band in AG-groupoids. The following shows that a band or AG-band does not exist for AG-groupoid semigroups.

Theorem 11. *An AG-groupoid semigroup S is paramedial AG-groupoid.*

Proof. Let $a, b, c, d \in S$. Then by repeated use of associative, invertive and medial laws, we have

$$\begin{aligned} ab \cdot cd &= (ab \cdot c)d = dc \cdot ab = (dc \cdot a)b = ba \cdot dc \\ &= bd \cdot ac = (bd \cdot a)c = ca \cdot bd = (ca \cdot b)d = db \cdot ca. \end{aligned}$$

Thus S is paramedial AG-groupoid. □

Corollary 7. *An AG-groupoid semigroup is commutative semigroup if it is an AG-band .*

Corollary 8. *An AG-groupoid semigroup S cannot be a rectangular semigroup.*

Also the medial property of AG-groupoids shows that this class is closed under idempotents.

Theorem 12. *An AG-groupoid semigroup S is closed under idempotents.*

Proof. Let $a, b \in S$ such that $a^2 = a, b^2 = b$ Then

$$ab = a^2b^2 = (ab)^2.$$

Thus S is closed under idempotents.

From the above theorem this also follows that non-idempotent elements of an AG-groupoid cannot be expressed as the product of idempotent elements. Thus □

Corollary 9. *An AG-groupoid semigroup S cannot be idempotent generated.*

Theorem 13. *An AG-groupoid semigroup S is commutative semigroup if S is an inverse semigroup.*

Proof. Let S be AG-groupoid semigroup such that S is also an inverse semigroup Let $a, b \in S$. Then by definition $aba = a, bab = b$. Now by repeated use of associative, invertive laws, we have
$ab = (aba)(bab) = (aba)(ba \cdot b) = ((aba)ba))b = (b \cdot ba)(aba) = (b \cdot (ba)a)(ba) = (b \cdot a^2 b)(ba) = (ba)(ab)(ba) = ba.$

Thus S is commutative semigroup. □

Corollary 10. *A non-commutative AG-groupoid semigroup cannot be an inverse semigroup and hence cannot be a Brandt semigroup.*

Theorem 14. *An AG-groupoid semigroup S is commutative semigroup if S is a regular semigroup.*

Proof. Let S be AG-groupoid semigroup such that S is also a regular semigroup. Let $a, b \in S$. Then by definition for every x in S there exists y in S such that $xyx = x$. Now by repeated use of associative, invertive laws, we have

$$xyx = x \Longrightarrow xy = xyxy = (xy)^2 \text{ and also } xyx = x \Longrightarrow yx = yxyx = (yx)^2 .$$

Since in S, $(xy)^2 = (yx)^2$ and hence $xy = yx$. Thus S is commutative semigroup. □

Corollary 11. *A non-commutative AG-groupoid semigroup cannot be regular and hence cannot be a Clifford semigroup or an orthodox semigroup.*

Our data of non-commutative AG-groupoid semigroups up to order 6 indicates that they are not simple, that is, they have a proper ideal so we have the following:

Conjecture 6. *Every non-commutative AG-groupoid semigroup is non-simple.*

4.7 Alternative and Flexible AG-groupoids

In an attempt to bring AG-groupoids a bit closer to quasigroups and loops, the concept of nucleus of AG-groupoids was introduced in [91] and by doing so six new classes of AG-groupoids were defined. Here we introduce the concept of flexibility and alternativity from loops. This will give us four more classes of AG-groupoids.

Definition 27. *An AG-groupoid is called **flexible** if it satisfies the identity*

$$xy \cdot x = x \cdot yx$$

Definition 28. *An AG-groupoid is called **left alternative** if it satisfies the identity*

$$xx \cdot y = x \cdot xy$$

Definition 29. *An AG-groupoid is called **right alternative** if it satisfies the identity*

$$xy \cdot y = x \cdot yy$$

Definition 30. *An AG-groupoid is called **alternative** if it is both left alternative and right alternative.*

Example 20. *A left alternative AG-groupoid of order* 4.

·	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	2
4	1	1	1	4

Example 21. *A right alternative AG-groupoid of order* 3.

·	1	2	3
1	1	1	1
2	1	1	1
3	1	2	1

Example 22. *An alternative AG-groupoid of order* 4.

·	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	2
4	1	3	1	1

Proposition 7. *Every AG-*3*-band is flexible.*

Proof. Let S be an AG-3-band and $x, y \in S$. Then

$$x \cdot yx = xx^2 \cdot yx = xy \cdot x^2x = xy \cdot x$$

Hence S is flexible. □

Proposition 8. *In a right alternative AG-groupoid, square of every element commute with every element.*

Proof. Let S be an AG-groupoid and $x, y \in S$. Then

$$x^2y = yx \cdot x = yx^2$$

□

The following now easily follows.

Corollary 12. *(i) Every right alternative AG-groupoid is locally associative.*

(ii) A right alternative AG-monoid is commutative monoid.

Though a non-associative left alternative can be AG-monoid (see the following Example) but then it cannot contain inverses because a left alternative AG-group is abelian group [94].

Example 23. *A left alternative AG-monoid of order* 4.

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	1	1	3
3	1	1	1	2
4	1	2	3	4

4.8 Self-dual AG-groupoids and Unipotent AG-groupoids

Here we introduce the notion of self-duality from semigroup into AG-groupoids. (Left) AG-groupoid and right AG-groupoid can be easily seen the dual of each other. Thus the transpose of the multiplication table of an AG-groupoid becomes right AG-groupoid. There are AG-groupoids whose transpose is also an AG-groupoid. In this section we discuss such AG-groupoids.

Definition 31. *An AG-groupoid is called **self-dual** if it is also a right AG-groupoid.*

Remark 5. *Though not studied but the existence of the above class can be found in the literature by the name **almost semigroup**.*

It is easy to prove that:

Corollary 13. *A self-dual AG-groupoid with left identity becomes commutative monoid.*

Definition 32. *An AG-groupoid S is called* ***unipotent*** *if for every $a, b \in S$, we have $a^2 = b^2$.*

Example 24. *A self-dual AG-groupoid which is also unipotent.*

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	2
4	1	3	1	1

Theorem 15. *In a left alternative self dual AG-groupoid, square of every element commutes with every element.*

Proof. Let S be an AG-groupoid and $x, y \in S$. Then

$$x^2y = x \cdot xy = yx^2.$$

□

4.9 Type 1, Type 2, Type 3 and Type 4 AG-groupoids

Definition 33. *An AG-groupoid S is called a* ***Type 1 AG-groupoid*** *denoted by T^1-AG-groupoid if for all $a, b, c, d \in S$,*

$$ab = cd \Longrightarrow ba = dc.$$

The following is an obvious fact.

Corollary 14. *Let S be an AG-groupoid. Then the following are equivalent.*

(i) $ab = cd \Longrightarrow ac = bd$ *for all* $a, b, c, d \in S$*;*

(ii) $ab = cd \Longrightarrow ca = db$ *for all* $a, b, c, d \in S$*.*

Definition 34. *An AG-groupoid S is called a* ***Type*** 2 ***AG-groupoid*** *denoted by T^2-AG-groupoid if for all $a, b, c, d \in S$,*

$$ab = cd \Longrightarrow ac = bd.$$

Definition 35. *An AG-groupoid S is called a* ***Left Type*** 3 ***AG-groupoid*** *denoted by T_l^3-AG-groupoid if for all $a, b, c \in S$,*

$$ab = ac \Longrightarrow ba = ca.$$

Definition 36. *An AG-groupoid S is called a* ***Right Type*** 3 ***AG-groupoid*** *denoted by T_r^3-AG-groupoid if for all $a, b, c \in S$,*

$$ba = ca \Longrightarrow ab = ac.$$

Definition 37. *An AG-groupoid S is called a* ***Type*** 3 ***AG-groupoid*** *denoted by T^3-AG-groupoid if it is both T_l^3-AG-groupoid and T_r^3-AG-groupoid.*

Definition 38. *An AG-groupoid S is called a* ***Forward Type*** 4 ***AG-groupoid*** *denoted by T_f^4-AG-groupoid if for all $a, b, c, d \in S$,*

$$ab = cd \Longrightarrow ad = cb.$$

Definition 39. *An AG-groupoid S is called a* ***Backward Type*** 4 ***AG-groupoid*** *denoted by T_b^4-AG-groupoid if for all $a, b, c, d \in S$,*

$$ab = cd \Longrightarrow da = bc.$$

Definition 40. *An AG-groupoid S is called a* ***Type*** 4 ***AG-groupoid*** *denoted by T^4-AG-groupoid if it is both T_f^4-AG-groupoid and T_b^4-AG-groupoid.*

Corollary 15. *Let S be an AG-groupoid. Then S is a commutative semigroup if any of the following holds.*

(i) $ab = cd \Longrightarrow ad = bc$ *for all* $a, b, c, d \in S$*;*

(ii) $ab = cd \Longrightarrow da = cb$ *for all* $a, b, c, d \in S$*.*

Proof. Since $\forall a, b \in S$ the equation $ab = ab$ trivially holds. Now an application of either of (i) and (ii) proves commutativity in S and thus becomes commutative semigroup. □

There are some other cases but either they become semigroups or are equivalent to the cases that we have already discussed.

The following are examples or counterexamples of some contained of the above types.

Example 25. *A T^3-AG-groupoid of order* 3.

$\cdot$	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

Example 26. *A T^4-AG-groupoid of order* 4 *which is not T^2-AG-groupoid..*

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	4	3	2	1
4	3	4	1	2

Example 27. *A T^2-AG-groupoid of order* 4 *which is not T^4-AG-groupoid.*

$\cdot$	1	2	3	4
1	1	1	3	4
2	1	1	3	4
3	4	4	1	3
4	3	3	4	1

Example 28. *A T^1-AG-groupoid of order* 4 *which is neither T^2-AG-groupoid nor T^4-AG-groupoid.*

$\cdot$	1	2	3	4
1	1	1	3	3
2	1	1	3	3
3	3	3	1	1
4	3	3	1	2

Let us first put the previous known facts involving these types into the new formate. Thus [57, Theorem 2.7, Page 68] now becomes:

Theorem 16. *Every AG-monoid is T^1-AG-groupoid.*

Two generalizations of the above theorem were done in [91] which now read in the new scenario as

Theorem 17. *Let S be an AG^{**}-groupoid. Then S is a T^1-AG-groupoid if S has a cancellative element.*

More generally,

Theorem 18. *Let S be an AG-groupoid. Then S is a T^1-AG-groupoid if S has a left invertive left cancellative element.*

Regarding T^3-AG-groupoid the following fact is known.

Theorem 19. *Every AG-band is T^3-AG-groupoid.*

The following theorem generalizes it to AG-3-band.

Theorem 20. *[74] Every AG-3-band S is T^3-AG-groupoid.*

Proof. Let $a, b, c \in S$. To prove S to be T_l^3-AG-groupoid, suppose $ab = ac$. Then $ba = b^2b \cdot a = ab \cdot b^2 = ac \cdot b^2 = ab \cdot cb = ac \cdot cb = (aa^2)c \cdot cb = (ca^2)a \cdot cb = (ca^2)c \cdot ab = (ca^2)c \cdot ac = (ca^2)a \cdot c^2 = ac \cdot c^2 = ca$. Now to prove S to be T_r^3-AG-groupoid, suppose $ba = ca$. Then $ab = a^2a \cdot b = ba \cdot a^2 = ca \cdot a^2 = ac$. □

Theorem 21. *Let S be a T^4-AG-groupoid. Then*

(i) Square of every element of S is idempotent;

(ii) If S is an AG-monoid then S is a unitary AG-group.

(An AG-group is said to be a ***unitary*** *if square of every element is equal to left identity [88])*

Proof. (i) Obviously the identity $(aa)a = (aa)a$ holds trivially for every AG-groupoid. Since S is a T^4-AG-groupoid, it becomes $(aa)a = a(aa)$. Hence S is locally associative.

(ii) Let S has left identity e then for all a in S we trivially have $ae \cdot e = ae \cdot e$, which by the property of T^4-AG-groupoid implies that $ae \cdot ae = ee$, which by medial law implies $a^2e = ee$, which then by cancellativity of e implies that $a^2 = e$. Hence the result.

□

Theorem 22. *Every T^1-AG-groupoid is Bol*-AG-groupoid.*

Proof. Let S be a T^1-AG-groupoid and $a, b, c, d \in S$. Then

$$\begin{aligned}
(ab \cdot c)d &= dc \cdot ab, \text{ by left invertive law} \\
\Rightarrow d(ab \cdot c) &= ab \cdot dc, \text{ by definition of } T^1\text{-AG-groupoid} \\
\Rightarrow d(ab \cdot c) &= (dc \cdot b)a, \text{ by left invertive law} \\
\Rightarrow d(ab \cdot c) &= (bc \cdot d)a, \text{ by left invertive law} \\
\Rightarrow (ab \cdot c)d &= a(bc \cdot d), \text{ by definition of } T^1\text{-AG-groupoid}
\end{aligned}$$

Hence the result. □

Remark 6. The converse is not true as the Bol*-AG-groupoid given in Example 15 is not T^1*-AG-groupoid.*

From Table 4.1 this is obvious that right Type-3-AG-groupoid is not necessarily left Type-3-AG-groupoid but one might gets the impression that the converse may be true. The following example shows that the converse is also false.

Example 29. *A T_l^3-AG-groupoid of order 4 which is not T_r^3-AG-groupoid.*

·	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	2
4	1	1	3	2

Theorem 23. *The following facts always hold,*

(i) A T^2-AG-groupoid is T^1-AG-groupoid;

(ii) A T^4-AG-groupoid is T^1-AG-groupoid;

(iii) A T^1-AG-groupoid is,

(a) T_l^3-AG-groupoid;

(b) T_r^3-AG-groupoid;

(c) T^3-AG-groupoid.

Proof. (i) Let $a, b, c, d \in S$ and let $ab = cd$ which by definition of T^2-AG-groupoid implies that $ac = bd$. But then obviously $bd = ac$. Applying definition again we have $ba = dc$. Hence S is T^1-AG-groupoid.

(ii) Let $a, b, c, d \in S$ and let $ab = cd$ which by definition of T^4_f-AG-groupoid implies that $ad = cb$. Now applying definition of T^4_b-AG-groupoid we have $ba = dc$. Hence S is T^1-AG-groupoid.

(iii) (a) Apply definition of T^1-AG-groupoid with $a = c, (b)$ is similar to (a) and (c) follows from (a) and (b).

$\square$

Corollary 16. *The following facts always hold,*

(i) A T^2-AG-groupoid is,

- *(a) T^3_l-AG-groupoid;*
- *(b) T^3_r-AG-groupoid;*
- *(c) T^3-AG-groupoid,*

(ii) A T^4-AG-groupoid is,

- *(a) T^3_l-AG-groupoid;*
- *(b) T^3_r-AG-groupoid;*
- *(c) T^3-AG-groupoid.*

4.10 Zero-AG-groupoid, Zero-AG-group

As in case of semigroups, there exist a zero-semigroup and zero-group, we prove the existence of zero-AG-groupoid and zero-AG-group. and the most interesting zero-AG-groupoid semigroup. Their definitions and examples are given in the following.

Definition 41. *An AG-groupoid S is called a* ***zero-AG-groupoid*** *if there exists an element z in S such that S without z is an AG-groupoid and for all x in S we have that $xz = zx = z$.*

Definition 42. *An AG-groupoid S is called a* ***zero-AG-group*** *if there exists an element z in S such that S without z is an AG-group and for all x in S we have that $xz = zx = z$.*

Example 30. *A zero-AG-groupoid of order* 4.

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	2	2	2
3	1	2	2	2
4	1	3	3	3

Example 31. *A zero-AG-group of order* 4*.*

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	2	3	4
3	1	4	2	3
4	1	3	4	2

Theorem 24. *Let G be an AG-group. Then $Ga = aG = G\,\forall a \in G$.*

Proof. (i) $Ga \subseteq GG \subseteq G$. Conversely, let $g \in G$ and let e be the left identity of G then

$$g = eg = aa^{-1} \cdot g = ga^{-1} \cdot a \in Ga.$$

Therefore, $G \subseteq Ga$. Hence $Ga = G$.

(ii) $aG \subseteq GG \subseteq G$. Conversely, let $g \in G$ and consider

$$g = ee \cdot g = ge \cdot e = ge \cdot aa^{-1} = a(ge \cdot a^{-1}) \in aG.$$

Therefore $G \subseteq aG$. Hence $aG = G$.

□

Corollary 17. *[51] Let G be an AG-group having left identity e. Then $G = eG = Ge$.*

Corollary 18. *Let G be an AG-group. Then for all $a, b \in G$, there exist $x, y \in G$ such that*

$$ax = b, ya = b$$

Proposition 9. *If an AG-groupoid S with zero is a zero-AG-groupoid-AG-group then $\forall a \in S\backslash \{0\}, Sa = aS = S$.*

Proof. $S = G \cup \{0\}$ is a zero-AG-groupoid-AG-group. Here $G = S \setminus \{0\}$. Let $a \in S \setminus \{0\} \implies a \in G = S \setminus \{0\}$. As G is an AG-group, so by Theorem 24 $aG = Ga = G$. Now

$$\begin{aligned} aS &= aG \cup \{0\} = G \cup \{0\} = S, \text{ and} \\ Sa &= Ga \cup \{0\} = G \cup \{0\} = S. \end{aligned}$$

Hence $Sa = aS = S$. □

Chapter 5

On The Cancellativity of AG-groupoids

5.1 Introduction

In this chapter we study some structural properties of AG-groupoids with respect to the cancellativity. We prove that cancellative and non-cancellative elements of an AG-groupoid S partition S and the two classes are AG-subgroupoids of S if S has left identity e. Cancellativity and invertibility coincide in a finite AG-groupoid S with left identity e. For a finite AG-groupoid S with left identity e having at least one non-cancellative element, the set of non-cancellative elements form a maximal ideal. We also prove that for an AG-groupoid S, the conditions (i) S is left cancellative (ii) S is right cancellative (iii) S is cancellative, are equivalent.

5.2 Cancellativity of AG-groupoids

In [57, Theorem 2.6], this has been proved that every left cancellative AG-groupoid S is cancellative while without having a counterexample this has been believed in the literature that the converse is not true in general but true only if S has left identity. We prove that this is incorrect. The converse is also true in general and does not require the existence of left identity. That is, every right cancellative AG-groupoid S is also left cancellative. So we begin by the following theorem.

Theorem 25. *The following conditions are equivalent for an AG-groupoid S.*

(i) S is left cancellative;

(ii) S is right cancellative;

(iii) S is cancellative.

Proof. (1) $\Rightarrow$ (2) Let S be left cancellative. Let a be an arbitrary element of S and let $xa = ya$ for all $x, y \in S$. Suppose k is any element of S. Then $(ka)x = (xa)k = (ya)k = (ka)y$ which by left cancellativity implies that $x = y$. Thus S is right cancellative (2) $\Rightarrow$ (3) Let S be right cancellative and let $ax = ay$ for all $x, y \in S$. Suppose k is any element of S. Then $((xk)a)a = (aa)(xk) = (ax)(ak) = (ay)(ak) = (aa)(yk) = ((yk)a)a$ which by repeated use of right cancellativity implies that $x = y$. Thus S is left cancellative (3) $\Rightarrow$ (1) Obvious. $\square$

Corollary 19. *The following conditions are equivalent for an AG-groupoid S.*

(i) S is left quasigroup;

(ii) S is right quasigroup;

(iii) S is quasigroup.

The previous discussion was about the whole left cancellativity or right cancellativity of the AG-groupoid. In what follows we focus on the cancellativity of an individual element of an AG-groupoid when the whole AG-groupoid is not necessarily left cancellative or right cancellative. But first observe that an AG-groupoid can have all, some or none of its elements as cancellative. For example all the elements of the following AG-groupoid are cancellative.

Example 32. *A cancellative AG-groupoid with left identity* 0*:*

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

The following AG-groupoid has two cancellative elements which are the left identity 0 and 3.

Example 33. *An AG-groupoid with left identity* 0*:*

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	4	2	2	4	4
2	2	2	2	2	2
3	3	1	2	0	4
4	1	1	2	1	2

The following AG-groupoid has four cancellative elements and one non-cancellative.

Example 34. *An AG-groupoid with* $\{0, 1, 2, 3\}$ *as cancellative elements and only* $\{4\}$ *as non-cancellative.*

$\cdot$	0	1	2	3	4
0	0	2	3	1	4
1	3	1	0	2	4
2	1	3	2	0	4
3	2	0	1	3	4
4	4	4	4	4	4

The following AG-groupoid has no cancellative element.

Example 35. *An AG-groupoid without left identity and without any cancellative element:*

$\cdot$	0	1	2	3	4
0	2	2	2	2	2
1	2	0	2	2	4
2	2	2	2	2	2
3	0	0	2	4	4
4	2	2	2	2	2

Theorem 26. *Every right cancellative element of an AG-groupoid* S *is (left) cancellative.*

Proof. Let S be an AG-groupoid. Let a be an arbitrary right cancellative element of S. Suppose $ax = ay$ for all $x, y \in S$. Then $((xa)a)a = (aa)(xa) = (ax)(aa) = (ay)(aa) = (aa)(ya) = ((ya)a)a$ which by repeated use of right cancellativity implies $x = y$. Thus a is left cancellative. Hence every right cancellative element of S is left cancellative. $\square$

Next we need the following theorem from [57].

Theorem 27. *In an AG-groupoid S with left identity e, $ab = cd \Rightarrow ba = dc$ for all $a, b, c, d \in S$.*

Theorem 28. *Let S be an AG-groupoid with left identity e. Then every left cancellative element is also right cancellative.*

Proof. Let a be an arbitrary left cancellative element of S. Suppose $xa = ya$ for all $x, y \in S$. Then by Theorem 27, we have $ax = ay$. Which by left cancellativity implies $x = y$. Thus a is right cancellative. Hence every left cancellative element of S is right cancellative. □

Remark 7. From Theorem 27, this is clear that if the AG-groupoid S has left identity e then e will always be cancellative because e by its definition is left cancellative.

Next we prove that the set of cancellative elements and the set of non-cancellative elements of an AG-groupoid S form a partition of S.

Theorem 29. *Let S be an AG-groupoid and let $a, b, c \in S$. Define on S the relation $\sim$ as, $a \sim b \Leftrightarrow a$ and b are both cancellative or non-cancellative. Then $\sim$ is an equivalence relation.*

Proof. Since a, a are both cancellative or non-cancellative. Therefore $a \sim a$. Thus $\sim$ is reflexive. Suppose now $a \sim b$ then a and b are both cancellative or non-cancellative. Which implies that b and a are both cancellative or non-cancellative. Which implies that $b \sim a$. Thus $\sim$ is symmetric. Next suppose that $a \sim b$ and $b \sim c$ then a and b are both cancellative or non-cancellative and b and c are both cancellative or non-cancellative. Which implies that a and c are both cancellative or non-cancellative and so $a \sim c$. Thus $\sim$ is transitive. Hence $\sim$ is an equivalence relation. □

Corollary 20. *Cancellative and non-cancellative elements of an AG-groupoid S partition S.*

Next we prove that the two classes will be AG-subgroupoids of S, if S has left identity.

Lemma 8. *The set of cancellative elements of an AG-groupoid S with left identity e is an AG-subgroupoid of S.*

Proof. Let $H = \{a \in S\colon\, a \text{ is cancellative}\}$. Clearly H is non-empty as $e \in H$ by Remark 7. Now let $a_1, a_2 \in H$ and let $a = a_1a_2$. We show that a is cancellative. Suppose $ax = ay$ for all $x, y \in S$. Then $(xa_2)a_1 = (a_1a_2)x = ax = ay = (a_1a_2)y = (ya_2)a_1$ which by cancellativity of a_1 and a_2 implies $x = y$. Thus a is left cancellative and hence cancellative by Theorem 28. This implies $a \in H$. Hence H is an AG-subgroupoid of S. □

In Example 32, $H = S$, in Example 33, $H = \{0, 3\}$, in Example 34, $H = \{0, 1, 2, 3\}$ that can be easily seen as an AG-subgroupoid of S.

Remark 8. *Computer search shows the smallest non-associative AG-groupoid to be of order* 3*. But how many non-isomorphic AG-groupoids of order 3 or higher order exist, no one has counted yet, neither computationally nor algebraically. So we suggest this as a future problem.*

Example 36. *A non-associative AG-groupoid of order* 3 :

$\cdot$	0	1	2
0	2	2	2
1	0	2	2
2	2	2	2

Lemma 9. *Every cancellative element of an AG-subgroupoid S with left identity e is the product of two cancellative elements of S.*

Proof. By Remark 7, e is cancellative and $e = ee$. Let a be an arbitrary non-trivial cancellative element of S. Let $a = a_1a_2$. We show that a_1, a_2 are both cancellative. Suppose $xa_2 = ya_2$ for all $x, y \in S$. Then $ax = (a_1a_2)x = (xa_2)a_1 = (ya_2)a_1 = (a_1a_2)y = ay$ which implies that $x = y$ since a is cancellative. Thus a_2 is right cancellative and hence cancellative by Theorem 26. Now suppose $a_1x = a_1y$. Then

$$\begin{aligned} a(xa_2) &= (a_1a_2)(xa_2) \\ &= (a_1x)(a_2a_2) = (a_1y)(a_2a_2) \\ &= (a_1a_2)(ya_2) = a(ya_2), \end{aligned}$$

which by cancellativity of a and a_2 implies that $x = y$. Thus a_1 is left cancellative and hence cancellative by Theorem 28. □

Note that Lemma 9 does not hold for a non-cancellative element. A non-cancellative element can be expressed as the product of a cancellative element and a non-cancellative element or as the product of two non-cancellative elements as in Example 33, $2 = 0{\cdot}2$ or $2 = 2{\cdot}2$, where 0 is cancellative and 2 is non-cancellative elements of S.

Corollary 21. *In an AG-subgroupoid S with left identity e the product of two non-cancellative elements or one cancellative and one non-cancellative is always non-cancellative, that is, if a or b is non-cancellative then ab is non-cancellative.*

Lemma 10. *The set of all non-cancellative elements of an AG-groupoid S with left identity e is either empty or an AG-subgroupoid of S.*

Proof. Let $K = \{a \in S\colon\ a \text{ is non-cancellative}\}$. Clearly K is empty if S is cancellative. Suppose S is not cancellative. Then $e \notin K$ since e is always cancellative. Now let $a_1, a_2 \in K$ and let $a = a_1a_2$. We show that a is non-cancellative,that is, $a \in K$. Suppose $a \notin K$ then a is cancellative and consequently a_1, a_2 are cancellative by Lemma 9 and thus $a_1, a_2 \notin K$, which is a contradiction. Therefore $a \in K$. Thus K is an AG-subgroupoid of S. □

In Example 32, $K = \phi$, in Example 33, $K = \{1, 2, 4\}$, in Example 34, $K = \{4\}$ and in Example 35, $K = S$ that can easily be seen as an AG-subgroupoid of S in the non-empty case.

Thus from Corollary 20, Lemma 8 and Lemma 10, it follows that:

Theorem 30. *Cancellative and non-cancellative elements of an AG-groupoid S with left identity e partition S into two AG-subgroupoids of S.*

As an application of our theory to the ideal theory of AG-groupoids, we have the following:

Corollary 22. *A proper (left,right) ideal I of an AG-groupoid S with left identity e cannot be a subset of H.*

Proof. Since the product of the non-cancellative elements of S with the elements of H cannot be contained in H by Lemma 9. So a proper (left,right) ideal of S cannot be a subset of H. □

Next we show that none of the elements of the proper (left,right) ideal can lie in H at least in finite case.

Corollary 23. *A proper (left,right) ideal of a finite AG-groupoid S with left identity e is a subset of K.*

Proof. Let $S = \{s_1, s_2, \dots s_n\}$ and let I be a proper left ideal of S. Let $a \in I$ be such that $a \in H$. Then since a is cancellative therefore $s_1a, s_2a, \dots s_na \in I$ are all distinct. This implies that I and S have the same number of elements which is a contradiction. So $a \notin H$. Therefore $I \subseteq K$. Other cases are similar. □

Corollary 24. *For an AG-groupoid S with left identity e having at least one non-cancellative element, K is always a maximal ideal.*

Proof. It follows from Corollary 21 and 23. □

Next we prove that cancellativity and invertibility coincide in a finite AG-groupoid S with left identity e.

Lemma 11. *Every invertible element of an AG-groupoid with left identity e is cancellative.*

Proof. Suppose a is an invertible element then there exists $a^{-1} \in S$ such that $aa^{-1} = a^{-1}a = e$. Suppose $xa = ya$ then $x = ex = (a^{-1}a)x = (xa)a^{-1} = (ya)a^{-1} = (a^{-1}a)y = ey = y$. Thus a is right cancellative and hence cancellative. □

Corollary 25. *An AG-group G is cancellative [51].*

Lemma 12. *Every cancellative element of a finite AG-groupoid S with left identity e is invertible.*

Proof. Let $S = \{s_1, s_2, \dots s_n\}$ and let a be an arbitrary cancellative element of S. Then clearly $as_1, as_2, \dots as_n$ are all distinct. Since S is finite therefore there must exists a positive integer $i \in \{1, 2, \dots n\}$ such that $as_i = e$ but then $s_ia = e$ follows by Theorem 27. Hence a is invertible. □

Now the following theorem follows.

Theorem 31. *Let S be a finite AG-groupoid with left identity e then a is invertible $\Leftrightarrow$ a is cancellative.*

In Example 32, all elements are cancellative as well as invertible, in Example 33, 0 and 3 are cancellative as well as invertible elements, in Example 34, the elements $0, 1, 2, 3$ are both cancellative and invertible and in Example 35, there is no cancellative and no invertible element.

Remark 9. If the AG-groupoid S does not have left identity, then Theorem 31 does not hold as the following example shows:

Example 37. *A cancellative AG-groupoid without left identity:*

$\cdot$	0	1	2	3	4
0	2	1	0	4	3
1	0	4	3	2	1
2	3	2	1	0	4
3	1	0	4	3	2
4	4	3	2	1	0

Corollary 26. *A finite cancellative AG-groupoid with left identity e is an AG-group.*

The AG-groupoid in Example 32 is an AG-group.

Theorem 32. *The direct product $S_1 \times S_2$ of two cancellative AG-groupoids S_1 and S_2 is cancellative.*

Proof. Suppose the AG-groupoids S_1 and S_2 are cancellative. Then $S_1 \times S_2$ is also an AG-groupoid by [55, Page 462]. Now let $a, x_1, y_1 \in S_1$ and $b, x_2, y_2 \in S_2$ then consider $(a, b)(x_1, y_1) = (a, b)(x_2, y_2)$, which implies $(ax_1, by_1) = (ax_2, by_2)$, from this we get that $ax_1 = ax_2, by_1 = by_2$, which by cancellativity of S_1 and S_2 implies that $x_1 = x_2$ and $y_1 = y_2$. Thus $S_1 \times S_2$ is cancellative. □

Finally let us apply the concept of cancellativity in the proof of the Theorem 27 which has been proved in [57] without this. The proof becomes a bit easier.

Proof. $(ba)e = (ea)b = ab = cd = (ec)d = (dc)e \Rightarrow ba = dc$, since e is cancellative. □

Conclusion: In this section we have proved that a right cancellative element of an AG-groupoid S (not necessarily having left identity) is left cancellative. This has also been shown that a left cancellative element of an AG-groupoid S is right cancellative if either S is cancellative or if S has left identity. But if S is not cancellative or S does not have a left identity then we are unable to prove that a left cancellative element is also right cancellative. Thus we had to take an AG-groupoid S with left identity e. This requires further investigation to remove this condition. If this could be proved then most of our results will hold in general. So we suggest it as an open problem:

Problem 1. *Prove or disprove that every left cancellative element is also right cancellative of an AG-groupoid S without left identity.*

5.3 Partial Solution to The Open Problem

In this section we partially resolve positively the open problem that was posed in the previous section. We also introduce the notion of nucleus from quasi-groups to the AG-groupoids and derive a number of useful consequences of this for AG**-groupoids. Moreover we generalize a couple of the most well-known results. In the end we prove the in-existence of AG-3-bands (and AG-bands) for the non-associative AG**-groupoids and AG*-groupoids and also the equivalence of commutativity and associativity for AG-3-bands.

