MOUFANG LOOPS, MAGMAS AND THE MOUFANG IDENTITIES

GARBA GAMBO ZAKU

UNIVERSITI SAINS MALAYSIA

2020

MOUFANG LOOPS, MAGMAS AND THE MOUFANG IDENTITIES

by

GARBA GAMBO ZAKU

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

February 2020

ACKNOWLEDGEMENT

My immense appreciation goes to the Almighty God and my Saviour the Lord Jesus Christ for His mercies, favor and guidance over every stage of my life.

I express my profound gratitude and appreciation to my supervisor, Associate Professor Dr. Andrew Rajah a/l Balasingam Gnanaraj, who was not just a supervisor but a mentor and friend to me. His guidance to me in the course of the research work was excellent, demonstrating his deep knowledge of the field. His patience, assistance (beyond academics), and understanding are sincerely appreciated.

I am grateful to Universiti Sains Malaysia, the School of Mathematical Sciences and all its staff for the enabling environment and adequate facilities that have helped me to complete my research work.

I also appreciate and acknowledge my home institution, the University of Jos, the Department of Mathematics and all its staff, for granting me scholarship through the "Needs Assessment Intervention" to undertake a PhD program.

I acknowledge the impressive contribution and assistance rendered by Professor Dr. J. D. Phillips of the Northern Michigan University, USA, towards one of the results in this research work.

I am grateful to all my PhD research colleagues at the Universiti Sains Malaysia who have, in one way or other, been of great encouragement to me in the course of this work.

I earnestly appreciate my beloved, pretty and precious Queen, Esther Onyela Zaku, who sincerely supported me at great cost and sacrifice, to ensure the success of this

program. Our children: Voma, Ma'avyon, Fojima and Amasan who also had to put up with my absence, have been a source of great cheer and inspiration to me. Thanks to my loving and caring parents in-law, Mr. and Mrs. J. A. T. Orume for their prayers. Special appreciation to all my siblings and that of my wife together with their spouses, for all their support, prayers and words of encouragement. Last, but not the least, I remember with great appreciation my late parents, Mr. and Mrs. Joro Akawu Gambo Zaku, and my late eldest brother, Mr. Atoshi Gambo Zaku, who played pivotal roles in both my up-bringing and training.

Garba Gambo Zaku

Penang, Malaysia 2019

TABLE OF CONTENTS

LIST OF SYMBOLS

$\mathbb{Z}$	The set of all integers
$\mathbb{Z}^+$	The set of all positive integers
$a\|b$	integer a is a divisor of integer b
$a \equiv b (\text{mod } n)$	a is congruent modulo n to b
$\in$	is an element of
$\subset$	is a subset of
$\leq$	is less or equal to; or is a subloop of
$<$	is less than; or is a proper subloop of
$\triangleleft$	is a normal subloop of
$\|S\|$	number of elements in a set S
$\|x\|$	order of an element x
L/K	quotient loop of L modulo K
L_a	associator subloop of a loop L
L_c	commutator subloop of a loop L
$N(L)$	nucleus of a loop L
$Z(L)$	centre of a loop L
$C_L(K)$	centraliser of a subloop K in a loop L
$I(L)$	inner mapping group of a loop L
$\langle S \rangle$	subloop generated by a subset S of a loop

LUP MOUFANG, MAGMA DAN IDENTITI MOUFANG

ABSTRAK

Teori lup adalah suatu generalisasi teori kumpulan; lup Moufang merupakan suatu jenis lup. Empat identiti (Moufang) yang setara digunakan untuk mengaksiomkan lup tersebut. Lup Moufang juga berkongsi banyak sifat dengan kumpulan walaupun secara am mereka tidak memenuhi hukum sekutuan; Teorem Moufang lah yang mewujudkan hubungan yang rapat ini. Bukti yang sedia ada mengenai kesetaraan empat identiti Moufang melibatkan konsep "autotopisma", suatu konsep yang benar-benar sukar dalam dirinya sendiri, sedangkan tidak terdapat sebarang bukti lengkap untuk Teorem Moufang (walaupun wujud beberapa bukti yang munasabah diterima). Tesis ini menyediakan bukti yang mudah, asas dan lengkap untuk kedua-dua teorem tersebut. Seterusnya, kesetaraan versi "tempatan" bagi empat identiti Moufang dikaji di bawah keadaan yang umum, iaitu magma di bawah syarat-syarat yang perlu dan mencukupi. Akhirnya, penyelidikan ini memberikan penyelesaian (separa) bagi lup Moufang berperingkat ganjil p^2q^4.

MOUFANG LOOPS, MAGMAS AND THE MOUFANG IDENTITIES

ABSTRACT

Loop theory is a generalization of group theory; Moufang loops are a variety of loops. Four equivalent (Moufang) identities axiomatize these loops. Moufang loops also share many similar properties as groups though generally they are not associative; Moufang's Theorem is pivotal in establishing this close relationship. The existing proof of the equivalence of the Moufang identities involves the notion of "autotopism", a completely difficult concept in itself, whereas there is no known complete proof of the Moufang's Theorem (though several reasonably acceptable proofs exist). This thesis provides a simple, basic and complete proof of both. Moreover, the equivalence of the localized versions of the four identities is studied under the generalized setting of magmas and proven under necessary and sufficient conditions. Finally, this research gives a (partial) resolution of Moufang loops of odd order p^2q^4.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Moufang loops were first introduced by the German mathematician, Ruth Moufang in her paper: "Zur Struktur von Alternativkorpern" [Moufang (1935)]. She originally presented loops that satisfy the identity $(xy \cdot x)z = x(y \cdot xz)$. She also wrote about loops that satisfy the identities: $xy \cdot zx = x(yz \cdot x)$ and $(xy \cdot z)y = x(y \cdot zy)$. In what appears to be three different varieties of loops axiomatized by the three identities, she proved the equivalence of the first and third identities. However she gave a separate definition for loops that satisfy the second identity which is (quite) obviously equivalent to the identity $xy \cdot zx = (x \cdot yz)x$. Bruck (1971) however proved that all of these (four) identities were equivalent in the variety of loops. These identities were later referred to as the Moufang Identities. Hence, the loops that satisfied any one of these (equivalent) identities could be simply called Moufang loops. Original definition of Moufang loops talks about quasigroups and loops but the proof of the equivalence of the Moufang identities provided by Bruck brought in an additional concept, that is autotopism. To study Moufang loops one needs to have a proper grasp of these identities and the fact that they are all equivalent. Hence, there is the need to also be at home with the proof of their equivalence. Reading through the work of others who have also proved the equivalence of these identities, it was also noticed that each of them made use of autotopism. For example, Pflugfelder (1990) also provided the proof for the equivalence of these Moufang identities but still using autotopism. Also Drapal (2010) again provided

