MOUFANG LOOPS OF ODD ORDER $p_1 p_2 \cdots p_n q^3$

CHONG KAM YOON

UNIVERSITI SAINS MALAYSIA

2007

MOUFANG LOOPS OF ODD ORDER $p_1 p_2 \cdots p_n q^3$

by

CHONG KAM YOON

Thesis submitted in fulfillment of the requirements

for the degree of

Master of Science

JUNE 2007

ACKNOWLEDGEMENTS

Firstly, I would like to take this opportunity to deliver the highest appreciation to my supervisor, Dr. Andrew Rajah of the School of Mathematical Sciences, Universiti Sains Malaysia. Without his aid and guidance, this thesis would not be completed in such prosperous way.

I would also like to extend the appreciation to my family for their support and encouragement during the process of completing this thesis. Besides this, I would like to thank Mr. Ang Chee Keong for his invaluable moral support too.

I am grateful to the Institute of Postgraduate Studies for their financial support in the form of scholarship. With this great help, I am able to fully concentrate on my research. I would like to thank the staff of the School of Mathematical Sciences, Universiti Sains Malaysia for their every single contribution in completing my research.

Finally, I would like to thank every single individual and organization that has involved itself in the process of completing this report.

TABLE OF CONTENTS

LUP MOUFANG BERBERINGKAT GANJIL $p_1 p_2 \cdots p_n q^3$

ABSTRAK

Suatu sistem dedua $\langle L, \cdot \rangle$ yang memenuhi syarat penetapan mana-mana dua unsur dari x, y dan z dalam persamaan $x \cdot y = z$ menentukan unsur ketiga secara unik dipanggil suatu kuasi-kumpulan. Jika sistem ini mengandungi suatu unsur identiti (dua hala), maka ia dipanggil lup. Suatu lup adalah lup Moufang jika ia memenuhi identiti Moufang: $(x \cdot y) \cdot (z \cdot x) = [x \cdot (y \cdot z)] \cdot x$.

Kewujudan lup-lup Moufang berperingkat 2^4, 3^4 dan p^5 (p nombor perdana, $p > 3$) yang tidak memenuhi hukum sekutuan memang diketahui. Pada tahun 1974, O. Chein telah membuktikan bahawa semua lup Moufang berperingkat p, p^2, pq dan p^3 ialah kumpulan apabila p dan q adalah nombor-nombor perdana (rujuk [4]).

F. Leong dan A. Rajah (1997) telah membuktikan bahawa semua lup Moufang berperingkat $p^{\alpha} q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$ memenuhi hukum sekutuan jika p dan q_i adalah nombor-nombor perdana yang ganjil dengan $p < q_1 < q_2 < \cdots < q_n$, dan

(i) $\alpha \leq 3, \beta_i \leq 2$; atau

(ii) $p \geq 5, \alpha \leq 4, \beta_i \leq 2$ (rujuk [15]).

A. Rajah (2001) telah membuktikan bahawa jika p dan q adalah nombor-nombor perdana ganjil yang berlainan, maka semua lup Moufang berperingkat pq^3 adalah kumpulan jika dan hanya jika $q \not\equiv 1 (\mathrm{mod}\ p)$.

Tujuan penyelidikan kami ialah untuk mengkaji lup-lup Moufang berperingkat $p_1 p_2 \cdots p_n q^3$, p_i dan q adalah nombor-nombor perdana, $2 < p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\ p_i)$ dan $p_i \not\equiv 1 (\mathrm{mod}\ p_j)$ bagi $i, j \in \{1, 2, \cdots, n\}$. Sebelum kami berjaya membuktikan bahawa semua lup sebegini adalah kumpulan, kami menurunkan masalah ini kepada masalah yang lebih ringkas supaya ia lebih mudah dikendalikan.

Dalam bab 3 (Chapter 3), kami membuktikan bahawa semua lup Moufang berperingkat pqr^3, p, q dan r ialah nombor-nombor perdana ganjil, $p < q < r$, $q \not\equiv 1 (\mathrm{mod}\ p)$, $r \not\equiv 1 (\mathrm{mod}\ p)$ dan $r \not\equiv 1 (\mathrm{mod}\ q)$, memenuhi hukum sekutuan.

Dalam bab 4 (Chapter 4), kami memperkembangkan hasil penyelidikan dalam bab 3 kepada lup Moufang berperingkat $p_1 p_2 \cdots p_n q^3$, p_i dan q adalah nombor-nombor perdana, $2 < p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\ p_i)$ dan $p_i \not\equiv 1 (\mathrm{mod}\ p_j)$ bagi $i, j \in \{1, 2, \cdots, n\}$ dan membuktikan bahawa semua lup Moufang berperingkat sedemikian memenuhi hukum sekutuan.

MOUFANG LOOPS OF ODD ORDER $p_1 p_2 \cdots p_n q^3$

ABSTRACT

A binary system $\langle L, \cdot \rangle$ in which specification of any two of the elements x, y and z in the equation $x \cdot y = z$ uniquely determines the third element is called a quasigroup. If furthermore it contains a (two-sided) identity element, then it is called a loop. A Moufang loop is a loop which satisfies the Moufang identity: $(x \cdot y) \cdot (z \cdot x) = [x \cdot (y \cdot z)] \cdot x$.

Nonassociative Moufang loops of orders 2^4, 3^4 and p^5 $(p > 3)$ are known to exist. In 1974, O. Chein proved that all Moufang loops of orders p, p^2, pq and p^3 are groups when p and q are primes (see [4]).

