WHICH MOUFANG LOOPS ARE ASSOCIATIVE

by

ANDREW RAJAH

Thesis submitted in fulfillment of the requirements

for the degree of Doctor of Philosophy

June 1997

ACKNOWLEDGMENTS

First of all, I thank God for His guidance in helping me to carry on my research to completion.

I am deeply indebted to my supervisor, Associate Professor Dr. Leong Fook for his help and motivation far beyond the call of duty.

I thank my mother, Mdm. A. Thanaletchumy and my uncle Mr. A. Selvaraj for their continuous encouragement. I also thank my friend Mr. Yanda Zaihifni Ishak for his help in printing this thesis. I am grateful to all my friends who have in many ways helped me through their words and actions.

My sincere thanks to the Institute of Postgraduate Studies for providing me with the scholarship to pursue further studies. Finally, my heartfelt thanks to the staff of the School of Mathematics, Universiti Sains Malaysia for the use of their facilities in completing my research.

TABLE OF CONTENTS

Appendices (Published Articles)

1. F. Leong and A. Rajah, On Moufang loops of odd order pq^2, *J. Algebra 176* (1995), 265-270.

2. F. Leong and A. Rajah, Moufang loops of odd order $p_1^2 p_2^2 \ldots p_m^2$, *J. Algebra 181* (1996), 876-883.

3. F. Leong and A. Rajah, Moufang loops of odd order $p^4 q_1 \ldots q_n$, *J. Algebra 184.* (1996), 561-569.

4. F. Leong and A. Rajah, Moufang loops of odd order $p^\alpha q_1^2 \ldots q_n^2 r_1 \ldots r_m$, *J. Algebra 190,* (1997), 474-486.

5. F. Leong and A. Rajah, All f-loops are groups, *Com. Algebra 24(1)* (1996), 385-394.

ABSTRAK

Lup-lup Moufang yang manakah memenuhi Hukum Sekutuan

Suatu lup adalah lup Moufang jika ia memenuhi identiti $xy \cdot zx = (x \cdot yz)x$. Diketahui kewujudan lup-lup Moufang berperingkat 2^4, 3^4 dan p^5(p ialah nombor perdana yang lebih besar dari 3) yang tidak memenuhi hukum sekutuan (iaitu, bukan kumpulan). Juga terbukti bahawa semua lup Moufang berperingkat $2^\alpha\ (\alpha \le 3)$, $3^\beta\ (\beta \le 3)$ dan $p^\gamma\ (\gamma \le 4)$ memenuhi hukum sekutuan.

Tujuan penyelidikan kami ialah untuk mengkaji masalah berikut:

"Diberi suatu integer positif m, haruskah semua lup Moufang berperingkat m memenuhi hukum sekutuan?"

Oleh kerana O. Chein telah mengkaji masalah di atas secara menyeluruh untuk nilai-nilai m yang genap, kami menghadkan kajian kami kepada nilai-nilai m yang ganjil di dalam Bab(Chapter) 2 dan Bab 3. Menulis m sebagai hasildarab kuasa-kuasa bagi nombor-nombor perdana ganjil yang berlainan, kami membuktikan bahawa jawapan kepada soalan di atas adalah "ya" untuk nilai-nilai m yang berikut:

(i) $pq^2\ (p < q)$;

(ii) $p_1^2 p_2^2 \cdots p_n^2$;

(iii) $p^4 q_1 \cdots q_n\ (3 < p < q_i)$;

(iv) $p^3 q_1^2 \cdots q_n^2\ (p < q_i)$; dan

(v) $p^4 q_1^2 \cdots q_n^2\ (3 < p < q_i)$.

Disebabkan oleh kewujudan lup-lup Moufang berperingkat 3^4 yang tidak memenuhi hukum sekutuan, keputusan-keputusan (iii) dan (v) kami tidak boleh diperluaskan supaya merangkumi kes $p = 3$. Kesemua keputusan di atas diperolehi dalam Bab 2.