proof for the equivalence of the Moufang identities. But going through the work, one discovers that he made use of the traditional style of using autotopism to prove it. Thus from available literature on this topic, the proofs for the equivalence of these Moufang identities use autotopism.

On the one hand, the study of autotopism can produce many new results about loops but the concept itself can be daunting to a novice. Now, given the fact that these identities and the proof of their equivalence serves as a gateway into the study of Moufang loops, there is the need to find a proof that is more direct and devoid of autotopism, making use of only basic properties of quasigroups and loops.

A magma is defined as a set with a binary operation and a two-sided neutral element; this makes magmas even more general than loops since a magma needs the additional "quasigroup" condition to be called a loop. Thus, the work extends to cover results for magmas satisfying either the right or left inverse property. So, this research investigates these identities in the general setting of magmas, rather than restricting attention to loops. Hence, the proof of the equivalence of the identities in the general setting of a magma extends the research on loops in Chapter 3.

Secondly, Moufang's theorem which states that if $\langle L, \cdot \rangle$ is a Moufang loop such that if three elements of L are associative in a particular order, then the same three elements generate an associative subloop of $\langle L, \cdot \rangle$, is a foundational result in the study of Moufang loops. Moreover, Moufang's Theorem continues with the statement, "any two elements in a Moufang loop generate an associative subloop of $\langle L, \cdot \rangle$." Though the "proof" of this theorem has been presented in Bruck (1971), it is merely an outline of the proof; hence, it is not complete. In fact, he notes (on page 119) that the proof he provides is valid only for a specific class of Moufang loops. Moreover, this proof is

technical and difficult to comprehend. Of recent, Pflugfelder (1990) provided a proof of the theorem but the proof still follows "Bruck's strategy" (see page 93). Later Drapal (2010) gave a proof of Moufang's Theorem with the aim of making the proof a simple one. However, a closer look at his work betrays the aim since most of the concepts used are not too different from that of Bruck's. This he admitted in the same work with the following statement: "All these ingredients are present in a varying degree of explicitness in Bruck's proof. The proof presented here only organizes them in a different way." So from existing literature, there is no complete proof of the theorem. Thus in Chapter 4, for the first time, a complete proof of Moufang's Theorem is being presented. Moreover, this proof uses basic methods that can be truly called "simplified."

Having settled the proofs of the basic and fundamental results on Moufang loops, the research look towards solving an open problem that uses much application of these results. Extensive work has been done in answering the question "Given a positive integer n, which Moufang loops of order n, are associative?" If the existence of a nonassociative Moufang loop $\langle L, \cdot \rangle$ of order n is known, then a nonassociative Moufang loop of order mn can be constructed using the direct product of $\langle L, \cdot \rangle$ with any (for example, the cyclic) group of order m. Thus, if all Moufang loops of order mn are proven to be associative, then all Moufang loops of order m (and n) are associative. This problem can be studied by dividing it into two cases of n even, and n odd. The case for n even were completely resolved by the works of Chein (1974) and, Chein and Rajah (2000) which left only the case of n odd to be studied. Chein (1974) also proved that all Moufang loops of order p^3 are groups, whereas Bruck (1946) proved the existence of nonassociative Moufang loops of order 3^4. Meanwhile Leong (1974) proved that all

Moufang loops of order p^4 (p a prime greater than 3) are groups. Also, Wright (1965) had proved the existence of nonassociative Moufang loops of order p^5 (p also a prime greater than 3). Chein (1974) started the ball rolling by studying the associativity of Moufang loops of a specific order by writing the order as the power of a prime or a product of powers of distinct primes. Continuing along this line, Leong and Rajah (1996a) proved that all Moufang loops of odd order pq^2 and p^2q^2 (where $p < q$ are primes) are associative. Rajah (2001) proved the existence of nonassociative Moufang loops of odd order pq^3 (p and q distinct primes) if and only if $q \equiv 1 (\text{mod } p)$ (that is, $q > p$). This was the first known construction of a minimally nonassociative Moufang loop of odd order whose order involves the product of distinct primes. Thus, for odd primes p and q with $q \equiv 1 (\text{mod } p)$, by using direct product one can easily construct a nonassociative Moufang loop whose order is a higher power of p or q in pq^3, or the product of pq^3 with (one or more) other primes. Hence, the question on nonexistence for "higher" powers than pq^3 requires that $q \not\equiv 1 (\text{mod } p)$ as a necessary condition. Moving in this direction, Rajah and Chee (2011a), Rajah and Chee (2011b), and Chee and Rajah (2014) respectively proved that all Moufang loops of odd order p^2q^3, p^3q^3 and pq^4 with $q \not\equiv 1 \ (\text{mod } p)$ are groups. Hence the next unresolved order involving powers of only two (distinct) primes is p^2q^4. This was actually an open problem raised by Chee and Rajah (2014). Ademola (2017) partially solved this problem with the added condition that $q \not\equiv -1 (\text{mod } p)$. Though this condition is a sufficient condition, its necessity is unjustified. Hence, there are two ways to completely resolve this: justify the necessity of this added condition by constructing a nonassociative Moufang loop when $q \equiv -1 (\text{mod } p)$, or prove that it is an unnecessary condition by removing it and proving it to be associative nevertheless.