It was proven by F. Leong and A. Rajah (1997) that all Moufang loops of odd order $p^{\alpha} q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$ are associative if p and q_i are odd primes with $p < q_1 < q_2 < \cdots < q_n$, and

(i) $\alpha \leq 3, \beta_i \leq 2$; or

(ii) $p \geq 5, \alpha \leq 4, \beta_i \leq 2$ (see [15]).

A. Rajah (2001) proved that if p and q are distinct odd primes, then all the Moufang loops of order pq^3 are groups if and only if $q \not\equiv 1 (\mathrm{mod}\ p)$.

The aim of our research is to study Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$ where p_i and q are primes, $2 < p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\, p_i)$ and $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ for $i, j \in \{1, 2, \cdots, n\}$. Before we managed to prove that all such Moufang loops are groups, we reduced the problem above into a smaller problem so that it is more easily solved.

In Chapter 3, we prove that all Moufang loops of order pqr^3, where p , q and r are odd primes, $p < q < r$, $q \not\equiv 1 (\mathrm{mod}\, p)$, $r \not\equiv 1 (\mathrm{mod}\, p)$ and $r \not\equiv 1 (\mathrm{mod}\, q)$ are associative.

In Chapter 4, we extend the result in Chapter 3 to Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$, where p_i and q are primes, $2 < p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\, p_i)$ and $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ for $i, j \in \{1, 2, \cdots, n\}$, and prove that all such Moufang loops are associative.

CHAPTER 1

INTRODUCTION

A binary system $\langle L, \cdot \rangle$ in which specification of any two of the elements x, y and z in the equation $x \cdot y = z$ uniquely determines the third element is called a quasigroup. If furthermore it contains a (two-sided) identity element, then it is called a loop.

A Moufang loop is a loop which satisfies the Moufang identity: $(x \cdot y) \cdot (z \cdot x) = [x \cdot (y \cdot z)] \cdot x$. In 1960, R. H. Bruck managed to show that (see [2]) this Moufang identity is actually equivalent to each of the following two identities:

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

and

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

Notice that in these three identities, denoting the operation in L by "$\cdot$" will just complicate and lengthen the equations. Therefore for the purpose of simplifying the equations and when there is no risk of misunderstanding, we will omit the "$\cdot$", for example, we will write xy instead of $x \cdot y$. So, from now on, L (instead of $\langle L, \cdot \rangle$) is defined as a finite Moufang loop.

Since the introduction of the Moufang identity by Ruth Moufang in [17], algebraists have embarked on a study of Moufang loops. Many of them aimed to obtain a

nonassociative Moufang loop. As a result of their efforts, many properties and theorems of Moufang loops were found (see [1], [2], [3] and [8]). However, only much later, in 1971, the combined efforts of O. Chein and H. O. Pflugfelder produced a nonassociative Moufang loop, that is, a Moufang loop which is not a group (see [6]).

Even though it is known that Moufang loops are not groups in general, yet we are interested in this question: “Which Moufang loops are associative?” This is important as we can apply any known theorems for groups onto Moufang loops if any of these Moufang loops are associative. In the study of Moufang loops, we invest and focus our study by examining the order of the Moufang loops.

The following statement is known to be true: “Given a nonassociative Moufang loop of order m, it is possible to construct a nonassociative Moufang loop of order mn for every $n \in \square$ ”. Consequently, if it is known that all Moufang loops of order mn (where $m, n \in \square$) are associative, then all Moufang loops of orders m (and n) are also associative. This makes us ask the following question: “Given a positive integer n, are all Moufang loops of order n associative? If not, are we able to construct a nonassociative Moufang loop of order n?”

In [7], O. Chein and A. Rajah proved that all Moufang loops of even order $2m$ are associative if and only if all groups of order m are abelian. So, the above question has been answered completely for the even case.

How about the case of Moufang loops of odd order? In [4], O. Chein proved that all Moufang loops of order p, p^2, pq and p^3 are groups when p and q are primes. This would suggest that we could extend the study in this area by writing the order of a Moufang loop as the product of powers of distinct primes. In fact, M. Purtill, in [20], did just that, by showing that all Moufang loops of odd order pqr and pq^2 are associative for distinct primes p, q and r. Though an error was discovered in his proof of the result for the case $p < q$ (see [21]), this case was later resolved by F. Leong and A. Rajah (see [12]) in 1995.

Soon after the above result was obtained, F. Leong and A. Rajah continued extending that result to Moufang loops of orders with higher powers of primes, that is of order $p_1^{\,2} p_2^{\,2} \cdots p_m^{\,2}$ and $p^4 q_1 q_2 \cdots q_n$ (see [13] and [14]). Finally, in [15], they proved that all Moufang loops of odd order $p^{\alpha} q_1^{\,\beta_1} q_2^{\,\beta_2} \cdots q_n^{\,\beta_n}$ are associative if p and q_i are odd primes with $p < q_1 < q_2 < \cdots < q_n$, and

(i) $\alpha \le 3, \beta_i \le 2$; or

(ii) $p \ge 5, \alpha \le 4, \beta_i \le 2.$

In the year 2001, A. Rajah proved that all the Moufang loops of order pq^3 are groups if and only if p and q are distinct odd primes and $q \not\equiv 1 (\mathrm{mod}\, p)$ (see [22]). So, one of the possible extension to that result would be to Moufang loops of odd order pqr^3 where p, q and r are odd primes, $p < q < r$, $q \not\equiv 1 (\mathrm{mod}\, p)$, $r \not\equiv 1 (\mathrm{mod}\, p)$ and $r \not\equiv 1 (\mathrm{mod}\, q)$.

