CLASSIFICATION OF MOUFANG LOOPS OF ODD ORDER

by

CHEE WING LOON

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

June 2010

ACKNOWLEDGEMENT

First and foremost, I would like to thank the almighty God for His grace, wisdom and guidance throughout my life.

I wish to express the highest appreciation to my supervisor, Assoc. Prof. Andrew Rajah a/l Balasingam Gnanaraj of the School of Mathematical Sciences, Universiti Sains Malaysia. With his enthusiasm, inspiration and great efforts to explain things clearly and simply, he helped to make mathematics fun for me. I also like to thank him for introducing me to the field of Moufang loops. He has been extremely generous with his insight and knowledge.

I would like to extend my gratitute to the many people who have taught and inspired me in the field of mathematics: Prof. Ong Boon Hua, Assoc. Prof. Sriwulan Adji, Assoc. Prof. V. Ravichandran, Dr. Ang Miin Huey, Dr. Hajar Sulaiman and Dr. Lee See Keong. Their constructive comments and valuable advice have had a remarkable influence on me.

I am deeply grateful to Universiti Sains Malaysia for the approval of my conversion from M.Sc. to Ph.D. I also wish to thank the Institute of Postgraduate Studies for their offer of USM Fellowship Scheme. With this financial aid, I am able to fully concentrate and focus on my research. I want to thank the School of Mathematical Sciences for providing me with a pleasant environment for working and studying. Thanks to all the staff for their every single contribution in completing my research.

Finally, I would like to give my special thanks to my wife, Tan Ching Ting and my family for their love and encouragement throughout all these years. This work is dedicated to them in appreciation of their tremendous support for my pursuit of my dream of obtaining a doctorate in mathematics.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF PUBLICATIONS

[1] Rajah, A. & Chee, W. L., Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$. To appear in the Bulletin of the Malaysian Mathematical Sciences Society.

LIST OF SYMBOLS

$\mathbb{Z}$	the set of all integers
$\mathbb{Z}^+$	the set of all positive integers
$a \mid b$	integer a is a divisor of integer b
(a, b)	greatest common divisor of integers a and b
$a \equiv b \pmod{n}$	a is congruent modulo n to b
$\forall$	for all
$\exists$	there exists
$\in$	is an element of
$\subseteq$	is a subset of
$\subset$	is a proper subset of
$\leq$	is a subloop of
$<$	is a proper subloop of
$\trianglelefteq$	is a normal subloop of
$\lhd$	is a proper normal subloop of
$\lvert S\rvert$	number of elements in a set S
$\lvert x\rvert$	order of an element x
(x, y, z)	associator of elements x, y and z
$[x, y]$	commutator of elements x and y
$L \times K$	direct product of loops L and K
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 set S

PENGELASAN LUP-LUP MOUFANG BERPERINGKAT GANJIL

ABSTRAK

Identiti Moufang $(x \cdot y) \cdot (z \cdot x) = [x \cdot (y \cdot z)] \cdot x$ pertama kali diperkenalkan oleh Ruth Moufang pada 1935. Kini, suatu lup yang memenuhi identiti Moufang dipanggil suatu lup Moufang. Minat kami adalah untuk mengkaji soalan: "Bagi suatu integer positif n, mestikah setiap lup Moufang berperingkat n kalis sekutuan?". Jika tidak, bolehkah kita bina suatu lup Moufang tak kalis sekutuan berperingkat n?

Soalan-soalan ini telah dikaji dengan menangani lup-lup Moufang berperingkat genap dan ganjil secara berasingan. Bagi peringkat genap, Chein (1974) telah membina suatu kelas lup Moufang tak kalis sekutuan, $M(G, 2)$ berperingkat $2m$ dengan menggunakan suatu kumpulan tak abelan G berperingkat m. Selepas itu, Chein dan Rajah (2000) telah membuktikan bahawa semua lup Moufang berperingkat $2m$ adalah kalis sekutuan jika dan hanya jika semua kumpulan berperingkat m adalah abelan.

Bagi kes lup-lup Moufang berperingkat ganjil, kewujudan lup-lup Moufang tak kalis sekutuan berperingkat 3^4 dan p^5 (bagi sebarang nombor perdana $p > 3$), telah ditunjukkan masing-masing oleh Bol (1937) dan Wright (1965). Kelas lup-lup Moufang tak kalis sekutuan yang terkini telah dibina oleh Rajah (2001) dengan menunjukkan bahawa bagi nombor-nombor perdana yang berlainan p dan q, wujud suatu lup Moufang tak kalis sekutuan berperingkat pq^3 jika dan hanya jika $q \equiv 1 \pmod{p}$. Sebaliknya, bukti bagi ketakwujudan lup-lup Moufang tak kalis sekutuan telah dijalankan selama kira-kira 4 dekad. Telah diketahui bahawa semua lup Moufang berperingkat (ganjil) seperti berikut merupakan kumpulan:

(i) $p^\alpha q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$; $p, q_1, q_2, \ldots, q_n$ ialah nombor-nombor perdana ganjil, $p < q_1 < q_2 < \cdots < q_n$, $\alpha \leq 4$ dan $\beta_i \leq 2$ ($p > 3$ jika $\alpha = 4$);

(ii) $p_1p_2\cdots p_nq^3$; $p_1, p_2, \ldots, p_n$ dan q ialah nombor-nombor perdana ganjil yang berlainan, $q \not\equiv 1 \pmod{p_1}$ dan $q^2 \not\equiv 1 \pmod{p_i}$ bagi semua $i \in \{2, \ldots, n\}$.

Dalam disertasi ini, kami mulakan dengan mentakrif konsep lup-lup Moufang tak kalis sekutuan secara minimum dan kami buktikan beberapa sifat lup-lup tersebut. Seterusnya, kami mengkaji beberapa kes terbuka bagi lup-lup Moufang berperingkat ganjil. Kami membuktikan bahawa lup-lup Moufang berperingkat berikut ialah kumpulan:

(i) $p_1\cdots p_mq^3r_1\cdots r_n$; $p_1, \ldots, p_m, q, r_1, \ldots, r_n$ ialah nombor-nombor perdana ganjil, $p_1 < \cdots < p_m < q < r_1 < \cdots < r_n$ dan $q \not\equiv 1 \pmod{p_i}$ bagi semua $i \in \{1, 2, \ldots, m\}$;

(ii) $p_1^2\cdots p_m^2q^3r_1^2\cdots r_n^2$; $p_1, \ldots, p_m, q, r_1, \ldots, r_n$ ialah nombor-nombor perdana ganjil, $p_1 < \cdots < p_m < q < r_1 < \cdots < r_n$ dan $q \not\equiv 1 \pmod{p_i}$ bagi semua $i \in \{1, 2, \ldots, m\}$;

(iii) p^3q^3; p dan q ialah nombor-nombor perdana ganjil, $p < q$ dan $q \not\equiv 1 \pmod{p}$; dan

(iv) pq^4; p dan q ialah nombor-nombor perdana ganjil, $p < q$ dan $q \not\equiv 1 \pmod{p}$.

Oleh sebab semua lup Moufang yang disenaraikan di atas adalah kalis sekutuan, kami tukar penumpuan kajian kami ke lup-lup Moufang tak kalis sekutuan yang berperingkat 3^4. Pengelasan yang dibuat oleh Nagy dan Vojtěchovský (2007) ke atas lup-lup Moufang ini adalah dibantu komputer. Maka, kami beri suatu bukti teoretikal bagi keputusan tersebut dengan mewujudkan suatu petua hasil darab bagi sebarang dua unsur dalam lup Moufang itu dan kami lengkapkan pengelasan tersebut.