Dalam Bab 3, kami mengkaji masalah kami tadi bagi kes $m = pq^3$ dengan $p < q$. Di sini kami menunjukkan kewujudan lup-lup Moufang berperingkat m yang tidak memenuhi hukum sekutuan bagi setiap pasangan nombor-nombor perdana p dan q dengan $q \equiv 1 (\text{mod } p)$. Disebabkan oleh keputusan-keputusan kami di Bab 2, secara spesifik, keputusan-keputusan (iv) dan (v) dalam perenggan di atas, kajian masalah kami selesai untuk nilai-nilai m yang ganjil.

Dalam Bab 4, kami mengkaji masalah yang sama, tetapi untuk suatu subkelas lup Moufang yang dipanggil lup F. Suatu lup F ialah suatu lup Moufang yang memenuhi identiti $x(x,y,z) = (x,y,z)x$. Diketahui bahawa lup-lup F berperingkat 2^4, 3^4 dan $p^5 (p > 3)$ yang tidak memenuhi hukum sekutuan wujud. Lup-lup F yang berperingkat $2^r 3^s p_1^{\alpha_1} \ldots p_n^{\alpha_n} (p_i > 3)$ disebut lup-lup - f jika $r \leq 3, s \leq 3$ dan $\alpha_i \leq 4$. Kami menunjukkan bahawa semua lup - f memenuhi hukum sekutuan.

ABSTRACT

A loop is a Moufang loop if it fulfills the identity $xy \cdot zx = (x \cdot yz)x$. Nonassociative (i.e., non-group) Moufang loops of order 2^4, 3^4 and p^5(p is a prime greater than 3) are known to exist. It has also been proven that all Moufang loops of order 2^α ($\alpha \leq 3$), 3^β ($\beta \leq 3$) and p^γ ($\gamma \leq 4$) are associative.

The aim of our research is to study the following problem:

"Given a positive integer m, are all Moufang loops of order m associative?"

Since O. Chein has studied the problem extensively for even values of m, we limit our research to odd values of m in Chapter 2 and Chapter 3. Writing m as the product of powers of distinct odd primes, we answer the question above affirmatively for the following values of m:

(i) pq^2 $(p < q)$;

(ii) $p_1^2 p_2^2 \ldots p_n^2$;

(iii) $p^4 q_1 \ldots q_n (3 < p < q_i)$;

(iv) $p^3 q_1^2 \ldots q_n^2 (p < q_i)$; and

(v) $p^4 q_1^2 \ldots q_n^2 (3 < p < q_i)$.

Because of the existence of nonassociative Moufang loops of order 3^4, our results in (iii) and (v) cannot be extended to include the case p=3. All the results above are proven in Chapter 2.

In Chapter 3, we study our problem for the case $m = pq^3$ with $p < q$. Here we show the existence of nonassociative Moufang loops of order m for every pair of odd primes p and q with $q \equiv 1 (\text{mod } p)$. In view of our results in Chapter 2, more specifically, the results (iv) and (v) in the paragraph above, our study is complete for odd values of m.

In Chapter 4, we study the same problem for a subclass of Moufang loops called the F loops. An F loop is a Moufang loop which satisfies the identity $x(x,y,z)=(x,y,z)x$. Nonassociative F loops of order 2^4, 3^4 and $p^5(p>3)$ are known to exist. F loops of order $2^r3^s p_1^{\alpha_1}\dots p_n^{\alpha_n}(p_i>3)$ are called f - loops if $r\le 3$, $s\le 3$ and $\alpha_i \le 4$. We show that all f - loops are associative.

DEFINITIONS AND NOTATIONS

A binary system $\langle L, \cdot \rangle$ in which specification of any two of the elements x, y, z in the equation $x \cdot y = z$ uniquely determines the third element is called a quasigroup. If further it contains a (two-sided) identity element, then it is called a loop. A loop $\langle L, \cdot \rangle$ is a Moufang loop if $xy \cdot zx = (x \cdot yz)x$ for all $x, y, z \in L$. From now on, L is defined as a finite Moufang loop.