In [7], O. Chein and A. Rajah proved that if L is a Moufang loop of order $p_1 p_2 ... p_k q^3$, where p_1, p_2, $\cdots$, p_k and q are distinct odd primes with q as the largest prime, and if $q \not\equiv 1 (\mathrm{mod}\, p_1)$ and for each $i > 1$, $q^2 \not\equiv 1 (\mathrm{mod}\, p_i)$, then L is a group. Now, the condition $q^2 \not\equiv 1 (\mathrm{mod}\, p_i)$ implies $q \not\equiv \pm 1 (\mathrm{mod}\, p_i)$. Here, the condition $q \not\equiv 1 (\mathrm{mod}\, p_i)$ is a necessary one for L to be a group, but the same is not true for the condition $q \not\equiv -1 (\mathrm{mod}\, p_i)$. So we conclude that although the condition "for each $i > 1$, $q^2 \not\equiv 1 (\mathrm{mod}\, p_i)$" is not a necessary condition, it was sufficient for them to prove their result. That is why at the end of their paper, the following open question was asked: "Are all Moufang loops L of order pqr^3 where $r \not\equiv 1 (\mathrm{mod}\, p)$ and $r \not\equiv 1 (\mathrm{mod}\, q)$ but $r \equiv -1 (\mathrm{mod}\, p)$ and $r \equiv -1 (\mathrm{mod}\, q)$ associative?" It was also mentioned that the smallest such open case is when $|L| = 3 \cdot 5 \cdot 29^3$. We notice that in this case $5 \not\equiv 1 (\mathrm{mod}\, 3)$. So, in Chapter 3 of this thesis, we study Moufang loops of order pqr^3 where $r \not\equiv 1 (\mathrm{mod}\, p)$ and $r \not\equiv 1 (\mathrm{mod}\, q)$, and prove that all such Moufang loops are associative provided $q \not\equiv 1 (\mathrm{mod}\, p)$. This result proves that the smallest open problem presented in [7] has been resolved.

Soon after the above result was obtained, a natural question came to us: "Are all Moufang loops of odd order $p_1 p_2 \cdots p_n q^3$, where p_i and q are primes, $2 < p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\, p_i)$ and $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$, associative as well?"

Using a method similar to that used in Chapter 3, we discover that the result also holds for Moufang loops of order $p_1 p_2 \cdots p_n q^3$. However, it revolved around a more

complicated calculation. It was quite simple to prove the existence of a cyclic Hall subloop of order pq when p and q are primes and $q \not\equiv 1 (\mathrm{mod}\, p)$ (in Chapter 3). But when we studied the Moufang loop of order $p_1 p_2 \cdots p_n q^3$, our problem grew larger as we needed to show that the concerned Hall subloop of order $p_1 p_2 \cdots p_n$ is indeed cyclic as well. Once this obstacle was overcome, our work became simpler. We just needed to modify some of the lemmas obtained in Chapter 3 so that they fit our needs for the proof in Chapter 4. We are somewhat satisfied to see our prediction proven true since construction of a nonassociative Moufang loop (if it had existed in this case) would have required a greater amount of effort.

In Chapter 5, we summarize all the significant results of our research. To open up possibilities of further research in this area, two open questions are put forward.

CHAPTER 2

DEFINITIONS, BASIC PROPERTIES AND KNOWN RESULTS ON MOUFANG LOOPS

2.1 Motivation

Before we start our discussion in the coming chapters, it is important for us to list down some of the definitions, basic properties and known results on Moufang loops so that this thesis would be as self-contained as possible.

2.2 Definitions

2.2.1 Define $zR(x,y) = (zx \cdot y)(xy)^{-1}$,

$$zL(x,y) = (yx)^{-1}(y \cdot xz),$$

$$zT(x) = x^{-1} \cdot zx.$$

$I(L) = \langle R(x,y), L(x,y), T(x) \mid x, y \in L \rangle$ is called the inner mapping group of L.

2.2.2 L_a, the associator subloop of L, is the subloop generated by all the associators (x, y, z) in L where $(x, y, z) = (x \cdot yz)^{-1}(xy \cdot z)$. We shall also denote $L_a = (L, L, L) = \langle (l_1, l_2, l_3) \mid l_i \in L \rangle$. Clearly L is associative if and only if $L_a = \{1\}$.

2.2.3 L_c, the commutator subloop of L, is the subloop generated by all the commutators $[x, y]$ in L where $[x, y] = (yx)^{-1}(xy)$.

2.2.4 Let K be a subloop of L and π a set of primes. Then

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

(ii) K is a normal subloop of L ($K \triangleleft L$) if

$K\theta = \{k\theta \mid k \in K,\ \theta \in I(L)\} = K$.

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

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

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

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

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

2.2.5 Let K be a normal subloop of L.

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

(ii) K is a minimal normal subloop of L if there exists no proper non-trivial normal subloop of L in K.

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

All other definitions follow those in [3].

2.3 Basic properties and known results on Moufang loops.

Let L be a finite Moufang loop.

2.3.1 L is diassociative, that is, $\langle x, y \rangle$ is a group for any $x, y \in L$. Moreover, if $(x, y, z) = 1$ for some $x, y, z \in L$, then $\langle x, y, z \rangle$ is a group [3, p.117, Moufang's Theorem].

2.3.2 If $x \in L$ and $\theta \in I(L)$, then $(x^n)\theta = (x\theta)^n$ for any integer n [3, p.117, Lemma 3.2 and p.120, 4.1].

2.3.3 Suppose $|L| = p^3$ where p is a prime. Then L is a group [4, p.34, Proposition 1].

2.3.4 Suppose $|L|$ is odd, K is a subloop of L, and π is a set of primes. Then

(a) $|K|$ divides $|L|$ [8, p.395, Theorem 2].

(b) K is a minimal normal subloop of $L \Rightarrow K$ is an elementary abelian group and $(K, K, L) = \langle (k_1, k_2, l) \mid k_i \in K, l \in L \rangle = \{1\}$ [8, p.402, Theorem 7].