CLASSIFICATION OF MOUFANG LOOPS OF ODD ORDER

ABSTRACT

The Moufang identity $(x \cdot y) \cdot (z \cdot x) = [x \cdot (y \cdot z)] \cdot x$ was first introduced by Ruth Moufang in 1935. Now, a loop that satisfies the Moufang identity is called a Moufang loop. Our interest is to study the question: "For a positive integer n, must every Moufang loop of order n be associative?". If not, can we construct a nonassociative Moufang loop of order n?

These questions have been studied by handling Moufang loops of even and odd order separately. For even order, Chein (1974) constructed a class of nonassociative Moufang loop, $M(G, 2)$ of order $2m$ where G is a nonabelian group of order m. Following that, Chein and Rajah (2000) have proved that all Moufang loops of order $2m$ are associative if and only if all groups of order m are abelian.

As for the case of Moufang loops of odd order, the existence of nonassociative Moufang loops of order 3^4 and p^5 (for any prime $p > 3$), has been shown by Bol (1937) and Wright (1965) respectively. The most recent class of nonassociative Moufang loops was constructed by Rajah (2001), where he showed that for distinct odd primes p and q, there exists a nonassociative Moufang loop of order pq^3 if and only if $q \equiv 1 \pmod{p}$. On the other hand, the proofs on nonexistence of nonassociative Moufang loops have progressed gradually for about four decades. All Moufang loops of the following (odd) orders are known to be groups:

(i) $p^\alpha q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$ where $p, q_1, q_2, \ldots, q_n$ are odd primes, $p < q_1 < q_2 < \cdots < q_n$, $\alpha \leq 4$ and $\beta_i \leq 2$ ($p > 3$ if $\alpha = 4$);

(ii) $p_1 p_2 \cdots p_n q^3$ where $p_1, p_2, \ldots, p_n$ and q are distinct odd primes, $q \not\equiv 1 \pmod{p_1}$ and $q^2 \not\equiv 1 \pmod{p_i}$ for all $i \in \{2, \ldots, n\}$.

In this dissertation, we begin by defining the concept of minimally nonassociative Moufang loops and proving some of their properties. From there, we

continue with some of the known open cases for Moufang loops of particular odd orders. We prove that Moufang loops of the following orders are groups:

(i) $p_1 \cdots p_m q^3 r_1 \cdots r_n$ where $p_1, \ldots, p_m, q, r_1, \ldots, r_n$ are odd primes, $p_1 < \cdots < p_m < q < r_1 < \cdots < r_n$ and $q \not\equiv 1 \pmod{p_i}$ for all $i \in \{1, 2, \ldots, m\}$;

(ii) $p_1^2 \cdots p_m^2 q^3 r_1^2 \cdots r_n^2$ where $p_1, \ldots, p_m, q, r_1, \ldots, r_n$ are odd primes, $p_1 < \cdots < p_m < q < r_1 < \cdots < r_n$ and $q \not\equiv 1 \pmod{p_i}$ for all $i \in \{1, 2, \ldots, m\}$;

(iii) $p^3 q^3$ where p and q are odd primes, $p < q$ and $q \not\equiv 1 \pmod{p}$; and

(iv) pq^4 where p and q are odd primes, $p < q$ and $q \not\equiv 1 \pmod{p}$.

In view of the fact that all the Moufang loops listed above are associative, we turn our attention to the study of nonassociative Moufang loops of order 3^4. The classification done by Nagy and Vojtěchovský (2007) on these Moufang loops was computer-aided. Hence, we give a theoretical proof of this result, establish a product rule for any two elements in that Moufang loop and complete the classification.

CHAPTER 1

INTRODUCTION

The Moufang identity was first introduced in 1935 by a German mathematician, Ruth Moufang in her paper *Zur Struktur von Alternativkörpern*. She defined an inverse property loop $\langle Q^*, \cdot \rangle$ that satisfies the identity

(i) $[(x \cdot y) \cdot x] \cdot z = x \cdot [y \cdot (x \cdot z)]$.

Bol (1937) soon showed that (i) implies another identity

(ii) $(x \cdot y) \cdot (z \cdot x) = x \cdot [(y \cdot z) \cdot x]$.

and Bruck (1971) later proved that they both are equivalent to

(iii) $[(z \cdot x) \cdot y] \cdot x = z \cdot [x \cdot (y \cdot x)]$.

Moufang showed that if any three elements in Q^* associate in some order, then they generate a group. A corollary of that is that $\langle Q^*, \cdot \rangle$ is diassociative. This result is known as Moufang's theorem and the identities (i)–(iii) are called the Moufang identities. Now, a Moufang loop is defined as a loop satisfying any one of these three identities. Bruck (1971) also showed that Moufang loops have the inverse property, which follows from diassociativity.

Looking at the definition of groups, we can see that if a Moufang loop is associative, then it becomes a group. Hence, there is a very close relationship between Moufang loops and groups. All groups are Moufang loops, but the converse is not true. Therefore, our interest is to determine which Moufang loops are associative, and which are not. Particularly, we study the question: "For a positive integer n, are all Moufang loops of order n associative?". If the answer is negative, then we wish to construct an explicit counterexample, i.e., a nonassociative Moufang loop of order n. Before we can do that, however, we need to study its properties and somehow establish a product rule between any two elements in that Moufang loop.

Suppose the existence of a nonassociative Moufang loop of order n is known, then we can construct a nonassociative Moufang loop of order mn ($m \in \mathbb{Z}^+$) as follows: Let $\langle L, \cdot \rangle$ be a nonassociative Moufang loop of order n and $\langle G, * \rangle$ a group of order m. Define M as the direct product of L and G, i.e., $M = L \times G = \{(x, y) \mid x \in L, y \in G\}$ and the binary operation $\odot$ on M as $(x_1, y_1) \odot (x_2, y_2) = (x_1 \cdot x_2, y_1 * y_2)$. Then $\langle M, \odot \rangle$ is a nonassociative Moufang loop of order mn. Consequently, for positive integers m and n, if all Moufang loops of order mn are associative, then so are all Moufang loops of order m (and n). We continue studying Moufang loops by dividing into the two cases of even order and odd order.

Chein (1974) gave a method to construct nonassociative Moufang loops of even order ($2m$) by using a nonabelian group of order m. Since the smallest nonabelian group is the symmetric group S_3 which is of order 6, the smallest nonassociative Moufang loop that can be constructed using this method would be of order 12. This is in fact the smallest nonassociative Moufang loop as Chein (1974) has also proved various theorems which show that all Moufang loops of order less than 12 are associative. (He proved that Moufang loops of order p, p^2, p^3 or pq (for primes p and q) must be groups.) We give the multiplication table of this Moufang loop in Table 1.1. Chein and Rajah (2000) have completely resolved the even case and proved that there exists a nonassociative Moufang loop of order $2m$ if and only if there exists a nonabelian group of order m.