1.2 Problem Statements

These statements arise from the discussion in the previous section:

1. The known existing proofs of the equivalence of the four Moufang identities made use of autotopism, a concept which could have been avoided.

2. The known existing proofs of the equivalence of the four Moufang identities are only for loops and not for the general variety of magmas.

3. The known existing proofs of the equivalence are given only for the four Moufang identities, not localized versions of the identities.

4. Though the theory of Moufang loops depend on Moufang's Theorem, no complete proof of this theorem exists in literature.

5. Nonassociative Moufang loops of order 3^4 (Bruck (1946)) and p^5 for prime $p > 3$ (Wright (1965)) are known to exist. Rajah (2001) had proved the existence of nonassociative Moufang loops of order pq^3 for odd primes p and q with $q \equiv 1 (\text{mod } p)$. Investigation on existence for higher powers of p and q, therefore, needs the necessary additional condition $q \not\equiv 1 (\text{mod } p)$. Moufang loops of odd order p^2q^3 and pq^4 satisfying this condition have been proven to be associative. So there remains the next case p^2q^4 with $q \not\equiv 1 (\text{mod } p)$. Though partially resolved (proven to be associative) by Ademola (2017) using the added condition $q \not\equiv -1 (\text{mod } p)$, its necessity is unjustified.

1.3 Research Objectives

The following are the objectives of this work:

1. To prove the equivalence of the four Moufang identities using basic properties of loops and avoiding autotopism.

2. To investigate localized versions of the four Moufang identities in the general setting of magmas.

3. To provide a complete proof of Moufang's Theorem.

4. To resolve the case of Moufang loops of order p^2q^4 for distinct odd primes p and q with $q \not\equiv 1 (\text{mod } p)$ (that is, without the added condition $q \not\equiv -1 (\text{mod } p)$), or alternatively prove that this is a necessary condition for associativity by constructing a nonassociative Moufang loop for some $q \equiv -1 (\text{mod } p)$.

1.4 Methodology

Since there are basically four research objectives (with only the first two having similarities), a break down of the methodology corresponding to each objective is given as follows:

1. The first objective is achieved using algebraic methods of equational reasoning and the definitions of loops and quasigroups.

   (i) First prove that loops that satisfy any of the four Moufang identities have other (additional) properties like flexible identity, (right and left) alternative

identities and (right and left) inverse properties.

(ii) Next, assume that an identity, say "A", holds and using this identity and strictly those basic properties that have been proven, to prove that another identity, "B", is true.

(iii) Continuing this method (in (ii)), to move next from "B" to "C", then to "D" and finally back to "A" to establish the equivalence of the four.

2. For the second objective:

(i) Define the 12 local versions of the four Moufang identities.

(ii) Define magmas that have the right (alternatively left) inverse property and establish some of their properties.

(iii) Establish properties that hold for four of the local elements.

(iv) Study conditions under which equivalence can exist amongst the four local versions under the general setting of magmas with the right (alternatively left) inverse property.

3. For the third objective:

(i) Start with the assumption that three fixed elements in a Moufang loop associate in a particular order, then prove that these same three elements associate in any order.

(ii) Next, prove that positive powers and inverses of these three elements associate.

(iii) Finally, using progressive lemmas, prove that any product of powers of these three elements associate.

The above is achieved through a systematic build up of proofs using the Moufang identities and properties.

4. The fourth objective is achieved by first taking note of these two equivalent statements:

(a) Suppose there exists a nonassociative Moufang loop L of order m. Then the direct product of L with any (for example, the cyclic) group of order n is a nonassociative Moufang loop of order mn.

(b) Suppose it has been proven that all Moufang loops of order m are associative, and n is a (positive integer) divisor of m. Then all Moufang loops of order n are associative.

(i) Assume that there exists a nonassociative Moufang loop of order p^2q^4, where $2 < p < q$ are primes and $q \not\equiv 1 (\text{mod } p)$.

(ii) Since Leong and Rajah (1997) have proven that the associator subloop of a nonassociative Moufang loop is a (minimal normal) elementary abelian group, all the possible orders of the associator subloop of this Moufang loop are considered case by case.

(iii) Whenever discussion of a particular case in (ii) contradicts other known results/facts (particularly about Moufang loops) move on to another case until every case is covered.

(iv) If no contradiction is reached in a particular case in (ii), then it is inferred that there is a possibility of the existence of a nonassociative Moufang loop of order p^2q^4 satisfying all the properties and conditions established. The next step is to provide an example of the existence of such a nonassociative Moufang loop by obtaining a product rule between any two of its elements using the properties of the Moufang loop under consideration.

1.5 Organisation of Thesis

This thesis begins by providing some basic definitions, notations and known results that are relevant and will be used in this work. It then proceeds to provide the "autotopism free" proof of the equivalence of the four Moufang identities and also investigate these identities in the general setting of magmas in Chapter 3. Chapter 4 presents the first known complete proof of Moufang's Theorem. Chapter 5 proves the nonexistence of nonassociative Moufang loops of odd order p^2q^4 when $p > 3$ and establishes conditions for the existence of nonassociative Moufang loops of odd order 3^2q^4 when $q \not\equiv 1 (\text{mod } 3)$.

1.6 Definitions and Notations

This section gives some basic definitions and properties that will be needed in subsequent chapters. For further definitions that are not listed here, the reader can consult

Bruck (1971) and Glauberman (1968).