Recall from Section 1 that every right cancellative element of an AG-groupoid S is left cancellative. It was then posed as an open problem that whether the converse also holds or not. To answer this problem in negative, we need a counterexample, that is, all we need a Cayley table of an AG-groupoid which is not AG-monoid whose nth row is duplicate free but nth column is not.

Order	3	4	5	6
Total	20	331	31913	40104513
Associative and commutative	12	58	325	2143
Associative and non-commutative	0	4	121	5367
Non-associative	8	269	31467	40097003

Also we are preparing a GAP package "AGGROUPOIDS" for AG-groupoids which will be published shortly. The package AGGROUPOIDS has many functions for working with AG-groupoids. Thus using AGGROUPOIDS we have checked all of our data of Non-associative AG-groupoids presented in Table 3.2 and thus concluded that there is no counterexample up to order 6.

This is also worth mentioning that there exist non-AG-groupoid semigroups even of small order 3 which has the required property. Example of one such semigroup of order 3 is given in the following table.

$\cdot$	1	2	3
1	1	1	1
2	1	1	1
3	1	2	3

We partially answer this problem in positive here. We prove that if a is a left cancellative element of an AG-groupoid S then a is also right cancellative at least in the cases (i) If a^2 is left cancellative (ii) If a is idempotent (iii) If there exists a left nuclear left cancellative element in S (Theorem 35) (iv) If a is the unique left cancellative element in S (Corollary 30) (v) If S is an AG-band (Corollary 27) (vi) If S is AG*-groupoid (Theorem 37) (vii) If S is AG*-groupoid (Theorem 39). Then using the cancellativity of AG*-groupoid and introducing the concept of nucleus from quasigroups and loops into AG-groupoids we prove that (i) Every AG**-groupoid S is left nuclear square (Lemma 13) (ii) Left nucleus is a semigroup for AG**-groupoid S (Theorem 40) (iii) If middle nucleus or right nucleus of AG**-groupoid S contains a cancellative element then S becomes commutative semigroup (Theorem 41 and Theorem 42) and consequently we have that the middle and right nuclei of a cancellative non-associative AG**-groupoid are always empty (Corollary 31 and Corollary 32). Further from the aspect of the cancellativity of AG-groupoids we have proved a number of results such as (i) Every left cancellative element of an AG-groupoid S is the product of a left cancellative element and a right cancellative element of S in this order and the product of two right cancellative elements is left cancellative (Theorem 36 and Lemma 14). A cancellative idempotent element of an AG*-groupoid S is left identity (Theorem 44). If k is a cancellative and locally associative element of an AG**-groupoid S then k is left nuclear (Theorem 46). The centre of a cancellative and non-associative AG**-groupoid is empty (Corollary 37). Moreover we generalize one of the most well-known result Mushtaq and Yusuf [57, Theorem 2.7, Page 68] for AG-monoids to AG**-groupoid and as well as to AG-groupoids. The result states "Let S be an AG-groupoid with left identity e. Then $ab = cd \Rightarrow ba = dc$ for every $a, b, c, d \in S$". Our generalizations are: (i) Let S be an AG**-groupoid. Let $a, b, c, d \in S$. Then $ab = cd \Rightarrow ba = dc$ if there exists a right cancellative in S and (ii) Let S be an AG-groupoid. Let $a, b, c, d \in S$. Then $ab = cd \Rightarrow ba = dc$ if there exists a left nuclear left cancellative element in S (Theorem 38 and Theorem 34). Some other generalizations can be found in (Theorem 43 and Corollary 37). Examples from [15] are provided whenever needed which we have checked by AGGROUPOIDS.

Definition 43. *Let S be an AG-groupoid. Then the set*

$$N_\lambda = \{x \in S; x(yz) = (xy)z \textit{ for every } y, z \in S\}$$

is called the left nucleus. Similarly, the set

$$N_\mu = \{x \in S; y(xz) = (yx)z \textit{ for every } y, z \in S\}$$

is called the middle nucleus and the set

$$N_\rho = \{x \in L; y(zx) = (yz)x \text{ for every } y, z \in S\}$$

is called the right nucleus of S.

Definition 44. *Let S be an AG-groupoid. Then $a \in S$ is called left nuclear if $a \in N_\lambda$, middle nuclear if $a \in N_\mu$, right nuclear if $a \in N_\rho$. Similarly $a \in S$ is called left nuclear square if $a^2 \in N_\lambda$, middle nuclear square if $a^2 \in N_\mu$, right square nuclear if $a^2 \in N_\rho$. S is called left nuclear square if $a^2 \in N_\lambda$, middle nuclear square if $a^2 \in N_\mu$, right nuclear square if $a^2 \in N_\rho \, \forall a \in S$.*

Before we embark on the open problem we generalize the following theorem from [57, Theorem 2.7, Page 68] which was claimed only for AG-monoids.

Theorem 33. *Let S be an AG-groupoid with left identity e. Then $ab = cd \Rightarrow ba = dc$ for every $a, b, c, d \in S$.*

In the following theorem, We generalize it to any AG-groupoid.

Theorem 34. *Let S be an AG-groupoid. Let $a, b, c, d \in S$. Then $ab = cd \Rightarrow ba = dc$ if there exists a left nuclear left cancellative element in S.*

Proof. Let k be a left nuclear and left cancellative element in S. Let $ab = cd$. consider $k(ba) = (kb)a = (ab)k = (cd)k = (kd)c = k(dc)$ which by left cancellation of k implies that $ba = dc$. □

Remark 10. If S has left identity e then since e is always left nuclear and left cancellative so taking $k = e$, Theorem 34 becomes Theorem 33.

The following theorem claims that the problem is resolved if at least one of the condition is met.

Theorem 35. *Let S be an AG-groupoid. Let a be a left cancellative element. Then a is also right cancellative if any of the following holds.*

(i) a^2 is left cancellative

(ii) a is idempotent

(iii) There exists a left nuclear left cancellative element in S.

Proof. (i) Let $xa = ya$ for all $x, y \in S$. Then $a^2x = (xa)a = (ya)a = a^2y \Rightarrow x = y$ by left cancellativity of a^2. Hence a is also right cancellative.

(ii) Let $xa = ya$ for all $x, y \in S$. Then $ax = a^2x = (xa)a = (ya)a = a^2y = ay$. This implies that $x = y$ by left cancellativity of a. Hence a is also right cancellative.

(iii) By using Theorem 34 and left cancellativity, we have $x = y$. Hence a is also right cancellative.

□

There may or may not be other situations in which the problem holds in general. Now we look at some special subclasses of AG-groupoids for which the problem holds. From Theorem 35 (ii), the problem solves for AG-bands as the following corollary claims:

Corollary 27. *In an AG-band every left cancellative element is also right cancellative and hence cancellative.*

From the following theorem we will derive two more situations in which the problem holds.

Theorem 36. *Every left cancellative element of an AG-groupoid S is the product of a left cancellative element and a right cancellative element of S in this order.*

Proof. Let a be an arbitrary left cancellative element of S. Let $a = a_1a_2$. We show that a_1 is left cancellative and a_2 is right cancellative. Suppose $xa_2 = ya_2$ for all $x, y \in S$. Then $ax = (a_1a_2)x = (xa_2)a_1 = (ya_2)a_1 = (a_1a_2)y = ay$ which implies $x = y$ by the left cancellativity of a. Thus a is right cancellative. Now suppose $a_1x = a_1y$ for all $x, y \in S$. Then $a(xa_2) = (a_1a_2)(xa_2) = (a_1x)(a_2a_2) = (a_1y)(a_2a_2) = (a_1a_2)(ya_2) = a(ya_2)$ which by left cancellativity of a and right cancellativity of a_2 implies $x = y$ thus a_1 is left cancellative. □

Since a right cancellative element is left cancellative. Thus:

Corollary 28. *Every left cancellative element of an AG-groupoid S is the product of two left cancellative elements of S.*

Remark 11. From Corollary 27 the converse, that is, the product of two left cancellative elements of an AG-groupoid S is left cancellative does not follow.

In the light of Corollary 27 and Theorem 35 Part (i), the open problem now reduces to :

Problem 2. *Prove or disprove that the product of two left cancellative elements of S is left cancellative.*

The following is another useful conclusion from Theorem 36.

Corollary 29. *If an AG-groupoid S has a unique left cancellative element then it must be idempotent.*

Proof. Let a be an arbitrary left cancellative element of S. Then by Corollary 27, $a = a_1a_2$ where a_1, a_2 are left cancellative and by uniqueness $a = a_1 = a_2$. Therefore $a = a^2$. Hence a is idempotent. □

From Corollary 28 and Theorem 35 Part(ii) the open problem resolves partially as the following corollary.

Corollary 30. *If an AG-groupoid S has a unique left cancellative element then it must be cancellative.*

Now we prove the problem holds for AG*-groupoids.

Theorem 37. *Let S be an AG*-groupoid. Let a be a left cancellative element. Then a is also right cancellative.*

Proof. Let a be a left cancellative element of S.

$$\begin{aligned} \text{Let } xa &= ya, \text{ for all } x, y \in S. \\ \text{Then } a^2x &= (xa)a = (ya)a = a^2y \\ &\Rightarrow a(ax) = a(ay) \text{ by definition of AG}^*\text{-groupoid} \\ &\Rightarrow x = y, \text{ by using twice the left cancellativity of } a. \end{aligned}$$

Hence a is also right cancellative. □

In what follows we resolve completely the open problem for AG**-groupoids which is a huge subclass of AG-groupoids. In fact it contains all AG-monoids. In this case every left cancellative element becomes right cancellative. But before proving that, we will prove the version of Theorem 34 for AG**-groupoid as a special case.

Lemma 13. *Every AG**-groupoid S is left nuclear square.*

Proof. Suppose a is arbitrary element of S. Using definition of AG**-groupoid, left invertive law and medial law, we have for all $x, y \in S$

$a^2(xy) = x(a^2y) = x[(ya)a)] = (ya)(xa) = (yx)a^2 = (a^2x)y \Rightarrow a^2 \in N_\lambda$.

Hence S is a left nuclear square. □

Lemma 14. *Let S be an AG-groupoid. Then the product of two right cancellative elements is left cancellative.*

Proof. Let $a_1, a_2 \in S$ are right cancellative elements and let $a = a_1a_2$. We show that a is left cancellative. Suppose $ax = ay$ then $(xa_2)a_1 = (a_1a_2)x = ax = ay = (a_1a_2)y = (ya_2)a_1$ which by right cancellativity of a_1 and a_2 implies $x = y$. Thus a is left cancellative. □

Remark 12. Lemma 14 does not conflict with Corollary 27 because a right cancellative element is left cancellative [88].

Theorem 38. *Let S be an AG**-groupoid. Let $a, b, c, d \in S$. Then $ab = cd \Rightarrow ba = dc$ if there exists a right cancellative in S.*

Proof. Let k be a right cancellative element in S. Then k^2 is left cancellative by Lemma 14 and $k^2 \in N_\lambda$ by Lemma 13 and thus by Theorem 34, $ab = cd \Rightarrow ba = dc$. □

Now we are ready to attack on the open problem for AG**-groupoids.

Theorem 39. *Every left cancellative element of AG**-groupoid S is also right cancellative.*

Proof. Let a be an arbitrary left cancellative element of S. Suppose $xa = ya$ for all $x, y \in S$. Since a is a left cancellative so there exist a left cancellative element l and a right cancellative element r such that $a = lr$ by Theorem 36. Thus by Theorem 38, we have $ax = ay$ which by left cancellativity of a implies $x = y$. Hence a is right cancellative. Thus for AG**-groupoid left cancellativity and right cancellativity coincide. □

In the following we derive some consequences for AG**-groupoids which we predict as much useful for further work on AG**-groupoids .

Theorem 40. *N_λ is semigroup for AG**-groupoid S.*

Proof. Clearly N_λ is non-empty as square of every element belongs to N_λ by Lemma 13. Let $a, b \in N_\lambda\, \forall y, z \in S$. Now

$$\begin{aligned}
(ab)(yz) &= a[b(yz)] \text{ since } a \in N_\lambda \\
&= a[(by)z] \text{ since } b \in N_\lambda \\
&= [a(by)]z \text{ since } a \in N_\lambda \\
&= [(ab)y]z \text{ since } a \in N_\lambda \\
&\Longrightarrow ab \in N_\lambda.
\end{aligned}$$

Thus N_λ is an AG**-subgroupoid of S. Associativity follows by definition of N_λ. Hence N_λ is a semigroup. □

Theorem 41. *If N_ρ of AG*-groupoid S contains a cancellative element. Then S is commutative semigroup.*

Proof. Let $a \in N_\rho$ such that a is cancellative then

$$\begin{aligned}
(yz)a &= y(za) \text{ for all } y,z \in S \\
\Rightarrow (yz)a &= z(ya) \text{ by definition of AG}^*\text{-groupoid} \\
\Rightarrow (yz)a &= (zy)a \text{ since } a \in N_\rho \\
\Rightarrow yz &= zy, \text{ by cancellativity of } a \\
&\Rightarrow S \text{ is commutative. Therefore } S \text{ is commutative semigroup.}
\end{aligned}$$

□

Corollary 31. *For a cancellative non-associative AG*-groupoid $N_\rho = \phi$.*

Theorem 42. *If N_μ of AG*-groupoid S contains a cancellative element. Then S is commutative semigroup.*

Proof. Let $a \in N_\mu$ such that a is cancellative then

$$\begin{aligned}
(ya)z &= y(az) \text{ for all } y,z \in S \\
(ya)z &= a(yz) \text{ by definition of AG}^*\text{-groupoid} \\
z(ya) &= (yz)a \text{ by Theorem 37} \\
y(za) &= (yz)a \text{ by definition of AG}^*\text{-groupoid} \\
&\Longrightarrow a \in N_\rho
\end{aligned}$$

which by Theorem 41 implies that S is commutative semigroup. □

Corollary 32. *For a cancellative non-associative AG**-groupoid $N_\mu = \phi$.*

It can easily be verified that in an AG**-groupoid S, $(ab)(cd) = (dc)(ba)$ and $(ab)^2 = (ba)^2$ for all $a, b, c, d \in S$.

Lemma 15. *If an AG**-groupoid S is also an AG-band then it becomes commutative semigroup.*

Proof. Let $a, b \in S$. Then $(ab) = (ab)^2 = (ba)^2 = (ba)$. Hence S is commutative semigroup. □

The following is a generalization of [78, Theorem 6, Page 1665].

Theorem 43. *A cancellative locally associative AG^{**}-groupoid S is commutative semigroup.*

Proof. Let S be a cancellative locally associative AG**-groupoid. Then for all $a, b \in S$ by using medial law and local associativity of S, we have

$$\begin{aligned}(ab)(ab)^2 &= (ab)(a^2b^2) = (aa^2)(bb^2) = (a^2a)(b^2b) = (a^2b^2)(ab) \\ &= (ba)(b^2a^2) = (ba)(ba)^2 = (ba)\end{aligned}$$

Since $(ab)^2 = (ba)^2$ so by cancellativity $ab = ba$. Thus S is commutative. and hence commutative semigroup. □

Theorem 44. *A cancellative idempotent element of an AG^{**}-groupoid S is left identity.*

Proof. Let x be an arbitrary element of S. By idempotency of a and Lemma 13, we have $a(ax) = a^2(ax) = (a^2a)x = ax$. Which by cancellativity of a implies that $ax = x$ for all $x \in S$. Which then implies that a is left identity of S. □

Corollary 33. *A cancellative AG^{**}-groupoid can have at most one idempotent.*

Proof. Because in AG-groupoid left identity is unique . □

Corollary 34. *A cancellative AG-monoid has exactly one idempotent which is the left identity.*

From this we recover [78, Theorem 7, Page 1666].

Corollary 35. *An AG-group has exactly one idempotent which is the left identity.*

Theorem 45. *Let S be an AG^{*}-groupoid. Let k be a cancellative element of S such that $ka = ak, kb = bk$ where $a, b \in S$. Then $ab = ba$.*

Proof. $k(ab) = a(kb) = a(bk) = b(ak) = b(ka) = k(ba)$. Which by cancellativity of k implies that $ab = ba$. □

Corollary 36. *Let S be an AG^{**}-groupoid. If the centre of S contains a cancellative element. Then S is commutative semigroup.*

Corollary 37. *The centre of a cancellative and non-associative AG^{**}-groupoid is empty.*

The following problem applies Theorem 45.

Problem 3. *Prove without using medial and paramedial laws that in AG-monoid S all squares commute with each other.*

Solution 1. *Since the left identity is always cancellative and commutes with every square. So by Theorem 45 all squares commute with each other.*

Theorem 46. *Let S be an AG^{**}-groupoid and k be a cancellative and locally associative element of S. Then k is left nuclear.*

Proof. We have for all $a, b \in S$

$$\begin{aligned}(ka.b)k^2 &= (ba.k)k^2 = k^2k \cdot ba = ab \cdot kk^2 = ab \cdot k^2k = k^2(ab \cdot k) = k^2(kb \cdot a) = (a \cdot kb)k^2 \\ &= (k \cdot ab)k^2.\end{aligned}$$

Since k is cancellative so is k^2 by [88] and therefore by right cancellation, we have $ka.b = k \cdot ab$ which proves that k is left nuclear. □

Lemma 16. *An AG-band is AG-3-band.*

Proof. Obvious. □

The converse of Lemma 16 is not true as the following example shows.

Example 38. *An AG-3-band of order 6 which is not an AG-band.*

$\cdot$	1	2	3	4	5	6
1	1	1	1	1	1	6
2	1	2	4	5	3	6
3	1	5	3	2	4	6
4	1	3	5	4	2	6
5	1	4	2	3	5	6
6	6	6	6	6	6	1

Remark 13. The above AG-groupoid is the smallest having this property.

This is easy to prove that every commutative AG-groupoid is also associative but the converse is not true (the counterexample is following) but for AG-3-band the converse is also true (Theorem 47).

Example 39. *An associative and non-commutative AG-groupoid of order* 4.

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	1	1	2	1

In the following theorem we prove that commutativity and associativity imply each other in AG-3-band.

Theorem 47. *For an AG-3-band S the following are equivalent.*

(i) S is commutative;

(ii) S is associative.

Proof. $(i) \Longrightarrow (ii)$. This is always true for an AG-groupoid. $(ii) \Longrightarrow (i)$

$$\begin{aligned}
ab &= [(ab)\,(ab)]\,(ab) \text{ by definition of AG-3-band} \\
&= [(ab)\,a]\,[b\,(ab)] \text{ by associativity} \\
&= [(ab)\,b]\,[a\,(ab)] \text{ by medial law} \\
&= [(bb)\,a]\,[b(aa)] \text{ by left invertive law and associativity} \\
&= [(bb)b][a(aa)] \text{ by medial law} \\
&= ba \text{ by definition of AG-3-band}
\end{aligned}$$

$\square$

Chapter 6

Enumerating AG-groups

We present the first enumeration result for AG-groups up to order 11 and give a lower bound for order 12. The counting is performed with the finite domain enumerator FINDER using bespoke symmetry breaking techniques. We have a few observations obtained from our results, some of which inspired us to examine and discuss Smarandache AG-group structures.

6.1 Introduction

In the study of small algebraic structures more general than groups, many interesting questions, such as open existence, classification, and counting problems, have been solved by software tools that enable efficient enumeration of structures. Typically this task involves identifying and exploiting symmetries in the problem at hand. Loops with inverse property (IP-loops) up to order 13 have been counted with model generators using hand crafted symmetry breaking constraints and *post-hoc* processing [102]. Monoids up to order 10 and semigroups up to order 9 have been enumerated [13] with off-the-shelf constraint satisfaction software by employing lexicographic symmetry breaking constraints computed using a GAP implementation of the methods described in [41]. A similar approach was more recently used for counting AG-groupoids — groupoids that are left invertive, in the sense $(ab)c = (cb)a$ — up to order 6 [15]. Finally, also related is the enumeration of quasigroups and loops up to size 11 using a mixture of combinatorial considerations and bespoke exhaustive generation software [44]. In Sec. 6.2 we first count the number of non-isomorphic AG-groups of order up to 11 and give a lower bound for order 12. We then discuss some of the observations we have made when examining the results (Sec. 6.3) and in particular develop and study a new type of AG-group structure, Smarandache AG-groups (Sec. 6.4).

6.2 Counting AG-groups up to Isomorphism

We counted AG-groups by exhaustive enumeration using the FINDER system. Our starting point is the approach developed for counting IP-loops up to isomorphism in [1, 78]. Here, as in that work, FINDER generates a set of candidate tables which contains one table for each minimal element given by a lex(icographic) order over each isomorphism class. A post-processing step — post-hoc processing — is used to reject tables that are not minimal in their isomorphism class.[1] In order to prevent FINDER from generating an impractical number of candidate tables, further symmetry breaking constraints are posed. Moreover, the validity of post-hoc processing is dependent on these constraints being satisfied. In our work we have had to modify those constraints. A summary of the constraints from [102] in their reduced form for AG-groups is given in the following definition.

Definition 6.2.1. *(Symmetry Breaking Constraints) Let N be the order of the AG-group, with elements $x, y \in \{0 \ldots, N-1\}$ and left identity e. Let $f(x)$ abbreviate $(e+1)(e+x)$ and let FLAG be a boolean variable that is set if the first six elements of the AG-group are self-inverse and $(e+1)(e+2)$ is not self-inverse. We then define the following 10 constraints:*

(i) $e \leq x$, *(ii)* $x^{-1} < (x+2)$,

(iii) $(x^{-1} = x \wedge x < y) \Rightarrow y^{-1} = y$.

For odd values of N:

(iv) $f(1) < (e+4)$, *(v)* $(x > 1 \wedge 2x < N) \Rightarrow f(x) < (e+2x)$.

For even values of N

(vi) $f(1) = e$,

(vii) $(-FLAG \wedge 0 < x < \frac{N}{2}) \Rightarrow f(x) < (e+2x+1)$,

(viii) $(FLAG) \Rightarrow (e+5)^{-1} = (e+5)$,

(ix) $(FLAG \wedge x > 1 \wedge (e+x)^{-1} = (e+x)) \Rightarrow (f(x)^{-1}) \neq f(x)$,

(x) $(FLAG \wedge 1 < x < y \wedge (e+y)^{-1} = (e+y)) \Rightarrow f(x) < f(y)$. □

The constraints imply that the Cayley table of the AG-group will be filled in an ascending order, where e is always the lexicographical minimal element (i.e., 0). They also have that elements which are self-inverse are ordered first, and otherwise that an element is adjacent to its inverse in the ordering. We have

[1] We consider it an important item for future work to develop *lex-leader* constraints that capture the symmetry breaking that is carried out during this post-hoc step.

omitted the constraint $x^{-1} = x \Leftrightarrow x = e$ from [102], because this is an invalid symmetry breaker for AG-group counting.

Our enumeration yields all Cayley tables explicitly. We can therefore validate the generated AG-groups using the GAP [20] computer algebra system. Because there was no functionality present in the GAP *loops* package [60] to test whether a Cayley table is an AG-group or not, we have implemented our own function that performs this test. The results of our enumeration were validated using our GAP function.[2] The algorithm is a straightforward implementation, testing that (1) the Cayley table is a Latin square; i.e., all elements occur exactly once in every row and every column, (2) the identity $(xy)z = (zy)x$ holds, and (3) there exists a left identity.

Our validated results are given in Table 6.1. We report the number of non-isomorphic AG-groups having order up to 11, and give a lower bound for order 12. In Table 6.1, for each order we give the total number of AG-groups up to isomorphism, which is further broken down into associative and non-associative AG-groups. Note, associative AG-groups are abelian groups. For each order we also give the total number of CPU-seconds required to enumerate all groups and the number of tables generated by FINDER that were tested for lex-minimality in post-hoc processing. All counting was carried out on an Intel quad core CPU Q9650 with 4GB of memory. It should be noted that our counting procedure uses negligible computer memory resources.

In the remainder of the chapter we discuss some of the observations we made using our enumeration results and, in particular, propose a new interesting class of AG-groups.

6.3 AG-group of Smallest Order

The smallest AG-group which is not a group is of order 3. The Cayley table for that is given in Example 6.3.1.

Example 6.3.1. *Smallest AG-group of order* 3 :

$\cdot$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

[2]Please contact the authors by email for either the GAP source code, or a copy of the enumerated tables.

Order	AG-groups	Assoc	Non-Assoc	CPU-Time	post-hoc tests
1	1	1	0	$< .01$	0
2	1	1	0	$< .01$	1
3	2	1	1	$< .01$	2
4	4	2	2	$< .01$	6
5	2	1	1	$< .01$	7
6	2	1	1	$< .01$	46
7	2	1	1	.47	97
8	10	3	7	8.44	796
9	5	2	3	102.37	3599
10	2	1	1	$1,735.25$	16144
11	2	1	1	$15,206.26$	86406
12	≥ 7	≥ 2	≥ 5	NA	NA

Table 6.1: Results of AG-group enumeration.

Clearly every abelian group is an AG-group, however the converse is certainly not always true. We now note a number of contrasts between groups and AG-groups. In particular, we establish the existence of non-associative AG-groups — i.e. non-abelian groups — of order p and p^2 where p is a prime. In detail, our observations are:

(i) Every group of order p is abelian. We find that non-associative AG-groups of order p exist. The AG-group of order 3 in Example 6.3.1 is not an abelian group.

(ii) Every group of order p^2 is abelian. We also have that non-associative AG-groups of order p^2 exist. The AG-group in Example 6.4.3 is not an abelian group.

(iii) Every group which satisfies the squaring property $(ab)^2 = a^2b^2$ is abelian. Although every AG-group clearly satisfies the squaring property, an AG-group is not necessarily abelian.

6.4 Smarandache AG-groups

In [69] Padilla Raul introduced the notion of a Smarandache semigroup, here written S-semigroup. An S-semigroup is a semigroup A such that a proper subset of A

is a group with respect to the same induced operation [103]. Similarly a Smarandache ring, written S-ring, is defined to be a ring A, such that a proper subset of A is a field with respect to the operations induced. Many other Smarandache structures have also appeared in the literature. The general concept of Smarandache structures is that, if a special structure happens to be a substructure of a general structure, then that general structure is called Smarandache. In that spirit we propose Smarandache AG-groups here and study them with the help of examples generated during the enumeration given in Sec. 6.2.

Definition 6.4.1. *Let G be an AG-group. G is said to be a Smarandache AG-group (S-AG-group) if G has a proper subset P such that P is an abelian group under the operation of G.*

The AG-groups G in Examples 6.4.3 and 6.4.4 are S-AG-groups, whereas the AG-group G in Examples 6.3.1 and 6.4.6 are not.

The following theorem guarantees that an AG-group having a unique nontrivial element of order 2 is always an S-AG-group.

Theorem 6.4.2. *If there is a unique nontrivial element a of order 2 in an AG-group G then $\{e, a\}$ is an abelian subgroup of G.*

Proof. Take $a \in G$ satisfying $a^2 = e$. Now we have to identify an element for the '?' cell in the following table:

$\cdot$	e	a
e	e	a
a	?	e

Taking $y = ae$ and using the paramedial law we have $y^2 = (ae)^2 = e^2a^2 = a^2 = e$. Thus, y has order 2. Since G has a single element of order 2, we have $y = ae = a$. Thus, a is the required element, and our table can now be completed:

$\cdot$	e	a
e	e	a
a	a	e

Here $\{e, a\}$ is an AG-subgroup of G of order 2, and is therefore an abelian group, hence G is an S-AG-group. $\square$

We illustrate Theorem 6.4.2, by considering the following example.

Example 6.4.3. *An AG-group of order 8:*

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	6	7	4	5
2	2	3	1	0	5	6	7	4
3	3	2	0	1	7	4	5	6
4	6	4	7	5	3	0	2	1
5	7	5	4	6	0	2	1	3
6	4	6	5	7	2	1	3	0
7	5	7	6	4	1	3	0	2

Here 1 has order 2, and 1 is the unique such element of G. Hence $\{0, 1\}$ is an abelian subgroup of G.

The converse of Theorem 6.4.2 is not true. That is, if an AG-group G has an abelian subgroup, then it is not necessary that G will have a unique non-trivial element of order 2. This can be observed with the following example:

Example 6.4.4. *An AG-group of order* 9*:*

$\cdot$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	2	0	1	5	6	7	8	3	4
2	1	2	0	7	8	3	4	5	6
3	5	3	7	8	0	4	2	6	1
4	6	4	8	0	7	2	3	1	5
5	3	7	5	6	1	8	0	4	2
6	4	8	6	1	5	0	7	2	3
7	7	5	3	4	2	6	1	8	0
8	8	6	4	2	3	1	5	0	7

The AG-group in Example 6.4.4 has $\{0, 7, 8\}$ as abelian subgroup and hence is a Smarandache AG-group. However, the element of order 2 is not unique. In fact, there are two nontrivial elements of order 2, namely $\{1, 2\}$.

Remark 6.4.5. Since AG-groups satisfy Lagrange's Theorem, the unique element of order 2 can exist in AG-groups of even order only.

However, if G has more than one element of order 2, then it is not necessary that G will have an abelian subgroup. In Example 6.4.6 all non-trivial elements of G are of order 2, however we also see that G has no abelian subgroup. Note that G has four proper AG-subgroups, namely $\{0, 1, 2\}$, $\{0, 3, 7\}$, $\{0, 4, 6\}$, and $\{0, 5, 8\}$. None of those is commutative.

Example 6.4.6. *An AG-group order of* 9*:*

$\cdot$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	2	0	1	4	5	3	7	8	6
2	1	2	0	5	3	4	8	6	7
3	7	6	8	0	2	1	5	3	4
4	6	8	7	1	0	2	4	5	3
5	8	7	6	2	1	0	3	4	5
6	4	3	5	8	6	7	0	2	1
7	3	5	4	7	8	6	1	0	2
8	5	4	3	6	7	8	2	1	0

AG-groups satisfy Lagrange's Theorem, so AG-groups of prime order cannot have a proper AG-subgroup, hence cannot have a proper abelian subgroup. We record this fact as the following theorem.

Theorem 6.4.7. *An AG-group G of prime order cannot be an S-AG-group.* □

The notion of S-AG-group can be generalized to S-AG-groupoid as follows.

Definition 6.4.8. *Let S be an AG-groupoid. S is said to be a Smarandache AG-groupoid (S-AG-groupoid) if S has a proper subset P such that P is a commutative semigroup under the operation of S.*

The examples given in the case of AG-groups can also be considered for S-AG-groupoids. We now provide two further examples to show that this notion holds generally.

Example 6.4.9. *An AG-groupoid of order* 4.

$\cdot$	0	1	2	3
0	0	0	2	3
1	0	1	2	3
2	3	3	0	2
3	2	2	3	0

Example 6.4.10. *An AG-groupoid of order* 4.

$\cdot$	0	1	2	3
0	1	2	0	3
1	3	0	2	1
2	2	1	3	0
3	0	3	1	2

The AG-groupoid S in Example 6.4.9 has a proper subset $\{0, 1\}$ which is a commutative semigroup, and therefore S is an S-AG-groupoid. Although somewhat tedious, one can check manually that the AG-groupoid S in Example 6.4.10 has no proper subset having the desired property, and therefore we have S is not a S-AG-groupoid.

Chapter 7

A Study of AG-Groups as Generalization of Abelian Groups

This chapter has two sections. In Section 1 we develop some structural properties of AG-groups. In Section 2 we study AG-groups as generalization of abelian groups.