For the case of Moufang loops of odd order, the existence of nonassociative Moufang loops of order 3^4 and p^5 for every prime $p > 3$, has been proved by Bol (1937) and Wright (1965) respectively. The most recent class was constructed by Rajah (2001): For any distinct odd primes p and q, there exists a nonassociative Moufang loop of order pq^3 if and only if $q \equiv 1 \pmod{p}$. The construction is as follows: For odd primes p and q satisfying $q \equiv 1 \pmod{p}$, define $L = \{(\alpha, \beta, \gamma, \delta) \mid$

Table 1.1: Cayley table of a nonassociative Moufang loop of order 12

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	3	1	5	6	4	8	9	7	12	10	11
3	3	1	2	6	4	5	9	7	8	11	12	10
4	4	6	5	1	3	2	10	11	12	7	8	9
5	5	4	6	2	1	3	11	12	10	9	7	8
6	6	5	4	3	2	1	12	10	11	8	9	7
7	7	9	8	10	11	12	1	3	2	4	5	6
8	8	7	9	11	12	10	2	1	3	6	4	5
9	9	8	7	12	10	11	3	2	1	5	6	4
10	10	11	12	7	9	8	4	6	5	1	2	3
11	11	12	10	8	7	9	5	4	6	3	1	2
12	12	10	11	9	8	7	6	5	4	2	3	1

$\alpha \in \{0, 1, \ldots, p-1\}$; $\beta, \gamma, \delta \in \{0, 1, \ldots, q-1\}\}$ and the product of two elements in L,

$$\begin{aligned} \ell_1 \cdot \ell_2 &= (\alpha_1, \beta_1, \gamma_1, \delta_1) \cdot (\alpha_2, \beta_2, \gamma_2, \delta_2) \\ &= (\alpha_{(1,2)}, \beta_{(1,2)}, \gamma_{(1,2)}, \delta_{(1,2)}) \end{aligned}$$

where

$$\alpha_{(1,2)} \equiv (\alpha_1 + \alpha_2) \pmod{p};$$

$$\beta_{(1,2)} \equiv (\beta_1 \mu^{(p-1)\alpha_2} + \beta_2) \pmod{q};$$

$$\gamma_{(1,2)} \equiv (\gamma_1 \mu^{(p-1)\alpha_2} + \gamma_2) \pmod{q};$$

$$\begin{aligned} \delta_{(1,2)} \equiv \{&\delta_1 \mu^{\alpha_2} + \delta_2 + \phi \beta_2 \gamma_1 \mu^{(p-1)\alpha_2} + [\beta_1 \gamma_1 (\mu^{\alpha_2} - \mu^{(p-2)\alpha_2}) \\ &+ (\beta_1 \gamma_2 - \beta_2 \gamma_1)(\mu^{\alpha_{(1,2)}} - \mu^{(p-1)\alpha_2})]/(\mu - 1)\} \pmod{q}; \end{aligned}$$

μ is an integer satisfying $\mu^p \equiv 1 \pmod{q}$ and $\mu \not\equiv 1 \pmod{q}$;

ϕ is an integer satisfying $\phi(\mu - 1) \equiv -2 \pmod{q}$ when $p \neq 3$

and ϕ is any integer when $p = 3$.

Then L is a nonassociative Moufang loop of odd order pq^3.

Much work has also been done in the "opposite" direction, i.e., in proving the nonexistence of nonassociative Moufang loops of particular orders. Below, we give a list of orders of Moufang loops for which all of them are proved to be groups:

(i) p, p^2, p^3 and pq where p and q are primes (Chein, 1974);

(ii) p^4 where p is a prime with $p > 3$ (Leong, 1974);

(iii) pqr and p^2q where p, q and r are odd primes with $p < q < r$ (Purtill, 1988);

(iv) pq^2 where p and q are odd primes with $p < q$ (Leong & Rajah, 1995);

(v) $p_1^2 p_2^2 \cdots p_n^2$ where $p_1, p_2, \ldots, p_n$ are distinct odd primes (Leong & Rajah, 1996a);

(vi) $p^3 q_1 q_2 \cdots q_n$ where $p, q_1, q_2, \ldots, q_n$ are odd primes with $p < q_1 < q_2 < \cdots < q_n$ (Leong, Teh & Lim, 1994);

(vii) $p^4 q_1 q_2 \cdots q_n$ where $p, q_1, q_2, \ldots, q_n$ are odd primes with $3 < p < q_1 < q_2 < \cdots < q_n$ (Leong & Rajah, 1996b);

(viii) $p^4 q_1^2 q_2^2 \cdots q_n^2$ where $p, q_1, q_2, \ldots, q_n$ are odd primes with $3 < p < q_1 < q_2 < \cdots < q_n$ (Leong & Rajah, 1997);

(ix) pq^3 where p and q are distinct odd primes with $q \not\equiv 1 \pmod{p}$ (Rajah, 2001);

(x) $p_1 p_2 \cdots p_n q^3$ where $p_1, p_2, \ldots, p_n, q$ are distinct odd primes with $q \not\equiv 1 \pmod{p_1}$ and $q^2 \not\equiv 1 \pmod{p_i}$ for each $i \in \{2, 3, \ldots, n\}$ (Chein & Rajah, 2000);

(xi) $p_1 p_2 \cdots p_n q^3$ where $p_1, p_2, \ldots, p_n, q$ are odd primes with $p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 \pmod{p_i}$, $p_i \not\equiv 1 \pmod{p_j}$ for all $i, j \in \{1, 2, \ldots, n\}$, and the nucleus is not trivial (Rajah & Chong, 2008).

The result (viii) is a significant one as it covers all the previous results (i)–(vii). Note also that (xi) is the only result with condition on the nucleus.

In this dissertation, we continue with the investigation of open problems that arise from these results. The organisation of this dissertation is as follows.

Chapter 2 is devoted to some basic definitions and known results in Moufang loops and number theory. In Chapter 3, we define minimally nonassociative Moufang loops and study their properties. In Section 4.1 of Chapter 4, we begin with the extension of the results above (particularly (vi), (x) and (xi)) and give a complete resolution for Moufang loops of odd order $p_1p_2\cdots p_nq^3$. In Section 4.2, we extend this result to include Moufang loops of odd order $p_1^2p_2^2\cdots p_n^2q^3$. The result is then used in Section 4.3 to study Moufang loops of odd order p^3q^3. In the last section of Chapter 4, we study Moufang loops of odd order pq^4 which arises after the result in Section 4.1. In Chapter 5, we give a theoretical proof on the construction of nonassociative Moufang loops of order 81 and the classification of them (up to isomorphism). A discussion on the direction of further research is put forward in Chapter 6. Finally, an appendix of the Cayley tables of all 5 nonisomorphic nonassociative Moufang loops of order 81 is provided.

On the journey of Moufang loops, our ultimate aim is to classify all Moufang loops of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ where $p_1, p_2, \ldots, p_n$ are distinct odd primes and $\alpha_i \leq 4$ (since there exist nonassociative Moufang loops of order p^5 for all primes p). This dissertation has yet to bring us to our destination but it serves as a stepping stone towards the classification of Moufang loops of odd order.

CHAPTER 2

PRELIMINARIES

Before we begin our discussion, we would like to list down some of the definitions, basic properties and known results that are needed in the subsequent chapters. For those not listed, we refer the reader to (Bruck, 1971) and (Glauberman, 1968).

2.1 Definitions and Notations

Definition 2.1.1. The ***order*** (or *cardinality*) of a set S, denoted by $|S|$, is the number of elements in S. If the order of S is finite, then S is called a finite set. Otherwise, S is called an infinite set.

Definition 2.1.2. A ***binary operation*** on a nonempty set S is a function from $S \times S$ to S.

Definition 2.1.3. A nonempty set G with a binary operation '$\cdot$' on G, denoted by $\langle G, \cdot \rangle$, is called a ***groupoid***.