(c) L contains a Hall $\pi-$subloop [8, p.409, Theorem 12].

(d) L is solvable [8, p.413, Theorem 16].

2.3.5 Suppose $|L|$ is odd and every proper subloop of L is a group. If there exists a minimal normal Sylow subloop in L, then L is a group [12, p.268, Lemma 2].

2.3.6 Let L be a Moufang loop of odd order such that every proper subloop and quotient loop of L is a group. Suppose Q is a Hall subloop of L such that $\left(\left|L_a\right|,\left|Q\right|\right)=1$ and $Q \lhd L_a Q$. Then L is a group [14, p.564, Lemmas 3 and 9, p.478, Lemma 1(a)].

2.3.7 Let L be a nonassociative Moufang loop of odd order such that all proper subloops and proper quotient loops of L are groups. Then:

(a) L_a is a minimal normal subloop of L; and

(b) L_a lies in every maximal normal subloop M of L. Moreover, $L = M\left\langle x\right\rangle$ for any $x \in L - M$ [15, p.478, Lemma 1].

2.3.8 Let L be a Moufang loop of odd order ${p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_m}^{\alpha_m}$ where $p_1, p_2, \ldots, p_m$ are distinct primes and $\alpha_i \le 2$. Then L is a group [13, p.882, Theorem].

2.3.9 Suppose p and q are distinct odd primes. There exists a nonassociative Moufang loop of order pq^3 if and only if $q \equiv 1 (\mathrm{mod}\, p)$ [22, p.78, Theorem 1 and 7, p.86, Theorem 2].

2.3.10 Let L be a Moufang loop of odd order $p^{\alpha} q_1 q_2 \ldots q_n$, where p and q_i are primes with $p < q_1 < \ldots < q_n$ and $\alpha \le 3$, then L is a group [16, p.349, Lemma 1, 2, p.350, Theorem].

2.3.11 L satisfies the following identities for all x, y and z in L:

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

b) $(x, y, z) = (x, yz, z)$

[3, p.124, Lemma 5.4, (5.19) and (5.17)].

2.3.12 $|x|\,\big|\,|L|$ for every $x \in L$ [3, p.92, Theorem 1.2].

2.3.13 Let N denote the nucleus of L. Then $N \lhd L$ [3, p.114, Theorem 2.1].

2.3.14 If q is a prime, then the congruence $\mu^n \equiv 1 (\mathrm{mod}\, q)$ has exactly $(n, q-1)$ number of solutions for μ [18, p.54, Theorem 2.27].

2.3.15 The order of any subloop of a finite Moufang loop is a factor of the order of the loop [9, p.109, Theorem 2].

2.3.16 $L_a \lhd L$ [11, p.33, Corollary].

2.3.17 If H is a subloop of L, u is an element of L, and d is the smallest positive integer such that $u^d \in H$, then $|\langle H, u\rangle| \geq d\,|H|$, with equality if and only if each element of $\langle H, u\rangle$ has a unique representation in the form hu^α, where $h \in H$ and $0 \leq \alpha < d$ [5, p.5, Lemma 0].

2.4 Basic properties and known results on groups.

Let G be a finite group.

2.4.1 Sylow's first theorem: If p is a prime and $p^{\alpha} \mid |G|$, then G has a subgroup of order p^{α} [10, p.92, Theorem 2.12.1].

2.4.2 Sylow's second theorem: If p a prime and $p^{n} \mid |G|$ but $p^{n+1} \nmid |G|$, then any two subgroups of G of order p^{n} are conjugates [10, p.99, Theorem 2.12.2].

2.4.3 Sylow's third theorem: The number of p-Sylow subgroups in G, for a given prime p, is of the form $1+kp$ and divides $|G|$ [10, p.100, Theorem 2.12.3].

2.4.4 Lagrange's theorem: If H is a subgroup of G, then $|H|$ is a divisor of $|G|$ [10, p.41, Theorem 2.4.1].

2.4.5 Let G be a finite group of odd order. If p is the smallest prime dividing $|G|$, P is a Sylow p-subgroup of G, and $|P| = p$ or p^2, then P has a normal p-complement in G [23, p.138, Theorem 6.2.11 and p.141, Exercise 6.3.15].

2.4.6 If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, with $p_1 < p_2 < \ldots < p_k$ odd primes and $\alpha_i > 0$ for all $i \in \{1, 2, \cdots, k\}$, then every group of order m is abelian if and only if both the following hold:

a) $\alpha_1 \leq 2$, for all $i \in \{1, 2, \ldots, k\}$;

b) $p_j^{\alpha_j} \not\equiv 1 (\mathrm{mod}\ p_i)$ for all $i, j \in \{1, 2, \cdots, k\}$

[7, p.239, Lemma 1.8].

CHAPTER 3

MOUFANG LOOPS OF ODD ORDER pqr^3

3.1 Motivation

It was proven by F. Leong and A. Rajah (see [15]) that all Moufang loops of odd order $p^{\alpha}q_1^{\beta_1}q_2^{\beta_2}\cdots q_n^{\beta_n}$ are associative if p and q_i are odd primes with $p < q_1 < q_2 < \cdots < q_n$, and

(i) $\alpha \le 3, \beta_i \le 2$; or

(ii) $p \ge 5, \alpha \le 4, \beta_i \le 2.$

In [22], A. Rajah showed that if p and q are distinct odd primes, then all Moufang loops of order pq^3 are groups if and only if $q \not\equiv 1 (\mathrm{mod}\ p)$. In [7], O. Chein and A. Rajah showed that if L is a Moufang loop of order pqr^3 where p, q and r are distinct odd primes, and if $r \not\equiv 1 (\mathrm{mod}\ p)$ and $r^2 \not\equiv 1 (\mathrm{mod}\ q)$, then L is a group. In this chapter, we will prove that all Moufang loops of order pqr^3 are associative if p, q and r are odd primes, $p < q < r$, $r \not\equiv 1 (\mathrm{mod}\ p)$, $r \not\equiv 1 (\mathrm{mod}\ q)$ and $q \not\equiv 1 (\mathrm{mod}\ p)$.