7.1 Some Structural Properties of AG-groups

An AG-group (AG-groupoid with left identity and inverses) is a non-associative structure in general and is a generalization of abelian group. In this section we discuss some structural properties of AG-groups. We prove that for an AG-group associativity and commutativity imply each other. Non-associative AG-groups can never be power associative. The duality between left AG-groups and right AG-groups is discussed. [26] and [51] started the study of the corresponding properties of groups in AG-groups. The present work provides a continuation and further development of that. The structure of AG-group is one of the most interesting structures. There is no commutativity or associativity in general. But unlike groups and other structures, commutativity and associativity imply each other in AG-groups and thus AG-group becomes abelian group if any one of them is allowed (Theorem 48). The order of elements cannot be defined in AG-group. That is AG-group cannot be locally associative otherwise it becomes abelian group (Theorem 53). The duality between left AG-groups and right AG-groups has been shown in Theorem 50.

Example 40. *Left AG-group of order* 3 :

$\cdot$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Example 41. *Right AG-group of order* 3 :

$\cdot$	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

Example 42. *Every abelian group* $(G, \cdot)$ *is an AG-group. This is the trivial case.*

Every abelian group$(G, \cdot)$ can be converted to an AG-group $(G, *)$ if $*$ is defined as $a * b = a^{-1} \cdot b$ or $b * a^{-1}$, by [26, Theorem 4.4, Page 46].

Example 43. *The set* Z *of integers, is an AG-group under* $*$ *defined as* $a * b = b - a$ *see [26, Example 4.2, Page 45].*

The only known examples of infinite AG-groups are of such type.

7.1.1 Basic Properties of AG-groups

The following lemma presents some fundamental results for AG-groups; these facts will be used frequently and normally we shall make no reference to this lemma.

Lemma 17. *Let* G *be an AG-group* G. *Let* $a, b, c, d \in G$ *and* e *is the left identity in* G. *Then the following conditions hold in* G.

(i) $(ab)(cd) = (ac)(bd)$ *medial law, [7, Lemma 1.1 (i)];*

(ii) $ab = cd \Rightarrow ba = dc$, *[57, Theorem 2.7, Page 68];*

(iii) $a \cdot bc = b \cdot ac$, *[58, Lemma 4, Page 58];*

(iv) $(ab)(cd) = (db)(ca)$ *paramedial law, [7];*

(v) $(ab)(cd) = (dc)(ba)$, *(we are unable to find reference);*

(vi) $ab = cd \Rightarrow d^{-1}b = ca^{-1}$*;*

(vii) *If* e *the right identity in* G *then it becomes left identity in* G*, i.e,* $ae = a \Rightarrow ea = a$*, [57, Theorem 2.3, Page 67];*

(viii) $ab = e \Rightarrow ba = e$*;*

(ix) $(ab)^{-1} = a^{-1}b^{-1}$*[26, Remark 4.6, Page 47];*

(x) $a(b \cdot cd) = a(c \cdot bd) = b(a \cdot cd) = b(c \cdot ad) = c(a \cdot bd) = c(b \cdot ad)$*;*

(xi) $a(bc \cdot d) = c(ba \cdot d)$*;*

(xii) $(a \cdot bc)d = (a \cdot dc)b$*;*

(xiii) $(ab \cdot c)d = a(bc \cdot d)$*.*

Proof. (i) see [7, Lemma 1.1(i)].

(ii) $ba \cdot e = ea \cdot b = ab = cd = ec \cdot d = dc \cdot e \Rightarrow ba = dc$ since e is cancellative.

(iii) Since G satisfies $bc \cdot a = ac \cdot b$ so by (ii), we get $a \cdot bc = b \cdot ac$.

(iv) By applications of (i) and (ii), we have $(ab)(cd) = (ac)(bd) \Rightarrow (cd)(ab) = (bd)(ac) \Rightarrow (cd)(ab) = (ba)(dc)$. $\Rightarrow (ab)(cd) = (dc)(ba) = (db)(ca) \Rightarrow (ab)(cd) = (db)(ca)$.

(v) By consecutive applications of (i) and (iv).

(vi) $ab = cd \Rightarrow ab \cdot d^{-1} = c \Rightarrow d^{-1}b \cdot a = c \Rightarrow d^{-1}b = ca^{-1}$.

(vii) Using (iii) and then hypothesis $a = ae = a \cdot ee = e \cdot ae = ea$.

(viii) $ab = e = ee$ now apply (ii).

(ix) $(a^{-1}b^{-1})(ab) = (a^{-1}a)(b^{-1}b) = e \Rightarrow (ab)^{-1} = a^{-1}b^{-1}$.

(x) By repeated use of Lemma 17 Part (iii).

(xi) Using Part (iii) and medial law,

$$a(b \cdot cd) = (bc)(ad) = (ba)(cd) = c(ba \cdot d).$$

(xii) Using Part (iii) and invertive law,

$$(a \cdot bc)d = (b \cdot ac)d = (d \cdot ac)b = (a \cdot dc)b.$$

(xiii) $(ab \cdot c)d = (dc)(ab) = a(dc \cdot b) = a(bc \cdot d)$.

□

The first 9 parts of the above lemma are already proved in scattered papers on AG-groupoid given in the references. We only claim that our proofs are new and more standard while the last four parts are new.

Theorem 48. *In AG-monoid and hence in AG-group the following are equivalent.*

(i) Associativity.

(ii) Commutativity.

Proof. $(i) \Longrightarrow (ii)$ Suppose $(G, \cdot)$ be an AG-groupoid with the left identity e. Let G be associative and $a, b \in G$. Then

$$\begin{aligned} ab &= e \cdot ab = ea \cdot b = ba \cdot e \\ &= b \cdot ae = (eb)(ae) = (ea)(be) \\ &= a \cdot be = ab \cdot e = eb \cdot a = ba. \end{aligned}$$

Thus G is commutative. $(ii) \Longrightarrow (i)$ is easy. □

Theorem 49. *An AG-group G with right identity e is abelian group.*

Proof. Let $a, b \in G$. Since $ab = ab \cdot e = eb \cdot a = ba$. Now apply Theorem 48. □

7.1.2 Duality Between Left AG-groups and Right AG-groups

Here we prove that left AG-groups and right AG-groups are equivalent. We shall prove that left AG-group and right AG-group are the opposite of each other.

Theorem 50. *Let $(G, \cdot)$ be a left AG-group. Define the operation $a * b = ba$ for every $a, b \in G$. Then $(G, *)$ is a right AG-group.*

Proof. Let $(G, \cdot)$ be a left AG-group. Define $a * b = ba$ for all $a, b \in (G, \cdot)$. Let $a, b, c \in G$.

$$\begin{aligned} a * (b * c) &= a * (cb) \\ &= (cb)a = (ab)c = c * (ab) = c * (b * a). \end{aligned}$$

Hence $(G,*)$ is a right AG-groupoid. If e is the left identity of $(G,\cdot)$ then $a*e = ea = a$. Hence e is the right identity of the right AG-groupoid $(G,*)$. It is clear that the inverses in $(G,*)$ remain the same as in $(G,\cdot)$. Hence $(G,*)$ is a right AG-group. $\square$

From now onward we will consider only left AG-group and will call it simply AG-group.

7.1.3 Power Associativity of AG-groups

Lemma 18. *In an AG-groupoid S with left identity e the following holds*

$$(ab)^2 = (ba)^2 \text{ for all } a, b \in S.$$

Proof. Let $(S,\cdot)$ be an AG-groupoid S with left identity e. Then for all $a, b \in S$. By using medial and paramedial laws, we have $(ab)^2 = (ab)(ab) = b^2a^2 = (ba)^2$. $\square$

Theorem 51. *If every element of a locally associative AG-groupoid S with left identity e is of order 2 then S is an abelian group.*

Proof. Let $(S,\cdot)$ be a locally associative AG-groupoid with the left identity e such that $a^2 = e$ for all $a \in S$.

If $a, b \in S$ then $a^2 = b^2 = e$. Also $ab \in S$ which implies that $(ab)^2 = e$, which further implies $(ba)^2 = e$ by Lemma 18. Now by using medial and paramedial laws and local associativity, we have

$$\begin{aligned} ab &= e(ab) = (ab)^2(ab) \\ &= (a^2b^2)(ab) = (a^2a)(b^2b) \\ &= (aa^2)(bb^2) = (b^2a^2)(ba) \\ &= (ba)^2(ba) = e(ba) = ba. \end{aligned}$$

Thus S is commutative. Hence S is commutative monoid. But every element of S is its own inverse and therefore S is an abelian group. $\square$

Next we need the following theorem from [51] or [88].

Theorem 52. *An AG-group G is cancellative.*

Theorem 53. *An AG-group G with local associativity is abelian group.*

Proof. Let $(G, \cdot)$ be a locally associative AG-group. Then for all $a, b \in G$ by using medial and paramedial laws and local associativity of S, we have $(ab)(ab)^2 = (ab)(a^2b^2) = (aa^2)(bb^2) = (a^2a)(b^2b) = (ba)(b^2a^2)$
$= (ba)(ba)^2$, which by Lemma 18 and cancellativity implies $ab = ba$. Thus G is commutative. So the left identity becomes the right identity. Thus by Theorem 49 G is abelian group. $\square$

Theorem 53 ensures that in a non-associative AG-group orders of elements cannot be defined due to lack of local associativity. However we can speak of the order of an element up to 2.

Definition 45. An element a of order 2 of an AG-group G is called **involution**.

For example in Example 40 all elements are involutions. But this is not necessary that all elements of an AG-group must be involutions as the elements $4, 5, 6, 7$ are not involutions in the AG-group given in the following example.

Example 44. *An AG-group of order* 8.

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	3	0	1	2	6	7	5	4
2	2	3	0	1	5	4	7	6
3	1	2	3	0	7	6	4	5
4	6	4	7	5	2	0	1	3
5	7	5	6	4	0	2	3	1
6	4	7	5	6	3	1	2	0
7	5	6	4	7	1	3	0	2

7.1.4 General Properties of AG-groups

Theorem 54. *An AG-group G has exactly one idempotent element, which is the left identity.*

Proof. Suppose a is an arbitrary element of G such that $aa = a$. Then $ea = a = aa$ which implies $a = e$ by right cancellation. Thus the left identity e is the only idempotent element of G. $\square$

Theorem 55. *A subset containing all the involutions of an AG-groupoid S with the left identity e is an AG-group contained in S.*

Proof. Let $(S, \cdot)$ be an AG-groupoid with the left identity e. Let $H = \{a \in S — a^2 = e\}$. H is non-empty since $ee = e \Rightarrow e \in H$. If $f, g \in H$ then $f^2 = g^2 = e$. Now $(fg)^2 = f^2g^2 = ee = e$. This implies $fg \in H$. Thus H is an AG-subgroupoid of S. Also since every element in H is its own inverse. Hence H is an AG-group. □

7.2 AG-groups as Generalization of Abelian Groups

In this section we now study AG-groups as generalization of abelian groups as suggested in [83].

We therefore will lift many of the standard concepts in group theory to AG-groups and investigate similarities and differences between the two theories. We will start our investigations by studying complexes (i.e., arbitrary subsets) and AG-subgroups together with cosets in detail, which were already introduced in [26] and [51];(§7.2.1). The main results show that while similar to group theory the union of two AG-subgroups is an AG-subgroup if and only if either one contains the other, contrary to group theory the product of two AG-subgroups is always an AG-subgroup.

We then study conjugate elements of AG-groups in Section 7.3) and establish some results such as (i) the relation of conjugacy between the elements of an AG-group is an equivalence relation; (ii) in an AG-group of prime order all elements are conjugate to each other; (iii) the conjugacy class of the left identity of an AG-group is an AG-subgroup; and (iv) most surprisingly, the centre of a non-associative AG-group is always empty.

We then define and study the concepts of normality, normalizer and commutator (§7.3.1—§7.3.3). We observe that although we can quotient an AG-group by any of its AG-subgroup without the requirement of normality, defining normality is beneficial in its own right. We can, for example, show that the quotient of an AG-group by a normal subgroup yields an abelian group. Similarly, we can demonstrate that the normalizer of an arbitrary subset of an AG-group is not necessarily an AG-subgroup.

Finally we consider direct products of AG-groups (§7.3.4) and define actions of AG-groups on sets (§7.3.5). Here again we observe that while some of the theory can be developed analogously to group theory, we can also demonstrate that, for instance, some natural groups actions can not simply be lifted to AG-groups. We now recall the definition of AG-subgroup, as presented in [26, 51].

Definition 46. *Let G be an AG-group and let H be a non-empty subset of G. We call H an* ***AG-subgroup*** *of G, written as $H \leq G$, if H is itself an AG-group with respect to the operation on G.*

The following results are easy to establish:

Theorem 56. *If H is a non-empty subset of an AG-group G then $H \leq G$ if and only if $ab^{-1} \in H$ for all $a, b \in H$. see [51, Theorem 3.3]*

One can easily establish the equivalence of the following condition for a subset H to be an AG-subgroup with that given in Theorem 56.

Theorem 57. *A non-empty subset H of an AG-group G is an AG-subgroup of G if and only if for any pair $a, b \in H, ab \in H$ and for each $a \in H, a^{-1} \in H$.*

Proofs of the following theorems are group theoretic.

Theorem 58. *Let Ω be a collection of AG-subgroups of an AG-group G. Then the intersection $\cap\Omega$ of the members of Ω is an AG-subgroup of G.*

Theorem 59. *Let H, K be AG-subgroups of an AG-group G of order m, n, respectively, and $(m, n) = 1$. Then $HK = \{hk | h \in H, k \in K\}$ has exactly mn elements.*

7.2.1 Complexes

Following [22] we call an arbitrary non-empty subset X of an AG-group G a complex in G. For two complexes X and Y in G we define their product as a complex XY and inverse of X as a complex X^{-1} given by $XY = \{xy | x \in X, y \in Y\}$ and $X^{-1} = \{x^{-1} \mid x \in X\}$, respectively.

These definitions allow us to restate Theorem 56 and Theorem 57 in terms of complexes as follows:

Theorem 60. *A non-empty complex H of the AG-group G is an AG-subgroup of G if $HH^{-1} \subseteq H$.*

Theorem 61. *A non-empty complex H of an AG-group G is an AG-subgroup of G if (i) $H^2 = H$ and (ii) $H^{-1} = H$.*

If the complexes H and K in a group G are subgroups of G then the product HK of H and K need not be a subgroup of G. However the product HK of H and K is a subgroup of G if and only if H and K are permutable. In contrast the product of two AG-subgroups of the AG-group is always an AG-subgroup of G as the following theorem proves:

Theorem 62. *Let H and K be AG-subgroups of an AG-group G. Then the product HK is also an AG-subgroup of G.*

Proof. Let $H, K \leq G \Rightarrow H^2 = H, H^{-1} = H$ and $K^2 = K, K^{-1} = K$. We then have $(HK)^2 = H^2K^2 = HK$, by medial law. Also by Theorem 61 we have $(HK)^{-1} = H^{-1}K^{-1} = HK \Rightarrow HK \leq G$. □

This theorem can now be used to establish the second part of the following general result for complexes of an AG-group.

Theorem 63. *Let ζ be the collection of all complexes of an AG-group G and let σ be the collection of all AG-subgroups of G. Then*

(i) ζ is an AG-monoid, an

(ii) σ is an AG-subgroupoid of ζ.

Proof. Let $\zeta = \{A \mid A \subset G, A \neq \emptyset\}$

(i) Let $A, B \in \zeta$. Then $AB = \{ab \mid a \in A, b \in B\} \subset G$. Clearly $AB \neq \emptyset$ as $A, B \in \zeta$, thus $AB \in \zeta$.

Let $A, B, C \in \zeta$. Then $(ab)c = (cb)a$ for all $a \in A, b \in B, c \in C$. Hence $(AB)C = (CB)A$.

Since $E = \{e\} \in \zeta$ where e is the left identity in G such that $EA = A$, for all $A \in \zeta$. Therefore ζ has left identity.

Therefore ζ is an AG-monoid.

(ii) Let $\sigma = \{A \in \zeta \mid A$ is an AG-subgroup of $G\}$. Let $A, B \in \sigma$ then $AB \in \sigma$ by Theorem 62. Thus σ is an AG-subgroupoid of ζ. Also $E = \{e\} \in \sigma$. Thus σ is an AG-subgroupoid of ζ with left identity.

□

The union of any two AG-subgroups of an AG-group G is not necessarily an AG-subgroup.

Example 45. *As example we consider the following AG-group of order* 8

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	3	0	1	2	5	6	7	4
2	2	3	0	1	6	7	4	5
3	1	2	3	0	7	4	5	6
4	6	5	4	7	0	3	2	1
5	5	4	7	6	1	0	3	2
6	4	7	6	5	2	1	0	3
7	7	6	5	4	3	2	1	0

Here $\{0,2\},\{0,7\}$ *are AG-subgroups but* $\{0,2\}\cup\{0,7\}=\{0,2,7\}$ *is not an AG-subgroup.*

The following is the necessary and sufficient condition for the union of two AG-subgroups to be an AG-subgroup.

Theorem 64. *Let* H_1*and* H_2 *be the AG-subgroups of an AG-group* G*. Then* $H_1\cup H_2$ *is an AG-subgroups of* $G \Leftrightarrow H_1\subseteq H_2$ *or* $H_2\subseteq H_1$*.*

Proof. Let H_1 and H_2 be AG-subgroups of an $AG-$group G. Suppose that either $H_1\cup H_2=H_1$ or $H_1\cup H_2=H_2$ then $H_1\cup H_2$ is an AG-subgroup of an AG-group G.

Conversely suppose that $H_1\nsubseteq H_2$ and $H_2\nsubseteq H_1$. Let $a\in H_1\backslash H_2$ and $b\in H_2\backslash H_1$ then $ab\in H_1\cup H_2$ because $H_1\cup H_2$ is an AG-subgroup of G. So either $ab\in H_1$ or $ab\in H_2$.

If $ab\in H_1$ then $b=eb=(a^{-1}a)b=(ba)a^{-1}=(ba)(ea^{-1})=(a^{-1}e)(ab)\in H_1$ since H_1 is an $AG-$subgroup, which is a contradiction. Similarly if $a=ea=(b^{-1}b)a=(ab)b^{-1}\in H_2$, is a contradiction.

Thus $H_2\backslash H_1=\emptyset$ or $H_1\backslash H_2=\emptyset$ and therefore either $H_1\subseteq H_2$ or $H_2\subseteq H_1$. □

Definition 47. *Let* H *be an AG-subgroup of an AG-group* G*, and let* $a\in G$*. The left coset* aH *of* H *is the set* $\{ah \mid h\in H\}$*. Similarly right coset* Ha *is defined as* $\{ha \mid h\in H\}$*.*

We define $(Ha)^{-1}$ by

$$(Ha)^{-1}=\big\{(ha)^{-1},h\in H\big\}=\big\{h^{-1}a^{-1},h\in H\big\}$$

Then $(Ha)^{-1}=Ha^{-1}=H(ea^{-1})=(a^{-1}e)H$. The mapping

$$Ha\longrightarrow(Ha)^{-1}=(a^{-1}e)H,\ \text{where } a\in G$$

is a one-one correspondence between the collection of right and left cosets. It shows that the right and left cosets of H in an AG-group G are equal in number.

Lemma 19. *Suppose G is an AG-group and $H \leq G$. Let $x, y \in G$ then we have*

(i) $Hx = H$ *if and only if* $x \in H$.

(ii) $xH = H$ *if and only if* $x \in H$.

(iii) $Hx = Hy$ *if and only if* $y^{-1}x \in H$.

(iv) $xH = \{g | xH = Hg\}$.

(v) $x \in Hx$.

(vi) $(xy)H = H(yx)$.

(vii) $(Hx)y = H(xy)$.

Proof. (i) If $Hx = H$, then $x = ex \in Hx = H$ so $x \in H$. Conversely, if $x \in H$ then $Hx \subseteq H$ because it is closed under multiplication. It remains to show that $H \subseteq Hx$. Choose any $h \in H$, then $h = (hx^{-1})x \in Hx$ because $h, x^{-1} \in H$. Thus $H \subseteq Hx$ and so $Hx = H$.

(ii) $xH = H$ if and only if $Hx = He = H$ by Lemma 17 (ii) if and only if $x \in H$ by (i).

(iii) $Hx = Hy \Leftrightarrow (Hx)y^{-1} = (Hy)y^{-1} \Leftrightarrow (y^{-1}x)H = (y^{-1}y)H \Leftrightarrow (y^{-1}x)H = eH \Leftrightarrow H(y^{-1}x) = He \Leftrightarrow H(y^{-1}x) = H \Leftrightarrow y^{-1}x \in H$.

(iv) If $g \in xH$, then $g = xh$ for some $h \in H$, so $Hg = H(xh) = x(Hh) = xH$. Therefore $xH \subseteq \{g|xH = Hg\}$. Conversely if $xH = Hg$ then $g = eg \in Hg = xH$ so $\{g|xH = Hg\} \subseteq xH$.

(v) This is trivial, since $x = ex \in Hx$.

(vi) See [51, Lemma 3.4(2)].

(vii) $(Hx)y = (yx)H = H(xy)$ by (vi).

□

In Lemma 19 (i), if $Hx = H$ then x can be determined as follows:

Since $Hx = H$ then for some $h \in H$, there is an $h' \in H$ such that $hx = h'$. This implies that $xh = h'e$ by Lemma 17 (ii). Thus $x = ex = (h^{-1}h)x = (xh)h^{-1} = (h'e)h^{-1}$.

Lemma 20. *Suppose that H is an AG-subgroup of an AG-group G and $x, y \in G$. It follows that either $Hx = Hy$ or $Hx \cap Hy = \emptyset$.*

Proof. Either $Hx \cap Hy = \emptyset$ or there exist $z \in Hx \cap Hy$ in which case $zx^{-1}, zy^{-1} \in H$. Thus $y^{-1}x = (zy^{-1})(z^{-1}x) = (zy^{-1})(zx^{-1})^{-1} \in H$. Thus by Lemma 19(iii), we have $Hx = Hy$. $\square$

An AG-group may or may not have an abelian group as its AG-subgroup. For instance the AG-group G in Example 46 has $\{0, 1, 2, 3\}$ as its AG-subgroup which is an abelian group while the AG-group G in Example 45 has none.

Thus we can state **Lagrange's Theorem** for AG-subgroups:

Theorem 65. *If H is an AG-subgroup of a finite AG-group G then the order of H divides the order of G see [51, Theorem 3.7].*

7.3 Conjugacy Relations in AG-groups

Let G be an AG-group. For any $a \in G$, the element $(ga)g^{-1}, g \in G$ is called the conjugate or transform of a by G. Two elements $a, b \in G$ are said to be conjugate if and only if there exist an element $g \in G$ such that $(ga)g^{-1} = b$. We frequently abbreviate the conjugate of $a \in G$ by $a^g = (ga)g^{-1}, g \in G$.

Theorem 66. *The relation of conjugacy between the elements of an AG-group is an equivalence relation.*

Proof. Let us denote the relation of conjugacy between the elements of an AG-group by R. Then

(i) R is reflexive that is $a\ R\ a$ because $\exists\ a^{-1} \in G$ and $a = (aa)a^{-1}$, by left invertive law.

(ii) R is symmetric because if $a\ R\ b$ for $a, b \in G$, then there exist $g \in G$ such that $b = (ga)g^{-1} \Rightarrow bg = ga \Rightarrow gb = ag \Rightarrow (gb)g^{-1} = a \Rightarrow a = (gb)g^{-1}$. Thus $b\ R\ a$.

(iii) R is transitive: Let $a\ R\ b$ and $b\ R\ c$, then there exist $g_{1,}g_2 \in G$ such that $b = (g_1a)g_1^{-1}, c = (g_2b)g_2^{-1}$. Hence

$$\begin{aligned} c &= (g_2b)g_2^{-1} = [g_2\{(g_1a)g_1^{-1}\}]g_2^{-1} = [g_2^{-1}\{(g_1a)g_1^{-1}\}]g_2 \\ &= [(g_1a)(g_2^{-1}g_1^{-1})]g_2 = [g_2(g_2^{-1}g_1^{-1})](g_1a) = (g_2g_1)[(g_2^{-1}g_1^{-1})a] \\ &= (g_2g_1)^{-1}[(g_2g_1)a] \end{aligned}$$

Thus $ce = [(g_2g_1)a](g_2g_1)^{-1}$, which implies that $a\ R\ ce$. But by reflexive property, $ce\ R\ ce$. So by the above argument from $a\ R\ ce$ and $ce\ R\ ce$, we have $a\ R\ (ce)e$. That is $a\ R\ c$. Thus R is transitive.

Hence R is an equivalence relation. □

In any AG-group G the relation of conjugacy between the elements of G, being an equivalence relation, partitions G into equivalence classes. Each equivalence class consist of elements which are conjugate to each other. An equivalence class determined by the conjugacy relation between the elements in G is called a class of conjugate elements or simply a conjugacy class. A conjugacy class consisting of elements conjugate to an element a of G will be denoted by C_a.

Example 46. *Consider the following AG-group G of order 4:*

$\cdot$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	3	2	1	0
3	2	3	0	1

The AG-group G has two conjugacy classes namely $C_0 = \{0, 1\}$ and $C_2 = \{2, 3\}$.

Lemma 21. *Let G be an AG-group and let $a, b \in G$. Let k be any fixed element of G such that $ak = ka$ and $bk = kb$. Then a, b commute with each other.*

Proof. Consider $k(ab) = a(kb) = a(bk) = b(ak) = b(ka) = k(ba)$ implies $ab = ba$ by left cancellation. □

Theorem 67. *If there is any self-conjugate element in an AG-group G then G is an abelian group.*

Proof. Suppose $a \in G$ such that $a = (ga)g^{-1}\, \forall g \in G$. This means that $ag = ga\, \forall g \in G$ which implies that every g commutes with a. Therefore all elements of G commute with each other and by Lemma 21 this implies G is an abelian group. □

From Theorem 67 follows that in a non-associative AG-group no element can be self-conjugate.

Corollary 38. *Let G be a non-associative AG-group. Then the centre of G is empty, i.e., $Z(G) = \emptyset$. Similarly the set of all self-conjugate elements of G is empty.*

Theorem 68. *Let G be an AG-group where e is the left identity of G. Then C_e, the conjugacy class of e, is an AG-subgroup of G.*

Proof. $C_e \neq \emptyset$ because $e \in C_e$. From Theorem 67 follows $C_e \neq \{e\}$. So let $a, b \in C_e$ with $a\ R\ e$ and $b\ R\ e$. Thus there exist $g_1, g_2 \in G$ such that $a = (g_1 e)g_1^{-1}, b = (g_2 e)g_2^{-1}$. We first consider ab:

$$\begin{aligned} ab &= \{(g_1 e)g_1^{-1}\}\{(g_2 e)g_2^{-1}\} \\ &= \{(g_1^{-1} e)g_1\}\{(g_2 e)g_2^{-1}\} \\ &= \{(g_1^{-1} e)(g_2 e)\}(g_1 g_2^{-1}) \\ &= \{(g_1^{-1} g_2)e)\}(g_1^{-1} g_2)^{-1} \end{aligned}$$

Thus we have $ab\ R\ e$ and therefore $ab \in C_e$.
Now consider a^{-1}:

$$\begin{aligned} a^{-1} &= [(g_1 e)g_1^{-1}]^{-1} = (g_1^{-1} e)g_1 \\ &= (g_1 e)g_1^{-1} \end{aligned}$$

Thus we have $a^{-1}\ R\ e$ and therefore $a^{-1} \in C_e$.
Hence C_e is an AG-subgroup of G. □

Theorem 69. *In an AG-group of prime order all elements are conjugate to each other. That is $C_e = G$.*

Proof. This follows by Lagrange's Theorem and by Theorem 68. □

Example 47. *Consider the AG-group G of order 5:*

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

In G we have $C_0 = \{0, 1, 2, 3, 4\}$.

Theorem 70. *Let G be an AG-group and $a, b, c \in G$. Then*
(i) $(a^c)(b^c) = (ab)^{c^2}$ *(ii)* $(a^2)^b = aa^b$.

Proof. 1.

$$\begin{aligned}(a^c)(b^c) &= \{(ca)c^{-1}\}\{(cb)c^{-1}\}\\ &= \{(ca)(cb)\}(c^{-1}c^{-1})\\ &= \{c^2(ab)\}(c^2)^{-1}\\ &= (ab)^{c^2}\end{aligned}$$

2.

$$\begin{aligned}(a^2)^b &= (ba^2)b^{-1}\\ &= (ba^2)[(b^{-1}a)a^{-1}]\\ &= (b^{-1}a)[(ba^2)a^{-1}]\\ &= (b^{-1}a)[a^{-1}a^2.b]\\ &= (b^{-1}a)(ab)\\ &= a[(b^{-1}a)b]\\ &= a[(ba)b^{-1}]\\ &= aa^b\end{aligned}$$

□

7.3.1 Normality in AG-groups

Although we can quotient by any AG-subgroup without the need of normality, we can still define a concept of normality in AG-groups.

Definition 48. *Let H be an AG-subgroup of G. H is said to be* ***normal AG-subgroup*** *of G if it coincides with all of its conjugate AG-subgroups of G. Thus H is normal in G if and only if $(gH)g^{-1} = H$, for all $g \in G$.*

We first note that $(gH)g^{-1} = (g^{-1}H)g$, for all $g \in G$ by left invertive law in the AG-group G.

Theorem 71. *The following statements about AG-subgroup H of an AG-group G are equivalent:*

(i) H is normal AG-subgroup of G.

(ii) The normalizer of H in G is the whole of G. That is $N_G(H) = G$.

(iii) Any left coset gH of H is equal to the right coset Hg for all $g \in G$. That is $gH = Hg$ for all $g \in G$.

(iv) For each $h \in H$ and any $g \in G, (gh)g^{-1} \in H$, that is H contains the whole class of conjugates of each of its elements.

Proof. We shall show (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i):

(i) $\Rightarrow$ (ii) Assume that H is a normal AG-subgroup of G then $(gH)g^{-1} = H$ for all $g \in G$. Hence $gH = Hg$ for all $g \in G$ so that every $g \in G$ is in the normalizer $N_G(H)$. Therefore $G \subseteq N_G(H)$. But $N_G(H)$ is an AG-subgroups of G and therefore contained in G. Thus $N_G(H) = G$ and hence (ii) is true.

(ii) $\Rightarrow$ (iii) Suppose that $N_G(H) = G$ holds, that is $N_G(H) = \{g \in G \mid gH = Hg\} = G$. Then $gH = Hg$ for all $g \in G$. Thus (iii) holds.

(iii) $\Rightarrow$ (iv) Suppose that $gH = Hg$ for all $g \in G$. Then given an $h \in H$ $\exists$ an $h' \in H$ such that $gh = h'g$ for all $g \in G$. Hence $(gh)g^{-1} = h' \in H$ for all $g \in G$. Thus G contains, together with any $h \in H$ all its conjugates namely the elements $(gh)g^{-1}, g \in G$. Therefore (iv) is true.

(iv) $\Rightarrow$ (i) Suppose that for each $h \in H$ and $g \in G$, $(gh)g^{-1} = h' \in H$. Hence $(gH)g^{-1} = \{(gh)g^{-1}; h \in H\} \subseteq H$ for all $g \in G$. Also for any $h \in H$ and $h = (g((gh)g^{-1}))g^{-1} \in (gH)g^{-1}$ because $(gh)g^{-1} \in H$. Thus $H \subseteq (gH)g^{-1}$ and therefore $(gH)g^{-1} = H$, for all $g \in G$. Hence H is a normal AG-subgroup of G and we have (i).

□

From the above theorem it follows that each one of the statement (ii), (iii), and (iv) can be taken as a definition of normal AG-subgroups.