Often, when there is no risk of confusion, the notation for a groupoid $\langle G, \cdot \rangle$ is simplified to G instead. Also, we write the product between any two elements by using juxtaposition, center dot $\cdot$ and parentheses ( ) simultaneously. Naturally, when multiplying elements, juxtaposition precedes center dot, which in turn precedes parentheses. Hence, we can write $[x \cdot (y \cdot z)] \cdot w$ simply as $(x \cdot yz)w$.

Definition 2.1.4. A groupoid G is called a ***group*** if it satisfies the following conditions:

(a) G has an identity element, i.e., there exists $1 \in G$ such that $1x = x1 = x$ for all $x \in G$.

(b) Every element in G has an inverse, i.e., for all $x \in G$, there exists $x^{-1} \in G$ such that $x^{-1}x = xx^{-1} = 1$.

(c) G is associative, i.e., $xy \cdot z = x \cdot yz$ for all $x, y, z \in G$.

Definition 2.1.5. A group G is called an ***abelian group*** if G is commutative, i.e., $xy = yx$ for all $x, y \in G$.

Definition 2.1.6. An abelian group G is called ***elementary abelian*** if every nonidentity element in G is of prime order p.

Remark 2.1.7. By the classification of finitely generated abelian groups, every elementary abelian group must be a direct product of a finite number of cyclic groups C_p.

Definition 2.1.8. A groupoid Q is called a ***quasigroup*** if for any $a, b \in Q$,

(a) there exists a unique element $x \in Q$ that satisfies the equation $ax = b$;

(b) there exists a unique element $y \in Q$ that satisfies the equation $ya = b$.

The unique solutions to these equations are written as $x = a\backslash b$ and $y = b/a$, where ‘ $\backslash$ ’ and ‘ $/$ ’ denote, respectively, the left and right division. A quasigroup is a groupoid where division is always possible.

Example 2.1.9.

(a) $\langle \mathbb{R}, - \rangle$ is a quasigroup. For any $a, b \in \mathbb{R}$, the two equations $a - x = b$ and $y - a = b$ have unique solutions $x = a - b$ and $y = a + b$.

(b) $\langle \mathbb{R} - \{0\}, \div \rangle$ is a quasigroup. For any $a, b \in \mathbb{R} - \{0\}$, we have unique solutions $x = a/b$ and $y = ab$ for the equations $a \div x = b$ and $y \div a = b$.

(c) All groups are quasigroups since there exist unique elements $x = a^{-1}b$ and $y = ba^{-1}$ that satisfy the equations $ax = b$ and $ya = b$ for any a and b in the group.

A convenient way to represent a finite quasigroup of small order is to construct a multiplication table (Cayley table). The multiplication table of a quasigroup of order 5 is given below.

Table 2.1: Cayley table of a quasigroup of order 5

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

The fact that x and y are unique solutions of the equations in Definition 2.1.8 guarantees that every element occurs exactly once in each row and each column in the multiplication table of a quasigroup.

Bruck (1971, p. 28) showed that if a quasigroup is associative, then it is a group. Therefore, a group is exactly an associative quasigroup.

Definition 2.1.10. A ***loop*** L is a quasigroup that possesses an identity element 1, i.e., $1x = x1 = x$ for all $x \in L$.

Example 2.1.11. This is the multiplication table of a loop of order 5.

Table 2.2: Cayley table of a loop of order 5

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

Definition 2.1.12. Let K be a subset of a loop $\langle L, \cdot\rangle$. K is called a ***subloop*** of L ($K \leq L$) if $\langle K, \cdot\rangle$ is a loop. A subloop K of L is called a ***proper subloop*** of L ($K < L$) if $K \neq L$ and is called ***trivial*** if $K = \{1\}$.

Definition 2.1.13. Let S be a subset of a loop L. The ***subloop generated by S***, denoted by $\langle S \rangle$, is the smallest subloop of L containing S.

Definition 2.1.14. A loop is a ***Moufang loop*** if it satisfies any one of the following (equivalent) Moufang identities:

$$\begin{aligned} &xy \cdot zx = (x \cdot yz)x && \text{Middle Moufang identity,} \\ &x(y \cdot xz) = (xy \cdot x)z && \text{Left Moufang identity,} \\ &(zx \cdot y)x = z(x \cdot yx) && \text{Right Moufang identity.} \end{aligned}$$

Definition 2.1.15. A loop L is ***power associative*** if $\langle x \rangle$ is a group for every $x \in L$.

Remark 2.1.16.

(a) Power associativity of a loop guarantees that x^n is well-defined for any element x in the loop and any positive integer n.

(b) The loop in Table 2.2 is not power associative since $(2 \cdot 2) \cdot 2 = 5 \cdot 2 = 4 \neq 3 = 2 \cdot 5 = 2 \cdot (2 \cdot 2)$.

Definition 2.1.17. A loop is ***diassociative*** if $\langle x, y \rangle$ is a group for any $x, y \in L$.

Remark 2.1.18. Diassociativity implies power associativity, but not the converse. The table below gives a power associative loop which is not diassociative.

Table 2.3: Cayley table of a non-diassociative, power associative loop

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

The power associativity of this loop can be verified easily since $x^2 = 1$ for all x. The loop is not diassociative as $(2 \cdot 2) \cdot 3 = 1 \cdot 3 = 3 \neq 5 = 2 \cdot 4 = 2 \cdot (2 \cdot 3)$.

Definition 2.1.19. The ***order*** of an element x in a power associative loop, denoted by $|x|$, is the smallest positive integer n such that $x^n = 1$. If such an integer does not exist, then the order of x is defined to be infinity.

Definition 2.1.20. The ***exponent*** of a power associative loop L is the smallest positive integer n such that $x^n = 1 \ \forall x \in L$, if this number exists.

Definition 2.1.21. Let K be a subloop of a loop L. For a fixed $x \in L$, $xK = \{xk \mid k \in K\}$ is a subset of L. This is called the ***left coset of K determined by x***. The right coset of K is defined in a similar manner.

Definition 2.1.22. Let K be a subloop of a loop L. K is a ***normal subloop*** of L (or K is normal in L), if $xK = Kx$, $x(yK) = (xy)K$ and $(Kx)y = K(xy)$ for all $x, y \in L$. We denote this by $K \trianglelefteq L$. As in the case of proper subloops, $K \triangleleft L$ means that K is a proper normal subloop of L.

Definition 2.1.23. Let L be a loop in which every element has a two-sided inverse. We define

$$\begin{aligned} zT(x) &= x^{-1} \cdot zx, \\ zL(x,y) &= (yx)^{-1}(y \cdot xz), \\ zR(x,y) &= (zx \cdot y)(xy)^{-1}. \end{aligned}$$

$I(L) = \langle T(x), L(x,y), R(x,y) \mid x, y \in L\rangle$ is called the ***inner mapping group*** of L. A subloop K is normal in L if $K\theta = \{k\theta \mid k \in K\} = K$ for all $\theta \in I(L)$.

Definition 2.1.24. Let K be a normal subloop of a loop L. Define the set of all left cosets of K as $L/K = \{xK \mid x \in L\}$ and a binary operation $\odot$ on L/K as $xK \odot yK = (xy)K$. Then L/K is a loop and is called the ***quotient loop of L modulo K***.

Definition 2.1.25. Let K be a normal subloop of a loop L.

(a) A quotient loop L/K is called a ***proper quotient loop*** if K is not trivial.

(b) K is a ***minimal normal subloop*** of L if K is not trivial and for any normal subloop H of L, $H \subset K \Rightarrow H = \{1\}$.