3.2 Results

3.2.1 Lemma: Let L be a Moufang loop and K a normal subloop of L. Then:

(a) L/K is a group $\Rightarrow L_a \subset K$;

(b) L/K is a commutative loop $\Rightarrow L_c \subset K$.

Proof:

Suppose L/K is a group. Then $xKyK \cdot zK = xK \cdot yKzK$ for every $x, y, z \in L$. So $(xy \cdot z)K = (x \cdot yz)K$ as $K \lhd L$. Hence $(x \cdot yz)^{-1}(xy \cdot z) = (x, y, z) \in K$. Therefore, $L_a \subset K$. This proves (a).

Now suppose L/K is a commutative loop. Then $xKyK = yKxK$ for each $x, y \in L$. So $(xy)K = (yx)K$ as K is normal in L. Thus $(yx)^{-1}(xy) = [x, y] \in K$. Hence $L_c \subset K$. This proves (b). □

3.2.2 Lemma: Suppose $M \lhd L$. If H is a Hall subloop of M such that $H \lhd M$, then $H \lhd L$.

Proof:

Since $H \subset M$, $H\theta \subset M\theta$ for all $\theta \in I(L)$. Also $M\theta = M$ since $M \lhd L$. Thus $H\theta \subset M$. Take $h \in H$ and $\theta \in I(L)$, then $h\theta \in M$. So $(h\theta)H \in M/H$ since $H \lhd M$. Thus, by 2.3.12,

$$|(h\theta)H| \text{ divides } |M/H| \qquad \ldots(1).$$

Now

$$[(h\theta)H]^{|H|} = (h\theta)^{|H|}H = (h^{|H|}\theta)H \qquad \text{(by 2.3.2)}$$

$$= (1\theta)H \qquad \text{(by 2.3.12)}$$

$$= 1H \qquad \text{(the identity element of } M/H\text{)}.$$

Hence, by 2.3.12,

$$|(h\theta)H \,|\,|\, H\,| \qquad \ldots(2).$$

Since H is a Hall subloop of M, $\left(|M/H|,|H|\right)=1$. So by (1) and (2), $(h\theta)H = 1H$, i.e., $h\theta \in H$. Therefore $H \lhd L$. □

3.2.3 Lemma: Let N be the nucleus of L. For any $x, y, z \in L$ and $n \in N$,

$$(x, y, zn) = (x, y, nz) = (x, yn, z) = (x, ny, z) = (xn, y, z) = (nx, y, z) = (x, y, z).$$

Proof:

For any $n \in N$, $(nx, y, z) = (nx \cdot yz)^{-1} \cdot (nxy \cdot z)$

$$= \left[n\left(x \cdot yz\right)\right]^{-1} \cdot \left[n\left(xy \cdot z\right)\right]$$

$$= (x \cdot yz)^{-1} n^{-1} \cdot n(xy \cdot z)$$

$$= (x \cdot yz)^{-1}(xy \cdot z) \qquad \text{(since } n \in N\text{)}$$

$$= (x, y, z) \qquad \ldots(1).$$

Now $(xn, y, z) = (n_1 x, y, z)$ for some $n_1 \in N$ since $xN = Nx$ by 2.3.13.

Then by (1), $(xn, y, z) = (x, y, z)$ …(2).

Also $(x, ny, z) = (x \cdot nyz)^{-1}(xny \cdot z)$

$$= (xn \cdot yz)^{-1}(xny \cdot z) \qquad \text{(since } n \in N\text{)}$$

$$= (xn, y, z).$$

Then by (2), $(x, ny, z) = (x, y, z)$ …(3).

Now $(x, yn, z) = (x, n_2 y, z)$ for some $n_2 \in N$ since $xN = Nx$ by 2.3.13.

Then by (3), $(x, yn, z) = (x, y, z)$ …(4).

Similarly $(x, y, nz) = (x, yn, z)$. Thus by (4), $(x, y, nz) = (x, y, z)$ …(5).

Also $(x, y, zn) = (x, y, n_3 z)$ for some $n_3 \in N$ since $xN = Nx$ by 2.3.13.

Then by (5), $(x, y, zn) = (x, y, z)$. □

3.2.4 Lemma: Let G be a group such that $|G| = pq$ where p and q are primes with $p < q$ and $q \not\equiv 1 (\mathrm{mod}\, p)$. Then there exists P, a normal subgroup of order p in G. Hence G is a cyclic group.

Proof:

By Sylow's first theorem, $\exists P < G$ such that $|P| = p$. Then by Sylow's third theorem, the number of $p-$ Sylow subgroups in G, n_p, is given as $n_p \equiv 1 (\mathrm{mod}\, p)$ where $n_p \,|\, |G|$.

Since $|G| = pq$, $n_p = 1$ or pq since $p \not\equiv 1 (\mathrm{mod}\, p)$ and $q \not\equiv 1 (\mathrm{mod}\, p)$.

Suppose $n_p = pq$.

Then $n_p \equiv 1 (\mathrm{mod}\, p) \Rightarrow pq \equiv 1 (\mathrm{mod}\, p)$

$\Rightarrow pq - 1 = kp$ for some $k \in$ □

$\Rightarrow p(q - k) = 1.$

This is a contradiction. Therefore $n_p = 1$. Then by Sylow's second theorem, $P \lhd G$. By 2.4.5 there exists a normal p-complement in G, i.e. $C_q \lhd G$. So G is generated by two normal subgroups, $C_p = P = \langle u \rangle$ and $C_q = \langle v \rangle$.