While the conjugate of a subgroup of a group is again a subgroup, the conjugate of an AG-subgroup may not be an AG-subgroup as the following example shows:

Example 48. *Consider the AG-group of order 12:*

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	0	3	2	6	7	4	5	10	11	8	9
2	3	2	1	0	8	11	10	9	4	7	6	5
3	2	3	0	1	10	9	8	11	6	5	4	7
4	6	4	8	10	9	0	11	1	7	2	5	3
5	7	5	11	9	0	8	1	10	3	6	2	4
6	4	6	10	8	11	1	9	0	5	3	7	2
7	5	7	9	11	1	10	0	8	2	4	3	6
8	8	10	6	4	5	2	7	3	11	0	9	1
9	9	11	5	7	3	4	2	6	0	10	1	8
10	10	8	4	6	7	3	5	2	9	1	11	0
11	11	9	7	5	2	6	3	4	1	8	0	10

The AG-group G has AG-subgroups $H_1 = \{0, 10, 11\}$, $H_2 = \{0, 1, 2, 3\}$. While H_2 is normal AG-subgroup and H_1 is not. $(gH_2)g^{-1}$ is an AG-subgroup for all $g \in G$ but $(gH_1)g^{-1}$ is not an AG-subgroup of G for $g = 2$.

From the above example we see that if G is an AG-group and H is a normal AG-subgroup of G then for each $g \in G$, $(gH)g^{-1}$ is an AG-subgroup. We now want to investigate if this also holds for other cases of AG-subgroups.

Theorem 72. *Let G be an AG-group and H be the AG-subgroup of G of index 2. Then H is normal in G.*

Theorem 73. *The intersection of any collection of normal AG-subgroups of an AG-group is a normal AG-subgroups.*

Proof. Proof is group theoretic. □

Similar to groups normality is not transitive in AG-groups, which can be demonstrated with the following example.

Example 49. *Consider an AG-group of order 8:*

$\cdot$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	7	6	4	5	1	0	3	2
5	5	4	7	6	0	1	2	3
6	4	7	6	5	3	2	1	0
7	7	6	5	4	2	3	0	1

Let $H_1 = \{0, 1, 2, 3\}$, $H_2 = \{0, 1\}$. Both H_1 and H_2 are AG-subgroups of G. H_1 being of index 2 in G is normal in G and H_2 being of index 2 in H_1 is normal in H_1, but $H_2 \ntrianglelefteq G$ since $6 \in G, 0 \in H_2$ but $(6 \cdot 0)\, 6^{-1} = 4 \cdot 7 = 2 \notin H_2$.

Theorem 74. *Let G be an AG-group and $H \leq G, N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$.*

Proof. Clearly $H \cap N \leq H$. Let $x \in H \cap N, h \in H$. Thus $x \in H$ and $x \in N$. Now $x \in H$ implies that $(hx)h^{-1} \in H$ (since $H \leq G$), and $x \in N$ and $N \trianglelefteq G$, so $(hx)h^{-1} \in N$. Thus $(hx)h^{-1} \in H \cap N$ for all $x \in H \cap N$ and $h \in H$. Hence $H \cap N \trianglelefteq H$. $\square$

Theorem 75. *Let G be an AG-group and $H, N \trianglelefteq G$. If any one of H and N is normal in G then $HN \trianglelefteq G$.*

Proof. By Theorem 62 $HN \leq G$. Let $H \leq G, N \trianglelefteq G$. Now let $g \in G$, then we have

$$\begin{aligned} g(HN) &= H(gN) \\ &= H(Ng), \text{ since } N \trianglelefteq G \\ &= (HN)g, \text{ since } H \leq G \end{aligned}$$

Hence $HN \trianglelefteq G$. Similarly if $H \trianglelefteq G$ and $N \leq G$ Then $HN \trianglelefteq G$. $\square$

Definition 49. *An AG-group G is called **simple** if G has no proper normal AG-subgroup.*

Now by Lagrange's theorem, it follows that:

Corollary 39. *Every AG-group of prime order is simple.*

Theorem 76. *If H is a normal AG-subgroup of an AG-group G then the following holds for all x, y of G:*

(i) $y(xH) = (yx)H$

(ii) $y(Hx) = (yH)x$

(iii) $(yx)H = (xy)H$

(iv) $H(yx) = H(xy)$.

Proof. (i) Using Lemma 17(iii), Theorem 71(iii), [83, Lemma 5(vi)] and left invertive law, we have

$$y(xH) = x(yH) = x(Hy) = H(xy) = (Hx)y = (yx)H$$

(ii) Using Lemma 17(iii),[83, Lemma 5(vi)] and Theorem 71(iii), we have

$$y(Hx) = H(yx) = (Hy)x = (yH)x$$

(iii) Using (i),Lemma 17(iii) and Theorem 71(iii), we have

$$(yx)H = y(xH) = x(yH) = (xy)H$$

(iv) It follows from (iii) by using [83, Lemma 5(v)].

□

Theorem 77. *If G is an AG-group and $H \leq G$. Then $G/H = \{Ha \mid a \in G\}$ is an AG-group [51, Theorem 3.8].*

Theorem 77 guarantees that we can quotient by any AG-subgroup without the need for normality.

Theorem 78. *Let G be an AG-group and let H be a normal AG-subgroup of G then G/H is an abelian group.*

Proof. Let $xH, yH \in G/H$ then by Theorem 77, G/H is an AG-group under the binary operation $xH \cdot yH = (xy)H$ for all x, y of G. Now by Theorem 76(iii), we have

$$xH \cdot yH = (xy)H = (yx)H = yH \cdot xH$$

Hence by [83, Theorem 1], G/H is an abelian group. □

7.3.2 Normalizer of an AG-subgroup of an AG-group

Given the concept of normal AG-subgroups we can now also define normalizers, similar to the same concept in group theory.

Definition 50. *Let G be an AG-group and X a non-empty subset of G. Then the set $N_G(X) = \{g \in G \mid gX = Xg\}$ is called* ***normalizer*** *of X in G.*

Observe, that the normalizer of merely a subset of an AG-group is not necessarily an AG-subgroup.

Example 50. *AG-group of order 5:*

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$N_G(4) = \{4\}$ *which is not an AG-subgroup.*

However, the normalizer of the AG-subgroup of an AG-group is an AG-subgroup itself, as the following theorem shows.

Theorem 79. *Let G be an AG-group and let $X \leq G$. Then $N_G(X) \leq G$.*

Proof. Since $e \in X$ and $eX = Xe$ we have $e \in N_G(X)$ and thus $N_G(X) \neq \emptyset$. Now let $a \in N_G(X)$, then $aX = Xa$. Using Lemma 19(vii) we get and $(aX)a^{-1} = (Xa)a^{-1} = X(aa^{-1}) = Xe = X$ and with the AG-groupoid property we have $(aX)a^{-1} = (a^{-1}X)a = X$. With $((a^{-1}X)a)a^{-1} = Xa^{-1}$ and $((a^{-1}X)a)a^{-1} = (a^{-1}a)(a^{-1}X) = a^{-1}X$ we get $Xa^{-1} = a^{-1}X$ and therefore $a^{-1} \in N_G(X)$.

Now let $a, b \in N_G(X)$, then $aX = Xa$, $bX = Xb$. Using Lemma 17(iii), it follows that $X(ab) = a(Xb) = a(bX) = b(Xa) = X(ba) = (ab)X$ and therefore $ab \in N_G(X)$. Hence $N_G(X) \leq G$. □

Theorem 80. *Let A be an AG-subgroup of an AG-group G and let $Cl(A)$ denote the class of conjugate subgroups of A in G. Then*

$$[G : N_G(A)] = |Cl(A)|.$$

where $[G : N_G(A)]$ is the index of the normalizer of A in G.

Proof. If $x, y \in G$, then

$$\begin{aligned}
A^x = A^y &\Longleftrightarrow (xA)x^{-1} = (yA)y^{-1} \\
&\Longleftrightarrow [(xA)x^{-1}]y = yA \\
&\Longleftrightarrow [\left(yx^{-1}\right)(xA)] = yA \\
&\Longleftrightarrow x[\left(yx^{-1}\right)A] = yA \\
&\Longleftrightarrow [\left(yx^{-1}\right)A]x = Ay \\
&\Longleftrightarrow [\left(yx^{-1}\right)A] = (Ay)x^{-1} \\
&\Longleftrightarrow \left(yx^{-1}\right)A = (x^{-1}y)A \\
&\Longleftrightarrow \left(yx^{-1}\right)A = A(yx^{-1}) && \text{by Lemma 19 (vi)} \\
&\Longleftrightarrow yx^{-1} \in N_G(A) \\
&\Longleftrightarrow y^{-1}x \in N_G(A) \\
&\Longleftrightarrow N_G(A)x = N_G(A)y
\end{aligned}$$

Thus the assertion follows. □

7.3.3 Commutators in AG-group

We now study the notion of commutators in AG-groups, that is quite different from the one found in group theory. For example if we multiply the left identity e on right side then a and b commutes. That is, $ab = ba \cdot a$. Thus e works as right commutator for every two elements a, b of the AG-group G. This is not so for groups in general but true for abelian groups. Thus we can generalize this property of abelian group so the non-asssociative structure of AG-group. The concept of commutators in AG-groups is interesting for left commutators which we will call just commutators.From here onward we develop this concept.

Definition 51. *Let G be an AG-group. Then for $a, b \in G$* ***the commutator*** *$[a, b]$ is defined as*

$$[a, b] = (ab)(b^{-1}a^{-1})$$

This definition is only one possible way to define commutators. The following lemma illustrates that there is a number of equivalent definitions.

Lemma 22. *Let G be an AG-group and let $a, b \in G$ with commutator $[a, b]$. Then the following holds*

$$[a, b] = [a, b]^{-1} = [a^{-1}, b] = [a, b^{-1}] = [a^{-1}, b^{-1}]$$

Proof.

$$
\begin{aligned}
[a,b]^{-1} &= \{(ab)(b^{-1}a^{-1})\}^{-1} \\
&= \{(a^{-1}b^{-1})(b^{-1}a^{-1})^{-1}\} \\
&= (a^{-1}b^{-1})(ba) = (ab)(b^{-1}a^{-1}) && = [a,b], \text{ by paramedial law.} \\
[a^{-1},b] &= (a^{-1}b)(b^{-1}a) = (ab)(b^{-1}a^{-1}) && = [a,b], \text{ by paramedial law.} \\
[a,b^{-1}] &= (ab^{-1})(ba^{-1}) = (ab)(b^{-1}a^{-1}) && = [a,b], \text{ by medial law.} \\
[a^{-1},b^{-1}] &= (a^{-1}b^{-1})(ba) = (ab)(b^{-1}a^{-1}) && = [a,b].
\end{aligned}
$$

□

This allows us to show a number of more general equalities for commutators.

Theorem 81. *In an AG-group G, the following identities hold.*

(i) $[a,b][c,d] = [ac,bd]$

(ii) $[ab,c] = [cb,a]$

(iii) $[a,bc] = [b,ac]$

(iv) $[a^g,b^g] = [b,a]$

(v) $[a,b]^a = [b,e]$

(vi) $[a,b]^b = [b,ba]$

(vii) $[a,b]^g = [g,ba]$

(viii) $(a^b)^c = (ab)(b^{-1})^c = [b,c]a$

(ix) $a^{bc} = a[c,b]$

(x) $a^b a^c = a^2[c,b]$.

Proof.

(i)

$$
\begin{aligned}
[a,b][c,d] &= \{(ab)(b^{-1}a^{-1})\}\{(cd)(d^{-1}c^{-1})\} \\
&= \{(ab)(cd)\}\{(b^{-1}a^{-1})(d^{-1}c^{-1})\} \\
&= \{(ac)(bd)\}\{(b^{-1}d^{-1})(a^{-1}c^{-1})\} \\
&= [ac,bd]
\end{aligned}
$$

Both steps follow with the medial law.

(ii)
$$\begin{aligned}[ab,c] &= \{(ab)c\}\{c^{-1}(a^{-1}b^{-1})\}\\ &= \{(cb)a\}\{a^{-1}(c^{-1}b^{-1})\}\\ &= [cb,a]\end{aligned}$$

(iii)
$$\begin{aligned}[a,bc] &= \{a(bc)\}\{(b^{-1}c^{-1})a^{-1}\}\\ &= \{b(ac)\}\{(a^{-1}c^{-1})b^{-1}\}\\ &= [b,ac]\end{aligned}$$

(iv)
$$\begin{aligned}[a^g,b^g] &= [(ga)g^{-1},(gb)g^{-1}]\\ &= (((ga)g^{-1})((gb)g^{-1}))(((gb)g^{-1})^{-1}((ga)g^{-1})^{-1})\\ &= (((ga)g^{-1})((gb)g^{-1}))((g^{-1}b^{-1})g)((g^{-1}a^{-1})g)\\ &= (((g^{-1}a)g)((gb)g^{-1}))((gb^{-1})g^{-1})((g^{-1}a^{-1})g)\\ &= (((g^{-1}a)g)((gb)g^{-1}))((gb^{-1})g^{-1})((g^{-1}a^{-1})g)\\ &= ((g^{-1}g)(ab)e)((gg^{-1})(b^{-1}a^{-1})e)\\ &= ((ab)e)((b^{-1}a^{-1})e) = (b^{-1}a^{-1})(ab)\\ &= (ba)(a^{-1}b^{-1})\\ &= [b,a].\end{aligned}$$

(v)
$$\begin{aligned}[a,b]^a &= (a[a,b])a^{-1}\\ &= (a\{(ab)(b^{-1}a^{-1})\})a^{-1}\\ &= ((ab)\{a(b^{-1}a^{-1})\})a^{-1}\\ &= ((ab)\{b^{-1}(aa^{-1})\})a^{-1}\\ &= ((ab)\{b^{-1}(e)\})a^{-1}\\ &= (b^{-1}\{(ab)e\})a^{-1}\\ &= (b^{-1}(ba))a^{-1}\\ &= (a^{-1}(ba))b^{-1}\\ &= (b(a^{-1}a))b^{-1}\\ &= (b(e))b^{-1}\\ &= (be)(e^{-1}b^{-1})\\ &= [b,e]\end{aligned}$$

(vi)
$$\begin{aligned}
[a,b]^b &= (b[a,b])b^{-1} \\
&= (b\{(ab)(b^{-1}a^{-1})\})b^{-1} \\
&= ((ab)\{b(b^{-1}a^{-1})\})b^{-1} \\
&= \{((b^{-1}a^{-1})b)(ba)\}b^{-1} \\
&= (b^{-1}(ba))((b^{-1}a^{-1})b) \\
&= (b(ba))((b^{-1}a^{-1})b^{-1}) \\
&= [b,ba]
\end{aligned}$$

(vii)
$$\begin{aligned}
[a,b]^g &= (g[a,b])g^{-1} \\
&= (g\{(ab)(b^{-1}a^{-1})\})g^{-1} \\
&= ((ab)\{g^{-1}(b^{-1}a^{-1})\})g \\
&= \{((b^{-1}a^{-1})g^{-1})(ba)\}g \\
&= (g(ba))((b^{-1}a^{-1})g^{-1}) \\
&= [g,ba].
\end{aligned}$$

(viii)
$$\begin{aligned}
(a^b)^c &= \{(ba)b^{-1}\}^c \\
&= [c\{(ba)b^{-1}\}]c^{-1} \\
&= [(ba)(cb^{-1})]c^{-1} \\
&= \{c^{-1}(cb^{-1})\}(ba) \\
&= (ab)\{(cb^{-1})c^{-1}\} \\
&= (ab)(b^{-1})^c
\end{aligned}$$

Second part

$$\begin{aligned}
(a^b)^c &= [c\{(ba)b^{-1}\}]c^{-1} \\
&= [(ba)(cb^{-1})]c^{-1} \\
&= \{c^{-1}(cb^{-1})\}(ba) \\
&= [c(c^{-1}b^{-1})](ba) \\
&= (cb)\{(c^{-1}b^{-1})a\} \\
&= [(acc^{-1}b^{-1})](bc) \\
&= [(bc)(c^{-1}b^{-1})]a \\
&= [b,c]a
\end{aligned}$$

(ix)
$$\begin{aligned} a^{bc} &= \{(bc)a\}(b^{-1}c^{-1}) \\ &= (c^{-1}b^{-1})\{a(bc)\} \\ &= a\{(c^{-1}b^{-1})(bc)\} \\ &= a\{(cb)(b^{-1}c^{-1})\} \\ &= a[c,b] \end{aligned}$$

(x)
$$\begin{aligned} a^b a^c &= \{(ba)b^{-1}\}\{(ca)c^{-1}\} \\ &= \{(ba)(ca)\}(b^{-1}c^{-1}) \\ &= \{(bc)a^2\}(b^{-1}c^{-1}) \\ &= \{a^2(cb)\}(b^{-1}c^{-1}) \\ &= a^2[(cb)(b^{-1}c^{-1})] \\ &= a^2[c,b] \end{aligned}$$

□

Note that (v) and (vi) can be obtained from (vii).

Theorem 82. *The set of all commutators of an AG-group G forms an AG-subgroup of G.*

Proof. Let $G' = \{[a,b], a,b \in G\}$. Clearly $G' \neq \emptyset$ as $[e,e] = e \in G'$. Now let $[a,b],[c,d] \in G'$ then by Theorem 81(i), $[a,b][c,d] = [ac,bd] \in G'$ and by Lemma 22, $[a,b]^{-1} = [a,b] \in G'$. Thus G' is an AG-subgroup of G. □

The AG-subgroup G' obtained in the above theorem is called derived AG-subgroup.

Theorem 83. *An AG-subgroup of G is an abelian group if and only if $G' = e$.*

Proof. Let G be an abelian group then for any $a,b \in G$ we have $[a,b] = (ab)(b^{-1}a^{-1}) = (ba)(b^{-1}a^{-1}) = (bb^{-1})(aa^{-1}) = e$. Hence $G' = e$.

Conversely, let $G' = e$ and let $a,b \in G$ with $[a,b] \in G'$. Then we get $[a,b] = e \Rightarrow (ab)(b^{-1}a^{-1}) = e \Rightarrow (ab)(ba)^{-1} = e \Rightarrow ab = ba$. Therefore G is an abelian group. □

Theorem 84. *Let G be an AG-group and $K \leq G$, then*

(i) G/G' is an abelian group.

(ii) G/K is an abelian group implies $G' \subseteq K$.

Proof. (i) Let $G'a, G'b \in G/G'$ then

$$\begin{aligned}[G'a, G'b] &= \{(G'a)(G'b)\}\{(G'b^{-1})(G'a^{-1})\} = G'\{(ab)(b^{-1}a^{-1})\} \\ &= G'[a,b] = G'.\end{aligned}$$

Therefore G/G' is an abelian group by Theorem 83.

(ii) Let G/K be an abelian group. Then $(Kb)(Ka) = (Ka)(Kb)$ and

$$\begin{aligned}K &= \{\{(Ka)(Kb)\}(Ka^{-1})\}Kb^{-1} \\ &= (Kb^{-1})(Ka^{-1})((Ka)(Kb)) \\ &= K((b^{-1}a^{-1})(ab)) \\ &= K((ba)(a^{-1}b^{-1})) \\ &= K[b,a]\end{aligned}$$

Thus $[b,a] \in K$. Since $[b,a] \in G'$ we have $G' \subseteq K$.

□

Theorem 85. *If a non-associative AG-group is simple then every nontrivial element is of order* 2.

Proof. Let G' be the derived AG-subgroup of G then if $G' = e$ then G is an abelian group which is a contradiction, since G is simple. Thus $G' = G$. But then every element of G' is its own inverse, which implies that every non trivial element of G is of order 2. □

The AG-group of order 8 given in Example 49 is simple. However, the converse of Theorem 85 is not true as the following example shows:

Example 51. *Consider the AG-group G of order* 6*:*

$\cdot$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	5	0	1	2	3	4
2	4	5	0	1	2	3
3	3	4	5	0	1	2
4	2	3	4	5	0	1
5	1	2	3	4	5	0

In G every nontrivial element is of order 2*. Nevertheless G is not simple as $\{0,4,2\} \subsetneq G$ is an AG-subgroup of order* 3*.*

7.3.4 Direct Products of AG-groups

We now investigate direct products of AG-groups. Let A and B be AG-groups with left identities e and e' respectively. The set

$$P = \{(a, b) \mid a \in A, b \in B\}$$

under the multiplication defined by

$$(a, b)(a', b') = (aa', bb')$$

is called **the direct product** of the AG-groups A and B and is denoted by $A \times B$. We say that A and B are the direct factors of $A \times B$.

Clearly P is an AG-group with (e, e') as the identity and (a^{-1}, b^{-1}) as the inverse of $(a, b) \in P$. Similarly, the left invertive law in P follows from the left invertive laws in A and B.

Theorem 86. *Let $A \times B$ be the direct product of the AG-groups A and B. Then the set*

$$\bar{A} = \{(ae, e'); a \in A\}\ ,\ \bar{B} = \{(e, b); b \in B\}$$

are normal AG-subgroups of $A \times B$ isomorphic to A and B, respectively, and $\bar{A} \cap \bar{B} = \{(e, e')\}$.

Proof. Let $\bar{a} = (ae, e')$, $\bar{a}_1 = (a_1 e, e') \in \bar{A}$. Then

$$\begin{aligned}
\bar{a}\bar{a}_1^{-1} &= (ae, e')(a_1 e, e')^{-1} \\
&= (ae, e')(a_1^{-1} e, e') \\
&= ((ae)(a_1^{-1} e), e') \\
&= ((aa_1^{-1})e, e') \\
&= (a_1^{-1} a, e') \in \bar{A}.
\end{aligned}$$

Thus $\bar{A}$ is an AG-subgroup $A \times B$.
Now let $\bar{b} = (e, b)$ and $\bar{b}_1 = (e, b_1)$. Then

$$\begin{aligned}
\bar{b}\bar{b}_1^{-1} &= (e, b)(e, b_1)^{-1} \\
&= (e, b)(e, b_1^{-1}) \\
&= (e, bb_1^{-1}) \in \bar{B}.
\end{aligned}$$

Thus $\bar{B}$ is an AG-subgroup of $A \times B$.

Next, to establish an isomorphism between A and $\bar{A}$ we define a mapping $\phi : A \to \bar{A}$ by

$$\phi(a) = (ae, e'),\ a \in A.$$

Then ϕ is obviously a bijective mapping. Moreover, we have

$$\begin{aligned}\phi(aa') &= ((aa')e, e')\\ &= ((aa')(ee), e')\\ &= ((ae)(a'e), e')\\ &= (ae, e')(a'e, e')\\ &= \phi(a) \cdot \phi(a')\end{aligned}$$

Hence ϕ is an isomorphism between A and $\bar{A}$.

Similarly, to establish an isomorphism between B and $\bar{B}$ we define a mapping $\psi : B \to \bar{B}$ by

$$\psi(b) = (e, b),\ b \in B.$$

Then ψ is obviously a bijective mapping. And moreover we have

$$\begin{aligned}\psi(bb') &= (e, bb')\\ &= (e, b)(e, b')\\ &= \psi(b) \cdot \psi(b').\end{aligned}$$

Hence ψ is an isomorphism between B and $\bar{B}$.

Finally to show that $\bar{A} \cap \bar{B} = \{(e, e')\}$, let $(a, b) \in \bar{A} \cap \bar{B}$, $(a, b) \in \bar{A}$, and $(a, b) \in \bar{B}$. This implies $b = e'$ and $a = e$, respectively.

Hence $(a, b) = (e, e')$. Thus $\bar{A} \cap \bar{B} = \{(e, e')\}$, the identity AG-subgroup of $A \times B$. □

With the above theorem, the AG-groups $A, \bar{A}$ and $B, \bar{B}$ are respectively isomorphic and therefore structurally the same. Identifying $\bar{A}$ with A and $\bar{B}$ with B, we can write a for (ae, e') and b for (e, b).

With this convention, every element of G can be expressed as ab, with $a \in A$ and $b \in B$ because

$$(a, b) = ((ae)e, e'b) = (ae, e')(e, b) = ab.$$

The multiplication rule in $A \times B$ then becomes

$$ab.a'b' = aa' \cdot bb'.$$

Theorem 87. *An AG-group G is the direct product of its AG-subgroups A and B if and only if every element of g of G is uniquely expressed as $g = ab$ with $a \in A$ and $b \in B$.*

Proof. Suppose that G is the direct product of its AG-subgroups A and B. So by definition each $g \in G$ can be expressed as $g = ab$ with $a \in A, b \in B$.

To see that this expression is unique, we assume there exist $a, a' \in A$ and $b, b' \in B$ such that $g = ab = a'b'$. We then have

$$\begin{aligned}(ab)b'^{-1} &= a'\\ (b'^{-1}b)a &= a'\\ b'^{-1}b &= a'a^{-1} \in A \cap B = \{e\}\end{aligned}$$

Hence $a = a'$ and $b = b'$ and thus the expression is unique.

Conversely, suppose every element of G is uniquely expressible as $g = ab$ with $a \in A$ and $b \in B$. It only remains to show that $A \cap B = \{e\}$. For this, let $x \in A \cap B$ then $x \in A$ and $x \in B$. Since $e \in A$ and $e \in B$ and since G is a quasigroup we have $x = ae$ for some $a \in A$ and $x = eb$ for some $b \in B$. Thus x has two expressions and one therefore must have $a = e$ and $b = e$ by hypothesis. Hence $A \cap B = \{e\}$ and G is the direct product of its AG-subgroups A and B. □

Theorem 88. *Suppose G is an AG-group and let $G = A \times B$. Then $G' = A' \times B'$ where G', A', B' are the derived subgroups of G, A and B.*

Proof. Let $[g, g_1] \in G'$ then there exist $a, a_1 \in A$ and $b, b_1 \in B$ such that $g = (a, b), g_1 = (a_1, b_1)$. Then we have

$$\begin{aligned}[g, g_1] &= [(a, b), (a_1, b_1)]\\ &= \{(a, b), (a_1, b_1)\}\{(a_1, b_1)^{-1}(a, b)^{-1}\}\\ &= \{(a, b), (a_1, b_1)\}\{(a_1^{-1}, b_1^{-1})(a^{-1}, b^{-1})\}\\ &= (aa_1, bb_1)(a_1^{-1}a^{-1}, b_1^{-1}b^{-1})\\ &= ((aa_1)(a_1^{-1}a^{-1}), (bb_1)(b_1^{-1}b^{-1}))\\ &= ([a, a_1], [b, b_1]) \in A' \times B'.\end{aligned}$$

Hence $G' = A' \times B'$. □

7.3.5 AG-group Actions

We conclude our study by investigating actions of AG-groups that are defined as follows:

Definition 52. *Let G be an AG-group and X be a set, then a* ***(right) AG-group action*** *of G on X is defined as*

(i) $(xg)h = x(gh)$ *for all* $g, h \in G$ *and* $x \in X$,

(ii) $xe = x$ *for all* $x \in X$.

Theorem 89. *Let G be an AG-group and $H \subseteq G$. Then for all $g, h \in G$*

(i) $(H^g)^h = [g, h]H$,

(ii) $H^{gh} = H[h, g]$.

Proof. Let $g, h \in G$. Then consider

(i)
$$\begin{aligned}
(H^g)^h &= [h\{(gH)g^{-1}\}]h^{-1} \\
&= [(gH)(hg^{-1})]h^{-1} \\
&= [(gh)(Hg^{-1})]h^{-1} \text{ by medial law} \\
&= [h^{-1}(Hg^{-1})](gh) \text{ by left invertive law} \\
&= [H(h^{-1}g^{-1})](gh) \\
&= [(gh)(h^{-1}g^{-1})]H \\
&= [g, h]H
\end{aligned}$$

(ii)
$$\begin{aligned}
H^{gh} &= \{(gh)H\}(gh)^{-1} \\
&= \{H(gh)\}(g^{-1}h^{-1}) \\
&= \{(gh)g^{-1}\}(Hh^{-1}) \\
&= H[\{(gh)g^{-1}\}h^{-1}] \\
&= H[(h^{-1}g^{-1})(gh)] \\
&= H[(hg)(g^{-1}h^{-1})] \\
&= H[h, g]
\end{aligned}$$

□

Theorem 90. *Let G be an AG-group and $H \leq G$. Then for all $g, h \in G$*

$$H^{gh} = [g, h]H.$$

Proof. Let $g, h \in G$. Then consider

$$\begin{aligned} H^{gh} &= \{(gh)H\}(gh)^{-1} \\ &= \{H(hg)\}(g^{-1}h^{-1}) \\ &= \{(g^{-1}h^{-1})(hg)\}H \\ &= \{(gh)(h^{-1}g^{-1})\}H \\ &= [g, h]H \end{aligned}$$

□

Corollary 40. *Let G be an AG-group and $H \leq G$. Then G acts on H by conjugation.*

Proof. By Theorem 89 and Theorem 90 we have $(H^g)^h = H^{gh}$. Furthermore with $H \leq G$ we have

$$H^e = (eH)e^{-1} = He = H$$

□

Theorem 91. *Let G be an AG-group and $H \leq G$. Then G acts on H on the right.*

Proof. Let $x, y \in G$ then

$$(H^x)^y = (Hx)^y = (Hx)y = H(xy) = H^{xy}$$

and

$$H^e = He = H.$$

□

For the following we define the coset space of G with respect to an AG-subgroup H as $cos(G : H) = \{Hx | x \in G\}$.

Theorem 92. *If $H \trianglelefteq G$ then G acts on coset space $cos(G : H)$ on the right transitively.*

Proof. Let $Hx \in cos(G:H)$ and $g, h \in G$. Then we have

$$\begin{aligned}
\{(Hx)^g\}^h &= \{(Hx)g\}h \\
&= H\{(xg)h\} \\
&= H\{(hg)x\} \\
&= (hg)(Hx) \\
&= (xH)(gh) \\
&= (Hx)(gh), \text{ since } H \trianglelefteq G \\
&= (Hx)^{gh}
\end{aligned}$$

We also have that

$$(Hx)^e = (Hx)e = (ex)H = xH = Hx.$$

Now to show $cos(G:H)$ is transitive G-space. For this let $Hx, Hy \in cos(G:H)$. Then there exits $yx^{-1} \in G$ such that

$$(Hx)^{yx^{-1}} = (Hx)(yx^{-1}) = H\{x(yx^{-1})\} = H(ye) = yH = Hy$$

Hence the coset space is transitive. □

AG-group actions generally behave differently to group actions. For example the following three natural group actions given in [104, Page 106, Example 3.26] are not necessarily AG-group actions. Let G be an AG-group, let $\Omega = G$ and let actions ω^g with $\omega \in \Omega$ be defined as:

(i) $\omega^g = \omega g$: Then $(\omega^g)^h = (\omega g)\, h = (hg)\, \omega \neq (\omega)\, gh = \omega^{gh}$.

(ii) $\omega^g = g^{-1}\omega$: Then $(\omega^g)^h = h^{-1}\,(g^{-1}\omega) \neq (g^{-1}h^{-1})\omega = (gh)^{-1}\,\omega = \omega^{gh}$.

(iii) $\omega^g = (g\omega)g^{-1}$: Then

$$\begin{aligned}
(\omega^g)^h &= \left[h\left\{(g\omega)g^{-1}\right\}\right]h^{-1} = \left[(g\omega)(hg^{-1})\right]h^{-1} = \left[h^{-1}(hg^{-1})\right](g\omega) \\
&= \left[h(h^{-1}g^{-1})\right](g\omega) = (hg)\left[(h^{-1}g^{-1})\omega\right] = (h^{-1}g^{-1})\left[(hg)\,\omega\right] \\
&\neq \left[(hg)\,\omega\right](h^{-1}g^{-1}) = \left[(hg)\,\omega\right](h^{-1}g^{-1}) = \left[(hg)\,\omega\right](hg)^{-1} = \omega^{gh}.
\end{aligned}$$

Thus neither case satisfies condition (i) of Definition 52.

Definition 53. *Let X be a G-set and let $x \in X$. The AG-subgroup $G_x = \{g \in G | xg = x\}$ is called **isotopy AG-subgroup** of x or **stabilizer AG-subgroup** of x.*

We now investigate the isotopy AG-subgroup G_x for the AG-group actions.

Theorem 93. *Let X be a G-set. Then G_x is an AG-subgroup of G for each $x \in X$.*

Proof. Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $xg_1 = x$ and $xg_2 = x$. Consequently, $x(g_1g_2) = (xg_1)g_2 = xg_2 = x$. So $g_1g_2 \in G_x$, and G_x is closed under the induced operation of G. Of course $xe = x$, so $e \in G_x$.