Definition 1.1. *Let L be a nonempty set. A function from $L \times L$ to L is defined as a binary operation on L. If "$\cdot$" is a binary operation on L then $\langle L, \cdot \rangle$ is defined as a binary system. Moreover, if "$\cdot$" maps $(x, y) \in L \times L$ to $z \in L$, write $x \cdot y = z$, or sometimes merely as $xy = z$ if the binary operation used has been clarified.*

Definition 1.2. *A binary system $\langle L, \cdot \rangle$ is said to have:*

(i) a left identity element $e_L \in L \quad if \quad e_L \cdot x = x \quad \forall\, x \in L$;

(ii) a right identity element $e_R \in L \quad if \quad x \cdot e_R = x \quad \forall\, x \in L$;

(iii) an identity element $e \in L \quad if \quad e \cdot x = x \cdot e = x \quad \forall\, x \in L$.

[Note: An identity element is usually called a "neutral element" in the variety of magmas though their definitions are identical.]

Definition 1.3. *Let $\langle L, \cdot \rangle$ be a binary system with an identity element e. An element $y \in L$ is said to be an inverse of the element $x \in L$ if $x \cdot y = y \cdot x = e$. If $x \in L$ has a unique inverse, denote its inverse as x^{-1}.*

Definition 1.4. *Let $\langle L, \cdot \rangle$ be a binary system and $a, b \in L$. Then $\langle L, \cdot \rangle$ is defined as a quasigroup if there exist unique (not necessarily distinct) elements $x, y \in L$ such that $a \cdot x = b$ and $y \cdot a = b$.*

[Note: It is common to denote the x and y in the last definition as $x = a \backslash b$ and $y = b/a$, where "$\backslash$" and "$/$" are called the left and right divisions respectively and in fact are also binary operations on L.] *So it is possible to define a quasigroup as $\langle L, \cdot, \backslash, / \rangle$, that is, a non-empty set L with the three binary operations "$\cdot$", "$\backslash$" and "$/$".*

Definition 1.5. *A quasigroup $\langle L, \cdot, \backslash, / \rangle$, that has an identity element is called a loop.*

[However, the simpler notation $\langle L, \cdot \rangle$ shall be used for a loop.]

Definition 1.6. *A Moufang loop is a loop $\langle L, \cdot \rangle$ that satisfies any of the following*

(equivalent) identities

$$(A): \quad z(xy\cdot z) = zx\cdot yz \qquad (C): \quad z(x\cdot zy) = (zx\cdot z)y$$

$$(B): \quad (z\cdot xy)z = zx\cdot yz \qquad (D): \quad (xz\cdot y)z = x(z\cdot yz)$$

for any $x,y,z \in L$.

[Henceforth, for the purpose of brevity, the loop $\langle L,\cdot\rangle$ shall simply be writen as (the loop) L. Moreover, while writing the product of many elements, the binary operation and parentheses can be omitted if no confusion arises and accept that juxtaposition precedes "$\cdot$" which then precedes parentheses. For example, $x\cdot(y\cdot(x\cdot z))$ will be written as $x(y\cdot xz)$ and this means first compute xz, then multiply y on its left, and again multiply x on the left of the element $y\cdot xz$.]

Definition 1.7. *A magma is a set with a binary operation and a two-sided neutral (or identity) element.*

Definition 1.8. *A local element in an identity (or law) is defined as the element that is held as a constant in the identity (law). Moreover, this "new" identity is called a local version of the (original) identity (law).*

Definition 1.9. *The three different sets of local elements in the associative law are defined as follows:*

(i) left nucleus, $\mathrm{N}_\lambda(L) = \{a : a\cdot xy = ax\cdot y, \forall\, x,y \in L\}$,

(ii) middle nucleus, $\mathrm{N}_\mu(L) = \{a : x\cdot ay = xa\cdot y, \forall\, x,y \in L\}$, *and*

(iii) right nucleus, $\mathrm{N}_\rho(L) = \{a : x\cdot ya = xy\cdot a, \forall\, x,y \in L\}$.

Definition 1.10. *The following identities:*

$$(i): \quad xy \cdot x = x \cdot yx \quad (iii): \quad yx \cdot x = y \cdot xx$$

$$(ii): \quad x \cdot xy = xx \cdot y$$

are called the flexible, left alternative and right alternative identities respectively. A loop $\langle L, \cdot \rangle$ is said to be an alternative loop if it satisfies both the left and right alternative identities. Moreover, in the local version of these identities, x is called the flexible, left alternative and right alternative element in (i), (ii) and (iii) respectively.

Definition 1.11. *Suppose L is a quasigroup (loop).*

(i) If there exists a bijection $\theta_\lambda : x \to x^\lambda$ such that $x^\lambda \cdot xy = y$ for all x and y in L, then L is said to have the left inverse property (LIP).

(ii) If there exists a bijection $\theta_\rho : x \to x^\rho$ such that $yx \cdot x^\rho = y$ for all x and y in L, then L is said to have the right inverse property (RIP).

(iii) L is said to have the inverse property and is called an IP quasigroup (loop), if it has both the LIP and the RIP.

[Note that a loop that satisfies the identity $x^{-1} \cdot xy = y = yx \cdot x^{-1}$ where x^{-1} is the inverse of x is an IP loop.]

Definition 1.12. *The Moufang identities defined in Definition 1.6 are localized into 12 different identities in a binary system $\langle Q, \cdot \rangle$ and labeled as follows, $\forall\ x, y, z \in Q$ and $a \in Q$:*

$$(A2): \quad a(xy \cdot a) = ax \cdot ya \qquad (C2): \quad a(x \cdot ay) = (ax \cdot a)y$$

$$(A1x): \quad z(ay \cdot z) = za \cdot yz \qquad (C1x): \quad z(a \cdot zy) = (za \cdot z)y$$

$$(A1y): \quad z(xa \cdot z) = zx \cdot az \qquad (C1y): \quad z(x \cdot za) = (zx \cdot z)a$$

$$(B2): \quad (a\cdot xy)a = ax\cdot ya \qquad (D2): \quad (xa\cdot y)a = x(a\cdot ya)$$

$$(B1x): \quad (z\cdot ay)z = za\cdot yz \qquad (D1x): \quad (az\cdot y)z = a(z\cdot yz)$$

$$(B1y): \quad (z\cdot xa)z = zx\cdot az \qquad (D1y): \quad (xz\cdot a)z = x(z\cdot az)$$