Clearly $u^{-1}v^{-1}uv \in C_p \cap C_q = \{1\}$ since $\langle u \rangle$ and $\langle v \rangle$ are normal in G. So,

$$uv = vu \qquad \text{and} \qquad (uv)^{pq} = u^{pq}v^{pq} = 1.$$

Also $(uv)^p = u^p v^p = v^p \neq 1$ and $(uv)^q = u^q v^q = u^q \neq 1$.

This forces $|uv| = pq = |G|$ and hence $\langle uv \rangle = G$. □

3.2.5 Lemma: Let L be a nonassociative Moufang loop of order pqr^3, where p, q and r are primes, $2 < p < q < r$, $r \not\equiv 1 (\mathrm{mod}\, p)$, $r \not\equiv 1 (\mathrm{mod}\, q)$ and $q \not\equiv 1 (\mathrm{mod}\, p)$. Then

(a) every proper subloop and proper quotient loop of L is a group;

(b) if $H \lhd L$ and $H \neq \{1\}$ then $L_a \lhd H$;

(c) $L = \langle x \rangle S$, for some $x \in L$ with $|x| = p$ and a maximal normal subloop S of order qr^3 in L;

(d) $|L_a| = r^2$.

Proof:

Let H be any proper subloop of L. By 2.3.15, $|H| \,\big|\, |L|$. So $|H| = p^\alpha r^\beta$, $q^\alpha r^\beta$ or pqr^γ with $\alpha \leq 1, \beta \leq 3$, $\gamma \leq 2$. By 2.3.3, 2.3.8 and 2.3.9, H is a group. For the same reason, every proper quotient loop of L is a group too. This proves (a).

If $H \lhd L$ and $H \neq \{1\}$, by 3.2.1(a), $L_a \subset H$ because L/H is a group by (a). Since $L_a \lhd L$, L_a is normal in H too. This proves (b).

By 2.3.7(a), L_a is a minimal normal subloop of L. By 2.3.4 (b), L_a is an elementary abelian group. Also if L_a is a Sylow subloop of L, then L must be

a group, by 2.3.5. This is a contradiction as L is not associative.

So,

$$|L_a| = r \quad \text{or} \quad r^2 \qquad \ldots(*) .$$

Now $|L/L_a| = pqr^2$ or pqr. Since L/L_a is a group by (a), by 2.4.5, there exists a normal p-complement in L/L_a, that is $S/L_a \lhd L/L_a$ where $|S/L_a| = qr^2$ or qr. In both cases, $S \lhd L$ and $|S| = qr^3$. So S is a maximal normal subloop of L. By 2.3.4(c), there exists an element x of order p in L. Clearly since $|x|$ does not divide $|S|$, by 2.3.12, $x \in L - S$. Since S is a maximal normal subloop of L, by 2.3.7 (b), $L = \langle x \rangle S$. This proves (c).

By (*), $|L_a| = r$ or r^2. Let us consider the case $|L_a| = r$. Let P be a $p-$Sylow subloop of L. Since $L_a \lhd L$, $L_a P$ is a subloop of L. We also know that

$$|L_a P| = \frac{|L_a||P|}{|L_a \cap P|} = \frac{rp}{1} = pr .$$

By 3.2.4, $P \lhd L_a P$. Also $(|L_a|, |P|) = (r, p) = 1$. By 2.3.6, L is a group. This is a contradiction. Therefore, $|L_a| = r^2$. This proves (d). □

3.2.6 **Lemma:** Let L be a Moufang loop with nucleus N such that $L = \langle N, x, y \rangle$ for some $x, y \in L$. Then L is a group.

Proof:

Note that $L = \langle N, x, y \rangle = N\langle x, y \rangle$ as $N \lhd L$ by 2.3.13.

Take $(l_1, l_2, l_3) \in L_a \Rightarrow l_1 = n_1 u$, $l_2 = n_2 v$ and $l_3 = n_3 w$ where $n_i \in N$ and

$u, v, w \in \langle x, y \rangle$ since $L = N\langle x, y \rangle$. Thus

$$(l_1, l_2, l_3) = (n_1 u, n_2 v, n_3 w)$$

$= (u, v, w)$ (by 3.2.3)

$= 1$ (as $u, v, w \in \langle x, y \rangle$ which is a group by diassociativity).

Hence $L_a = (L, L, L) = \langle (l_1, l_2, l_3) \mid l_i \in L \rangle$

$= \{1\}$.

Therefore, L is a group. □

3.2.7 Lemma: Let L be a nonassociative Moufang loop of order pqr^3, where p, q and r are primes, $2 < p < q < r$, $r \not\equiv 1 (\mathrm{mod}\, p)$, $r \not\equiv 1 (\mathrm{mod}\, q)$ and $q \not\equiv 1 (\mathrm{mod}\, p)$. Then the nucleus of L is trivial.