If $g \in G_x$ then $xg = x$, so $x = xe = x(gg^{-1}) = (xg)g^{-1} = xg^{-1}$, and consequently $g^{-1} \in G_x$. Thus G_x is an AG-subgroup of G. $\square$

Theorem 94. *Let X be a G-set. Then $G_x \trianglelefteq G$.*

Proof. By Theorem 93, $G_x \leq G$. let $g_1 \in G$ and $g \in G_x$ then

$$\begin{aligned} x[(g_1g)g_1^{-1}] &= [x(g_1g)]g_1^{-1} \\ &= [(xg_1)g]g_1^{-1} \\ &= (xg_1)g_1^{-1} \\ &= x(g_1g_1^{-1}) \\ &= xe \\ &= x, \text{ for all } x \in X. \end{aligned}$$

Therefore we have $(g_1g)g_1^{-1} \in G_x$ and hence $G_x \trianglelefteq G$. $\square$

Corollary 41. *Let X be a G-set. Then G/G_x is abelian group.*

Proof. It follows from Theorem 94 and Theorem 78. $\square$

So far all the AG-group actions given in this chapter are right actions and indeed we are not able to find any left actions yet. This motivates the next research question whether there even exist any left AG-group actions.

Chapter 8

A Study of AG-groups as Quasigroups

8.1 Introduction

In this chapter we study AG-group as a special quasigroup, a quasigroup which is also an AG-groupoid having left identity and unique inverses. We see that AG-groups have many properties which other quasigroups do not have and there are several concepts of loops that can be generalized to AG-groups. For example we usually do not assume commutativity and associativity in AG-groups. In [83] it has been proved that commutativity and associativity are equivalent for AG-groups. Also it is easy to see that a non-associative AG-group cannot be idempotent. We also give an infinite family of AG-groups whose members have order of the form $3n, n \geq 2$.

8.2 AG-groups as Invertible Quasigroups

According to [6] a quasigroup is an algebraic structure having a binary multiplication operation $x \cdot y$ usually written xy which satisfies the conditions for any a, b in the quasigroup the equations

$$ax = b \text{ and } ya = b$$

have unique solutions for x and y lying in the quasigroup. A loop is a quasigroup with a nullary operation e called the identity with respect to multiplication, i.e.

$$ex = x \text{ and } xe = x \text{ for all } x.$$

Since AG-groups are always cancellative (see [26] or for another proof see [88]), by [70, Theorem 1.1.3] we can define a finite AG-group as a quasigroup having a nullary operation e with respect to multiplication, called the left identity element, as follows:

$$ex = x \text{ for all } x.$$

Thus the concept of a finite AG-group is a generalization of abelian group and a special case of quasigroup. In Theorem 95, we prove that in fact an AG-group is a quasigroup in the infinite case, too. It follows from the above discussion that in the non-associative case (i.e., in cases other than abelian groups) an AG-group cannot be idempotent, a Steiner quasigroup, or a semi-symmetric quasigroup. However, an AG-group is always a medial quasigroup by Lemma 17 Part(i). Some interesting results are proved such as that for an AG-group G of order n the L_S is an abelian group of order n and its multiplication group is a non-abelian group of order $2n$. The inner mapping group of an AG-group is always a cyclic group of order 2 no matter what its order is.
We recall the axiomatic definition of AG-group. A groupoid G is an *AG-group* if
(i) $(xy)z = (zy)x$ for all $x, y, z \in G$,
(ii) There exists left identity $e \in G$ (that is $ex = x$ for all $x \in G$),
(iii) For all $x \in G$ there exists $x^{-1} \in G$ such that $x^{-1}x = xx^{-1} = e$. x and x^{-1} are called inverses of each other.

8.2.1 Main Results

We will now present the main results of our study.

Theorem 95. *An AG-group G is a quasigroup.*

Proof. The axiomatic definition is given in the introduction. It only remains to show that for any $a, b \in G$ the equations

$$ax = b \text{ and } ya = b$$

have unique solutions for x and y lying in G. Let us consider the first equation $ax = b$. This can be written as $ax = eb$, where e is the left identity in G. From this by Lemma 17 Part(ii), we get $xa = be$. This now by inverses and by Theorem 98 Part(i) implies that $x = (be)a^{-1} \in G$. Let x_1 be another solution then $ax_1 = b = ax$, which by left cancellativity implies that $x = x_1$. The second equation without the application of Lemma 17 Part(ii) implies the unique solution for y similarly. □

Theorem 96. *Let G be an AG-group. Then G is an abelian group if any one of the following holds:*

(i) G is flexible.

(ii) G is left alternative.

(iii) G is right alternative.

Proof. (i) Suppose $ab{\cdot}a = a{\cdot}ba \,\forall\, a, b \in G$. Put $b = e$. Then $ae{\cdot}a = a{\cdot}ea = a{\cdot}a$. By right cancellation, we have $ae = a \Rightarrow e$ is the right identity in G. Thus G is an abelian group.

(ii) Suppose $aa \cdot b = a \cdot ab \,\forall\, a, b \in G$. Put $b = e$. Then $aa \cdot e = a \cdot ae \Rightarrow ea \cdot a = a \cdot ae \Rightarrow a \cdot a = a \cdot ae$. By left cancellation, we have $a = ae \Rightarrow e$ is the right identity in G. Thus G is an abelian group.

(iii) Suppose $ab{\cdot}b = a{\cdot}bb \,\forall\, a, b \in G$. Put $b = e$. Then $ae{\cdot}e = a{\cdot}ee \Rightarrow ae{\cdot}e = a{\cdot}e$. By right cancellation, we have $ae = a \Rightarrow e$ is the right identity in G. Thus G is abelian group.

□

Corollary 42. *An AG-group satisfying the left Bol identity is an abelian group.*

Proof. Proof is similar to the previous discussion. □

Theorem 97. *Let G be an AG-group. Then*

(i) Every AG-group G is left nuclear square quasigroup.

(ii) Every right nuclear square AG-group G is an abelian group.

(iii) Every middle nuclear square AG-group G is an abelian group.

Proof. Let G be an AG-group and let $x, y, z \in G$:

(i) By Lemma 17 Part $(xiii)$, $(xx)(yz) = (zy)(xx) = (xx \cdot y)z$. Thus G is left nuclear square.

(ii) Let G be a right nuclear square AG-group. Then by definition, $x(y \cdot zz) = (xy)(zz)$. Put $y = e$. Then $x(e \cdot zz) = (xe)(zz) \Rightarrow x(zz) = (zz)(ex) \Rightarrow x(zz) = (zz)x \Rightarrow x(zz) = (xz)z$. Thus G is right alternative. This by Theorem 96 Part(iii) implies that G is abelian group.

(iii) Let G be a middle nuclear square AG-group. Then by definition, $x(yy \cdot z) = (x \cdot yy)z$. Put $z = e$. Then $x(yy \cdot e) = (x \cdot yy)e \Rightarrow x(ey \cdot y) = (e \cdot yy)x$ $\Rightarrow x(yy) = (yy)x \Rightarrow x(yy) = (xy)y$. Thus G is right alternative, which by Theorem 96 Part(iii) implies that G is an abelian group.

□

Corollary 43. *Every AG-group G satisfies the Jordan identity.*

Proof. By Theorem 97 (i) we have $x^2 \cdot yx = x^2y \cdot x \,\forall\, x, y \in G$ which is the Jordan identity. □

Theorem 98. *Let G be an AG-group, then*

(i) G always satisfies the right inverse property, and

(ii) if G satisfies the left inverse property then G is an abelian group.

Proof. (i) Let G be an AG-group and let $x, y \in G$. Then

$$(xy)y^{-1} = (y^{-1}y)x = ex = x.$$

(ii) Let an AG-group G satisfies left inverse property. Then

$$\begin{array}{rrcll} & y^{-1}(yx) & = & x & \forall x, y \in G. \\ \Longrightarrow & (yx)y^{-1} & = & xe & \text{by Lemma 17 Part}(ii) \\ \Longrightarrow & yx & = & (xe)y & \text{by right inverse property} \\ \Longrightarrow & yx & = & (ye)x & \text{by left invertive law} \\ \Longrightarrow & y & = & ye & \text{by right cancellation} \end{array}$$

Hence G is an abelian group.

□

Corollary 44. *An AG-group G that satisfies the Moufang identity, the C-identity, or the extra identity is an abelian group.*

According to [22], a quasigroup can have the inverse property. On the other hand, AG-groups are examples of quasigroups that always have the right inverse property but can never have the left inverse property if it is non-associative.

We now discuss left central (LC) and right central (RC) identities for loops. We thereby concentrate on the following 8 LC- and RC-identities (4 each) that have been collected in [25] and were studied by Fenyves [18, 19] and Philips and Vojtěchovský [73, 71, 72]. We follow the ordering of the identities as given in [25]:

(1)	$xx \cdot yz = (x \cdot xy)z$	left central identity
(2)	$(x \cdot xy)z = x(x \cdot yz)$	left central identity
(3)	$(xx \cdot y)z = x(x \cdot yz)$	left central identity
(4)	$yz \cdot xx = y(zx \cdot x)$	right central identity
(5)	$(yz \cdot x)x = y(zx \cdot x)$	right central identity
(6)	$(yz \cdot x)x = y(z \cdot xx)$	right central identity
(7)	$(y \cdot xx)z = y(x \cdot xz)$	left central identity
(8)	$(yx \cdot x)z = y(xx \cdot z)$	right central identity

Consider an AG-group G with one of the above identities. Taking $y = e$ in equations (3)–(8) yields one of the identities from Theorem 96 and hence G is an abelian group. In equation (1) taking $y = e$ and then applying cancellation laws shows that e is also a right identity and therefore G is an abelian group.

All the LC-identities and all the RC-identities are equivalent among themselves for loops. But for AG-groups (and hence for quasigroups) they are not equivalent because an AG-group G satisfying equation (2) does automatically become an abelian group. The following examples demonstrate that we can have (a) non-associative AG-groups that satisfy equation (2), (b) non-associative AG-groups that do not satisfy (2), as well as (c) non-associative quasigroups that satisfy (2) but are not necessarily AG-groups.

Example 52. *A non-associative AG-group of order* 4 *satisfying* (2)*:*

$\cdot$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	3	2	0	1
3	2	3	1	0

Example 53. *A non-associative AG-group of order* 5 *not satisfying* (2)*:*

$\cdot$	0	1	2	3	4
0	0	1	2	3	4
1	2	0	4	1	3
2	1	3	0	4	2
3	4	2	3	0	1
4	3	4	1	2	0

Example 54. *A non-associative quasigroup of order* 6 *satisfying* (2) *that is not an AG-group:*

$\cdot$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	4	5	3
2	2	0	1	5	3	4
3	4	5	3	1	2	0
4	5	3	4	2	0	1
5	3	4	5	0	1	2

Theorem 99. *(i) The left nucleus N of an AG-group G is an abelian group.*

(ii) The right nucleus of a non-associative AG-group G is empty.

(iii) The middle nucleus of a non-associative AG-group G is empty.

Proof. (i) Clearly $N_\lambda \neq \emptyset$ as $e \in N_\lambda$ since $e(yz) = (ey)z = yz$. Let $a \in N_\lambda \Rightarrow a(yz) = (ay)z \, \forall y, z \in G$.

Consider

$$\begin{aligned}
a^{-1}(yz) &= [(a^{-1}a^{-1})a](yz) && \text{by right inverse property} \\
&= (a^{-1}a^{-1})[a(yz)] && \text{by left nuclear square property} \\
&= (a^{-1}a^{-1})[(ay)z] && \text{since } a \in N_\lambda \\
&= [(a^{-1}a^{-1})(ay)z] && \text{by left nuclear square property} \\
&= [((a^{-1}a^{-1})a)y]z && \\
&= (a^{-1}y)z && \text{by right inverse property} \\
&\Rightarrow a^{-1} \in N_\lambda. &&
\end{aligned}$$

Now let $a, b \in N_\lambda$. Then consider

$$\begin{array}{rcll} (ab)(yz) & = & a[b(yz)] & \text{since } a \in N_\lambda \\ & = & a[(by)z & \text{since } b \in N_\lambda \\ & = & [a(by)]z & \text{since } a \in N_\lambda \\ & = & [(ab)y]z & \text{since } a \in N_\lambda \\ & \Longrightarrow & ab \in N_\lambda. & \end{array}$$

Thus N_λ is an AG-Subgroup of G.

Now let $a, b, c \in N_\lambda$ then clearly $a(bc) = (ab)c$. Since in AG-groups associativity implies commutativity we conclude that N_λ is an abelian group.

(ii) Suppose $N_\rho \neq \emptyset$. Let $a \in N_\rho$ then

$$\begin{array}{rll} & (yz)a = y(za) & \forall y, z \in G \\ \Rightarrow & (yz)a = z(ya) & \text{by Lemma 17 Part(xiii)} \\ \Rightarrow & (yz)a = (zy)a & \text{since } a \in N_\rho \\ \Rightarrow & yz = zy & \text{by cancellation} \\ \Rightarrow & \multicolumn{2}{l}{G \text{ is an abelian group which is a contradiction.}} \end{array}$$

Hence $N_\rho = \emptyset$.

(iii) Suppose $N_\mu \neq \emptyset$. Let $a \in N_\mu$ then

$$\begin{array}{rcl} & (ya)z = y(az) & \forall y, z \in G \\ \Rightarrow & (ya)z = a(yz) & \text{by Lemma 17 Part(xiii)} \\ \Rightarrow & z(ya) = (yz)a & \text{by Lemma 17 Part(ii)} \\ \Rightarrow & [z(ya)]a^{-1} = [(yz)a]a^{-1} & \\ \Rightarrow & [a^{-1}(ya)]z = yz & \text{by left invertive law and right inverse property} \\ \Rightarrow & [y(a^{-1}a)]z = yz & \text{by Lemma 17 Part(xiii)} \\ \Rightarrow & (ye)z = yz & \\ \Rightarrow & ye = y & \text{by right cancellation.} \\ \Rightarrow & \multicolumn{2}{l}{G \text{ is an abelian group, which is a contradiction.}} \end{array}$$

Hence $N_\mu = \emptyset$.

□

In the following theorem we prove that an AG-group G is Right Conjugacy Closed but not Left Conjugacy Closed. For this we are using the definitions given in [5], however adapted to our notation.

Definition 54. *Let G be a groupoid and let $x, y, z \in G$, then we say G is*
Left Conjugacy Closed (LCC)*if* $[x(yx^{-1})](xz) = x(yz),$ *and*
Right Conjugacy Closed (RCC)*if* $(xz)[(z^{-1}y)z] = (xy)z.$

Theorem 100. *An AG-group G is RCC but not LCC.*

Proof. Let G be an AG-group and $x, y, z \in G$, then

(i)
$$\begin{aligned} (xz)[(z^{-1}y)z] &= [z(z^{-1}y)](zx) && \text{by Lemma 17 Part}(v) \\ &= z^2[(z^{-1}y)x] && \text{by Lemma 17 Part}(i) \\ &= [(z^2z^{-1})y)]x && \text{by twice use of Theorem 97 Part}(i) \\ &= (zy)x \\ &= (xy)z \end{aligned}$$

Thus G is RCC.

(ii)
$$\begin{aligned} [x(yx^{-1})](xz) &= x^2[(yx^{-1})z] && \text{by Lemma 17 Part}(i) \\ &= [(xy)e]z && \text{by Lemma 17 Part}(i) \\ &= (yx)z && \text{by left invertive law} \\ &\neq x(yz) \end{aligned}$$

Thus G is not LCC.

□

Theorem 101. *Let G be an AG-group. Then*

(i) $a \in G \Longrightarrow ae = a$ if $a(aa) = (aa)a$.
(ii) The set $H = \{a \in G : a(aa) = (aa)a\}$ forms an abelian group.

Proof. (i) Let $a(aa) = (aa)a$. Then consider $(ae)a^2 = (a^2e)a = a^2a = aa^2$ which by right cancellation implies that $ae = a$.

(ii) Clearly $H \neq \emptyset$ as $e \in H$. Let $a \in H$. Then $a(aa) = (aa)a$. Taking inverses on both sides and applying Lemma 17 Part(ix), we get that $a^{-1} \in H$. Now let $a, b \in H$ then using Lemma 17 Part(i) consider $(ab)^2(ab) = (a^2a)(b^2b) = (aa^2)(bb^2) = (ab)(ab)^2$ which implies that $ab \in H$. Thus H is an AG-subgroup of G. Now by (i), H is an abelian group.

□

Corollary 45. *A* 3*-power associative (and hence power associative) AG-group is an abelian group.*

This corollary can be considered as a second proof of [83, Theorem 6].

Theorem 102. *An AG-group G satisfying the Bruck identity is an abelian group.*

Proof. Let $x, y \in G$. By the Bruck identity, $xy \cdot xy = x(y \cdot yx)$. Put $x = e$, we get $y \cdot y = y \cdot ye$ which by left cancellation implies that $y = ye$. Hence G is an abelian group. $\square$

Since the commutant $C(G)$ (centre in the sense of groups) of non-associative AG-group G is always empty (see [93]), therefore $Z(G)$ (in sense of loops) is also always empty.

8.2.2 Constructing a Family of AG-groups via Quasigroup Extension

Here we present an infinite family of AG-groups. This is obtained through extension of quasigroups. The smallest member of this family is an AG-group of order 6. Let G be a multiplicative AG-group with left identity 1, and A an abelian group written additively with neutral element 0. We call any map $\mu : G \times G \to A$ satisfying $\mu(1, g) = 0$ for every $g \in G$ a factor set. When $\mu : G \times G \to A$ is a factor set, we can define multiplication on $G \times A$ by

$$(g, a)(h, b) = (gh, a + b + \mu(g, h)) \tag{A}$$

It is clear that the resulting groupoid is a quasigroup with left identity $(1, 0)$. We will denote this by (G, A, μ). Additional properties of (G, A, μ) can be enforced by additional requirements on μ.

Lemma 23. *Let $\mu : G \times G \to A$ be a factor set. Then (G, A, μ) is an AG-group iff*

$$\mu(g, h) + \mu(gh, k) = \mu(k, h) + \mu(kh, g) \text{ for every } g, h \in G. \tag{B}$$

Proof. The loop (G, A, μ) is an AG-group iff

$$((g, a)(h, b))(k, c) = ((k, c)(h, b))(g, a)$$

holds for every $g, h \in G$ and every $a, b \in A$. Easy calculation with (A) shows that this happens iff (B) is satisfied.

$\square$

We call a factor set μ satisfying (A) and (B) an AG-factor set. We now use a particular AG-factor set to obtain the construction of the above-mentioned family of AG-groups.

Proposition 10. *Let $n > 1$ be an integer. Let A be an abelian group of order n, and $\alpha \in A$ an element of order 2. Let $G = \{1, u, v\}$ be the AG-group with left identity 1. Define $\mu : G \times G \to A$ by*

$$\mu(x,y) = \begin{cases} \alpha & \text{if } (x,y) = (u,1) \text{ or } (v,1) \text{ or } (v,u), \\ 0 & \text{otherwise} \end{cases}$$

then (G, A, μ) is a AG-group with left nucleus $N_\lambda = \{(1, a) : a \in A\}$.

Proof. The map μ is clearly a factor set. It can be depicted as follows:

μ	1	u	v
1	0	0	0
u	α	0	0
v	α	α	0

The Cayley table of the AG-group G is

$\cdot$	1	u	v
1	1	u	v
u	v	1	u
v	u	v	1

To show that (G, A, μ) is an AG-group, we verify (B). Since μ is a factor set, therefore when $g = 1$ then (B) becomes $\mu(h,k) + \mu(k,h) = \mu(kh, 1)$. If $k = 1$, then both sides of this equation are equal, regardless of the value of h. If $k = u$ then both sides of this equation are equal to α if $h = 1, v$ and to zero when $h = u$. If $k = v$ then both sides of this equation are equal to α if $h = 1, u$ and to 0 when $h = v$.

When $g = u$ then (B) becomes $\mu(u,h) + \mu(uh,k) = \mu(k,h) + \mu(kh,u)$. If $k = 1$, then $\mu(u,h) + \mu(uh,1) = \mu(h,u)$ and both sides of this equation are equal to 0 if $h = 1$ or $h = u$ and equal to α if $h = v$. If $k = u$, then $\mu(u,h) + \mu(uh,u) = \mu(u,h) + \mu(uh,u)$ and both sides of this equation are equal regardless of the value of h. If $k = v$, then $\mu(u,h) + \mu(uh,v) = \mu(v,h) + \mu(vh,u)$ and both sides of this equation are equal to 0 if $h = u$ or $h = v$ and equal to α if $h = 1$. When $g = v$ then (B) becomes $\mu(v,h) + \mu(vh,k) = \mu(k,h) + \mu(kh,v)$. If $k = 1$, then

$\mu(v,h)+\mu(vh,1)=\mu(1,h)+\mu(h,v)$ and both sides of this equation are equal to 0 regardless of the value of h. If $k=u$, then $\mu(v,h)+\mu(vh,u)=\mu(u,h)+\mu(uh,v)$ and both sides of this equation are equal to 0 if $h=u$ or $h=v$ and equal to α if $h=1$. If $k=v$, then $\mu(v,h)+\mu(vh,v)=\mu(v,h)+\mu(vh,v)$ and both sides of this equation are equal, regardless of the value of h. Hence (B) is satisfied and therefore (G,A,μ) is an AG-group. Since from the definition it is clear that (G,A,μ) is non-commutative and hence (G,A,μ) is non-associative, we now have that $((u,a)(u,a))\cdot(v,a)\neq(v,a)\neq(1,a)=(u,a)((u,a)\cdot(v,a))$. This implies that $(u,a)\notin N_\lambda$. Similarly $(v,a)\notin N_\lambda$. Also we have that $(1,a)((h,b)(g,c))=((1,a)(h,b))(g,c)$ for all $h,g\in G$ and $a,b,c\in A$. This implies that $(1,a)$ belongs to left nucleus N_λ. Thus $N_\lambda=\{(1,a);\ a\in A\}$ is the left nucleus of the loop (G,A,μ). □

Corollary 46. *For every natural number n there exists a non-associative AG-group having left nucleus of order n.*

Proof. It is sufficient to show that there is a non-associative AG-group with left nucleus of size 1. But this is true by Example 55. □

Example 55. *An AG-group of order* 3 (*with* $N_\lambda=\{0\}$) :

$\cdot$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Example 56. *The smallest group A satisfying assumptions of Proposition 10 is the* 2*-element cyclic group* $\{0,1\}$*. Following the construction given in Proposition 10 and taking $\alpha=1$, we get the following non-associative AG-group of order* 6*.*

$\cdot$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	2	5	4
2	4	5	0	1	2	3
3	5	4	1	0	3	2
4	2	3	4	5	0	1
5	3	2	5	4	1	0

8.2.3 A Word about Applications of AG-groups

It has been referenced in the literature (for example see [34]) that AG-groupoids have applications in flock theory initiated by M. Naseeruddin [61]. So AG-groups being AG-groupoids should have more applications than mere AG-groupoids.

The following theorem indicates another application of AG-groups.

Theorem 103. *Every AG-group G is a right Bol quasigroup.*

Proof. By Lemma 17 Part $(xiii)$, we have $x((yz)y) = ((xy)z)y \forall\ x, y, z \in G$. Hence G is right Bol quasi group. $\square$

Bol loops and Bol quasigroups have found applications in differential geometry so AG-groups being the subclass of Bol quasigroups should have applications in that area too. Also AG-groups are medial quasigroups, which have applications in geometry see [109, 115, 75] and [92]. All these applications of AG-groups should be explored in more detail in future. And as we are currently only at the beginning of studying AG-groups we envision that once their theory develops more applications for AG-groups are encountered, similar to those of groups, quasigroups, and loops.

8.3 Multiplication Group of an AG-group

Multiplication group and innermapping group of a loop have been investigated in a number of papers for example [16, 65, 28, 66, 67, 63, 62, 64, 9]. This has always been remained the most interesting topic of group theorists in loop theory. Quasigroup does not have innermapping group because it does not have an identity element unless it is not a loop. But an AG-group though not a loop but it has a left identity so it has multiplication group as well as innermapping group. We will prove here some interesting results about the multiplication group and innermapping group of an AG-group that do not hold in case of a loop. For example for an AG-group G of order n the L_S is an abelian group of order n. Its multiplication group is a nonabelian group of order $2n$. The innermapping group of an AG-group is always a cyclic group of order 2 regardless of its order. Let G be an AG-group and $a \in G$ an arbitrary element. Mapping $L_a : G \to G$ defined by $L_a(x) = ax$ is called left translation on G and mapping $R_a : G \to G$ defined by $R_a(x) = xa$ is called right translation on G.

Lemma 24. *Let G be an AG-group. Let $a, b \in G$ and e is left identity in G. Then*

(i) $L_a R_b = R_{ab}$.

(ii) $R_a R_b = L_{ab}$.

(iii) $L_a L_b = R_{(ae)} R_b$.

(iv) $L_a L_b = L_{(ae)b} = L_{(be)a}$.

(v) $R_a L_b = R_{(ae)b}$.

(vi) $L_a L_b = L_b L_a$.

(vii) $R_a L_b = R_b L_a$.

Proof. (i) $L_a R_b(x) = L_a(xb) = a(xb) = x(ab) = R_{ab}(x)$. $\Rightarrow L_a R_b = R_{ab}$.

(ii) $R_a R_b(x) = R_a(xb) = (xb)a = (ab)x = L_{ab}(x)$. $\Rightarrow R_a R_b = L_{ab}$.

(iii) $L_a L_b(x) = L_a(bx) = a(bx) = (ea)(bx) = (xb)(ae) = R_{(ae)}(xb) = R_{(ae)} R_b(x) \Rightarrow L_a L_b = R_{(ae)} R_b$.

(iv) By (ii) and (iii) and left invertive law.

(v) $R_a L_b(x) = R_a(bx) = (bx)a = (bx)(ea) = (ae)(xb) = L_{ae}(xb) = L_{ae} R_b(x) \Rightarrow R_a L_b = L_{ae} R_b \Rightarrow R_a L_b = R_{(ae)b}$ by (i).

(vi) $L_a L_b = L_{(be)a}$ by (iv) $\Rightarrow L_a L_b = L_b L_a$ again by (iv).

(vii) $R_a L_b = R_{(ae)b}$ by (v). $= R_{(be)a}$ by left invertive law. $= R_b L_a$ again by (v). $\square$

Remark 14. *From Lemma 24 we note that if G is an AG-group, then the left translation L_a and the right translation R_a behave like an even permutation and an odd permutation respectively, that is;*

$$L_a L_a = L_a, R_a R_a = L_a, L_a R_a = R_a, R_a L_a = R_a.$$

Definition 55. *Let G be an AG-group. Then the set $L_S = \{L_a : L_a(x) = ax \, \forall \, x \in G\}$ is called* ***left section*** *of G and the set $R_S = \{R_a : R_a(x) = xa \, \forall \, x \in G\}$ is called* ***right*** *section of G.*

Theorem 104. *Let G be an AG-group of order n. Then L_S is an abelian group of order n.*

Proof. By definition $L_S = \{L_a : L_a(x) = ax \,\forall\, x \in G\}$. Let $L_a, L_b \in L_S$ for some $a, b \in G$. Then by Lemma 24 Part(iv), we have $L_aL_b = L_{(ae)b} \in L_S \Rightarrow L_S$ is an AG-groupiod. $L_eL_a = L_{(ee)a} = L_a$ and $L_aL_e = L_{(ae)e} = L_{(ee)a} = L_a$. Therefore L_e is the identity in L_S.

Let $L_a, L_b, L_c \in L_S$. Consider $(L_aL_b)L_c = L_{(ae)b}L_c = L_{[\{(ae)b\}e]c} = L_{(ce)((ae)b)} = L_{(ce)((be)a)} = L_{(ae)((be)c)}$
$= L_aL_{(be)c} = L_a(L_bL_c)$.

Let $L_a \in L_S \Rightarrow a \in G \Rightarrow a^{-1} \in G \Rightarrow a^{-1}e \in G$. Let $a^{-1}e = b$ then $L_b \in L_S$.

Now $L_aL_b = L_{(ae)b} = L_{(ae)(a^{-1}e)} = L_e = L_bL_a \Rightarrow L_b$ is the inverse of L_a. Thus L_S is a group. Since from Lemma 24, we have $L_aL_b = L_bL_a$. Therefore L_S is an abelian group. $\square$

Example 57. *An AG-group of order* 3 :

$\cdot$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

The Multiplication group of the AG-group given in Example 57 is isomorphic to S_3, the symmetric group of degree 3.

$\cdot$	L_0	L_1	L_2	R_0	R_1	R_2
L_0	L_0	L_1	L_2	R_0	R_1	R_2
L_1	L_1	L_2	L_0	R_2	R_0	R_1
L_2	L_2	L_0	L_1	R_1	R_2	R_0
R_0	R_0	R_1	R_2	L_0	L_1	L_2
R_1	R_1	R_2	R_0	L_2	L_0	L_1
R_2	R_2	R_0	R_1	L_1	L_2	L_0

Here $L_S = \{L_0, L_1, L_2\}$ which is an abelian group as the following table shows:

$\cdot$	L_0	L_1	L_2
L_0	L_0	L_1	L_2
L_1	L_1	L_2	L_0
L_2	L_2	L_0	L_1

But $R_S = \{R_0, R_1, R_2\}$ does not form an AG-group as the following table shows:

$\cdot$	R_0	R_1	R_2
R_0	L_0	L_1	L_2
R_1	L_2	L_0	L_1
R_2	L_1	L_2	L_0

Remark 15. *Right section does not form even an AG-groupoid.*

Definition 56. *Let G be an AG-group. The set $\langle L_a, R_a : a \in G\rangle$ forms a group which is called multiplication group of the AG-group G and is denoted by $M(G)$ i.e $M(G) = \langle L_a, R_a : a \in G\rangle$.*

Lemma 24 guarantees that for an AG-group G, $M(G) = \langle L_a, R_a : a \in G\rangle = \{L_a, R_a : a \in G\}$

Theorem 105. *Let G be an AG-group of order n. The set $\{L_a, R_a : a \in G\}$ forms a non-abelian group of order $2n$ which is called multiplication group of the AG-group G and is denoted by $M(G)$ i.e $M(G) = \{L_a, R_a : a \in G\}$.*

Proof. From Lemma 24, it is clear that $M(G)$ is closed. L_e plays the role of identity as $L_aL_e = L_eL_a = L_a$.

$R_aL_e = R_{(ae)e} = R_{(ee)a} = R_a = R_{ea} = L_eR_a$.

Let $L_a \in M(G) \Rightarrow a \in G \Rightarrow a^{-1} \in G \Rightarrow R_{a^{-1}} \in M(G)$ and $R_aR_{a^{-1}} = L_{aa^{-1}} = L_e = L_{a^{-1}a} = R_{a^{-1}}R_a$. Therefore $R_{a^{-1}}$ of R_a is in $M(G)$. Associativity in $M(G)$ follows from the associativity of mappings. Thus $M(G)$ is a group. Note that $M(G)$ is non-abelian because $R_aR_b \neq R_bR_a$. $\square$

The multiplication group of the AG-group given in Example 57 is isomorphic to S_3, the symmetric group of degree 3.

To make things a bit more clearer we consider the following example.

Example 58. *An AG-group of order* 4.

$\cdot$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	3	2	1	0
3	2	3	0	1

Its multiplication group is:

$\cdot$	L_0	L_1	L_2	L_3	R_0	R_1	R_2	R_3
L_0	L_0	L_1	L_2	L_3	R_0	R_1	R_2	R_3
L_1	L_1	L_2	L_3	L_0	R_3	R_0	R_1	R_2
L_2	L_2	L_3	L_0	L_1	R_2	R_3	R_0	R_1
L_3	L_3	L_0	L_1	L_2	R_1	R_2	R_3	R_0
R_0	R_0	R_1	R_2	R_3	L_0	L_1	L_2	L_3
R_1	R_1	R_2	R_3	R_0	L_3	L_0	L_1	L_2
R_2	R_2	R_3	R_0	R_1	L_1	L_2	L_3	L_0
R_3	R_3	R_0	R_1	R_2	L_2	L_3	L_0	L_1

From Example 58 we observe that: (1) The multiplication group of an AG-group is not necessarily dihedral. For example, $(L_1 \cdot R_3)^2 = R_2^2 = L_3 \neq L_0$. So here $M(G)$ is not $D_{4.}$ From Examples 57 and 58 we observe that: (2) The left sections in both the examples are C_3 and C_4 respectively.