Definition 1.13. *The element "a" that satisfies the identity* $(A1x)$ *is called an* $(A1x)$ *element, and* $(A1x)_Q$ *denotes the set of all* $(A1x)$ *elements in Q. The analogous definitions for the other 11 identities are given in a similar fashion.*

[Note that $(A2)$ is equivalent to $(B2)$ in the variety of magmas (this is seen by setting y in $(A2)$ and x in $(B2)$ equal to the identity element e); aside this trivial equivalence, none of these identities implies the other in the variety of magmas [Phillips (2009)]. So, for any given magma, these 12 different "local Moufang laws" axiomatize up to 11 different "Moufang subsets" (none of which has to be a submagma) [Phillips (2019)].]

[Unlike in groups, the definition of normality of subloops of a loop has additional properties due to their nonassociativity (in general). The following three definitions help define normal subloops of a loop.]

Definition 1.14. *Suppose L is a loop. Then* $\mathscr{L}(x) : y \to y\mathscr{L}(x) = xy$ *and* $\mathscr{R}(x) : y \to y\mathscr{R}(x) = yx$ *are respectively called the left and right translations of an element* $y \in L$ *by an element* $x \in L$.

Definition 1.15. $I(L) = \langle \mathscr{R}(x,y),\ \mathscr{L}(x,y),\ \mathscr{T}(x) | x,y \in L \rangle$ *is called the inner mapping group of a loop L, where*

$$\begin{aligned} \mathscr{R}(x,y) &= \mathscr{R}(x)\mathscr{R}(y)\mathscr{R}(xy)^{-1}, \\ \mathscr{L}(x,y) &= \mathscr{L}(x)\mathscr{L}(y)\mathscr{L}(yx)^{-1}, \\ \mathscr{T}(x) &= \mathscr{R}(x)\mathscr{L}(x)^{-1}. \end{aligned}$$

Definition 1.16. *A bijection mapping of a triple* (α,β,γ) *from a loop* $\langle L,\cdot\rangle$ *onto a loop* $\langle H,\circ\rangle$ *is called an isotopism if* $x\alpha\circ y\beta=(x\cdot y)\gamma$, $\forall\ x,y\in L$, *in which case the loop* $\langle H,\circ\rangle$ *is called an isotope of the loop* $\langle L,\cdot\rangle$. *The loops* $\langle L,\cdot\rangle$ *and* $\langle H,\circ\rangle$ *are said to be isotopic to each other. This isotopism is called an autotopism if* $\langle H,\circ\rangle=\langle L,\cdot\rangle$.

Definition 1.17. *The associator subloop of a loop* L, *denoted by* L_a, *is the subloop generated by all the associators* (x,y,z) *in* L *where* $xy\cdot z=(x\cdot yz)(x,y,z)$. L_a *is also defined as* $L_a=(L,L,L)=\langle(l_1,l_2,l_3)|l_i\in L\rangle$.

[L is associative if and only if $L_a=\{1\}$.]

Definition 1.18. L_c, *the commutator subloop of* L, *is the subloop generated by all the commutators* $[x,y]$ *in* L *where* $xy=yx\cdot[x,y]$.

[L is commutative if and only if $L_c=\{1\}$.]

Definition 1.19. *Let* K *be a subloop of* L. K *is said to be a normal subloop of* L, *denoted* $K\lhd L$, *if* $K\theta=\{k\theta|k\in K\}=K$ *for all* $\theta\in I(L)$.

Definition 1.20. *Let* K *be a normal subloop of* L.

(i) K *is a proper normal subloop of* L *if* $K\neq L$.

(ii) L/K *is a proper quotient loop of* L *if* $K\neq\{1\}$.

Definition 1.21. *Suppose* K *is a normal subloop of* L.

(i) K *is called a minimal normal subloop of* L *if* K *is non-trivial and contains no proper non-trivial subloop which is normal in* L.

(ii) K *is called a maximal normal subloop of* L *if* K *is not a proper subloop of every other proper normal subloop of* L.

Definition 1.22. *The nucleus of* L *is the subloop generated by all* $x\in \mathrm{N}_\lambda(L)\cap\mathrm{N}_\mu(L)\cap\mathrm{N}_\rho(L)$ *and is denoted as* $N=N(L)$.

Definition 1.23. *Let* H *be a subloop of* L. *The centraliser of* H *in* L, *is defined as*

$C_L(H) = \{g \in L | gh = hg \text{ for all } h \in H\}$.

Definition 1.24. *Let K be a subloop of L and π a set of primes.*

(i) A positive integer n is a π-number if every prime divisor of n lies in π.

(ii) For each positive integer n, let n_π be the largest π-number that divides n.

(iii) K is a π-loop if the order of every element of K is a π-number.

(iv) K is a Hall π-subloop of L if $|K| = |L|_\pi$.

(v) K is a Sylow p-subloop of L if K is a Hall π-subloop of L such that π contains only one prime p.

Definition 1.25. *Let L be a loop.*

(i) $x \in L$ is defined as a power associative element if $xx \cdot x = x \cdot xx$.

(ii) L is a power associative loop if every element in L is power associative.

(iii) Suppose p is a prime and x is a power associative element of L. If x has a finite order, then x is defined as a p-element if $|x| = p^\alpha$ for some non-negative integer α.

Definition 1.26. *(m,n) is defined as the greatest common divisor of the integers m and n.*

Definition 1.27. *A Moufang loop L is said to be minimally nonassociative if it is not associative but all proper subloops and proper quotient loops of L are associative.*

CHAPTER 2

BASIC PROPERTIES AND KNOWN RESULTS

2.1 Introduction

Presented in this chapter are some known results that will be used in Chapter 5 only. In view of the fact that the results in Chapters 3 and 4 are alternative proofs to existing ones (except for the results on magmas which are entirely new and fresh), there is no quote or use of already established results. Instead, in keeping faith with the goal of providing direct alternative proofs, all the results needed and used in these chapters are proved using direct algebraic methods.