Define

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

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

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

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

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 $L_a = (L, L, L) = \langle (\ell_1, \ell_2, \ell_3) | \ell_i \in L \rangle$. Clearly L is associative if and only if $L_a = \{1\}$.

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

$N = N(L)$, the nucleus of L, is the subloop generated by all n in L such that $(n, x, y) = (x, n, y) = (x, y, n) = 1$ for all x, y in L.

$Z = Z(L)$, the centre of L, is the subloop generated by all z in N such that $[z, x] = 1$ for all x in L.

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, we let n_π be the largest π-number that divides n.

(iii) K is a normal subloop of L,$(K \lhd L)$, if $K\theta = \{k\theta | k \in K,\ \theta \in I(L)\} = K$.

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

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

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

Let H be a subloop of L. Then $C_L(H) = \{c | c \in L$ and $ch = hc$ for all $h \in H\}$.

Let K be a normal subloop of L.

(i) K is a proper normal subloop of L if $K \neq \{1\}$ and $K \neq L$.

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

Let K be a proper normal subloop of L and H a normal subloop of L.

(i) K is a minimal normal subloop of L if $H \subset K \Rightarrow H = \{1\}$ or $H = K$.

(ii) K is a maximal normal subloop of L if $K \subset H \Rightarrow H = L$ or $H = K$.

L is an F loop if $[(x, y, z), x] = 1$ for all x, y, z in L.

L is an f - loop if L is an F loop, $|L| = 2^r 3^s p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, p_i are distinct primes greater than 3, $r \leq 3$, $s \leq 3$ and $\alpha_i \leq 4$.

INTRODUCTION

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

A loop $\langle L,\cdot\rangle$, is a Moufang loop if $(x\cdot y)\cdot(z\cdot x)=[x\cdot(y\cdot z)]\cdot x$ for all x,y,z in L. It was the German lady Ruth Moufang who in 1935 first obtained this identity while studying certain aspects of geometry[31]. She also realized that there was a very close relationship between Moufang loops and groups. Though Moufang loops are generally nonassociative, she proved that "every Moufang loop is diassociative" and that "if x,y,z are elements of L such that $(x\cdot y)\cdot z=x\cdot(y\cdot z)$, then x,y,z generate a group".

Since group theory was very well established at that time, it is not surprising that many other mathematicians (especially those familiar with groups) were attracted to Moufang loops. The most notable contributions came from R.H. Bruck, the "King of Moufang Loops" from the University of Wisconsin, who during the Second World War studied the general and abstract properties of Moufang loops[1 - 11]. The following two decades saw the emergence of many more papers by other researchers. However it was in the late 60's that G. Glauberman from the University of Chicago produced an outstanding paper on Moufang loops of odd order. In [17], he proved that "all Moufang loops of odd order are solvable". This result was equivalent to the "Field Medal Award" winning paper on groups of odd order by Feit and Thompson[15]. Ten years later, O. Chein of Temple University investigated the structure of Moufang loops of order less than 64 and showed many techniques to construct nonassociative Moufang loops[13]. However, all his loops were found to be of even order.

In 1988, M. Purtill from the California Institute of Technology proved that "all Moufang loops of order the product of three odd primes (i.e., pqr, p^2q and pq^2, where $p<q<r$) are groups"[36]. It was obvious that his results could be extended. Thus P. E.

Teh, a Master's student of University Sains Malaysia in the early 90's embarked on this unknown journey. He managed to prove that "all Moufang loops of odd order $p^{\alpha}q_1 \ldots q_n$ are groups if $\alpha \leq 3$"[40]. This was an extension of Purtill's first two results. Subsequently, when Teh tried to extend the third result (i.e., order pq^2), he realized that there was a flaw in Purtill's proof. This was pointed out to Purtill who admitted his mistake. Although they guessed that the result could still be true, they were unable to make the amendment. Consequently, that result was withdrawn[37]. Hence it remained as an open problem.

I started my research on Moufang loops in June 1993. Since my supervisor, Dr. F. Leong had earlier supervised Teh to do his research on "Which Moufang Loops are Groups"[40], naturally I was asked to continue from where Teh had stopped, and look at the open problems left behind by him. Hence came my research topic: "Which Moufang Loops are Associative".