Proof:

From 3.2.5(d), we know that $|L_a| = r^2$. Assume the nucleus N of L is non-trivial. Then by 3.2.5(b), $L_a < N$. Since $|L_a| = r^2$, it follows by 2.3.15 that $|L_a| = r^2 \big| |N|$. So $|N| \geq r^2$. By Sylow's theorem, there exists $R < L$ where $|R| = r^3$. Thus there exists $y \in R - L_a$ such that $|\langle L_a, y \rangle| = r^3$. By Hall's theorem, there exists T, a Hall subloop of L, where $|T| = pq$. By 2.3.8, T is a group. Since $q \not\equiv 1 (\mathrm{mod}\, p)$, $T = \langle t \rangle$, for some $t \in L$ by 3.2.4. So by 2.3.17, $|\langle L_a, y, t \rangle| = pqr^3 = |L|$. Thus $L = \langle L_a, y, t \rangle$. Since $L_a \subset N$, $L = \langle N, y, t \rangle$. By 3.2.6, L is a group. This is a contradiction. Thus N is trivial. □

3.2.8 Lemma: Let L be a nonassociative Moufang loop of order pqr^3, where p, q and r are primes, $2 < p < q < r$, $r \not\equiv 1 (\mathrm{mod}\, p)$, $r \not\equiv 1 (\mathrm{mod}\, q)$ and $q \not\equiv 1 (\mathrm{mod}\, p)$. Then

(a) there exists a normal subloop R of order r^3 in L;

(b) $L = R\langle t \rangle$ for some $t \in L$ where $\langle t \rangle = C_{pq}$;

(c) $L = \langle t, u, v \rangle$ for some $u, v \in R$ and $t \in L$ where $\langle t \rangle = C_{pq}$;

(d) $\forall w \in R - \{1\}$, $|w| = r$ or r^2.

Proof:

By 3.2.5(c), there exists $S \lhd L$ such that $|S| = qr^3$. By 2.4.5, there exists a $q-$complement, $R \lhd S$ such that $|R| = r^3$. Since R is a Hall subloop of S, by 3.2.2, $R \lhd L$. This proves (a).

By 2.3.4, there exists T a Hall subloop of order pq in L. By 3.2.5(a), T is a group. So by 3.2.4, $T = C_{pq}$. It follows that we can write $T = \langle t \rangle$ for some element t of order pq in L. Since $R \lhd L$,

$$|R\langle t \rangle| = \frac{|R||T|}{|R \cap T|} = \frac{r^3 pq}{1} = |L|.$$

So $L = R\langle t \rangle$. This proves (b).

Suppose $\forall l_1, l_2 \in L$, $(t, l_1, l_2) = 1$. Then by the definition of the nucleus, $t \in N$. Thus $|N| \geq |t| = pq$. This contradicts with 3.2.7. Therefore

$$(t, l_1, l_2) \neq 1 \qquad \text{for some } l_1, l_2 \in L. \qquad \ldots(1)$$

Now by (b), $l_1 = ut^{\alpha}$ and $l_2 = vt^{\beta}$ for some $u, v \in R$ and $\alpha, \beta \in \{0, 1, 2, \ldots, pq\}$.

Now

$$(t, l_1, l_2) = (t, ut^{\alpha}, vt^{\beta})$$

$$= (t, ut^{\alpha}, v) \neq 1 \qquad \text{(by (1) and 2.3.11(a))} \qquad \ldots(2).$$

Suppose $(t,u,v)=1$. Then $(t,v,u)=1$ by Moufang's theorem. So $(t,v,ut^{\alpha})=1$ by 2.3.11(a). This forces $(t,ut^{\alpha},v)=1$ by Moufang's theorem; contradicting (2). So $(t,u,v)\neq 1$. Therefore $\langle t,u,v\rangle$ is not a group. So $L=\langle t,u,v\rangle$ since every proper subloop of L is a group by 3.2.5(a). This proves (c).

By 2.3.12, $\forall w \in R-\{1\}$, $|w| \mid |R| = r^3$. So $|w| = r$, r^2 or r^3. Suppose there exists $w \in R-\{1\}$ such that $|w| = r^3$, then $|\langle t,w\rangle| = pqr^3 = |L|$ by 2.3.17. So $L=\langle t,w\rangle$ is a group by diassociativity. This is a contradiction. Thus $\forall w \in R-\{1\}$, $|w| = r$ or r^2. □

3.2.9 Lemma: Let p and q be primes and $r \in \square$ such that $r \not\equiv 1 (\mathrm{mod}\, p)$ and $r \not\equiv 1 (\mathrm{mod}\, q)$. Then $(pq, r-1) = 1$.

Proof:

Since p and q are primes, $(pq, r-1) = 1$, p, q or pq.

Now $r \not\equiv 1 (\mathrm{mod}\, p) \Rightarrow p \nmid (r-1) \Rightarrow (pq, r-1) \neq p$ or pq. Similarly, $r \not\equiv 1 (\mathrm{mod}\, q)$ $\Rightarrow q \nmid (r-1) \Rightarrow (pq, r-1) \neq q$. So $(pq, r-1) = 1$. □

3.2.10 Theorem: Let L be a Moufang loop of odd order pqr^3, where p, q and r are primes, $2 < p < q < r$, $r \not\equiv 1 (\mathrm{mod}\, p)$, $r \not\equiv 1 (\mathrm{mod}\, q)$ and $q \not\equiv 1 (\mathrm{mod}\, p)$. Then L is a group.

Proof:

Suppose L is not a group …(1).

Then by 3.2.8(b), $L = R\langle t \rangle$ where R is a normal subloop of L of order r^3 and $t \in L$ where $\langle t \rangle = C_{pq}$. Let $u \in R - \{1\}$.

Now

$$t^{-1}ut = u^{\theta} \qquad \text{for some } \theta \in \square \text{ since } R \lhd L,$$
$$t^{-2}ut^2 = u^{\theta^2},$$
$$\vdots$$
$$t^{-pq}ut^{pq} = u^{\theta^{pq}}.$$

Since $|t| = pq,\ t^{-pq} = t^{pq} = 1$, then $t^{-pq}ut^{pq} = u = u^{\theta^{pq}}$.

So we have $u^{\theta^{pq}-1} = 1 \ \Rightarrow |u| \,\big|\, (\theta^{pq} - 1)$.