Theorem 106. *Let G be an AG-group. Let a be an element of G distinct from e. Then a is self-inverse $\Longleftrightarrow R_a^{-1} = R_a$ is self-inverse.*

Proof. Suppose a is self-inverse. Since $R_a(x) = xa$, then R_a is of order 2 , as $R_a(R_a(x)) = (xa)a = (xa)a^{-1} = x \Longrightarrow R_a^2 = L_e \Longrightarrow R_a^{-1} = R_a$.

Conversely let $R_a^2 = L_e$ then $R_a^2(x) = L_e(x)\,\forall x \in G \Longrightarrow (xa)a = ex = x$. Now by left invertive law, $a^2x = x$. This by right cancellation implies $a^2 = e$ or $a^{-1} = a$. □

Remark 16. *R_a cannot fix all the elements of AG-group G. For if we suppose that R_a fixes all the elements. That is;$R_a(x) = x\,\forall x \in G \Longrightarrow xa = x\,\forall x \in G \Longrightarrow$ a is the right identity and hence G is abelian.*

Theorem 107. *The inner mapping group of every AG-group G is $Inn(G) = \{L_0, R_0\} \cong C_2$.*

Proof. As $R_a(0) = 0a = a$. This implies that only R_0 maps 0 on 0. On the other hand $L_0(0) = 0$ and no other L_a can map 0 on 0. Because let $L_a(0) = 0$ where $a \neq 0$. Then $a0 = 0$. This implies $R_0(a) = 0$. But $R_0(0) = 0$. This implies that R_0 is not a permutation which is a contradiction. Hence $Inn(G) = \{L_0, R_0\} \equiv C_2$. The following table verifies the claim.

$\cdot$	L_0	R_0
L_0	L_0	R_0
R_0	R_0	L_0

Hence the proof. □

Again the following are some quick observations:

(i) The $Inn(G)$ is not necessarily normal in $M(G)$ for example consider the multiplication group of the AG-group given in 58. Here $L_1 \{L_0, R_0\} = \{L_1, R_3\} \neq \{L_1, R_1\} = \{L_0, R_0\} L_1$.

(ii) For every AG-group G, L_S being of index 2 is normal in $M(G)$ and hence $M(G)/L_S \equiv C_2$.

(iii) For every AG-group G, left multiplication group of G coincides with L_S and right multiplication group of G coincides with $M(G)$.

A non-associative quasigroup can be left distributive as well as right distributive but a non-associative AG-group can neither be left distributive nor right distributive as the following theorem shows.

Theorem 108. *Every left distributive AG-group and every right distributive AG-group is abelian group.*

Proof. Let G be a left distributive AG-group. Then $\forall\ a, b, c \in G$, we have

$$\begin{aligned} a(bc) &= (ab)(ac) \\ &= (aa)(bc) \text{ by Lemma 17 Part(i)} \\ \text{which implies that } a &= aa \text{ by right cancellation.} \end{aligned}$$

This further implies that G is an abelian group. The second part is similar. A non-associative quasigroup can be left distributive as well as right distributive but a non-associative AG-group can neither be left distributive nor right distributive as the following theorem shows. □

Theorem 109. *If G is an AG-group then the $M(G)$ cannot be the group of automorphisms of G.*

Proof. Assume that the $M(G)$ is the group of automorphisms of G. It means that every element of $M(G)$ is an automorphism of G. Since $L_a, R_a \in M(G)$ for all $a \in G$. Thus L_a and R_a are both automorphisms of G. So we can write

$$\begin{aligned}(xy)L_a &= (x)L_a \cdot (y)L_a \because L_a \text{ is homomorphism}\\ &\Rightarrow a(xy) = (ax)(ay) \text{ for all } x, y \in G\\ &\Rightarrow G \text{ is left distributive}\end{aligned}$$

Similarly

$$\begin{aligned}(xy)R_a &= (x)R_a \cdot (y)R_a \because R_a \text{ is homomorphism}\\ &\Rightarrow (xy)a = (xa)(ya) \text{ for all } x, y \in G\\ &\Rightarrow G \text{ is right distributive}\end{aligned}$$

and hence G is distributive which is a contradiction to Theorem 108. Hence our supposition was wrong and it is proved that the $M(G)$ of an AG-group G cannot be the group of automorphisms of G. □

Lemma 25. *Let G be an AG-group and $M(G)$ its multiplication group. Let $x, y \in G$ and e is the identity element in G. Then*

(i) $R_x^{-1} = R_{x^{-1}}$;

(ii) $L_x^{-1} = L_{x^{-1}e}$.

Proof. (i) Since G satisfies right inverse property. Therefore

$$\begin{aligned}(yx)x^{-1} &= y\\ &\Rightarrow R_{x^{-1}}R_x(y) = y = L_e(y)\, \forall x, y \in G\\ &\Rightarrow R_{x^{-1}}R_x = L_e\\ &\Rightarrow R_x^{-1} = R_{x^{-1}}.\end{aligned}$$

(ii) By Lemma 24 Part(iv)

$$\begin{aligned}L_xL_{x^{-1}e} &= L_{(xe)(x^{-1}e)} = L_{(xx^{-1})e} = L_e\\ &\Rightarrow L_x^{-1} = L_{x^{-1}e}.\end{aligned}$$

□

Chapter 9

A Study of AG-groups as a Parallelogram Space

9.1 Introduction

AG-groups were first identified in [51] as an important subclass of Abel Grassmann Groupoids. They generalize the concept of abelian groups. They can also be studied in the context of quasigroup and loop theory [94]. In fact, AG-groups can be considered as a special type of quasigroup as proved in the previous chapter.

Recall that a quasigroup is a groupoid $(Q, \cdot)$ such that for any a, b in G the equations

$$a \cdot x = b, \qquad y \cdot a = b$$

have unique solutions for x and y lying in G. $x \cdot y$ is usually written xy. The unique solutions x and y are sometimes denoted by left division and right division as $x = a\backslash b$ and $y = b/a$, respectively.

A quasigroup Q is called medial quasigroup if the identity $ab \cdot cd = ac \cdot bd$ holds. If the additional identity $aa = a$ holds then it is called IM-quasigroup (idempotent medial quasigroups) [111]. By Lemma 17, given below, it is clear that every AG-group is medial. So all the geometric concepts that have been introduced for a medial quasigroup in [109, 115, 75] certainly hold for AG-groups as well. It can be easily verified that an idempotent AG-group is an abelian group and therefore a non-associative AG-group cannot be idempotent and hence cannot be a hexagonal quasigroup [112], GS-quasigroup [110], Steiner quasigroup [69], or quadratical quasigroup [113]. Thus AG-groups are altogether a different subclass of medial quasigroups in contrast to those subclasses of medial quasigroups, in which the concept of geometry has been considered previously.

We first show that if G is an AG-group then given any three points $a, b, c \in G$ there exists a unique $d \in G$ such that a, b, c, d form a parallelogram. In [109] it has been shown that a medial quasigroup Q is a parallelogram space. We give a direct proof in Theorem 111 of this fact for AG-groups using the definition of parallelogram space from [68].

For various types of quasigroups, explicit formulae have been given to express the fourth vertex of a parallelogram as a function of the other three (see [40, 110, 114, 115]). We provide such a formula for AG-groups in Theorem 110 together with an efficient way to compute it.

For some other classes of quasigroup one can provide methods to compute the points of a parallelogram if at least two points are known. In our final result we go beyond this by giving some methods of finding the remaining points of a parallelogram if only one non-trivial point is known.

9.2 Parallelograms

Let Q be a quasigroup. We shall say $a, b, c, d \in Q$ form a parallelogram, denoted by $Par(a, b, c, d)$, if there are points $p, q \in Q$ such that $pa = qb$ and $pd = qc$.

Theorem 110. *Let G be an AG-group and $a, b, c, d \in G$. Then $Par(a, b, c, d)$ holds iff there are $x, y \in G$ such that $xb = a, by = c$ and $b \cdot xy = d$.*

Proof. Let $x, y \in G$ be elements satisfying $xb = a, by = c$ and $b(xy) = d$. Let e denotes the left identity in G. By taking $p = e$ and $q = x$, we see that $pa = qb$ and by Lemma 17 Part(xiii) $pd = b(xy) = x(by) = qc$, i.e., $par(a, b, c, d)$ holds. Now suppose $par(a, b, c, d)$ holds and denote $x = a/b, y = b\backslash c$ then $xb = a$ and $by = c$. According to [3, Corollary 5], for any $p \in G$ there is a unique $q \in G$ such that $pa = qb$ and $pd = qc$. Specially, for $p = e$ we see that $a = qb \Rightarrow q = x$ and $d = qc = xc = x.by = b.xy$. □

In [109], it has been proved that if Q is medial quasigroup then this quaternary relation satisfies the following properties of parallelogram space.

(i) For any three points a, b, c there is one and only one point d such that $Par(a, b, c, d)$.

(ii) If (e, f, g, h) is any cyclic permutation of (a, b, c, d) or of (d, c, b, a), then $Par(a, b, c, d)$ implies $Par(e, f, g, h)$.

(iii) From $Par(a, b, c, d)$ and $Par(c, d, e, f)$ it follows $Par(a, b, f, e)$.

Definition 57. *[68] A parallelogram space is a nonempty set Q with quaternary relation $P \subseteq Q^4$ such that the following conditions are satisfied:*

(P1) If $Par(a, b, c, d)$ holds then $Par(a, c, b, d)$ holds for all $a, b, c, d \in Q$.

(P2) If $Par(a, b, c, d)$ holds then $Par(c, d, a, b)$ holds for all $a, b, c, d \in Q$.

(P3) If $Par(a, b, f, g)$ and $Par(f, g, c, d)$ hold then $Par(a, b, c, d)$ holds for all $a, b, c, d, f, g \in Q$.

(P4) For any three points a, b, c there is one and only one point d such that $Par(a, b, c, d)$ holds.

Again in [109], it has been shown that if Q is medial quasigroup then the structure (Q,Par) is a special case of Desargues systems in the terminology of D. Vakarelov [108] and (Q,P) is a parallelogram space in the terminology of F. Ostermann and T. Schmit [68], where

$$P(a, b, c, d) \Leftrightarrow Par(a, b, d, c) \tag{8}$$

. (Q,Par) is also called the parallelogram space for the sake of simplicity.

For an AG-group G, using definition 57 and (8) we give a direct proof that (G,Par) is a parallelogram space. But first we prove the following lemma.

Lemma 26. *(i) If $Par(a, b, c, d)$ holds then $Par(c, d, a, b)$ holds for all $a, b, c, d \in G$.*

(ii) For any three points a, b, c there is one and only one point d such that $Par(a, b, c, d)$ holds.

Proof. (i) Let $Par(a, b, c, d)$ holds then there exist $p, q \in G$ such that the following holds:

$$\begin{aligned} pa = qb \text{ and } pd = qc &\implies qc = pd \text{ and } qb = pa \\ &\implies Par(c, d, a, b) \end{aligned}$$

(ii) (a) Taking $d = cb^{-1} \cdot a$, we prove that $Par(a, b, c, d)$ holds. So let $p, q \in G$ such that $pa = qb$. Now

$$pd = p(cb^{-1} \cdot a) = cb^{-1} \cdot pa = cb^{-1} \cdot qb = q(cb^{-1} \cdot b) = qc.$$

Thus $Par(a, c, b, d)$ holds.

(b) For uniqueness, let $d_1, d_2 \in G$ be such that $pa = qb$ and $pd_1 = qc, pd_2 = qc$. From last two equations, by left cancellation we have $d_1 = d_2$.

□

Theorem 111. *An AG-group G is a parallelogram space.*

Proof. (P1) Let $P(a,b,c,d)$ holds therefore $Par(a,b,d,c)$ holds. Then by Theorem 110 there exist $x_1, y_1 \in G$ such that

$$x_1 b = a, by_1 = d, b \cdot x_1 y_1 = c \Rightarrow x_1 d = c.$$

Taking $x_2 = ac^{-1}, y_2 = de \cdot c^{-1}$, we have $x_2 c = a, cy_2 = d$, and $c \cdot x_2 y_2 = x_2 \cdot cy_2 = x_2 d = ac^{-1} \cdot d = dc^{-1} \cdot a$
$= dc^{-1} \cdot x_1 b = dx_1 \cdot c^{-1} b = ce \cdot c^{-1} b = bc^{-1} \cdot c = b$.
Thus $Par(a,c,d,b)$ holds and hence $P(a,c,b,d)$ holds.

(P2) Let $P(a,b,c,d)$ holds. That is, $Par(a,b,d,c)$ holds. Then there exist $p, q \in G$ such that the following holds:

$$pa = qb \text{ and } pc = qd \quad \Rightarrow \quad pc = qd \text{ and } pa = qb$$

Thus $Par(c,d,b,a)$ holds and hence $P(c,d,a,b)$ holds.

(P3) Let $P(a,b,f,g)$ and $P(f,g,c,d)$ hold. That is, $Par(a,b,g,f)$ and $Par(f,g,d,c)$ hold. Then by Theorem 110 there exist $x_1, y_1, x_2, y_2 \in G$ such that

$$x_1 b = a, by_1 = g, b \cdot x_1 y_1 = f \Rightarrow x_1 g = f \text{ and } x_2 g = f, gy_2 = d, g \cdot x_2 y_2 = c \Rightarrow x_2 d = c.$$

Taking $x_3 = x_1 = x_2, y_3 = de \cdot b^{-1}$, we have $x_3 b = a, by_3 = d$, and

$$b \cdot x_3 y_3 \quad = \quad x_3 b\{y_3 = x_3 d = x_2 d = c.$$

Thus again by Theorem 110 we have proved that $Par(a,b,d,c)$ holds and hence $P(a,b,c,d)$ holds.

(P4) The proof is similar to Lemma 26(ii) with interchanging $p = q$.
Hence (G, Par) is a parallelogram space. □

Corollary 47. *Let G be an AG-group and let $Par(a,b,c,d)$ holds for some $p, q \in G$. Then*

$$ab^{-1} = p^{-1} q$$

Proof. First we prove that $Par(a, b, c, cq \cdot p^{-1})$ holds. Let $pa = qb$ for some $p, q \in G$. Now

$$p(cq \cdot p^{-1}) = cq \cdot e = qc.$$

Thus $Par(a, b, c, cq \cdot p^{-1})$ holds. Now by Theorem 111 (P4), we have

$$cb^{-1} \cdot a = cq \cdot p^{-1} \implies ab^{-1} \cdot c = p^{-1}q \cdot c$$

Hence by right cancellation, we have proved the claim. □

The above corollary provides us with a method of finding $p, q \in G$ if we know that $Par(a, c, b, d)$ holds. Since G is a quasigroup so for $a, b \in G$ we can find $p^{-1}q$. Then we can find p^{-1} by fixing q arbitrarily and finally we have p as the inverses of p^{-1}. The illustration is done in the following example.

Example 59. Consider the following AG-group of order 12:

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	0	3	2	6	7	4	5	10	11	8	9
2	3	2	1	0	8	11	10	9	4	7	6	5
3	2	3	0	1	10	9	8	11	6	5	4	7
4	6	4	8	10	9	0	11	1	7	2	5	3
5	7	5	11	9	0	8	1	10	3	6	2	4
6	4	6	10	8	11	1	9	0	5	3	7	2
7	5	7	9	11	1	10	0	8	2	4	3	6
8	8	10	6	4	5	2	7	3	11	0	9	1
9	9	11	5	7	3	4	2	6	0	10	1	8
10	10	8	4	6	7	3	5	2	9	1	11	0
11	11	9	7	5	2	6	3	4	1	8	0	10

Let us take $a = 3, b = 7$, then by Theorem 110 we have that $Par(3, 7, 2, 6)$ holds. Now we want that for this parallelogram what p, q actually are. So by using Corollary 47, we can do that in the following way.

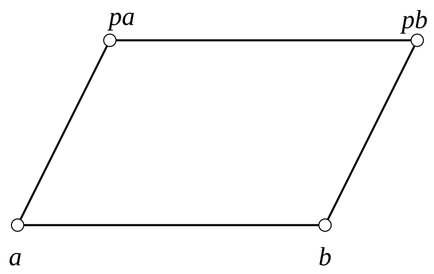
We have $3 \cdot 7^{-1} = p^{-1}q$ which implies that $8 = p^{-1}q$. Now take $q = 10$ (say). So we have $8 = p^{-1} \cdot 10$. this implies that $p^{-1} = 1$. This finally gives that $p = 1^{-1} = 1$. we can check them to be correct as $2 = 1 \cdot 3 = 10 \cdot 7 = 2$ and $4 = 1 \cdot 6 = 10 \cdot 2 = 4$. Had we taken $q = 4$, we would have gotten $p = 3$.

Theorem 111 (P4) provides the fourth point or element d, for any three points elements a, b, c of G to form a parallelogram. The following theorems describes how to form a parallelogram if any two points are given.

Theorem 112. *Let G be an AG-group and $a, b, p \in G$. Then $Par(a, b, pb, pa)$ holds.*

Proof. Let $c = pb, d = pa$. Take $q \in G$ such that $pa = qb$. Now $qc = q(pb) = p(qb) = q(pa) = pd$. Hence $Par(a, b, pa, pb)$ holds. □

The following is a diagrammatic depiction of the result of Theorem 112:



Let us also illustrate the above theorem by an example.

Example 60. *Take arbitrarily $a = 2, b = 7, p = 9$ in Example 59. Then we can find $q = 1$ such that $Par(2, 7, 6, 5)$ holds. Note that $p = 9$ is already understood.*

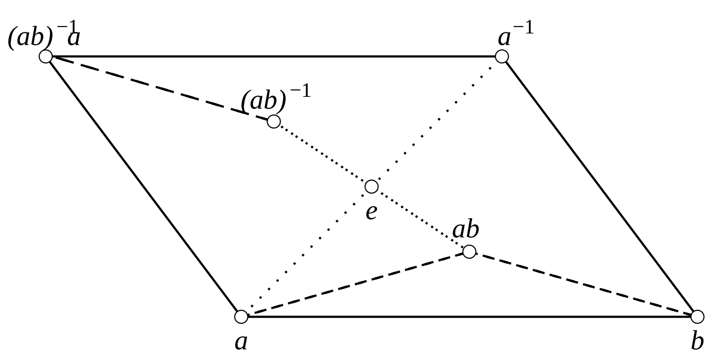
Theorem 113. *Let G be an AG-group. Then $Par(a, b, a^{-1}, (ab)^{-1}a)$ holds.*

Proof. Let $p, q \in G$ such that $pa = qb$.

$$\begin{aligned} \text{Now } qa^{-1} &= [(b^{-1}a)p]a^{-1} \\ &= (a^{-1}p)(b^{-1}a) \text{by invertive law} \\ &= (a^{-1}b^{-1})(pa) \text{ by Lemma 17 Part(i)} \\ &= p[(a^{-1}b^{-1})a] \text{ by Lemma 17 Part(iii)} \\ &= p[(ab)^{-1}a] \text{ by Lemma 17 Part(ix)} \end{aligned}$$

Hence $Par(a, b, a^{-1}, (ab)^{-1}a)$ holds. □

Again we will illustrate the above theorem by a diagrammatic depiction and then by an example.



Example 61. *Take arbitrarily $a = 3, b = 8$ in Example 59. Then $Par(3, 8, 2, 11)$ holds. Here $p = 1$ and $q = 7$.*

Theorem 114. *Let G be an AG-group and let $a, b \in G$ such that $e \neq a$. Then $Par(a, ab, (ae)a^{-1}, b)$ holds*

Proof. Let $p, q \in G$ such that $pa = q(ab)$. Now

$$\begin{aligned} pa &= a(qb) \text{ by Lemma 17 Part(xiii)} \\ ap &= (qb)a \text{ by Lemma 17 Part(ii)} \\ qb &= (ap)a^{-1}\text{by right inverse property} \\ qb &= (ap)(ea^{-1}) \\ qb &= (a^{-1}e)(pa) \text{ by Lemma 17 Part(iv)} \\ qb &= p((a^{-1}e)a) \text{ by Lemma 17 Part(iii)} \\ qb &= p((ae)a^{-1}). \end{aligned}$$

Hence $Par(a, ab, (ae)a^{-1}, b)$ holds. □

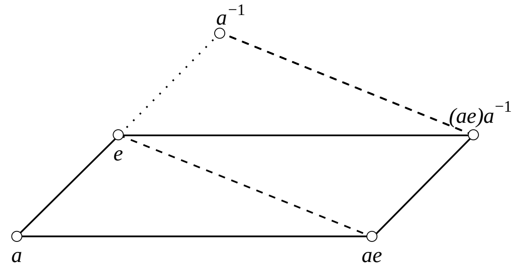
Let us consider the following example.

Example 62. *Take arbitrarily $a = 5, b = 2$ in Example 59. Then $Par(5, 11, 1, 2)$ holds. Here $p = 10$ and $q = 4$.*

The following corollary provides a fast method to compute the parallelogram space for any one non-trivial element of an AG-group G.

Corollary 48. *Let G be an AG-group and let $a \in G$ such that $e \neq a$. Then $Par(a, ae, (ae)a^{-1}, e)$ holds.*

Observe that since e is the left unit element in the AG-group, the element ae is in generally different from a and thus $Par(a, ae, (ae)a^{-1}, e)$ is non-trivial. We again illustrate the corollary with a diagram followed by a concrete example.



Example 63. *Take arbitrarily $a = 6$ in Example 59. Then $Par(6, 4, 1, 0)$ holds. Here $p = 3$ and $q = 2$.*

Theorem 115. *Let G be an AG-group, if $Par(a_1, b_1, c_1, d_1)$ and $Par(a_2, b_2, c_2, d_2)$ then $Par(a_1a_2, b_1b_2, c_1c_2, d_1d_2)$ also holds.*

Proof. Since $Par(a_1, b_1, c_1, d_1)$ and $Par(a_2, b_2, c_2, d_2)$ hold, by Theorem 110 there exist $x_1, y_1, x_2, y_2 \in G$ such that

$$x_1a_1 = b_1, b_1y_1 = c_1, b_1 \cdot x_1y_1 = d_1, x_2a_2 = b_2, b_2y_2 = c_2, b_2 \cdot x_2y_2 = d_2$$

Taking $x_3 = x_1x_2, y_3 = c_2b_1^{-1} \cdot c_1b_2^{-1}$, we have $x_3 \cdot a_1a_2, b_1b_2 \cdot y_3 = c_1c_2$. Now

$$\begin{aligned}
b_1b_2 \cdot x_3y_3 &= (b_1b_2)\{(x_1x_2)(c_2b_1^{-1} \cdot c_1b_2^{-1})\} \\
&= (b_1b_2)\{(x_1x_2)(c_2c_1 \cdot b_1^{-1}b_2^{-1})\} \\
&= (x_1x_2)\{(c_2c_1)(b_1b_2 \cdot b_1^{-1}b_2^{-1})\} \\
&= (x_1x_2)(c_2c_1 \cdot e) \\
&= x_1x_2 \cdot c_1c_2 \\
&= x_1c_1 \cdot x_2c_2 \\
&= (b_1 \cdot x_1y_1) \cdot (b_2 \cdot x_2y_2) \\
&= d_1d_2
\end{aligned}$$

Hence by Theorem 110 we are done. □

Theorem 116. *Let G be an AG-group then the parallelogram space (G, Par) is again an AG-group.*

Proof. Define a binary operation @ on (G, Par) by

$$\begin{aligned}
Par(a_1, b_1, c_1, d_1)@Par(a_2, b_2, c_2, d_2) &= Par(a_1a_2, b_1b_2, c_1c_2, d_1d_2) \\
&\qquad \text{for all } a_1, b_1, c_1, d_{1,}a_2, b_2, c_2, d_2 \in G
\end{aligned}$$

By Theorem 115 (G, Par) is closed under @.

Let $x = Par(a_1, b_1, c_1, d_1), y = Par(a_2, b_2, c_2, d_2), z = Par(a_3, b_3, c_3, d_3) \in (G, Par)$

then

$$\begin{aligned}
(x@y)@z &= [Par(a_1,b_1,c_1,d_1)@Par(a_2,b_2,c_2,d_2)]@Par(a_3,b_3,c_3,d_3) \\
&= Par(a_1a_2,b_1b_2,c_1c_2,d_1d_2)@Par(a_3,b_3,c_3,d_3) \\
&= Par(a_1a_2\cdot a_3,b_1b_2\cdot b_3,c_1c_2\cdot c_3,d_1d_2\cdot d_3) \\
&= Par(a_3a_2\cdot a_1,b_3b_2\cdot b_1,c_3c_2\cdot c_1,d_3d_2\cdot d_1) \\
&= Par(a_3a_2,b_3b_2,c_3c_2,d_3d_2)@Par(a_1,b_1,c_1,d_1) \\
&= [Par(a_3,b_3,c_3,d_3)@Par(a_2,b_2,c_2,d_2)]@Par(a_1,b_1,c_1,d_1) \\
&= (z@y)@x
\end{aligned}$$

Thus (G,Par) is an AG-groupoid under @.
$Par(e,e,e,e)\in(G,Par)$ plays the role of left identity as for all $Par(a,b,c,d)\in(G,Par)$, we have

$$Par(e,e,e,e)@Par(a,b,c,d)=Par(ea,eb,ec,ed)=Par(a,b,c,d)$$

Every element $Par(a,b,c,d)$ in (G,Par) has an inverse $Par(a^{-1},c,b,d)$ as

$$\begin{aligned}
Par(a,b,c,d)@Par(a^{-1},b^{-1},c^{-1},d^{-1}) &= Par(e,e,e,e) \text{ and} \\
Par(a^{-1},b^{-1},c^{-1},d^{-1})@Par(a,b,c,d) &= Par(e,e,e,e)
\end{aligned}$$

Hence $(G,Par,@)$ is an AG-group. □

Corollary 49. *Let G be an abelian group, then $(G,Par,@)$ is an abelian group.*

We can now generalize the above results to the following theorem.

Theorem 117. *Let G be a medial quasigroup, then $(G,Par,@)$ is also a medial quasigroup.*

The proof of this theorem is analogous to that of Theorem 116.

Chapter 10

AG-groups and Other Classes of Right Bol Quasigroups

10.1 Introduction

By a result of Sharma, right Bol quasigroups are obtainable from right Bol loops via an involutive automorphism. We prove that the class of AG-groups, introduced by Kamran, is obtained via the same construction from abelian groups. We further introduce a new class of Bol* quasigroups, which turns out to correspond, as above, to the class of groups.

Sharma's correspondence allows an efficient implementation and we present some enumeration results for the above three classes. It was noticed in [94] that AG-groups belong to the class of right Bol quasigroups. It is well known that right Bol quasigroups and right Bol loops have applications in differential geometry [78]. In [83] enumeration of AG-groups was proposed as an interesting problem. In [86] the enumeration was carried out computationally up to order 12. Here we completely classify AG-groups by showing that every AG-group arises from an abelian group via an involutive automorphism.

Theorem 118. *Suppose G is an abelian group and $\alpha \in \mathrm{Aut}(G)$ satisfying $\alpha^2 = 1$. Define a new binary operation on G by $a \cdot b = \alpha(a) + b$. Then $G_\alpha = (G, \cdot)$ is an AG-group. Furthermore, every AG-group is obtainable in this way. Finally, the AG-groups G_α and H_β are isomorphic if and only if the abelian groups G and H are isomorphic and automorphisms α and β are conjugate.*

This description of the class of AG-groups allows us to classify various subclasses of them. For example, it easily follows from Theorem 118 that the AG-

Order	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Group	1	2	1	1	1	3	2	1	1	2	1	1	1	5	1	2	1	2
Other	1	2	1	1	1	7	3	1	1	6	1	1	3	24	1	3	1	6
Total	2	4	2	2	2	10	4	2	2	8	2	2	4	29	2	5	2	8

Table 10.1: Number of AG-groups of order n, $3 \leq n \leq 20$

group G_α is a group if and only if α is the identity automorphism of the abelian group G. In the similar spirit let an AG-group be called *involutory* if its every element is an involution, that is, it satisfies $a^2 = e$, where e is the (left) identity element. The following is a corollary of Theorem 118.

Theorem 119. *An AG-group G_α is involutory if and only if α is the minus identity automorphism that is $\alpha(g) = -g$ for all $g \in G$. In particular, there is a natural bijection between abelian groups and involutory AG-groups.*

The groups of order one and two are the only cyclic groups for which the identity automorphism is the same as minus identity. In particular, for all orders $n > 2$ there exists a non-associative AG-group.

There have been a lot of publications (see for example, [17]) about the multiplication groups of loops and quasigroups. By definition, the multiplication group $M(Q)$ of a quasigroup Q is the subgroup of $\mathrm{Sym}(Q)$ generated by all left and right translations. The multiplication group of an AG-group was studied in [90] where it was established that for a non-associative AG-group of order n its multiplication group is non-abelian of order $2n$ and, correspondingly, the so called inner mapping group has order two. Based on Theorem 118, we can give a more precise description of the multiplication group.

Theorem 120. *Suppose G_α is a non-associative AG-group, that is, α is non-identity. Then $M(G_\alpha)$ is isomorphic to the semidirect product $G : \langle\alpha\rangle$. Note also that the order two group $\langle\alpha\rangle$ is the inner mapping group $I(G_\alpha)$, that is, the stabilizer in $M(G_\alpha)$ of the identity element.*

The construction of the AG-groups from the abelian groups, as described in Theorem 118, can easily be implemented in a computer algebra system. In fact, we implemented it in GAP [60] and were able to enumerate AG-groups for very large orders n. As just a sample of the computation, we provide here (see Table 10.1) the information about the number of AG-groups up to order 20.

The correspondence between the classes of abelian groups and AG-groups is very simple, so naturally, we were wondering whether a similar construction had been known. And indeed, we found a paper by Sharma [100] establishing a correspondence between the classes of left Bol loops and left Bol quasigroups. By duality, there is a similar correspondence between right Bol loops and right Bol quasigroups. This dual correspondence is essentially the same as our correspondence. Clearly, the class of abelian groups is a subclass of the class of right Bol loops. It is not so immediately clear, but still can be shown that the class of AG-groups is a subclass of the class of right Bol quasigroups. Hence our correspondence is simply a special case of Sharma's correspondence adjusted for the case of right Bol loops. In this sense, our Theorem 118 shows that the class of AG-groups is the counterpart of the class of abelian groups under Sharma's correspondence. On the other hand since the class of AG-groups is a subclass of medial quasigroups so our Theorem 118 turned out to be a special case of Bruck-Toyoda theorem for a special class of medial quasigroups. We consider it an interesting problem to determine which classes of quasigroups are the counterparts of other subclasses of right Bol loops, such as say, the class of groups or the class of Moufang loops. In this chapter we give an answer to the first of these questions, namely, we provide the axioms for the class of quasigroups corresponding to the class of groups.

Definition 58. *A* right Bol* quasigroup *is a quasigroup satisfying*

$$a(bc \cdot d) = (ab \cdot c)d$$

for all elements a, b, c, d.

Note that the substitution $d = b$ turns the above equality into the right Bol law, which shows that the class of the right *Bol** quasigroups is a subclass of right Bol quasigroups. In the future we will just speak of Bol quasigroups and Bol* quasigroups, skipping 'right'.