In this thesis, we first look at the open problem: "Are all Moufang loops of odd order pq^2 associative?" In trying to solve this problem, we establish a new way of looking at the properties of a Moufang loop, that is, by considering its associators. Using mainly Bruck's lemma for associators from [10] (actually it was after many excitements and disappointments, including several occasions when we thought of giving up this seemingly impossible task), we finally manage to exclaim "Eureka!" This result was published in the Journal of Algebra[26].

Having conquered this hill, we are led to imagine that the summit is "all Moufang loops of order $3^3 p_1^4 \ldots p_n^4$ (where p_i are distinct primes greater than 3) are also associative!" Since there exist nonassociative Moufang loops of order 3^4 and $p^5 (p \geq 5)$ [4, 40],this conjecture is the highest we can expect. Furthermore since all Moufang loops of order 3^3 and $p^4 (p \geq 5)$ are associative[12, 20], we really begin on a journey full of hope.

One has to conquer many hills before reaching Mount Everest. The same applies to our summit. The next hill we aim at is: "Moufang loops of odd order $p_1^2 p_2^2 \ldots p_n^2$". Realizing that a group of odd order $p_1^2 p_2^2 \ldots p_n^2$ has a normal subgroup of order p_n^2, we establish a

similar result for a Moufang loop. With this as a stepping stone, we have made another exclamation of "Eureka!" This result was also published in the Journal of Algebra[27].

After proving in [25] that "all Moufang loops of odd order $p^3q_1\ldots q_n$ are groups", Leong, Teh and Lim had posed an open problem: "Are all Moufang loops of odd order $p^4q_1\ldots q_n$ associative as well?" Due to the existence of nonassociative Moufang loops of order 3^4, we need to consider only the case $p \geq 5$. By using Glauberman's theorem that a minimal normal subloop of a Moufang loop of odd order is elementary abelian, we conquer this third hill also. This result was published in the Journal of Algebra as well[29].

Our next destination is the twin peaks: "Moufang loops of odd order $p^\alpha q_1^2\ldots q_n^2$ for $\alpha = 3$; and $\alpha = 4$ when $p \geq 5$". We have a very difficult time with this problem as compared to our previous experiences. However, we discover that the nucleus N of the Moufang loop L is nontrivial in each of the two cases. Thus L/N is a group by induction. This becomes the ladder for us to successfully climb up to the twin peaks. This result was published in the Journal of Algebra recently[30].

Now, to go one step higher, we inquire, "Are all Moufang loops of odd order pq^3 associative?" In the beginning, this problem did not appear to be too difficult. However, after 1001 attempts, we could not make any headway. So we felt very curious: could it be the dead end of our long march? If that was the case, then we would have to provide a counterexample. But we had no experience in constructing nonassociative Moufang loops! (Sometimes it is easier to prove something than to contradict it.) However, we had no choice but to walk on an unfamiliar path.

Firstly, we show that any Moufang loop L of order pq^3 can be written as $L = C_p \leftthreetimes Q$, i.e., a semidirect product of a cyclic group C_p of order p and a group Q of order q^3. Then we show that if $q \not\equiv 1 (\mathrm{mod}\ p)$, then L would be a group. Since we wish to study a nonassociative Moufang loop of order pq^3, we only examine the case $q \equiv 1\ (\mathrm{mod}\, p)$. Next, we show that Q is a group of exponent q, and that Q is nonabelian if $p \neq 3$. Then we work out the product rule for any two elements of L. Finally, by using messy

calculations, we show that a set L of pq^3 elements with the product rule worked out is indeed a nonassociative Moufang loop (of order pq^3).

Suddenly, we realize that we have reached the summit. This summit is much lower than the one we had imagined in the beginning. Anyway, we have the feeling of being at the top of the world. The night is still young and our spirits are still high. Instead of resting on our laurels, we march on to the final open problem left by Teh: "Which F loops are associative?"