Now we wish to show that

$$\langle t, u \rangle = \langle tu \rangle \qquad \text{...(2).}$$

By 3.2.8(d), we know that $|u| = r$ or r^2.

Case 1: $|u| = r$. So

$$r \,\big|\, (\theta^{pq} - 1) \quad \Rightarrow \quad \theta^{pq} \equiv 1 (\mathrm{mod}\, r).$$

By 3.2.9, $(pq, r-1) = 1$. So by 2.3.14 there only exists one solution for the

congruence $\theta^{pq} \equiv 1 (\mathrm{mod}\, r)$. Since $1^{pq} = 1 \equiv 1 (\mathrm{mod}\, r)$, $\theta = 1$ is the only solution for θ. Therefore $t^{-1}ut = u$. So $[t,u] = 1$. Since $|t| = pq$ and $|u| = r$ with $(|u|,|t|) = (r, pq) = 1$, we can easily show that $\langle t,u \rangle = \langle tu \rangle$. This proves (2).

Case 2: $|u| = r^2$. Now

$$r^2 \mid (\theta^{pq} - 1)$$

$$\Rightarrow \quad r \mid (\theta^{pq} - 1)$$

$$\Rightarrow \quad \theta^{pq} \equiv 1 (\mathrm{mod}\, r).$$

As in case 1, $\theta = 1$ by 3.2.9 and 2.3.14.

Now $t^{-1}ut = u$. So $[t,u] = 1$. Since $|t| = pq$ and $|u| = r^2$ with $(|u|,|t|) = (r^2, pq) = 1$, so $\langle t,u \rangle = \langle tu \rangle$. This proves (2).

From 3.2.8(c), $L = \langle t,u,v \rangle = \langle tu, v \rangle$ by (2).

By diassociativity, L is a group. This contradicts (1).

Hence L is a group nevertheless. □

CHAPTER 4

MOUFANG LOOPS OF ODD ORDER $p_1 p_2 \cdots p_n q^3$

4.1 Motivation

In Chapter 3, we proved that all Moufang loops of order pqr^3 are groups if p, q and r are primes, $2 < p < q < r$, $r \not\equiv 1 (\mathrm{mod}\, p)$, $r \not\equiv 1 (\mathrm{mod}\, q)$ and $q \not\equiv 1 (\mathrm{mod}\, p)$. Right after the above result is obtained, another question is asked: "If p_i and q are primes with $2 < p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\, p_i)$ and $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ for $i, j \in \{1, 2, \cdots, n\}$, are all Moufang loops of order $p_1 p_2 \cdots p_n q^3$ associative as well?" In this chapter, we give a positive answer for this question.

4.2 Results

4.2.1 Lemma: Let n be the smallest positive integer such that there exists a nonassociative Moufang loop L of order $p_1 p_2 \cdots p_n q^3$ where p_i and q are primes, $2 < p_1 < p_2 < \cdots < p_n < q$, $q \not\equiv 1 (\mathrm{mod}\, p_i)$ and $p_i \not\equiv 1 (\mathrm{mod}\, p_j)$ for $i, j \in \{1, 2, \cdots, n\}$. Then

(a) $n > 2$;

(b) every proper subloop and proper quotient subloop of L is a group;

(c) $L_a \lhd H$ if $H \lhd L$ and $H \neq \{1\}$;

(d) $|L_a| = q^2$;

(e) $L = \langle x \rangle Q$, for some $x \in L$ with $|x| = p_1$ and some maximal normal

subloop Q of order $p_2 p_3 \cdots p_n q^3$ in L.

Proof:

Suppose $n \leq 2$. Then L is a group by 2.3.9 and 3.2.10. So $n > 2$. This proves (a).

Let H be any proper subloop of L. By 2.3.15, $|H| \mid |L|$.

So $|H| = p_{\alpha_1} p_{\alpha_2} \cdots p_{\alpha_m} q^3$ where $\alpha_m < n$ or $|H| = p_{\beta_1} p_{\beta_2} \cdots p_{\beta_k} q^{\beta}$ where $\beta_k \leq n$ and $\beta \leq 2$. If $|H| = p_{\alpha_1} p_{\alpha_2} \cdots p_{\alpha_m} q^3$, then H is a group since n is the smallest positive integer such that L is a nonassociative Moufang loop. If $|H| = p_{\beta_1} p_{\beta_2} \cdots p_{\beta_k} q^{\beta}$, then H is a group by 2.3.8. Hence, every proper subloop of L is a group. By the same argument, every proper quotient loop of L is a group too. This proves (b).

If $H \lhd L$ and $H \neq \{1\}$, by 3.2.1(a), $L_a \subset H$ because L/H is a group by (b). Since $L_a \lhd L$, $L_a \lhd H$ too. This proves (c).

By 2.3.7(a), L_a is a minimal normal subloop of L. By 2.3.4(b), L_a is an elementary abelian group. Also if L_a is a Sylow subloop of L, then L must be a group, by 2.3.5. This is a contradiction as L is not associative. So,

$$|L_a| = q \quad \text{or} \quad q^2 \qquad \ldots(*)$$

Assume $|L_a| = q$. By Sylow's first theorem, there exists a $p_1 -$Sylow subloop of L, P_1, where $|P_1| = p_1$. Since $L_a \lhd L$, $L_a P_1$ is a subloop of L. We also know that

$$|L_a P_1| = \frac{|L_a||P_1|}{|L_a \cap P_1|} = \frac{qp_1}{1} = p_1 q.$$

By 3.2.4, $P_1 \lhd L_a P_1$. Also $(|L_a|, |P_1|) = (q, p_1) = 1$. Then by 2.3.6, L is a group.