(c) K is a ***maximal normal subloop*** of L if K is a proper subloop of L and for any normal subloop H of L, $K \subset H \Rightarrow H = L$.

Definition 2.1.26. Let K be a subloop of a finite power associative loop L and π a set of primes.

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

(b) L is a ***π-loop*** if the order of every element of L is a π-number.

(c) K is a ***Hall π-subloop*** of L if K is a π-loop and $|K|$ is the largest π-number that divides $|L|$.

(d) K is a ***Sylow p-subloop*** of L if K is a Hall π-subloop of L and $\pi = \{p\}$.

Definition 2.1.27. The ***associator*** of three (fixed) elements x, y, z in a loop L is the unique element (x, y, z) in L such that $xy{\cdot}z = (x{\cdot}yz)(x, y, z)$. The ***associator subloop*** of L, denoted by L_a, is the subloop generated by all associators (x, y, z) in L. If X, Y and Z are subsets of L, we shall denote $(X, Y, Z) = \langle (x, y, z) \mid x \in X, y \in Y, z \in Z\rangle$.

Remark 2.1.28.

(a) A loop L is associative if and only if $L_a = \{1\}$. Generally, the more elements that do not associate in a loop, the more nontrivial associators we would expect to find. In such a case, we would expect L_a to become bigger and the loop to be more difficult to handle. Therefore, Leong (1976) called L_a the devil of loops.

(b) Some authors define associator subloop as

(i) the smallest normal subloop generated by all associators; or

(ii) the smallest normal subloop L_a such that L/L_a is associative.

But for the Moufang case, the three definitions conincide.

Definition 2.1.29. The ***commutator*** of two (fixed) elements x, y in a loop L is the unique element $[x, y]$ in L such that $xy = (yx)[x, y]$. The ***commutator subloop*** of L, denoted by L_c, is the subloop generated by all commutators $[x, y]$ in L.

Definition 2.1.30. The ***nucleus*** of a loop L, denoted by $N(L)$ or simply N, is the subloop consisting of all $n \in L$ such that $(n, x, y) = (x, n, y) = (x, y, n) = 1$ for all $x, y \in L$. In other words, elements in N associate with every element in L.

Remark 2.1.31.

(a) Clearly, N itself is a group. A loop L is associative if and only if $N(L) = L$. So, Leong (1976) called N the angel of loops.

(b) We can even give the definitions for the left nucleus, middle nucleus and right nucleus of a loop L. The left nucleus of L, denoted by $N_\lambda(L)$, is the set consisting of all $n \in L$ such that $(n, x, y) = 1 \quad \forall x, y \in L$. The middle nucleus and the right nucleus, $N_\mu(L)$ and $N_\rho(L)$ respectively, are defined analogously. Subsequently, N is defined as the intersection of these sets, i.e., $N = N_\lambda \cap N_\mu \cap N_\rho$. However, for Moufang loops (by Moufang's theorem), $N = N_\lambda = N_\mu = N_\rho$. Hence, in Moufang loops, we only consider the nucleus N of L.

Definition 2.1.32. Let K be a subloop of a loop L. The ***centraliser*** of K in L, denoted by $C_L(K)$, is the set consisting of all $\ell \in L$ such that $\ell k = k\ell$ for all $k \in K$.

Remark 2.1.33.

(a) $C_L(L)$ is called the ***commutant*** of L, and is usually written simply as $C(L)$.

(b) For a Moufang loop L, $C(L)$ is also called the ***Moufang centre*** of L.

Definition 2.1.34. The ***centre*** of a loop L, denoted by $Z(L)$, is the intersection of its nucleus and commutant, i.e., $Z(L) = N(L) \cap C(L)$. In other words, the centre of L consists of elements that associate and commute with every element in L.

Remark 2.1.35. For a group G, $Z(G) = C(G)$ since $N(G) = G$.

Definition 2.1.36. (m, n) is defined as the ***greatest common divisor*** of the integers m and n.

Definition 2.1.37. Let $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. a is ***congruent modulo*** n to b, denoted by $a \equiv b \pmod{n}$, if n is a factor of $a - b$.

Definition 2.1.38. Let $n \in \mathbb{Z}^+$.

(a) If $a \in \mathbb{Z}$, then $[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$ is called the ***congruence class (modulo n) determined by a***.

(b) Defined a set $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ and a binary operation $+_n$ on $\mathbb{Z}_n$ as $[a] +_n [b] = [a + b]$. Then $\langle \mathbb{Z}_n, +_n \rangle$ is an abelian group.

2.2 Known Results in Moufang Loops, Groups and Number Theory

Lemma 2.2.1 (Moufang's theorem)**.** *Let L be a Moufang loop. Then L is diassociative. Moreover, if $(x, y, z) = 1$ for some $x, y, z \in L$, then $\langle x, y, z \rangle$ is a group* (Bruck, 1971, p. 117, Moufang's theorem).

Remark 2.2.2. There is now a short proof of Moufang's theorem due to Aleš Drápal. It will appear in the Proceedings of the American Mathematical Society.

Lemma 2.2.3. *Let L be a Moufang loop.*

(a) *Suppose $x \in L$ and $\theta \in I(L)$. Then $(x^n)\theta = (x\theta)^n$ for any integer n* (Bruck, 1971, p. 117, Lemma 3.2; and p. 120, (4.1))*;*

(b) *Suppose* $x, y, u, v \in L$ *and* $\theta \in I(L)$. *Then* $(xy)\theta \cdot c = (x\theta) \cdot (y\theta \cdot c)$ *where* $c = [u^{-1}, v^{-1}]$ *if* $\theta = L(u, v)$, *and* $c = u^{-3}$ *if* $\theta = T(u)$ (Bruck, 1971, p. 112, Lemma 2.1; p. 113, Lemma 2.2; and p. 117, Lemma 3.2).

Lemma 2.2.4. *All Moufang loops satisfy the following identities:*

(a) $R(x^{-1}, y^{-1}) = L(x, y)$;

(b) $xL(z, y) = x(x, y, z)^{-1}$;

(c) $(x, y, z) = (x, yz, z)$;

(d) $(x, y, z) = (x, y, zy)$;

(e) $(x, y, z) = (xy, z, y)^{-1}$;

(f) $(x, y, z) = (x, y, zx)$

(Bruck, 1971, p. 124, Lemma 5.4).

Lemma 2.2.5. *Let* L *be a Moufang loop. Then* L *satisfies all or none of the following identities:*

(i) $[(x, y, z), x] = 1$;

(ii) $(x, y, [y, z]) = 1$;

(iii) $(x, y, z)^{-1} = (x^{-1}, y, z)$;

(iv) $(x, y, z)^{-1} = (x^{-1}, y^{-1}, z^{-1})$;

(v) $(x, y, z) = (x, zy, z)$;

(vi) $(x, y, z) = (x, z, y^{-1})$;

(vii) $(x, y, z) = (x, xy, z)$.

When these identities hold, the associator (x, y, z) *lies in the centre of the subloop generated by* x, y, z; *and the following identities hold for all integers* n:

$$(x, y, z) = (y, z, x) = (y, x, z)^{-1},$$

$$(x^n, y, z) = (x, y, z)^n,$$

$$[xy, z] = [x, z][[x, z], y][y, z](x, y, z)^3$$

(Bruck, 1971, p. 125, Lemma 5.5).