Going back further, F. Fenyves defined Extra Loops, a special class of Moufang loops in [16] and [17]. His idea was expounded by Chein and D. A. Robinson in An "Extra Law" for Characterizing Moufang Loops[14]; followed by Robinson in Holomorphy Theory of Extra Loops[38]; and H. O. Pflugfelder in A Special Class of Moufang Loops[35]. In 1972, Leong and his Ph. D. supervisor Bruck defined a class of Moufang loops (called the F loops) which contained all these subclasses of Moufang loops. An F loop is a Moufang loop which satisfies the identity $x(x,y,z) = (x,y,z)x$. An F loop of order $2^r 3^s p_1^{\alpha_1} \dots p_n^{\alpha_n}$ (where p_i are distinct primes greater than 3) is an f - loop if $r \leq 3$, $s \leq 3$ and $\alpha_i \leq 4$.

Teh has shown in [23] that "all f - loops with $r \leq 2$ are groups". The success of his proof lies in the fact that 120 is a divisor of any nonassociative simple Moufang loop. So, if L is a nonassociative f - loop such that 120 does not divide the order of L, then it is nonsimple. Then there exists a proper normal subloop in L. Hence, Teh uses induction to achieve his result. However, we cannot assume that L is nonsimple if $r = 3$ since 120 may divide the order of L.

While searching for a solution to this problem, we discovered L. J. Paige's [34]. By examining the elements of the class of simple Moufang loops described in that paper, we show that all nonassociative f - loops are nevertheless nonsimple. Then we use induction to prove that "all f -loops are associative". This result appears in [28]. There exist Moufang loops of order 2^4, 3^4 and $p^5 (p \geq 5)$ which can be shown to be nonassociative F loops. Hence, our result is the best possible.

In the beginning, when we had just started our research, we did not dare dream that we could achieve any stupendous result. However, we believed: "blessed are those who persevere". Our perseverance managed to see us through. This wisdom will be our everlasting weapon for any journey in the future: be it in life or in mathematics.

Chapter 1: BASIC PROPERTIES AND KNOWN RESULTS WITH MOUFANG LOOPS

Let L be a finite Moufang loop.

1.1 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 [10, p. 117, Moufang's Theorem].

1.2 If $x \in L$ and $\theta \in I(L)$, then $(x^n)\theta = (x\theta)^n$ for any integer n [10, p.117, Lemma 3.2 and p.120, (4.1)].

1.3 Suppose $x, y, u, v \in L$ and $\theta \in I(L)$. Then $(xy)\theta \cdot c = x\theta[y\theta \cdot c]$ where c is called the companion of $L(u, v)$ with $c=[u^{-1}, v^{-1}]$ if $\theta = L(u, v)$ and $c = u^{-3}$ if $\theta = T(u)$ [10, p.112, Lemma 2.1, p.113, Lemma 2.2 and p.117, Lemma 3.2].

1.4 L satisfies the following identities:

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

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

(g) $y[x(x, y, z)^{-1}]=(yx)(y, x, z)$

[10, p.124, Lemma 5.4].

1.5 $|x|$ divides $|L|$ for every $x \in L$ [10, p.92, Thm. 1.2].

1.6 Z and N are normal subloops of L [10, p.60, Lemma 1.1 and p.114, Thm. 2.1].

1.7 $x(y \cdot xz) = (xy \cdot x)z$ for all $x, y, z \in L$ [10, p.115, Lemma 3.1 (3.3)].

1.8 L satisfies all or none of the following identities:

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

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

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

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

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

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

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

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

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

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

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

[10, p.125, Lemma 5.5].

1.9 If $|L| = p, p^2, p^3$ or pq where p and q are distinct primes, then L is a group [12, p.35, Corollary 4 and Proposition 3, and p.34, Proposition 1].

1.10 $|L|$ is odd if and only if each of its elements has odd order [18, p.395, Thm.1].