2.2 Known Results

The following theorem is, in fact, Moufang's Theorem which will be proved in Chapter 4. Many of the subsequently stated theorems or propositions below were proven using this theorem; some were proven by assuming the equivalence of the Moufang identities. So, when proving Moufang's Theorem none of them will be used; in fact, every result in Chapter 4 is proven directly using either the basic definitions stated in Chapter 1 or some results obtained in Chapter 3. More importantly, all the results in Chapter 3 were proven from scratch.

Theorem 2.1. *(Bruck, 1971, Moufang's Theorem, p.117) Suppose L is a Moufang loop. Then L is diassociative, that is, $\langle x,y\rangle$ is a group for any x,y in L. In addition, if $(x,y,z)=1$ for some x,y,z in L, then $\langle x,y,z\rangle$ is a group.*

Theorem 2.2. *(Bruck, 1971, Theorem 2.1, p.114) Suppose L is a Moufang loop. Then the nucleus $N = N(L)$ is a normal subloop of L.*

Proposition 2.3. *(Bruck, 1971, Lemmas 5.4(5.16), p.124; 3.2, p.117 and (4.1), p.120) Let $x, y, z \in L$ be elements of a Moufang loop L. Then*

(a) $x\mathscr{L}(z,y) = x(x,y,z)^{-1}$,

(b) $(x^n)\theta = (x\theta)^n$ *for any integer n with* $x \in L$ *and* $\theta \in I(L)$.

Proposition 2.4. *(Leong and Rajah, 1997, Lemma 6) Suppose L is a minimally nonassociative Moufang loop of odd order. Then* L_a *is a Sylow subloop of* $N \implies L_a = N$.

Proposition 2.5. *(Chee and Rajah, 2012, Proposition 3.4) Suppose L is a minimally nonassociative Moufang loop of odd order. Then* $(k_1k_2, l_1, l_2) = (k_1, l_1, l_2)(k_2, l_1, l_2)$ *for each* $k_i \in L_a$ *and* $l_i \in L$.

Theorem 2.6. *(Rajah and Chee, 2011a, Lemmas 3.18, 3.19), (Chee and Rajah, 2012, Theorem 3.7, 4.7), (Leong and Rajah, 1996b, Lemma 6(a), (c)), (Leong and Rajah, 1997, Lemma 1(b)) Suppose L is a minimally nonassociative Moufang loop of odd order and M is a maximal normal subloop of L. Then*

(a) $(k,w,l) \neq 1$ *for some* $k \in L_a, w \in M$, $l \in L \implies L_a$ *contains a proper non-trivial subloop which is normal in M.*

(b) for any $w \in M$ *and* $l \in L$, *there exists some* $k_0 \in L_a \setminus \{1\}$ *such that* $(k_0,w,l) = (u^{-1}k_0u,w,l) = 1$ *for all* $u \in M$.

(c) $(k,w,l) = (l,k,w^{-1})^{-1}$ *for any* $k \in L_a, w \in M$, *and* $l \in L$.

(d) $((k,w,l)[k,w],w,l) = 1$ *for any* $k \in L_a, w \in M$, *and* $l \in L$.

(e) $L_a \lhd N$ *if and only if* $(L_a, M, L) = \{1\}$.

(f) L_a *and* L_c *lie in M, and* $L = M\langle x\rangle$ *for any* $x \in L \setminus M$.

Theorem 2.7. *(Chee and Rajah, 2014, Lemma 4.4) Suppose L is a minimally nonassociative Moufang loop of odd order and M a maximal normal subloop of L.*

(a) Suppose there exist some $k \in L_a$, $w \in M$ *and* $l \in L$ *such that* $(k,w,l) = 1$. *Then* $(k, L_a\langle w\rangle, l) = \{1\}$.

(b) Suppose there exist some $k \in L_a$, $w \in M$ *and* $l \in L$ *such that* $[k,w] = 1$. *Then* $[k, L_a\langle w\rangle] = \{1\}$.

Theorem 2.8. *(Chee and Rajah, 2014, Lemma 4.5), (Rajah and Chee, 2011c, Lemma 4.2, 4.4) Suppose L is a minimally nonassociative Moufang loop of odd order and M a maximal normal subloop of L.*

(a) Suppose there exist some $k \in L_a \setminus \{1\}$ *and* $x \in L \setminus M$ *such that* $(k,M,x) = [k,M] = \{1\}$. *Then* $L_a \lhd N$.

(b) If $L_a \subseteq N$, *then for every* $x \in L \setminus M$, *there exist some* $g,h \in M \setminus L_a$ *such that* $(x,g,h) \neq 1$.

(c) If $L_a \subseteq N$, *then* $[M,(L \setminus M,M,M)] = \{1\}$.

Proposition 2.9. *(Rajah and Chee, 2011a, Lemma 3.17) Suppose L is a Moufang loop of odd order and K a normal Hall subloop of L. Let* $K = \langle x\rangle L_a$ *for some* $x \in K \setminus L_a$ *and* $L_a \subseteq N$. *Then* $K \subseteq N$.

Proposition 2.10. *(Rajah and Chee, 2011c, Lemma 4.5) If G is a group and* $r,s,t \in G$ *with* $[r,t] = [s,t] = 1$ *such that* $r^{-1}sr = s^{\alpha}t^{\beta}$, *for some* α, $\beta \in \mathbb{Z}^+$; *then* $r^{-n}sr^n = s^{\alpha^n}t^{\beta(\alpha^0+\alpha^1+\ldots+\alpha^{n-1})}$.