Lemma 2.2.6. *Let L be a Moufang loop. Then $(xn, y, z) = (x, yn, z) = (x, y, zn)$ $= (x, y, z)$ for any $x, y, z \in L$ and $n \in N$* (Leong & Rajah, 1995, p. 267, Lemma 1)*.*

Lemma 2.2.7. *Let L be a Moufang loop and $x, y, z \in L$. If $L_a \subseteq N$, then $(x, y, z) = (z, y, x)^{-1} = (y, z, x)$* (Rajah, 2001, p. 71, Lemma 2)*.*

Lemma 2.2.8. *Let L be a Moufang loop and M an associative subloop of L. Suppose $L_a, L_c \subseteq M$, $u, v \in M$ and $v \in C_L(L_a)$. Then $(uv, \ell_1, \ell_2) = (v, \ell_1, \ell_2)(u, \ell_1, \ell_2)$ for each $\ell_i \in L$* (Rajah, 2001, p. 71, Lemma 4)*.*

Lemma 2.2.9. *Let L be a Moufang loop.*

(a) *$L_a \trianglelefteq L$* (Leong, 1976, p. 33, Corollary)*;*

(b) *$N \trianglelefteq L$* (Bruck, 1971, p. 114, Theorem 2.1)*;*

(c) *$L_a \subseteq C_L(N)$* (Leong, 1976, p. 34, Corollary)*.*

Lemma 2.2.10 (Lagrange's theorem)**.** *Let L be a finite Moufang loop and K a subloop of L. Then $|K|$ divides $|L|$* (Grishkov & Zavarnitsine, 2005)*.*

Lemma 2.2.11. *Let L be a finite Moufang loop. Then for any $x \in L$, $|x|$ divides $|L|$* (Bruck, 1971, p. 92, Theorem 1.2)*.*

Lemma 2.2.12. *Let L be a finite Moufang loop. Suppose K is a subloop of $C_L(L_a)$ and $(|K|, |L_a|) = 1$. Then $K \subseteq N$* (Leong & Rajah, 1997, p. 480, Lemma 5)*.*

Lemma 2.2.13. *Let L be a Moufang loop of odd order. Suppose $H \trianglelefteq M \trianglelefteq L$ and H is a Hall subloop of M. Then $H \trianglelefteq L$* (Leong & Rajah, 1996a, p. 879, Lemma 1)*.*

Lemma 2.2.14. *Let L be a Moufang loop of odd order.*

(a) *L is solvable* (Glauberman, 1968, p. 413, Theorem 16)*;*

(b) *L contains a Hall π-subloop where π is any set of primes* (Glauberman, 1968, p. 409, Theorem 12)*;*

(c) *K is a minimal normal subloop of $L \Rightarrow K$ is an elementary abelian group and $(K, K, L) = \langle (k_1, k_2, \ell) \mid k_i \in K, \ell \in L \rangle = \{1\}$* (Glauberman, 1968, p. 402, Theorem 7)*;*

(d) *$K \trianglelefteq L$, $(K, K, L) = 1$ and $(|K|, |L/K|) = 1 \Rightarrow K \subseteq N$* (Glauberman, 1968, p. 405, Theorem 10).

Lemma 2.2.15. *Let L be a Moufang loop of odd order and K a normal subloop of L. Suppose $K \subseteq N$. Then $C_L(K) \trianglelefteq L$ and $|L/C_L(K)|$ divides $|\mathrm{Aut}(K)|$* (Leong, 1976, p. 33, Theorem 3(a)).

Lemma 2.2.16. *Let L be a Moufang loop of odd order, K a minimal normal subloop of L and M an associative subloop of L such that $L_a \subseteq K \subseteq M$ and $L_c \subseteq M$. Then the following identities hold for all $k \in K$, $w \in M$ and $\ell \in L$:*

(a) $(k, w, \ell) = (\ell, k, w^{-1})^{-1}$*;*

(b) $((k, w, \ell)[k, w], w, \ell) = 1$

(Leong & Rajah, 1996b, p. 565, Lemma 6).

Lemma 2.2.17. *Let L be a Moufang loop of odd order and M a maximal normal subloop of L. Then L_a and L_c lie in M; and $L = M\langle x \rangle$ for any $x \in L - M$* (Leong & Rajah, 1997, p. 478, Lemma 1(b)).

Lemma 2.2.18. *Let L be a finite Moufang loop.*

(a) *Suppose $|L| = p^\alpha m$ where p is a prime, $(p, m) = (p - 1, p^\alpha m) = 1$ and L has an element of order p^α. Then there exists a subloop P of order p^α and a normal subloop M of order m in L such that $L = PM$.*

(b) *Suppose $|L| = p^2m$ where p is the smallest prime dividing $|L|$ and $(p, m) = 1$. Then there exists a subloop P of order p^2 and a normal subloop M of order m in L such that $L = PM$.*

(Leong & Rajah, 1998, p. 39, Theorem 1; and p. 40, Theorem 2)

Lemma 2.2.19. *Let L be a Moufang loop of odd order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ where $p_1, p_2, \ldots,$ p_n are primes, $p_1 < p_2 < \cdots < p_n$ and $1 \leq \alpha_n \leq 2$. Suppose all proper subloops and proper quotient loops of L are groups, and L contains a normal Sylow p_n-subloop. Then L is a group* (Leong & Rajah, 1996a, p. 879, Lemma 3).

Lemma 2.2.20. *Let L be a Moufang loop of order p, p^2 or p^3 where p is a prime. Then L is a group* (Chein, 1974, p. 34, Proposition 1; and p. 35, Corollary 4).

Lemma 2.2.21. *Let L be a Moufang loop of order p^4 where $p > 3$ is a prime. Then L is a group* (Leong, 1974, p. 33, Theorem).

Lemma 2.2.22. *Let L be a Moufang loop of odd order $p^{\alpha}q_1\cdots q_n$, where $\alpha \leq 4$ and $p, q_1, \ldots, q_n$ are distinct primes with $3 < p < q_1 < \cdots < q_n$. Then L is a group* (Leong & Rajah, 1996b, p. 567, Theorem).

Lemma 2.2.23. *Let L be a Moufang loop of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ where $p_1, p_2, \ldots,$ p_n are distinct odd primes and $\alpha_i \leq 2$ for all i. Then L is a group* (Leong & Rajah, 1996a, p. 882, Theorem).

Lemma 2.2.24. *For distinct odd primes p and q, there exists a nonassociative Moufang loop of order pq^3 if and only if $q \equiv 1 \pmod{p}$* (Rajah, 2001, p. 78, Theorem 1; and p. 86, Theorem 2).

Lemma 2.2.25. *Let $H \neq \{1\}$ be a normal subgroup of a finite p-group G. Then $H \cap Z(G) \neq \{1\}$* (Humphreys, 1996, p. 155, Proposition 18.3; and p. 158, Proposition 18.10).

Lemma 2.2.26. *Suppose a, b and m are integers such that $(a, m) = 1$. Then there exists an integer x which satisfies the congruence $ax \equiv b \pmod{m}$* (Niven & Zuckerman, 1966, p. 25, Corollary 2.9).

Lemma 2.2.27. *If q is a prime, then the congruence $\mu^n \equiv 1 \pmod{q}$ has $(n, q-1)$ solutions for μ* (Niven & Zuckerman, 1966, p. 54, Theorem 2.27).