Theorem 121. *Suppose G is a group and $\alpha \in \mathrm{Aut}(G)$ satisfying $\alpha^2 = 1$. Define a new binary operation on G by $a * b = \alpha(a)b$. Then $G_\alpha = (G, *)$ is a Bol* quasigroup. Furthermore, every Bol* quasigroup is obtainable in this way. Finally, the Bol* quasigroups G_α and H_β are isomorphic if and only if the groups G and H are isomorphic and automorphisms α and β are conjugate.*

10.2 Preliminaries

The following property of AG-groups was established in [83].

Lemma 27. *Every AG-group satisfies the identity $(ab \cdot c)d = a(bc \cdot d)$. In other words, every AG-group is a Bol* quasigroup.*

We now embark on proving Theorem 118. We start with the first claim in that theorem.

Proposition 11. *Let G be an abelian group under addition and let $\alpha \in Aut(G)$ be such that $\alpha^2 = 1$. Define $x \cdot y = \alpha(x) + y$ for all $x, y \in G$. Then $G_\alpha = (G, \cdot)$ is an AG-group with left identity $e = 0$.*

Proof. We start by checking the left invertive law in G_α. Let $x, y, z \in G$. Then $xy \cdot z = \alpha(\alpha(x)+y)+z = \alpha^2(x)+\alpha(y)+z = x+\alpha(y)+z$, since $\alpha^2 = 1$. Similarly, $zy \cdot x = z + \alpha(y) + x$, and so $zy \cdot x = z + \alpha(y) + x = x + \alpha(y) + z = xy \cdot z$.

It is easy to see that 0 is the left identity in G_α. Indeed, $0x = \alpha(0)+x = 0+x$, for all $x \in G$. Finally, we claim that $\alpha(-x)$ is the left inverse of x. Indeed, $\alpha(-x)x = \alpha(\alpha(-x)) + x = -x + x = 0$.

This shows that G_α is an AG-group. □

We next need to show that every AG-group can be obtained as above. Let G be an AG-group with a left identity e. We first show how to build an abelian group from G.

Proposition 12. *Consider the set G together with the new operation $+$ defined as follows:*

$$x + y = xe \cdot y,$$

for all $x, y \in G$. Then $(G, +)$ is an abelian group. The zero element of this group is e and, for every $x \in G$, the inverse $-x$ is equal to $x^{-1}e$.

Proof. We start by checking associativity of addition. Let $x, y, z \in G$. Then $(x + y) + z = (xe \cdot y)e \cdot z$. Using Lemma 27 with $a = xe$, $b = y$, $c = e$, and $d = z$, we get that $(xe \cdot y)e \cdot z = xe \cdot (ye \cdot z) = x+(y+z)$. Therefore, $(x+y)+z = x+(y+z)$, proving associativity.

Commutativity of addition follows essentially by the definition. Indeed, $x + y = xe \cdot y = ye \cdot x = y + x$ by the left invertive law. Similarly, $e + x = ee \cdot x = ex = x$. Now by commutativity e is the zero element of $(G, +)$. Finally,

$x^{-1}e+x = (x^{-1}e)e \cdot x = ((ee)x^{-1})x = ex^{-1} \cdot x = x^{-1}x = e$. Again, commutativity shows that $x^{-1}e$ is the inverse $-x$. □

We remark that in place of the identity e we could use any fixed element $c \in G$. Namely, if we define addition via: $x \oplus y = xc \cdot y$ then we again get an abelian group, whose zero element is c and where the inverses are computed as follows: $\ominus x = x^{-1}c$. The proof is essentially the same. Furthermore, the groups obtained for different elements c are all isomorphic. Namely, the isomorphism between $(G, +)$ and $(G, \oplus)$ is given by $x \mapsto x * c$.

Our next step is to prove that the mapping $\alpha : G \to G$ defined by $g \mapsto ge$ is an involutive automorphism of the abelian group $(G, +)$.

Proposition 13. *For all $x, y \in G$, we have $\alpha(x+y) = \alpha(x)+\alpha(y)$ and, furthermore, $\alpha^2 = 1$. Therefore, α is an involutive automorphism of $(G, +)$.*

Proof. We first note that by the left invertive law $\alpha^2(x) = xe \cdot e = ee \cdot x = ex = x$ for all $x \in G$. Therefore, $\alpha^2 = 1$, the identity mapping on G. By Lemma 27, $\alpha(x + y) = \alpha(xe \cdot y) = (xe \cdot y)e = x(ey \cdot e) = x(ye)$. On the other hand, $\alpha(x) + \alpha(y) = (xe)e \cdot ye$. We saw above that $xe \cdot e = x$, hence $\alpha(x)+\alpha(y) = x(ye)$, which we have shown to be equal to $\alpha(x+y)$. Therefore, α is an automorphism. □

The last two results show that every AG-group G canonically defines an abelian group $(G, +)$ and its involutive automorphism α. It remains to see that the AG-group G can be recovered from $(G, +)$ and α as in Proposition 11.

Proposition 14. *Suppose G is an AG-group and let $(G, +)$ and α be the corresponding abelian group and its involutive automorphism. Then for all $x, y \in G$ we have $xy = \alpha(x) + y$. That is, $G = G_\alpha$.*

Proof. This is clear: indeed, $\alpha(x) + y = (xe \cdot e)y = xy$. We used the identity $xe \cdot e = x$, which we showed before. □

We now turn to homomorphisms between AG-groups.

Proposition 15. *Suppose G and H are abelian groups and let $\alpha \in Aut(G)$ with $\alpha^2 = 1$ and $\beta \in Aut(H)$ with $\beta^2 = 1$. Then the set of homomorphisms between AG-groups G_α and H_β coincides with the set of group homomorphisms $\pi : G \to H$ satisfying $\pi\alpha = \beta\pi$.*

Proof. Suppose $\pi : G_\alpha \to H_\beta$ is a homomorphism of AG-groups, that is, it is a mapping $G \to H$ such that $\pi(gh) = \pi(g)\pi(h)$. By cancellativity, π sends the left identity of G_α to the left identity of H_β. Therefore, for $x, y \in G$, we have $\pi(x + y) = \pi(xe \cdot y) = \pi(xe)\pi(y) = \pi(x)\pi(e) \cdot \pi(y) = \pi(x)e \cdot \pi(y) = \pi(x) + \pi(y)$. This shows that π is a homomorphism of abelian groups. Next, let $x \in G$. Then $\pi\alpha(x) = \pi(xe) = \pi(x)e = \beta\pi(x)$. Since $x \in G$ is arbitrary, we conclude that $\pi\alpha = \beta\pi$.

For the converse, suppose that $\pi : G \to H$ is a homomorphism of abelian groups and that π satisfies $\pi\alpha = \beta\pi$. Then, for $x, y \in G$, we have $\pi(xy) = \pi(\alpha(x) + y) = \pi\alpha(x) + \pi(y) = \beta\pi(x) + \pi(y) = \pi(x)\pi(y)$. Hence π is a homomorphism of AG-groups. $\square$

This allows to complete the proof of Theorem 118.

Corollary 50. *Two AG-groups G_α and H_β are isomorphic if and only if there is an isomorphism π between G and H, satisfying $\pi\alpha\pi^{-1} = \beta$.*

Proof. Immediately follows from Proposition 15. Indeed, if π is bijective then the condition $\pi\alpha = \beta\pi$ is equivalent to $\pi\alpha\pi^{-1} = \beta$. $\square$

We record here a further corollary of Proposition 15, which describes the full automorphism group of the AG-group G_α.

Corollary 51. *The automorphism group of the AG-group G_α coincides with $C_{Aut(G)}(\alpha)$, the centralizer in $Aut(G)$ of the involution α.*

Proof. If $G_\alpha = H_\beta$ (and so $G = H$ and $\alpha = \beta$) then the condition $\pi\alpha = \beta\pi = \alpha\pi$ means simply that $\pi \in Aut(G)$ must commute with α. $\square$

It is interesting that the involutory twist construction can be used repeatedly.

Proposition 16. *Let $(G, \circ)$ be an AG-group with a left identity e. Let $\alpha \in$ $\mathrm{Aut}(G)$ such that $\alpha^2 = 1$. Define $x \cdot y = \alpha(x) \circ y$ for all $x, y \in G$. Then $(G, \cdot)$ is again an AG-group.*

Proof. Initially this had an independent proof. However, with all the theory that we have developed, this result follows easily. Indeed, by Theorem 118, the AG-group $(G, \circ)$ must be equal to G_β, for an abelian group G and its involutory automorphism β.

Note that this means that $x \circ y = \beta(x) + y$, where, as usual, plus indicates addition in the abelian group G. According to Corollary 51, α is an automorphism of the group G commuting with β. In particular, $\gamma = \beta\alpha$ is again an involutory automorphism of G.

We now notice that $x \cdot y = \alpha(x) \circ y = \beta(\alpha(x)) + y = \gamma(x) + y$. This means that $(G, \cdot)$ is simply the AG-group G_γ. $\square$

10.3 Particular Classes of AG-groups

It is natural to ask when the AG-group G_α is associative, that is, a group. It was shown in [83] that for AG-groups associativity is equivalent to commutativity and also to the property that the left identity e is a two-sided identity. We can show that, in fact, G_α is never a group, when $\alpha \neq 1$.

Proposition 17. *Suppose G is an abelian group and $\alpha \in \mathrm{Aut}(G)$ with $\alpha^2 = 1$. Then G_α is a group if and only if $\alpha = 1$.*

Proof. If $\alpha = 1$ then $\alpha(x)+y = x+y$, hence G_α is simply the group G. Conversely, assume that G_α is a group. Note that $e = 0$ is the left identity of G_α, since $0 \cdot x = \alpha(0) + x = 0 + x = x$. However, in a group the left identity is the same as the right identity. Therefore, for all $x \in G$, we must have $x \cdot 0 = x$. However, $x \cdot 0 = \alpha(x) + 0 = \alpha(x)$. Hence, $\alpha(x) = x$ for all $x \in G$, which means that $\alpha = 1$. $\square$

This proof already verifies that G_α is a group whenever it has a two-sided identity. Quite similarly, if G_α is commutative then for every $x \in G$ we have $x \cdot 0 = 0 \cdot x = x$. On the other hand, $x \cdot 0 = \alpha(x) + 0 = \alpha(x)$. Hence we must have that $\alpha(x) = x$ for all $x \in G$, and so $G_\alpha = G$ is a group. This shows that indeed commutativity is also equivalent to associativity.

The second interesting class of AG-groups is the class of involutary AG-groups. Recall from the introduction that an AG-group G is called involutory if its every nontrivial element is an involution, i.e., $x^2 = e$ for all $x \in G$ where e is the left identity of G.

Proposition 18. *Suppose G is an abelian group and $\alpha \in \mathrm{Aut}(G)$ with $\alpha^2 = 1$. Then G_α is an involutory if and only if $\alpha = -1$. (This means that $\alpha(x) = -x$ for all $x \in G$.)*

Proof. Recall that $x \cdot x = \alpha(x) + x$, so $x \cdot x = e = 0$ if and only if $\alpha(x) + x = 0$, that is, $\alpha(x) = -x$, so G_α is involutory if and only if $\alpha(x) = -x$ for all x. $\square$

As a consequence, we get the following.

Corollary 52. *For every order $n \geq 3$ there exists a non-associative AG-group of order n.*

Proof. Indeed, we can take $G = C_n$, the cyclic group of order n, and $\alpha = -1$. When $n \geq 3$, we have $\alpha \neq 1$, which means that G_α is non-associative by Proposition 17. $\square$

Since for every prime order $n = p > 2$ there exists exactly one abelian group, the cyclic group C_p, and since $\mathrm{Aut}(C_p) \cong C_{p-1}$, which has a unique element of order two, we have the following result.

Corollary 53. *For every prime order $n = p \geq 3$, there is only one non-associative AG-group of order n.*

10.4 Some Examples

For illustration of some our results we provide some examples. The case of the prime order has been dealt with in the preceding section.

Example 64. *For order 6, we have only one abelian group, namely C_6. Since $\mathrm{Aut}(C_6)$ has only one nontrivial involution, there are exactly two AG-groups of order 6, one associative, C_6, and one non-associative, namely, $(C_6)_\alpha$, where $\alpha = -1$.*

The same is true for all orders $2p$, where p is an odd prime. So this case is similar to the case of the odd prime order.

Example 65. *For order 12, there are exactly two abelian groups, namely C_{12} and $C_6 \times C_2$. In the first case, $\mathrm{Aut}(C_{12})$ is an elementary abelian group of order four. Hence its every element can be used to construct a new AG-group. This gives us four AG-groups (one associative, one non-associative involutory, and two further non-associative non-involutory). In the second case, $\mathrm{Aut}(C_6 \times C_2)$ is isomorphic to $C_2 \times Sym(3)$, and so is non-abelian of order 12. In addition to the identity element, this group has three conjugacy classes of involutions. Hence, in this case, too, we get four different AG-groups.*

In total, we obtain eight AG-groups of order 12, out of which six are non-associative.

Example 66. *Let us consider the order $2009 = 7^2 \cdot 41$. Again, there are two abelian groups of this order, C_{2009} and $C_{287} \times C_7$. In the first case the automorphism group is abelian, containing three involutions. Hence this group leads* *to four AG-groups. The automorphism group of $C_{287} \times C_7$ is isomorphic to $C_{40} \times GL(2,7)$. This group has five conjugacy classes on involutions in addition to the identity element, hence in this case we obtain six different AG-groups.*

In total, there are 10 different AG-groups of order 2009, out of which eight are non-associative.

10.5 Re-visiting Multiplication Group of an AG-group

The concept of the multiplication group of a loop and, more generally, a quasigroup is well known. In a quasigroup Q, multiplication on the left (or right) by an element $x \in Q$ is a permutation L_x (respectively, R_x) of Q called the *left* (respectively, *right*) *translation* by x. The set of all left translations is called the *left section*, and similarly, the set of right translations is called the *right section* of Q. We will write L_S and R_S for the left and right sections, respectively. Therefore, $L_S = \{L_x \mid x \in Q\}$ and $R_S = \{R_x \mid x \in Q\}$.

The multiplication group $M(Q)$ is the subgroup of the symmetric group $Sym(Q)$ generated by $L_S \cup R_S$. If Q is a loop, the stabilizer in $M(Q)$ of the identity is called the *inner mapping group* and is denoted by $\mathrm{Inn}(Q)$.

Since every AG-group G_α is a quasigroup we can consider its multiplication group $M(G_\alpha)$. Since G_α has a left identity 0, we can generalize the concept of the inner mapping group to the class of AG-groups by setting $\mathrm{Inn}(G_\alpha)$ to be the stabilizer of 0 in $M(G_\alpha)$.

Proposition 19. *Let G be an abelian group and $\alpha \in \mathrm{Aut}(G)$ with $\alpha^2 = 1$. Then the following hold:*

(1) $M(G_\alpha) = L_S \cup R_S$;

(2) $\mathrm{Inn}(G_\alpha) = \langle \alpha \rangle$;

(3) *L_S is a normal subgroup of $M(G_\alpha)$ and it is naturally isomorphic to G;*

(4) *$R_S = \alpha L_S$; and*

(5) *$M(G_\alpha)$ is isomorphic to the semidirect product of G with the cyclic group $\langle \alpha \rangle$.*

Proof. First note that the mapping $\psi : x \mapsto L_x$ is a homomorphism from G to $Sym(G)$. Indeed, $L_{x+y}(z) = (x+y)\cdot z = \alpha(x+y)+z = \alpha(x)+\alpha(y)+z = x\cdot(\alpha(y)+z) = x\cdot(y\cdot z) = L_x(L_y(z))$ for all $z \in G$. This means that L_{x+y} is indeed the product of L_x and L_y. Since ψ is a homomorphism, its image L_S is a subgroup of $\mathrm{Sym}(G)$. Furthermore, if $L_x(z) = z$ for some $z \in G$ then $\alpha(x) + z = z$, which implies that $x = 0$. Therefore, ψ is injective and so it is an isomorphism from G onto L_S.

Next, note that $\alpha(z) = \alpha(z)+0 = z\cdot 0 = R_0(z)$. This means that $\alpha = R_0$ is an element of R_S. Furthermore, $R_x(z) = \alpha(z)+x = \alpha(z)+\alpha^2(x) = \alpha(\alpha(x))+\alpha(z) = \alpha(\alpha(x)+z) = (\alpha L_x)(z)$. This means that $R_x = \alpha L_x$ for all $x \in G$, that is, R_S is the coset of L_S containing α.

We now turn to Part (1). We claim that α normalizes L_S. Indeed, $(\alpha L_x \alpha)(z) = \alpha L_x(\alpha(z)) = \alpha(\alpha(x)+\alpha(z)) = x+z = \alpha(\alpha(x))+z = L_{\alpha(x)}(z)$. Thus, $\alpha L_x \alpha = L_{\alpha(x)}$, proving that α normalizes the subgroup L_S. Since $R_S = \alpha L_S$, we conclude that every element of R_S normalizes L_S, which means that L_S is normal in $M(G_\alpha)$. Also, it means that $M(G_\alpha) = \langle L_S, \alpha\rangle$, which implies that L_S has index at most two in $M(G_\alpha)$. (This proves (1).) To be more precise, the index is two if and only if $\alpha \notin L_S$. Clearly, α fixes 0 and, as we have already seen, the only element of L_S fixing 0 is L_0, the identity element of L_S. Hence L_S has index two in $M(G_\alpha)$ if and only if $\alpha \neq 1$.

From the above, we also have that $|\mathrm{Inn}(G_\alpha)| = |\alpha|$, since L_S is regular on G and so $|\mathrm{Inn}(G_\alpha)|$ is equal to the index of L_S in $M(G_\alpha)$. Since α fixes 0, we have $\alpha \in \mathrm{Inn}(G_\alpha)$, which implies (2). Parts (3) and (4) have already been proven. Finally, since $\alpha \notin L_S$ and $M(G_\alpha) = \langle L_S, \alpha\rangle$, (5) follows as well. □

As an example of how the multiplication group can be used to identify the AG-group, we present the following result.

Theorem 122. *Suppose $M = M(G_\alpha)$ for a non-associative AG-group G_α and $M \cong D_{2n}$. Then either G is the Klein four-group (and so $n = 4$) or $G \cong C_n$ is cyclic. In the latter case $\alpha = -1$, and hence G_α is involutory.*

Proof. First of all, since G_α is non-associative, α is a nontrivial automorphism of G and so $n = |G| \geq 3$. By Proposition 19, the abelian group G is isomorphic to an index two subgroup of M. From this, it immediately follows that either $n = 4$ and G is the Klein four-group, or $n \geq 3$ is arbitrary and G is cyclic. Finally, in the cyclic case, since $M(G_\alpha)$ is isomorphic to the semidirect product of G and $\langle\alpha\rangle$, we conclude that α inverts every element of G and so $\alpha = -1$. □

We also give a general characterization of all groups that arise as multiplication group of an AG-group.

Theorem 123. *A non-abelian group M is isomorphic to a multiplication group of some non-associative AG-group if and only if $M \cong T \rtimes R$ where T is abelian and $|R| = 2$.*

Proof. If $M = M(G_\alpha)$ then $M = G \rtimes \langle\alpha\rangle$ and so all the claimed properties hold. Conversely, suppose $M = T \rtimes R$ where T is abelian and $|R| = 2$. Let $\alpha \in \mathrm{Aut}(T)$ be the automorphism induced by the generator of R on T. Then $M \cong M(T_\alpha)$ by Proposition 19 (5). $\square$

10.6 Sharma's Correspondence

In his paper [100] from 1976 Sharma proved the following theorem. We recall that the identity $(ab \cdot c)b = a(bc \cdot b)$ is known as the right Bol identity. The loops (respectively, quasigroups) satisfying this identity are called the right Bol loops (respectively, right Bol quasigroups).

Theorem 124. *Suppose G is a right Bol loop and $\alpha \in \mathrm{Aut}(G)$ satisfying $\alpha^2 = 1$. Define a new binary operation on G by $a * b = \alpha(a)b$. Then $G_\alpha = (G, *)$ is a right Bol quasigroup. Furthermore, every right Bol quasigroup is obtainable in this way. Finally, the right Bol quasigroups G_α and H_β are isomorphic if and only if the right Bol loops G and H are isomorphic and the automorphisms α and β are conjugate.*

In reality Sharma proved the "left" version of this theorem, but we switched to the above, "right" version because it matches better our own results.

In particular, Sharma's theorem implies that every right Bol quasigroup automatically has a left identity element.

We note that Sharma's construction is essentially the same as ours, except it is done for a different, larger class of objects, the Bol loops instead of abelian groups. In other words, what we proved in Theorem 118 means simply that the class of AG-groups is the counterpart of the subclass of abelian groups under Sharma's correspondence. It would be interesting to ask what are the counterparts of other subclasses of Bol loops, such as, say, groups or Moufang loops. We leave the Moufang loops case as an open question, but we have an answer for the class of groups.

Recall from the introduction that by a *Bol* quasigroup* we mean a quasigroup satisfying

$$a(bc \cdot d) = (ab \cdot c)d$$

for all a, b, c, d. Note that this is clearly a subclass of Bol quasigroups. In particular, every Bol* quasigroup automatically has a left identity element.

Theorem 125. *Suppose G is a group and $\alpha \in \mathrm{Aut}(G)$ satisfying $\alpha^2 = 1$. Define a new binary operation on G by $a * b = \alpha(a)b$. Then $G_\alpha = (G, *)$ is a Bol* quasigroup. Furthermore, every Bol* quasigroup is obtainable in this way. Finally, the Bol* quasigroups G_α and H_β are isomorphic if and only if the groups G and H are isomorphic and the automorphisms α and β are conjugate.*

Proof. Let us first see that G_α as above satisfies the identity

$$a * ((b * c) * d) = ((a * b) * c) * d.$$

Indeed, $a*((b*c)*d) = \alpha(a)(\alpha(\alpha(b)c)d) = \alpha(a)\alpha^2(b)\alpha(c)d = \alpha(a)b\alpha(c)d$, since $\alpha^2 = 1$. Similarly, $((a*b)*c)*d = \alpha(\alpha(\alpha(a)b)c)d = \alpha^3(a)\alpha^2(b)\alpha(c)d = \alpha(a)b\alpha(c)d$. So the identity holds, proving that G_α is a Bol* quasigroup.

Conversely, assume that $(G, *)$ is a Bol* quasigroup with left identity e. For $x \in G$, define $\alpha(x) = x * e$ and also, for $x, y \in G$, define $xy = \alpha(x)y$. We need to see that (1) G with this new product is a group; (2) α is an automorphism of this group of order two; and (3) $(G, *) = G_\alpha$.

First of all, for $x, y, z \in G$, $x(yz) = \alpha(x) * (\alpha(y) * z) = (x * e) * ((y * e) * z)$. By the identity, the latter is equal to $(((x * e) * y) * e) * z$ and this is equal to $(x*((e*y)*e)*z$. On the other hand, $(xy)z = \alpha(\alpha(x)*y)*z = (((x*e)*y)*e)*z$, so we have $x(yz) = (xy)z$ for all $x, y, z \in G$, proving that the new operation is associative. Cancellativity is clear, so we have an associative quasigroup, hence a group. Note that e is the identity element of the group, since $ex = \alpha(e) * x = (e * e) * x = e * x = x$.

For (2), we first need to show that α is a permutation of order two: $\alpha^2(x)*z = ((x * e) * e) * z = x * ((e * e) * z) = x * z$, and so by cancellativity, $\alpha^2(x) = x$. Thus, $\alpha^2 = 1$. To show that α is an automorphism, we compute: $\alpha(xy) = (xy) * e = (\alpha(x) * y) * e = ((x * e) * y) * e = x * ((e * y) * e) = x * (y * e)$ and $\alpha(x)\alpha(y) = \alpha(\alpha(x)) * \alpha(y) = x * (y * e)$. Thus, $\alpha(xy) = \alpha(x)\alpha(y)$. Finally, (3) is clear since $x * y = \alpha^2(x) * y = \alpha(x)y$. Hence $x * y = \alpha(x)y$, which means that $(G, *) = G_\alpha$.

Order	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Group	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5
Non-group	1	2	1	2	1	12	3	2	1	14	1	2	3	88	1	9	1	13
Total	2	4	2	4	2	17	5	4	2	19	2	4	4	102	2	14	2	18

Table 10.2: Number of Bol* quasigroups of order n, $3 \leq n \leq 20$

Order	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bol loop	1	2	1	1	1	3	1	1	1	2	1	1	1	5
Other	1	2	1	1	1	7	3	1	1	6	1	1	3	24
Total	2	4	2	4	2	41	5	4	2	23	2	4	10	16581

Order	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Bol loop	1	2	1	1	1	3	1	1	1	2	1	1	1	5
Other	1	2	1	1	1	7	3	1	1	6	1	1	3	24
Total	2	16	2	30	12	4	2	≥ 713	5	4	36	28	2	≥ 22

Table 10.3: Number of Bol quasigroups of order n, $3 \leq n \leq 30$

For the final claim in the theorem, we note that the proofs of Proposition 15 and Corollary 51 depend neither on commutativity of the group operation, nor on the left invertive identity, so they fully apply in our present case. □

The package AGGROUPOIDS mentioned above also contains functions enumerating Bol* quasigroups and Bol quasigroups based on Theorem 125 and Sharma's Theorem 124. In Tables 10.2 and 10.3 we provide the counting for the Bol* quasigroups and Bol quasigroups up to order 20 and 30, respectively.

It might be worth mentioning that we can enumerate Bol* quasigroups for much larger orders, as long as the list of groups of that order is available. For Bol quasigroups, we can only go up to the order 31, as the list of Bol loops of order 32 is an open problem.

Chapter 11

AG-monoids from Commutative Monoids

In this chapter we provide the rigorous foundation for the counting of AG-monoids. It is based on the following result.

Theorem 126. *Suppose* $(S,+)$ *is a commutative monoid and suppose* $\alpha \in \mathrm{Aut}(S)$ *satisfies* $\alpha^2 = 1$*. Let the product be defined on* S *by* $a \cdot b = \alpha(a) + b$*. Then* $(S,\cdot)$ *is an AG-monoid. Furthermore, every AG-monoid can be obtained in this way from a unique pair* (S,α)*.*

Proof. First, suppose that $(S,+)$ is a commutative monoid and $\alpha \in \mathrm{Aut}(S)$ with $\alpha^2 = 1$. Let us check that the new product $\cdot$ satisfies the left invertive law.

Let $x, y, z \in S$. Then $(x \cdot y) \cdot z = \alpha(\alpha(x)+y)+z = \alpha^2(x)+\alpha(y)+z = x+\alpha(y)+z$, since $\alpha^2 = 1$. Since also $(z \cdot y) \cdot x = z+\alpha(y)+x = x+\alpha(y)+z$ by commutativity, we conclude that $(x \cdot y) \cdot z = (z \cdot y) \cdot x$. In order to show that $(S,\cdot)$ is an AG-monoid it remains to check that 0 is a left identity. Taking $x \in S$, we get $0 \cdot x = \alpha(0) + x = 0 + x = x$, and the first claim is proven.

For the second claim we need to show that, given an arbitrary AG-monoid $(S,\cdot)$ (where the left identity is denoted by 0), we can recover from it a suitable commutative monoid $(S,+)$ and an involutive automorphism α.

Define $\alpha : S \to S$ by $\alpha(x) = x \cdot e$. Furthermore, define addition on S by $x + y := \alpha(x) \cdot y$. We need to see that $(S,+)$ is a commutative monoid and that α is an automorphism of it, as above.

We start by showing that $+$ satisfies commutativity. Using left invertive law, we have $x + y = \alpha(x) \cdot y = (x \cdot 0) \cdot y = (y \cdot 0) \cdot x = \alpha(y) \cdot x = y + x$. For associativity, recall that AG-monoids (being an AG-groupoid) satisfy the medial law $(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$, which implies, together with the left identity property, that $a \cdot (b \cdot c) = b \cdot (a \cdot c)$ for all $a, b, c \in S$.

Now, using left invertive law and $a \cdot (b \cdot c) = b \cdot (a \cdot c)$, we get $(x + y) + z = ((x \cdot 0) \cdot y) + z = (((x \cdot 0) \cdot y) \cdot 0) \cdot z = (z \cdot 0) \cdot ((x \cdot 0) \cdot y) = (x \cdot 0) \cdot ((z \cdot 0) \cdot y) = (x \cdot 0) \cdot ((y \cdot 0) \cdot z) = x + ((y \cdot 0) \cdot z) = x + (y + z)$. Hence $(S, +)$ is associative. It remains to see that 0 is the identity of $(S, +)$. Indeed, $0+x = (0\cdot 0)\cdot x = 0\cdot x = x$, since 0 is the left identity of $(S, \cdot)$. Thus, by commutativity of addition we have $x + 0 = 0 + x = x$. We have shown that $(S, +)$ is a commutative monoid.

Turning to α, notice that $\alpha^2(x) = (x \cdot 0) \cdot 0 = (0 \cdot 0) \cdot x = 0 \cdot x = x$ for every $x \in S$. Therefore, $\alpha^2 = 1$, which in particular means that α is bijective. Also, $\alpha(x+y) = (x+y)\cdot 0 = ((x\cdot 0)\cdot y)\cdot 0$. By the left invertive law, the latter is equal to $(0\cdot y)\cdot(x\cdot 0) = y\cdot(x\cdot 0)$. On the other hand, $\alpha(x)+\alpha(y) = ((x\cdot 0)\cdot 0)\cdot(y\cdot 0) = ((y \cdot 0) \cdot 0) \cdot (x \cdot 0) = ((0 \cdot 0) \cdot y) \cdot (x \cdot 0) = (0 \cdot y) \cdot (x \cdot 0) = y \cdot (x \cdot 0)$. Thus, $\alpha(x + y) = \alpha(x + \alpha(y))$, which shows that α is an involutive automorphism of $(S, +)$.

Finally, $x \cdot y = \alpha^2(x) \cdot y = \alpha(x) + y$. This shows that $(S, \cdot)$ can be recovered from $(S, +)$ in the prescribed way. Clearly, both $(S, +)$ and α were recovered from $(S, \cdot)$ in a canonical way, which means that this pair is unique for $(S, \cdot)$. $\square$

We now illustrate our construction with an example.

Example 67. *We start with the following commutative monoid S:*

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	5	2	3	4	0
2	2	2	2	3	3	2
3	3	3	3	3	3	3
4	4	4	3	3	4	4
5	5	0	2	3	4	1

It can be checked that the permutation $\alpha = (1, 5)(2, 4)$ is an automorphism of this commutative monoid, and it clearly has order two. Applying this α to $(S, +)$ we get the following non-associative AG-monoid.

Example 68.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	5	0	2	3	4	1
2	4	4	3	3	4	4
3	3	3	3	3	3	3
4	2	2	2	3	3	2
5	1	5	2	3	4	0

In order to be able to count the number of non-isomorphic AG-monoids we need to make the uniqueness claim in Theorem 126 even more precise, as follows.

Theorem 127. *Suppose $(S,+)$ and $(S',+)$ are two commutative monoids and let $\alpha \in \mathrm{Aut}(S)$, $\alpha' \in \mathrm{Aut}(S')$ be their involutive automorphisms. Finally, let $(S,\cdot)$ (respectively, $(S',\cdot)$) be the AG-monoid derived from S and α (respectively, S' and α'). Then a mapping $\phi : S \to S'$ is an isomorphism of $(S,\cdot)$ onto $(S',\cdot)$ if and only if ϕ is an isomorphism of $(S,+)$ onto $(S',+)$ and, furthermore, $\phi\alpha = \alpha'\phi$.*

Proof. We first assume that ϕ is an isomorphism from $(S,\cdot)$ onto $(S',\cdot)$. Then, for $x, y \in S$, we have $\phi(x)+\phi(y) = (\phi(x)\cdot 0')\cdot\phi(y)$, where $0'$ is the left identity in S'. Note that the left invertive law implies that every AG-monoid has a unique left identity, which means that $0' = \phi(0)$, where 0 is the left identity of S. Therefore, $(\phi(x)\cdot 0')\cdot\phi(y) = (\phi(x)\cdot\phi(0))\cdot\phi(y) = \phi((x\cdot 0)\cdot y) = \phi(x+y)$. We have shown that ϕ is an isomorphism of $(S,+)$ onto $(S',+)$.