Proposition 2.11. *(Chee and Rajah, 2014, Lemma 4.2) Let L be a nonassociative Moufang loop of odd order and* $x \in L$. *Suppose* $|L_a| = p^2$ *for some prime p and* $(|x|, p-1) = 1$. *If there exists some* $k_0 \in L_a \setminus \{1\}$ *such that* $[k_0,x] = 1$, *then* $[L_a,x] \subseteq \langle k_0\rangle$.

Proposition 2.12. *(Chee and Rajah, 2014, Cor. 4.3) Let L be a nonassociative Moufang loop of odd order and $x \in L$. Suppose $|L_a| = p^2$ for some prime p and $(|x|, p) = (|x|, p-1) = 1$. If there exists some $k_0 \in L_a \setminus \{1\}$ such that $[k_0, x] = 1$, then $[L_a, x] = \{1\}$.*

Theorem 2.13. *(Niven et al., 2008, Theorem 2.27, p.54) Let q be a prime. Then the congruence $\mu^n \equiv 1 (mod\ q)$ has $(n, q-1)$ solutions for μ.*

Theorem 2.14. *(Glauberman, 1968, Theorem 12, 16) Let L be a Moufang loop of odd order, K a subloop of L, and π a set of primes. Then*

(a) L is solvable,

(b) L contains a Hall π -subloop.

Theorem 2.15. *(Grishkov and Zavarnitsine, 2005, Lagrange's Theorem) Suppose L is a Moufang loop. Then $|K|$ divides $|L|$ for every K a subloop of L.*

Theorem 2.16. *Any Moufang loop L is a group if $|L|$ is any of the following orders:*

(a) (Chein, 1974, Cor. 4, Prop. 3) p, p^2, p^3 or pq; for p and q distinct primes.

(b) (Purtill, 1988, Theorem 3.1, 3.3) pqr or p^2q; for p, q and r odd primes with $p < q < r$.

(c) (Leong and Rajah, 1995, Theorem) pq^2; for p and q distinct odd primes.

(d) (Leong and Rajah, 1996a, Theorem) $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$; for $1 \leq \alpha_i \leq 2$ and each p_i distinct primes and $\alpha_i \leq 2$.

(e) (Leong and Rajah, 1997, Theorem 1) $p^{\alpha} q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$; for p and q_i primes with $p < q_1 < ... < q_n$, and $\beta_i \leq 2$, with $\alpha \leq 3$, or $\alpha \leq 4$ when $p > 3$.

(f) (Rajah and Chee, 2011b, Theorem 4.2) $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} q^3$; for distinct odd primes $p_1, p_2, ..., p_n, q$ with $q \not\equiv 1 (mod\ p_i)$, $q > p_i$ and $1 \leq \alpha_i \leq 2$.

(g) (Chee and Rajah, 2014, Theorem 4.8) pq^4, for p and q odd primes with $p < q$, and $q \not\equiv 1 (mod\ p)$.

Proposition 2.17. *(Leong and Rajah, 1995, Lemma 2) Let L be a Moufang loop of odd order and every proper subloop of L be a group. If there exists a minimal normal Sylow subloop in L, then L is a group.*

Proposition 2.18. *(Leong and Rajah, 1996b, Lemma 3) Suppose L is a Moufang loop of odd order such that every proper subloop and proper quotient loop of L is a group. Let Q be a Hall subloop of L such that* $(|L_a|,|Q|)=1$*, and* $Q \lhd L_aQ$*. Then L is a group.*

Proposition 2.19. *(Leong and Rajah, 1996b, Lemma 2) Let L be a Moufang loop of odd order and every proper subloop of L be a group. If N contains a Hall subloop of L, then L is a group.*

Theorem 2.20. *(Leong and Rajah, 1996b, Lemma 1) Let L be a Moufang loop and* $R \lhd L$*. If the quotient* L/R *is a group then* $L_a \subset R$*.*

Theorem 2.21. *(Leong and Rajah, 1997, Lemma 1(a)), (Glauberman, 1968, Theorem 7), (Chee and Rajah, 2012, Lemma 3.3(b)) Suppose L is a minimally nonassociative Moufang loop of odd order. Then*

(a) L_a *is a minimal normal subloop of L; and is an elementary abelian group.*

(b) L_a *is the unique minimal normal subloop of L and* $(L_a,L_a,L)=\{1\}$*.*

Proposition 2.22. *(Leong and Rajah, 1997, Lemma 5) Let K be a subloop of* $C_L(L_a)$ *and* $(|K|,|L_a|)=1$*. Then* $K \subset N$*.*

Proposition 2.23. *(Ademola and Rajah, 2016, Lemma 4.1) Suppose* $|L|=p^{\alpha}m$ *where p is the smallest prime dividing* $|L|$ *with* $(p,m)=1$*,* $|L|$ *is odd and* $\alpha \in \{1,2\}$*. Then there exists a subloop M of order m normal in L.*

Theorem 2.24. *(Rajah and Chee, 2011c, Lemma 4.1) Suppose L is a Moufang loop of order* $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}q$*, where* $p_1,p_2,...,p_n$ *and q are odd primes with* $p_1<p_2<...<p_n<q$ *and* $\alpha_1,\alpha_2,...,\alpha_n \in \mathbb{Z}^+$*,* $q \not\equiv 1(mod\ p_i)$ *for all i. Then there exists a normal*

subloop of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ *in L.*

Theorem 2.25. *(Chee and Rajah, 2012, Cor. 4.2) Suppose L is a nonassociative Moufang loop. If L is finite, then* $|L|/|N| \neq 1$, *p or pq; where p and q are (not necessarily distinct) primes.*

Proposition 2.26. *(Ademola, 2017, Lemma 5.3) Let L be a Moufang loop of odd order and R be a normal Hall subloop of L. Then there does not exist any element* $x \in R \setminus N$ *such that* $R \subset \langle x \rangle N$.