CHAPTER 3

MINIMALLY NONASSOCIATIVE MOUFANG LOOPS

3.1 Motivation

The concept of "minimally nonassociative Moufang loops" was first introduced by Chein and Goodaire (2001). They were defined as Moufang loops that are not associative but every proper subloop is associative. Through our reading of various results in relevant papers (Leong & Rajah, 1995, 1996b, 1997), we have come to realise that if the additional condition "every proper quotient loop is associative" is imposed, many of those results could have been used to solve problems with Moufang loops in other cases. However, in most of these papers, the scope of the results have been somewhat narrowed to include only those Moufang loops that were being studied in that paper. By introducing the alternative definition of minimally nonassociative Moufang loops in this chapter, we hope to produce results that will be applicable to a bigger range of Moufang loops.

3.2 Properties of Minimally Nonassociative Moufang Loops

Definition 3.2.1. A Moufang loop L is ***minimally nonassociative*** if L is nonassociative but all proper subloops and proper quotient loops of L are associative. (We shall also call this as the minimally nonassociative property of L.)

Lemma 3.2.2. *Let L be a minimally nonassociative Moufang loop.*

(a) *$L_a \trianglelefteq K$ where K is any nontrivial normal subloop of L;*

(b) *If $|L|$ is odd, then L_a is the unique minimal normal subloop of L, and is an elementary abelian group. Moreover, $(L_a, L_a, L) = \{1\}$.*

Proof. Since K is nontrivial, L/K is a proper quotient loop of L. This implies that L/K must be a group by the minimally nonassociative property of L. Then $xKyK \cdot zK = xK \cdot yKzK$ for each $x, y, z \in L$. So $(xy \cdot z)K = (x \cdot yz)K$ as $K \trianglelefteq L$. Thus $(x \cdot yz)^{-1}(xy \cdot z) = (x, y, z) \in K$. Hence $L_a \subseteq K$. Since $L_a \trianglelefteq L$ by Lemma 2.2.9(a), L_a is also normal in K. This proves (a).

By Lemma 2.2.14(a), L is solvable. So there exists a minimal normal subloop K in L. By the definition of minimal normal subloop, K must be nontrivial. So $L_a \trianglelefteq K$ by (a). Since L is not a group, $L_a \neq \{1\}$. So $L_a = K$. Hence, by Lemma 2.2.14(c), L_a is an elementary abelian group and $(L_a, L_a, L) = \{1\}$. This completes the proof of this lemma. □

Lemma 3.2.3. *Let L be a minimally nonassociative Moufang loop of odd order. Then $(k_1k_2, \ell_1, \ell_2) = (k_1, \ell_1, \ell_2)(k_2, \ell_1, \ell_2)$ for each $k_i \in L_a$ and $\ell_i \in L$.*

Proof. Let $c = [\ell_2^{-1}, \ell_1^{-1}]$. By Lemma 2.2.3(b), $(k_1k_2)L(\ell_2, \ell_1) \cdot c = k_1L(\ell_2, \ell_1)$ $[k_2L(\ell_2, \ell_1) \cdot c]$. Hence

$$\begin{aligned}
&(k_1k_2)(k_1k_2, \ell_1, \ell_2)^{-1} \cdot c \\
&= k_1(k_1, \ell_1, \ell_2)^{-1}[k_2(k_2, \ell_1, \ell_2)^{-1} \cdot c] && \text{by Lemma 2.2.4(b)} \\
&= k_1(k_1, \ell_1, \ell_2)^{-1}k_2(k_2, \ell_1, \ell_2)^{-1} \cdot c && \text{as } (L_a, L_a, L) = \{1\} \text{ by Lemma 3.2.2(b)} \\
&= (k_1k_2)(k_1, \ell_1, \ell_2)^{-1}(k_2, \ell_1, \ell_2)^{-1} \cdot c && \text{as } L_a \text{ is abelian by Lemma 3.2.2(b).}
\end{aligned}$$

Thus $(k_1k_2, \ell_1, \ell_2) = (k_1, \ell_1, \ell_2)(k_2, \ell_1, \ell_2)$ by cancellation. □

Theorem 3.2.4. *Let L be a minimally nonassociative Moufang loop of odd order and K a subloop of L. Suppose $K \subseteq N$. Then:*

(a) *$L \neq \langle x, y\rangle K$ for all $x, y \in L$;*

(b) *K is not a Hall subloop of L.*

Proof. Suppose $L = \langle x, y \rangle K$ for some $x, y \in L$. Then

$$\begin{aligned} L_a &= (L, L, L) \\ &= (\langle x, y\rangle K, \langle x, y\rangle K, \langle x, y\rangle K) \\ &= (\langle x, y\rangle, \langle x, y\rangle, \langle x, y\rangle) && \text{by Lemma 2.2.6} \\ &= \{1\} && \text{by diassociativity.} \end{aligned}$$

Hence, L is a group which is a contradiction. Thus (a) is proved.

Suppose K is a Hall subloop of L. By Lemma 2.2.14(b), there exists a Hall subloop H of order $|L/K|$ in L. Now consider $\langle H, K\rangle$, a subloop generated by H and K. By Lagrange's theorem, $|H|$ and $|K|$ divide $|\langle H, K\rangle|$. Since $(|H|, |K|) = 1$, $|H||K| = |L|$ divides $|\langle H, K\rangle|$. Thus $L = \langle H, K\rangle$.

Then $L = \langle H, K\rangle = \langle H, N\rangle = HN$ as $N \trianglelefteq L$ by Lemma 2.2.9(b). Now

$$\begin{aligned} L_a &= (L, L, L) \\ &= (HN, HN, HN) \\ &= (H, H, H) && \text{by Lemma 2.2.6} \\ &= \{1\} && \text{since } H \text{ is a proper subloop of } L. \end{aligned}$$

Similar to the previous case, we have a contradiction. This completes the proof of this theorem. □

Theorem 3.2.5. *Let L be a minimally nonassociative Moufang loop of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots\ p_n^{\alpha_n}$ where $p_1, p_2, \ldots, p_n$ are distinct odd primes and $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}^+$. Then*

(a) *there exists some i such that $\alpha_i \geq 2$ and $|L_a| = p_i^{\beta_i}$ for some β_i satisfying $0 < \beta_i < \alpha_i$;*

(b) *$p_i^{\alpha_i} \nmid |N|$ for all i.*

Proof. By Lemma 3.2.2(b), L_a is elementary abelian, i.e., $|L_a| = p_i^{\beta_i}, 0 \leq \beta_i \leq \alpha_i$

for some i.

Case 1. $\alpha_i = 1$.

$|L_a| = p_i^{\beta_i}, 0 \leq \beta_i \leq 1$ implies $\beta_i = 0$ or 1. Suppose $\beta_i = 0$, then $L_a = \{1\}$ which implies L is a group. This is a contradiction. Suppose $\beta_i = 1$, then L_a is a Sylow subloop of L and $(|L_a|, |L/L_a|) = 1$. By Lemma 2.2.14(d), $L_a \subseteq N$. This contradicts Theorem 3.2.4(b).

Case 2. $\alpha_i \geq 2$.

Since L is not a group, $L_a \neq \{1\}$, which implies $|L_a| \neq 1$. Thus $\beta_i \neq 0$. Suppose $|L_a| = p_i^{\alpha_i}$, then L_a is a Sylow subloop of L and we get a contradiction similar to Case 1. Hence $\beta_i \neq \alpha_i$. This proves (a).