Also, $\phi(\alpha(x)) = \phi(x\cdot 0) = \phi(x)\cdot\phi(0) = \phi(x)\cdot 0' = \alpha'(\phi(x))$. Since this is true for all $x \in S$, we conclude that $\phi\alpha = \alpha'\phi$, as claimed.

Conversely, suppose that ϕ is an isomorphism of $(S,+)$ onto $(S',+)$ satisfying $\phi\alpha = \alpha'\phi$. Then, first of all, $\phi(0) = 0'$, as these are the unique identity elements in the respective commutative monoids. Thus, $\phi(x\cdot y) = \phi(\alpha(x)+y) = \phi(\alpha(x)) + \phi(y) = \alpha'(\phi(x)) + \phi(y) = \phi(x)\cdot\phi(y)$, proving that ϕ is an isomorphism of $(S,\cdot)$ onto $(S',\cdot)$. ☐

As a consequence, we immediately get the following.

Corollary 54. *Suppose $(S,+)$ is a commutative monoid and $\alpha, \alpha' \in \mathrm{Aut}(S)$ satisfy $\alpha^2 = 1 = (\alpha')^2$. Then the AG-monoids obtained from S and α, and from S and α' are isomorphic if and only if α and α' are conjugate in $\mathrm{Aut}(S)$.*

We omit the proof. It is easy to see that an AG-group is associative if and only if it is commutative and if and only if the left identity in it is a two sided identity. A further equivalent condition is that $\alpha = 1$. In particular, the number of non-associative AG-monoids obtainable from a particular commutative monoid S is equal to the number of conjugacy classes of involutive (nonidentity) automorphisms in $\mathrm{Aut}(S)$.

The number of non-isomorphic commutative monoids is known up to order 10. The list up to order 8 is available in the SMALLSEMI package under GAP. Using functions from the package AGGROUPOIDS we were able to apply the above method to all those commutative monoids which resulted in Table 11.

Order	3	4	5	6	7	8
Commutative monoids	5	19	78	421	2637	20486
Non-associative AG-monoids	1	6	29	188	1359	11386
Total	6	25	107	609	3996	31872

Table 11.1: Number of AG-monoids of order n, $3 \leq n \leq 8$

Chapter 12

AG-GROUPOIDS: A GAP Package

In this chapter we describe some of the commands of our under construction GAP package AG-GROUPOIDS. We hope that the entire package (not limited to these functions) will shortly be available from the GAP repository.

12.1 Testing Cayley Tables

- `IsAGGroupoidTable(M)`
  Returns true if M is a Cayley table of AG-groupoid and returns false otherwise.

Remark 12.1.1. The first eight types are those which already exist. The remaining types are those which have been defined in this thesis.

The following commands return true if the AG-groupoid table M is a specific type of AG-groupoid and returns false otherwise.

- `IsCancellativeAGGroupoidTable(M)`
- `IsAGMonoidTable(M)`
- `IsAGGroupTable(M)`
- `IsAGBandTable(M)`
- `IsAG3BandTable(M)`
- `IsLocallyAssociativeAGGroupoidTable(M)`
- `IsStarAGGroupoidTable(M)`
- `Is2StarAGGroupoidTable(M)`
- `IsLeftNuclearSquareAGGroupoidTable(M)`

- `IsRightNuclearSquareAGGroupoidTable(M)`
- `IsMiddleNuclearSquareAGGroupoidTable(M)`
- `IsNuclearSquareAGGroupoidTable(M)`
- `IsT1AGGroupoidTable(M)`
- `IsT2AGGroupoidTable(M)`
- `IsT3LAGGroupoidTable(M)`
- `IsT3RAGGroupoidTable(M)`
- `IsT3AGGroupoidTable(M)`
- `IsT4FAGGroupoidTable(M)`
- `IsT4BAGGroupoidTable(M)`
- `IsT4AGGroupoidTable(M)`
- `IsT5FAGGroupoidTable(M)`
- `IsT5BAGGroupoidTable(M)`
- `IsT5AGGroupoidTable(M)`
- `IsT6AGGroupoidTable(M)`
- `IsUnipotentAGGroupoidTable(M)`
- `IsAntirectangularAGbandTable(M)`
- `IsLeftAlternativeAGGroupoidTable(M)`
- `IsRightAlternativeAGGroupoidTable(M)`
- `IsAlternativeAGGroupoidTable(M)`
- `IsFlexibleAGGroupoidTable(M)`
- `IsRequiredAGGroupoidTable(M)`
- `IsAntirectangularAGBandTable(M)`
- `IsAnticommutativeAGGroupoidTable(M)`
- `IsTransitivelycommutativeAGGroupoidTable(M)`
- `IsParamedialAGGroupoidTable(M)`
- `IsAGGroupoidSemigroupTable(M)`
- `IsBolStarGroupoidTable(M)`
  Returns true if M is a Cayley table of Bol* groupoid and returns false otherwise.
- `IsBolStarQuasigroupTable(M)`
  Returns true if M is a Cayley table of Bol* quasigroup and returns false otherwise.
- `IsParamedialTable(M)`
  Returns true if M is a Cayley table of Paramedial groupoid and returns false otherwise.

- `IsAssociativeTable(M)`
  Returns true if the Cayley table M has associativity and returns false otherwise.
- `IsCommutativeTable(M)`
  Returns true if the Cayley table M has commutativity and returns false otherwise.

The following commands return true if the AG-groupoid table M has left zero, right zero, zero respectively and return false otherwise.

- `IsLeftZeroAGGroupoidTable(M)`

- `IsRightZeroAGGroupoidTable(M)`

- `IsZeroAGGroupoidTable(M)`

12.2 Testing Magma

- `IsAGGroupoid(M)`
  Returns true if the magma M is an AG-groupoid and returns false otherwise.
- `LeftIdentity(M)`
  Returns the left identity if the magma M is an AG-groupoid and has left identity and returns fail otherwise.

The following commands correspond to those given in the above section for the case of the magma M.

- `IsCancellativeAGGroupoid(M)`
- `IsAGMonoid(M)`
- `IsAGGroup(M)`
- `IsAGBand(M)`
- `IsAG3Band(M)`
- `IsLocallyAssociativeAGGroupoid(M)`
- `IsStarAGGroupoid(M)`
- `Is2StarAGGroupoid(M)`
- `IsLeftNuclearAGGroupoid(M)`
- `IsRightNuclearAGGroupoid(M)`
- `IsMiddleNuclearAGGroupoid(M)`
- `IsParamedial(M)`
- `IsParamedialAGGroupoid(M)`

- `IsAGGroupoidSemigroup(M)`
- `IsIsBolStarGroupoid(M)`
- `IsT1AGGroupoid(M)`
- `IsT2AGGroupoid(M)`
- `IsT3LAGGroupoid(M)`
- `IsT3RAGGroupoid(M)`
- `IsT3AGGroupoid(M)`
- `IsT4FAGGroupoid(M)`
- `IsT4BAGGroupoid(M)`
- `IsT4AGGroupoid(M)`
- `IsT5FAGGroupoid(M)`
- `IsT5BAGGroupoid(M)`
- `IsT5AGGroupoid(M)`
- `IsT6AGGroupoid(M)`
- `IsUnipotentAGGroupoid(M)`
- `IsLeftAlternativeAGGroupoid(M)`
- `IsRightAlternativeAGGroupoid(M)`
- `IsAlternativeAGGroupoid(M)`
- `IsFlexibleAGGroupoid(M)`
- `IsAGGroupoidWithLeftZero(M)`
- `IsAGGroupoidWithRightZero(M)`
- `IsAGGroupoidWithZero(M)`

The following three commands check (left,right) quasi-cancellativity of the AG-groupoid M and return true if it has that property and return false otherwise.

- `IsLeftQuasicancellativeAGGroupoid(M)`
- `IsRightQuasicancellativeAGGroupoid(M)`
- `IsQuasicancellativeAGGroupoid(M)`

12.3 Some Useful Operations

The following three commands return all the left zeros, right zeros, zeros respectively of an AG-groupoid M.

- `AllLeftZerosOfAGGroupoid(M)`
- `AllRightZerosOfAGGroupoid(M)`
- `AllZerosOfAGGroupoid(M)`

- `AllLocallyAssociativeElementsOfAGGroupoid(M)`
  Returns all the locally associative elements of an AG-groupoid M.
- `All3BandElementsOfAGGroupoid(M)`
  Returns all the 3 band elements of an AG-groupoid M.

The following three commands return all the left nuclear, right nuclear, nuclear elements respectively of an AG-groupoid M.

- `AllLeftNuclearElementsOfAGGroupoid(M)`
- `AllRightNuclearElementsOfAGGroupoid(M)`
- `AllMiddleNuclearElementsOfAGGroupoid(M)`
- `IsSAGGroup(M)`
  Returns true if the AG-group M is a Smarandache AG-group and returns false otherwise.
- `IsRightBolQuasigroup(M)`
  Returns true if the quasigroup M is right Bol quasigroup and returns false otherwise.
- `IsLeftBolQuasigroup(M)`
  Returns true if the quasigroup M is left Bol quasigroup and returns false otherwise.

12.4 Some Counting Operations

The following commands are the results of the constructions developed in this thesis. We describe them one by one.

- `NrAllSmallnon-associativeAGGroups(n)`
  Returns the total number of non-associative AG-groups of order n. Since all abelian groups of a given order are easy to construct. This function uses that construction.
- `AllSmallNonassociativeAGGroups(n)`
  Returns the list of all non-associative AG-groups of the given order. Each AG-group is represented as a GAP quasigroup.
- `NrAllSmallNonassociativeAGGroupsFromAnAbelianGroup(G)`
  Returns the total number of non-associative AG-groups that can be obtained from the abelian group G. This is equal to the number of conjugacy classes of involutions in $\mathrm{Aut}(G)$.
- The function `AllSmallNonassociativeAGGroupsFromAnAbelianGroup(G)`
  Returns the list of non-associative AG-groups obtainable from G, again as

GAP quasigroups.

- `NrAllSmallNonassociativeLeftBolQuasigroups(n)`
Returns the total number of non-associative left Bol quasigroups of order n provided that the SmallGroups library contains the list of groups of order n.
- `AllSmallNonassociativeLeftBolQuasigroups(n)`
Returns the list of all non-associative left Bol quasigroups of the given order n provided that the SmallGroups library contains the list of groups of order n.
- `NrAllSmallNonassociativeLeftBolQuasigroupsFromOneGroup(G)`
Returns the total number of non-associative left Bol quasigroups that can be obtained from the group G.
- `AllSmallNonassociativeLeftBolQuasigroupsFromOneGroup(G)`
Returns the list of all non-associative left Bol quasigroups that can be obtained from from the group G.
- `NrAllSmallNonassociativeLeftBolQuasigroupsFromOneLeftBolLoop(G)`
Returns the total number of non-associative left Bol quasigroups that can be obtained from from the left Bol loop G.
- `AllSmallNonassociativeLeftBolQuasigroupsFromOneLeftBolLoop(G)`
Returns the list of all non-associative left Bol quasigroups that can be obtained from the left Bol loop G.
- `NrAllSmallNonassociativeBolStarQuasigroups(n)`
Returns the total number of non-associative Bol* quasigroups of order n. Since all abelian groups of a given order are easy to construct. This function uses that construction.
- `AllSmallNonassociativeBolStarQuasigroups(n)`
Returns the list of all non-associative Bol* quasigroups of the given order.
- `NrAllSmallNonassociativeBolStarQuasigroupsFromAnAbelianGroup(G)`
Returns the total number of non-associative Bol* quasigroups that can be obtained from the abelian group G. This is equal to the number of conjugacy classes of involutions in $\mathrm{Aut}(G)$.
- `AllSmallNonassociativeBolStarQuasigroupsFromAnAbelianGroup(G)`
Returns the list of non-associative Bol* quasigroups obtainable from G.
- `NrAllSmallNonassociativeAGMonoids(n)`
Returns the total number of non-associative AG-monoids of order $n, n \leq 8$.
- `AllSmallNonassociativeAGMonoids(n)`
Returns the list of all non-associative AG-monoids of the given order $n, n \leq$

8.

- `NrAllSmallNonassociativeAGMonoidsFromACommutativeMonoid(G)`
  Returns the total number of non-associative AG-monoids that can be obtained from the commutative monoid G.
- The function `AllSmallNonassociativeAGMonoidsACommutativeMonoid(G)`
  Returns the list of non-associative AG-monoids obtainable from G.
- `AllSubAGGroups(M)`
  Returns all the AG-subgroups of an AG-group M.

Chapter 13

Conclusion

In this chapter we briefly discuss what we have achieved in the thesis. We also suggest some future directions.

- We have proved that an AG-group G of order n has its multiplication group as a non-abelian group of order $2n$ and its L_S is an abelian group of order n. It is now an interesting question like loops that which non-abelian group can occur as a multiplication group of an AG-group G which cannot and which abelian group can occur as its left section and which cannot.
- We have defined about 24 new classes and also have discussed some basic results about them but every class needs investigation on its own. Specially the class of semigroup as we discovered in this thesis and which we call non-commutative AG-groupoid semigroup wants a thorough study and full exploration. More particularly using our under construction package AGGROUPOIDS and SMALLSEMI we have found that there are non-commutative AG-groupoid semigroups that can occur as a multiplicative semigroup of near-ring. One such non-commutative AG-groupoid semigroup is being given in the following table.

  Example 69. *A non-commutative AG-groupoid semigroup of order* 4.

$\cdot$	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	1	1	2	2

  We expect such multiplicative semigroup will cause many results to near-rings which need to be explored. Thus we suggest the study of such near-rings as an interesting future problem.

- We have begun characterizing S-AG-groups here, however that notion requires significant further study.
- We have given the following open problem in the thesis.

  Problem 4. *Prove or disprove that every left cancellative element is also right cancellative of an AG-groupoid S without left identity.*

  We then partially answered this problem in positive in the thesis. Thus we proved that if a is a left cancellative element of an AG-groupoid S then a is also right cancellative at least in the following cases

  (i) If a^2 is left cancellative,

  (ii) If a is idempotent,

  (iii) If there exists a left nuclear left cancellative element in S,

  (iv) If a is the unique left cancellative element in S,

  (v) If S is an AG-band,

  (vi) If S is AG*-groupoid,

  (vii) If S is AG**-groupoid.

  (i) Thus for other than the above mentioned cases the problem is still open.
- Naseeruddin has found application of AG-groupoids within the theory of flocks [61]. We have discussed some application of AG-groups in geometry. But finding more application of AG-groupoids and AG-groups is the need of the day.
- We got enumeration of AG-groupoids up to order 6. We suggest enumeration of AG-groupoids of order 7 as interesting future problem.

Bibliography

[1] A. Ali and J. Slaney. Counting loops with the inverse property. *Quasigroups and Related Systems*, 16(1):13–16, 2008.

[2] A. Beg. A theorem on c-loops. *Kyungpook Math. J*, 17(1):91–94, 1977.

[3] A. Beg. On lc-, rc-, and c-loops. *Kyungpook Math. J*, 20(2):211–215, 1980.

[4] I. E. Burmistrovich. The commutative bands of cancellative semigroups. *Sib. Mat. Zh.*, 6:284–299, 1965. Russian.

[5] R. Cawagas. Introduction to: Non-associative finite invertible loops, 2009. available at arXiv `arXiv:0907.5059[math.GR]`.

[6] O. Chein, H. Pflugfelder, and J. Smith, editors. *Quasigroups and Loops: Theory and Applications*. Heldermann Verlag, 1990.

[7] J. Cho, Pusan, J. Jezek, and T. Kepka. Paramedial groupoids. *Czechoslovak Mathematical journal*, 49(124), 1996.

[8] J. M. Crawford, M. L. Ginsberg, E. Luks, and A. Roy. Symmetry-breaking predicates for search problems. In *Proc. of KR'96*, pages 148–159. Morgan Kaufmann, 1996.

[9] P. Csörgö and M. Niemenmaa. On connected transversals to nonabelian subgroups. *European Journal of Combinatorics*, 23(2):179–185, 1994.

[10] J. Denes and A. D. Keedwell. *Latin squares and its applications*. Academic Press, 1974.

[11] A. Distler. *Classification and Enumeration of Finite Semigroups*. PhD thesis, University of St Andrews, 2010.

[12] A. Distler and T. Kelsey. The monoids of order eight and nine. In *Proc. of AISC 2008*, volume 5144 of *LNCS*, pages 61–76. Springer, 2008.

[13] A. Distler and T. Kelsey. The monoids of orders eight, nine & ten. *Ann. Math. Artif. Intell.*, 56(1):3–21, 2009.

[14] A. Distler and J. D. Mitchell. *Smallsemi - A library of small semigroups.* `http://tinyurl.com/jdmitchell/smallsemi/`, 2010. A GAP 4 package [20], Version 0.6.2.

[15] A. Distler, M. Shah, and V. Sorge. Enumeration of AG-groupoids. In *Intelligent Computer Mathematics — Joint Proceedings of Calculemus 2011 and MKM 2011*, volume 6824 of *Lecture Notes in Artificial Intelligence*, pages 1–14. Springer Verlag, 2011.

[16] A. Drápal. Multiplication groups of finite loops that fix at most two points. *Journal of Algebra*, 235:154–175, 2001.

[17] A. Drápal, T. Kepka, and P. Maršálek. Multiplication groups of quasigroups and loops. ii. *Acta Univ. Carolin. Math. Phys.*, 35(1):9–29, 1994.

[18] F. Fenyves. Extra loops I. *Publ. Math. Debrecen*, 15:235–238, 1968.

[19] F. Fenyves. Extra loops II. *Publ. Math. Debrecen*, 16:187–192, 1969.

[20] The GAP Group, `http://www.gap-system.org`. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[21] I. Gent, C. Jefferson, and I. Miguel. Minion: A fast scalable constraint solver. In *Proc. of ECAI-06*, pages 98–102. IOS Press, 2006.

[22] M. Hall. *The Theory of Groups.* The Macmillan Company, New York, NY, USA, 1959.

[23] P. Holgate. Groupoids satisfying a simple invertive law. *Math. Student.*, 61:101–106, 1992.

[24] J. Humphreys. *A Course in Group Theory.* Oxford University Press, 1996.

[25] T. G. Jaiyeola and J. O. Adeniran. On the derivatives of central loops. *Advances in Theoretical and Applied Mathematics*, 1(3), 2006.

[26] M. S. Kamran. *Conditions for LA-semigroups to resemble associative structures.* PhD thesis, Quaid-i-Azam University, Islamabad, Pakistan, 1993. Available at `http://eprints.hec.gov.pk/2370/1/2225.htm`.

[27] M. A. Kazim and M. Naseerudin. On almost semigroups. *Alig. Bull. Math.*, 2:1–7, 1972.

[28] T. Kepka and M. Niemenmaa. On loops with cyclic innermapping groups. *Archiv der Mathematik, Springer*, 60(3):233–236, 1993.

[29] A. Khan, Y. B. Jun, and T. Mahmood. Generalised fuzzy interior ideals in abel grassmann's groupoids. *Intern. Jour. Math and math. Sci.*, pages 1–14, 2010.

[30] A. Khan, M. Shabir, and Y. B. Jun. Generalised fuzzy abel grassmann's groupoids. *Intern. Jour. Fuzzy System*, 4:340–349, 2010.

[31] M. Khan and S. Anis. Characterizations of intra-regular left almost semigroups by their fuzzy ideals. *International Journal Of Algebra*, 2(3):87–95, 2010.

[32] M. Khan and T. Asif. Characterizations of left regular ordered abel grassmann's groupoids. *Journal of Mathematics Reseach*, 5(11):499–521, 2011.

[33] M. Khan and Q. Mushtaq. On left almost ring. In *to appear in Proceedings of 7th International Pure Mathematics Conference*, 2006.

[34] M. Khan, M. Nouman, and A. Khan. On fuzzy Abel Grassmann's groupoids. *Advances in Fuzzy Mathematics*, 5(3):349–360, 2010.

[35] M. K. Kinyon, K. Kunen, and J. D. Philips. A generalization of moufang and steiner loops. *Algebra Universalis*, 48(1):81–101, 2002.

[36] M. K. Kinyon, J. D. Philips, and P. Vojtechovsky. Loops of bol-moufang type with a subgroup of index 2. *Bul. Acad. Stiinte Repub. Mold. Mat.*, 3:71–87, 2005.

[37] M. K. Kinyon, J. D. Philips, and P. Vojtechovsky. C-loops: extensions and constructions. *J. Algebra Appl.*, 6(1):1–20, 2007.

[38] M. K. Kinyon and J. D. Phillips. Commutants of bol loops of odd order. *Proc. Amer. Math. Soc.*, 132(3):617–619, 2004.

[39] M. K. Kinyon, K. Pula, and P. Vojtechovsky. Admissible orders of jordan loops. *Journal of Combinatorial Designs*, 17(2):103–118, 2009.

[40] V. Krcadinac and V. Volenec. A class of quasigroups associated with a cubic Pisot number. *Quasigroups and Related Systems*, 13:269–280, 2005.

[41] S. Linton. Finding the smallest image of a set. *In Proc of ISSAC*, pages 229–234, 2004.

[42] K. McCrimmon. *A taste of Jordan algebras*. Springer, 2004.

[43] W. McCune. *Mace4 Reference Manual and Guide.* Mathematics and Computer Science Division, Argonne National Laboratory, August 2003. ANL/MCS-TM-264.

[44] B. McKay, A. Meynert, and W. Myrvold. Small Latin squares, quasigroups and loops. *J. of Combinatorial Designs*, 15:98–119, 2007.

[45] B. McKay and I. Wanless. On the number of Latin squares. *Ann. Combin.*, 9:335–344, 2005.

[46] R. A. R. Monzo. On the structure of abel grassmann union of groups. *International Journal Of Algebra*, 4(26):1261–1275, 2010.

[47] R. A. R. Monzo. Power groupoids and inclusion classes of abel grassmann groupoids. *International Journal Of Algebra*, 5(2):1261–1275, 2011.

[48] Q. Mushtaq. Zeroids and idempoids in AG-groupoids. *Quasigroups and Related Systems*, 11:79–84, 2004.

[49] Q. Mushtaq and Q. Iqbal. Decomposition of locally associative LA-semigroup. *Semigroup forum*, 41:155–164, 1990.

[50] Q. Mushtaq and M. Kamran. Finite AG-groupoid with left identiy and left zero. *IJMMS*, 27(6):387–389, 2001.

[51] Q. Mushtaq and M. S. Kamran. On left almost groups. *Proc. Pak. Acad. of Sciences*, 33:1–2, 1996.

[52] Q. Mushtaq and M. Khan. Ideals in left almost semigroups. In *Proceedings of 4th International Pure Mathematics Conference*, pages 65–77, 2003.

[53] Q. Mushtaq and M. Khan. Decomposition of a locally associative AG**-groupoid. *Advances in Algebra and Analysis*, 2:115–122, 2006.

[54] Q. Mushtaq and M. Khan. Ideals in AG-band and AG*-groupoid. *Quasigroups and Related Systems*, 14:207–215, 2006.

[55] Q. Mushtaq and M. Khan. Direct product of Abel Grassmann's groupoids. *journal of Interdisciplinary Mathematics*, 11(4):461–467, 2008.

[56] Q. Mushtaq and K. Mahmood. Characterization of division μ-LA-semigroups. *Quasigroups and Related Systems*, 11:85–90, 2004.

[57] Q. Mushtaq and S. Yusuf. On LA-semigroups. *Alig. Bull. Math.*, 8:65–70, 1978.

[58] Q. Mushtaq and S. M. Yusuf. On locally associative LA-semigroups. *J. Nat. Sci. Math.*, XIX(1):57–62, April 1979.

[59] Q. Mushtaq and S. M. Yusuf. On LA-semigroup defined by a commutative inverse semigroup. *Mate. Bech.*, 40:59–62, 1988.

[60] G. P. Nagy and P. Vojtechovsky. *LOOPS: Computing with quasigroups and loops in GAP v*1.0*, computational package for GAP.* http://www.math.du.edu/loop.

[61] M. Naseeruddin. *Some studies on almost semigroups and flocks.* PhD thesis, The Aligarg Muslim University, India, 1970.

[62] M. Niemenmaa. On loops which have dihedral 2-groups as innermapping groups. *Bulletin of the Australian Mathematical Society*, 52:153–160, 1995.

[63] M. Niemenmaa. On connected transversals to subgroups whose order is a product of two primes. *European Journal of Combinatorics*, (8):915–919, 1997.

[64] M. Niemenmaa. On finite loops whose innermapping groups are abelian. *Bulletin of the Australian, Mathematical Society*, 65:477–484, 2002.

[65] M. Niemenmaa. Finite loops with nilpotent innermapping groups are centrally nilpotent. *Bulletin of the Australian Mathematical Society*, 79:109–114, 2009.

[66] M. Niemenmaa and T. Kepka. On connected transverals to abelian subgroups in finite groups. *Bulletin of the London, Mathematical Society*, 1992.

[67] M. Niemenmaa and T. Kepka. On connected transverals to abelian subgroups. *Bulletin of the Australian*, 1994.

[68] F. Ostermann and J. Schmidt. Begründung der Vektorrechnung aus Parallelogrammeigenschaften. *Math.-Phys. Semesterberichte*, 10(1):47–64, 1963.

[69] M. J. Pellingal and D. G. Rogersa. Steiner quasigroups ii: Combinatorial aspects. *Bull. Austral. Math. Soc.*, 20:321–344, 1979.

[70] H. O. Pflugfelder. *Quasigroups and Loops: Introduction*, volume 7 of *Sigma Series in Pure Mathematics*. Heldermann Verlag, Berlin, Germany, 1990.

[71] J. D. Philips and P. Vojtechovsky. The varieties of loops of bol-moufang type. *Algebra Universalis*, 54(3):259–271, 2005.

[72] J. D. Philips and P. Vojtechovsky. The varieties of quasigroups of bol-moufang type: An equational reasoning approach. *J. Algebra*, 293:17–33, 2005.

[73] J. D. Philips and P. Vojtechovsky. M-systems: an introduction. *Publicationes Mathematicae Debrecen*, 68(1–2):115–137, 2006.

[74] P. V. Protic and N. Stevanovic. Abel-grassmann's bands. *Quasigroups and Related Systems*, 11(1):95–101, 2004.

[75] N. K. Puharev. Geometric questions of certain medial quasigroups. *Sibirsk. Mat. Zh.*, 9:891–897, 1968. In Russian.

[76] V. S. Ramamurthi and A. R. T. Solarin. On finite right central loops. *Publ. Math.Debrecen*, 35:260–264, 1988.

[77] F. Rossi, P. van Beek, and T. Walsh. *Handbook of Constraint Programming (Foundations of Artificial Intelligence)*. Elsevier Science Inc., 2006.

[78] L. Sabinin. *Smooth Quasigroups and Loops*. Kluwer, 1999.

[79] M. Shah, I. Ahmad, and A. Ali. Discovery of new classes of AG-groupoids. *Res.J.Recent Sci.*, 2012. to appear.

[80] M. Shah, I. Ahmad, and A. Ali. On introduction of new classes of AG-groupoids. *Res.J.Recent Sci.*, 2012. to appear.

[81] M. Shah, I. Ahmad, and A. Ali. On quasi-cancellativity of AG-groupoids. *Int. J. Contemp. Math. Sciences*, 7(42):2065 – 2070, 2012.

[82] M. Shah and A. Ali. nuclei and commutants of c-loops. to appear.

[83] M. Shah and A. Ali. Some structural properties of AG-groups. *Int. Mathematical Forum*, 6(34):1661–1617, 2011.

[84] M. Shah, A. Ali, and I. Ahmad. Paramedial and bol* AG-groupoids and AG-groupoid semigroups. *submitted*.

[85] M. Shah, C. Gretton, and A. Ali. On jordan loops. submitted.

[86] M. Shah, C. Gretton, and V. Sorge. Enumerating AG-groups with a study of smarandache AG-groups. *International Mathematical Forum*, 6(62):3079–3086, 2011.

[87] M. Shah, V. Serge, and A. Ali. The first survey of AG-groupoids. submitted.

[88] M. Shah, T. Shah, and A. Ali. On the cancellativity of AG-groupoids. *Int. Mathematical Forum*, 6(44):2187–2194, 2011.

[89] M. Shah, S. Shpectorov, and A. Ali. AG-groups and other classes of right bol quasigroups. *Available at* `http://arxiv.org/abs/1106.2981v2`, 2011.

[90] M. Shah, V. Sorge, and A. Ali. On multiplication group of an AG-group. submitted.

[91] M. Shah, V. Sorge, and A. Ali. A partial positive solution to a problem on AG-groupoids. submitted.

[92] M. Shah, V. Sorge, and A. Ali. A study of AG-groups as a parallelogram space. submitted.

[93] M. Shah, V. Sorge, and A. Ali. A study of AG-groups as abelian groups. submitted.

[94] M. Shah, V. Sorge, and A. Ali. A study of AG-groups as quasigroups. submitted.

[95] T. Shah, G. Ali, and F. Rehman. Direct sum of ideals in a generalised LA-ring. *International Mathematical Forum*, 6(22):1095–1101, 2011.

[96] T. Shah, M. Raees, and G. Ali. On la-modules. *J. Contemp. Math. Sciences*, 6(5):209–222, 2010.

[97] T. Shah and I. Rehman. M-systems in *gamma Proc. Pak. Acad. Sci*, 47(1):33–39, 2010.

[98] T. Shah and I. Rehman. On *gamma*-ideals and *gamma*–bi-ideals in *gamma*-AG-groupoids. *International Journal Of Algebra*, 4(6):267–276, 2010.

[99] T. Shah and I. Rehman. On LA-rings of finite nonzero functions. *J. Contemp. Math. Sciences*, 5(21):999–222, 2011.

[100] B. L. Sharma. Left loops which satisfy the left bol identity. *Proc. AMS*, 61:189–195, 1976.

[101] J. Slaney. *FINDER, Notes and Guide.* Center for Information Science Research, Australian National University, 1995.

[102] J. Slaney and A. Ali. Generating loops with the inverse property. In *Sutcliffe G., Colton S., Schulz S. (eds.); Proceedings of ESARM*, pages 55–66, 2008.

[103] F. Smarandache. Special algebraic structures. *In Collected Papers, Abaddaba, Oradea*, 3(22):78–81, 2000.

[104] G. Smith and O. Tabachnikova. Topics in group theory. *springer Verlag*, 2000.

[105] V. Sorge, A. Meier, R. McCasland, and S. Colton. Classification results in quasigroup and loop theory via a combination of automated reasoning tools. *Comm. Univ. Math. Carolinae*, 49(2-3):319–340, 2008.

[106] N. Stevanovic and P. V. Protic. Inflations of the AG-groupoids. *Novi Sad J. Math.*, 29(1):19–26, 1999.

[107] N. Stevanovic and P. V. Protic. Composition of Abel-Grassmann's 3-bands. *Novi Sad J. Math.*, 34(2):175–182, 2004.

[108] D. Vakarelov. Dezargovi sistemi. *Godinik univ. Sofija. Mat. fak.*, 64:227–235, 1971.

[109] V. Volenec. Geometry of medial quasigroups, rad jugoslav. *Rad Jugoslav. Akad. Znan. Umjet.*, 421(5):79–91, 1986.

[110] V. Volenec. GS-quasigroups. *Casopis Pest. Mat.*, 115:307–318, 1990.

[111] V. Volenec. Geometry of IM-quasigroups. *Rad Hrvat. Akad. Znan. Umjet.*, 456:139–146, 1991.

[112] V. Volenec. Hexagonal quasigroups. *Arch. Math.*, 27a:113–122, 1991.

[113] V. Volenec. Quadratical groupoids. *Note di Matematica*, 13(1):107–115, 1993.

[114] V. Volenec and R. Kolar-Šuper. Parallelograms in quadratical quasigroups, 1997. Preprint.

[115] V. Volenec and V. Krcadinac. A note on medial quasigroups. *Mathematical Communications*, 11:83–85, 2006.