Proposition 2.27. *(Ademola, 2017, Lemma 5.5) Let L be a finite Moufang loop and* $K \lhd L$ *such that* $\frac{|L|}{|K|}$ *is a prime or the product of two (not necessarily distinct) primes. Then* $L = HK$ *for some associative subloop H of L. Moreover,* $H = \langle x \rangle$ *for some* $x \in L \setminus K$ *if* $\frac{|L|}{|K|}$ *is a prime.*

Theorem 2.28. *(Gagola III, 2014, Theorem 1) Suppose L is a finite Moufang loop with an order that is coprime to six. Then any minimal normal subloop of L will be contained in the nucleus of L.*

CHAPTER 3

MOUFANG IDENTITIES ON LOOPS AND MAGMAS

3.1 Introduction

A Moufang loop $\langle L, \cdot \rangle$ is a loop that satisfies any one of the identities: $xy \cdot zx = (x \cdot yz)x$, $xy \cdot zx = x(yz \cdot x)$, $(xy \cdot z)y = x(y \cdot zy)$ or $x(y \cdot xz) = (xy \cdot x)z$. This definition, in itself, quietly assumes the equivalence of these four identities, since on the one hand, it is defining a single variety of loops, but on the other hand, four apparently different identities are used (to define it). Bruck (1971), Pflugfelder (1990) and Drapal (2010) contain proofs that these four identities are equivalent for loops. However, these proofs are cumbersome as they require additional knowledge about autotopism and hence making it highly technical. This chapter, provides an alternative proof of the equivalence - a proof that is done in an algebraic manner which can be followed and understood with little or no difficulty. It also proves that, not only these identities, but localized (generalized) versions of these identities, are equivalent in magmas (which are generalized versions of loops).

3.2 Equivalence of the Four Identities in Loops

Though the main objective is to prove the equivalence of the Moufang identities by using purely algebraic methods, the proof involves establishing several other (well-known) properties of Moufang loops as well. This includes the properties of left and right cancelation laws, associativity between any two elements, existence of a (unique)

inverse element for every element and the inverse property. Though proofs of these properties do exist in literature, but it is to be noted that some of them do use additional concepts and definitions as well (Bruck (1971), Pflugfelder (1990) and Drapal (2010)). So, in order to maintain the claim that the equivalence of the four Moufang identities can be proven by using a purely algebraic method, these other properties are also proven in a likewise manner. This ensures that this work is as self-contained as possible.

In the following theorems, various properties of loops that satisfy any one of the following (Moufang) identities are obtained. So, in the statement of Lemmas 3.3, 3.4, 3.5, 3.6 and Theorem 3.7, these are the identities that are referred to:

$$xy \cdot zx = (x \cdot yz)x \tag{3.1}$$

$$(xy \cdot z)y = x(y \cdot zy) \tag{3.2}$$

$$x(y \cdot xz) = (xy \cdot x)z \tag{3.3}$$

Note that instead of the four Moufang identities listed in the introduction, only three of them are chosen (and numbered). This is because the identity $xy \cdot zx = x(yz \cdot x)$ can be shown to be equivalent to the identity (3.1). The equivalence of (3.1), (3.2) and (3.3) is first proved before proving (3.1) is equivalent to the other "missing" identity, invariably proving the equivalence of all four Moufang identities.

Lemma 3.1. ***(Left and right cancelation laws)*** *Let $\langle L, \cdot \rangle$ be a quasigroup and $x, y, z \in L$. Then $\langle L, \cdot \rangle$ satisfies the left and right cancelation laws, that is, $x \cdot y = x \cdot z \Rightarrow y = z$ (LCL); and $x \cdot y = z \cdot y \Rightarrow x = z$ (RCL) respectively.*

Proof. Let $x \cdot y = x \cdot z \Rightarrow x \cdot y - x \cdot z = 0 \Rightarrow x(y-z) = 0 \Rightarrow y = z$. Similarly if $x \cdot y = z \cdot y$ then $x = z$. □

Lemma 3.2. *A binary system that contains both left and right identities contains a unique identity element which is the unique left and right identity element of the system.*

Proof. Use Definition 1.2(a) and (b) to get $e_R = e_L \cdot e_R = e_L$ if e_R and e_L are respectively some right and left identities. Then, if e'_R and e'_L are also right and left identities respectively, also $e'_R = e_L$ and $e_R = e'_L$. This completes the proof of this lemma. □

Lemma 3.3. ***(Associativity of two elements)*** *Let $\langle L, \cdot \rangle$ be a loop. Suppose L satisfies any one of the three Moufang identities (3.1), (3.2) or (3.3). Then L is both a flexible and alternative loop.*

Proof. Since L is a loop, it contains the identity element e.

Case 1: Suppose (3.1) holds. For any $x, y \in L$, $\quad xe \cdot yx = (x \cdot ey)x$ by (3.1) $\Rightarrow x \cdot yx = xy \cdot x$, which proves the flexible identity. Also for $x, y \in L$, by the quasigroup property, there exists $u \in L$ such that $xu = y$. Now by (3.1) and the flexible identity

$xu \cdot xx = (x \cdot ux)x = (xu \cdot x)x \Rightarrow y \cdot xx = yx \cdot x$, which proves the right alternative identity. Similarly for $x, y \in L$, there exists $v \in L$ such that $vx = y$. Then by (3.1) and the right alternative identity, $xx \cdot vx = (x \cdot xv)x = x(xv \cdot x) = x(x \cdot vx) \Rightarrow xx \cdot y = x \cdot xy$, which proves the left alternative identity.

Case 2: Suppose (3.2) holds. Then $(ex \cdot y)x = e(x \cdot yx)$ by (3.2), for any $x, y \in L$. So $xy \cdot x = x \cdot yx$ which proves the flexible identity. Also by (3.2) and the flexible identity, $(xx \cdot y)x = x(x \cdot yx) = x(xy \cdot x) = (x \cdot xy)x$. By RCL, $xx \cdot y = x \cdot xy$. This proves the left alternative identity. Similarly $(yx \cdot e)x = y(x \cdot ex)$ by (3.2), and this implies that