Suppose $p_i^{\alpha_i}$ divides $|N|$ for some i. Since N is a group, by Sylow theorem for groups, there exists P_i, a subloop of order $p_i^{\alpha_i}$ in N. But P_i is also a Hall subloop of L. This contradicts Theorem 3.2.4(b). Hence $p_i^{\alpha_i} \nmid |N|$ for all i. □

Theorem 3.2.6. *Let L be a minimally nonassociative Moufang loop of finite order. Then $|L|/|N| \neq 1, p$ or pq where p and q are primes.*

Proof. Suppose $|L|/|N| = 1$. Then $L = N$ which is a group. This is a contradiction as L is nonassociative.

Suppose $|L|/|N| = p$. Take any $x \in L - N$. Then $|N| < |\langle x\rangle N| \leq |L|$. Hence $L = \langle x\rangle N$, contrary to Theorem 3.2.4(a).

Now suppose $|L|/|N| = pq$. Take any $x \in L - N$. Then $|N| < |\langle x\rangle N| \leq |L|$. As in the previous case, we are through if $L = \langle x\rangle N$. Now if $L \neq \langle x\rangle N$, take $y \in L - \langle x\rangle N$. Then $|\langle x\rangle N| < |\langle x, y\rangle N| \leq |L|$. Thus $L = \langle x, y\rangle N$, contrary to Theorem 3.2.4(a). □

Theorem 3.2.7. *Let L be a minimally nonassociative Moufang loop of odd order and M a maximal normal subloop of L. Then, for any $w \in M$ and $\ell \in L$, there exists some $k_0 \in L_a - \{1\}$ such that $(k_0, w, \ell) = 1$.*

Proof. By Lemma 3.2.2(b), L_a is the minimal normal subloop of L. By Lemma 2.2.17, L_a and L_c lie in M. Since M is a proper subloop of L, M is a group by minimally nonassociative property of L. Take $k \in L_a - \{1\}$, $w \in M$ and $\ell \in L$. By Lemma 2.2.16(b), $((k,w,\ell)[k,w],w,\ell) = 1$ and $((k,w,\ell^{-1})[k,w],w,\ell^{-1}) = 1$. So by Moufang's theorem (Lemma 2.2.1), $((k,w,\ell^{-1})[k,w],w,\ell) = 1$ also. Since $L_a \trianglelefteq L$, $[k,w] = (wk)^{-1}(kw) = k^{-1}w^{-1}kw = k^{-1} \cdot kT(w) \in L_a$. So $(k,w,\ell)[k,w], (k,w,\ell^{-1})[k,w] \in L_a$.

Suppose $(k,w,\ell)[k,w] \neq 1$ or $(k,w,\ell^{-1})[k,w] \neq 1$. Then that is the k_0 we are looking for. So we can assume that $(k,w,\ell)[k,w] = (k,w,\ell^{-1})[k,w] = 1$. By cancellation, we have $(k,w,\ell) = (k,w,\ell^{-1})$. Next, by Lemma 2.2.16(a), $(k,w,\ell) = (\ell,k,w^{-1})^{-1}$ and $(k,w,\ell^{-1}) = (\ell^{-1},k,w^{-1})^{-1}$. Let

$$k_1 = (k,w,\ell) = (\ell,k,w^{-1})^{-1} = (\ell^{-1},k,w^{-1})^{-1}. \tag{3.1}$$

Now

$$\begin{aligned}
& \ell^{-1}L(w^{-1},k) = [\ell L(w^{-1},k)]^{-1} && \text{by Lemma 2.2.3(a)}\\
\Rightarrow\quad & \ell^{-1}(\ell^{-1},k,w^{-1})^{-1} = [\ell(\ell,k,w^{-1})^{-1}]^{-1} && \text{by Lemma 2.2.4(b)}\\
\Rightarrow\quad & \ell^{-1}k_1 = (\ell k_1)^{-1} && \text{by (3.1)}\\
\Rightarrow\quad & \ell^{-1}k_1\ell = k_1^{-1} && (3.2)\\
\Rightarrow\quad & \ell^{-2}k_1\ell^2 = \ell^{-1}[\ell^{-1}k_1\ell]\ell && \text{by diassociativity}\\
& \qquad\quad = \ell^{-1}k_1^{-1}\ell && \text{by (3.2)}\\
& \qquad\quad = [\ell^{-1}k_1\ell]^{-1} && \\
& \qquad\quad = k_1 && \text{by (3.2)}\\
\Rightarrow\quad & k_1\ell^2k_1^{-1} = \ell^2. &&
\end{aligned}$$

By Lemma 2.2.11, $|\ell|$ divides $|L|$. So $|\ell|$ is odd. Hence, $(|\ell|+1)/2$ is an integer. Thus, we can write $(k_1\ell^2k_1^{-1})^{(|\ell|+1)/2} = (\ell^2)^{(|\ell|+1)/2}$. Then $k_1\ell k_1^{-1} = \ell$, i.e., $\ell^{-1}k_1\ell = k_1$. Thus, by comparing this with (3.2), we have $k_1 = k_1^{-1}$ which implies that $k_1^2 = 1$. By Lemma 2.2.11, $|k_1|$ is odd. So $k_1 = (k,w,\ell) = 1$. □

Theorem 3.2.8. *Let L be a minimally nonassociative Moufang loop of odd order* *and M a maximal normal subloop of L. Suppose $(k, w, \ell) = 1$ for all $k \in L_a, w \in M$ and $\ell \in L$. Then $L_a \subseteq N$.*

Proof. Take $k \in L_a$, $x \in L - M$ and $\ell \in L$. By Lemma 2.2.17, we can write $L = M\langle x\rangle$. So $\ell = wx^\alpha$ for some $w \in M$ and $\alpha \in \mathbb{Z}^+$. Now

$$\begin{aligned}(k, x, \ell) &= (k, x, wx^\alpha) \\ &= (k, x, w) && \text{by Lemma 2.2.4(d) repeatedly} \\ &= 1 && \text{by Moufang's theorem as } (k, w, x) = 1.\end{aligned}$$

Since $(L_a, M, L) = \{1\}$ and $(L_a, L - M, L) = \{1\}$, it follows that $(L_a, L, L) = \{1\}$. Thus $L_a \subseteq N$ by the definition of N. □

Corollary 3.2.9. *Let L be a minimally nonassociative Moufang loop of odd order. Suppose L_a is cyclic. Then $L_a \subseteq N$.*

Proof. By Lemma 2.2.14(a), there exists a maximal normal subloop M in L. Take $w \in M$ and $\ell \in L$. By Theorem 3.2.7, there exists some $k_0 \in L_a - \{1\}$ such that $(k_0, w, \ell) = 1$. Since L_a is cyclic, $L_a = \langle k_0\rangle$. Thus, for every $k \in L_a$,

$$\begin{aligned}(k, w, \ell) &= (k_0^\alpha, w, \ell) && \text{for some } \alpha \in \mathbb{Z}^+ \\ &= 1 && \text{by Moufang's theorem.}\end{aligned}$$

Hence $L_a \subseteq N$ by Theorem 3.2.8. □

Corollary 3.2.10. *Let L be a minimally nonassociative Moufang loop of odd order and M a maximal normal subloop of L. Suppose N is trivial. Then $L = \langle k, w, x\rangle$ for some $k \in L_a$, $w \in M - L_a$ and $x \in L - M$.*

Proof. Since L is nonassociative, $L_a \neq \{1\}$. Hence, $L_a \not\subseteq N$. By Theorem 3.2.8, there exist some $k \in L_a$, $w \in M$ and $x \in L$ such that $(k, w, x) \neq 1$. Suppose $w \in L_a$. Then by Lemma 3.2.2(b), $(k, w, x) = 1$. This is a contradiction. Hence,