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

(a) L is solvable [18, p.413, Thm.16];

(b) $|K|$ divides $|L|$ [18, p.395, Thm.2];

(c) If K is a minimal normal subloop of L, then K is an elementary abelian group and $(K,K,L)=\langle (k_1, k_2, \ell) \mid k_i \in K, \ell \in L \rangle = \{1\}$ [18, p.402, Thm.7];

(d) If $K \triangleleft L$, $(K,K,L) = \{1\}$ and $(|K|, |L/K|) = 1$, then $K \subset N$ [18, p.405, Thm.10];

(e) L contains a Hall π-subloop [18, p.409, Thm.12].

1.12 $|L| = 2^{\alpha}$ for some positive integer α if and only if each of its element is a 2-element [19, p.415, Thm.].

1.13 Suppose $|L| = p^4$ where p is a prime greater than 3. Then L is a group [20, p.33, Thm.].

1.14 $L_a \triangleleft L$ [21, p.33, Corollary].

1.15 Suppose $H \triangleleft L$ and $H \subset N$. Then $C_L(H) \triangleleft L$ and $|L / C_L(H)|$ divides $|\mathrm{Aut}(H)|$ [21, p.33, Thm. 3(a)].

1.16 $L_a \subset C_L(N)$ [21, p.34, Corollary].

1.17 Suppose $|L| = 2m$ where $(2, m) = 1$. Then there exists a normal subloop M of order m in L such that $L = C_2 M$ [24, p.411, Lemma 1].

1.18 Suppose $|L| = p^{\alpha} q_1 \ldots q_n$ where $\alpha \leq 3$ and $p, q_1, \ldots, q_n$ are distinct odd primes with $p < q_i$. Then L is a group [25, p.349, Lemma 1 and Lemma 2, and p.350, Thm.].

1.19 Suppose a, b and m are integers and $(a,m) = 1$. Then there exists an integer x which satisfies the congruence $ax \equiv b \pmod{m}$ [33, p.25, Corollary 2.9].

1.20 If q is a prime, then the congruence $\mu^n \equiv 1 (\mathrm{mod}\, q)$ has $(n, q-1)$ solutions for μ

[33, p.54, Thm. 2.27].

1.21 Let $F = GF(p^n)$, the Galois field with p^n elements. Let $R = \left\{ \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \middle| a, b \in F, \right.$

$\left. \alpha \text{ and } \beta \text{ are 3 dimensional coordinate vectors over } F \right\}$.

Define $\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \circ \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \circ \gamma + bd \end{pmatrix}$ where "$\circ$" and

"$\times$" are the usual scalar and vector products.

Define $M = \left\{ \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \middle| ab - \alpha \circ \beta = 1 \right\} \subset R$. Then:

(a) M is a nonassociative Moufang loop.

(b) $Z = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is the centre of M.

(c) M/Z is a nonassociative simple Moufang loop which is denoted by $M(p^n)$

[34, p.473, Thm.3.3, p.474, Lemma 3.5, p.473, Lemma 3.4, and p.475, Thm.4.1].

1.22 L is a simple Moufang loop if and only if L is a simple group or L is isomorphic to one of the simple loops $M(p^n)$ [32, p.33, Thm.].

1.23 Let G be a finite group of odd order. If p is the smallest prime dividing $|G|$, P is a Sylow p-subloop of G and $|P| = p$ or p^2, then P has a normal p-complement in G [39, p.138, Thm.6.2.11 and p.141, Exercise 6.3.15].

Chapter 2: WHICH MOUFANG LOOPS OF ODD ORDER ARE ASSOCIATIVE?

2.1 Moufang Loops of Odd Order pq^2

Motivation

It is known that all Moufang loops of order p, p^2, pq and p^3 are groups when p and q are primes [12]. Are Moufang loops of odd order pqr and pq^2 associative for distinct primes p, q and r? [36] gave an affirmative answer. However, a flaw was discovered in the proof for the case pq^2 where $p < q$ [37]. Here, we prove that the conjecture is still true.

Results

2.1.1 Lemma: Let N be the nucleus of a Moufang loop L. Then for any $x, y, z \in L$ and $n \in N$, $(xn, y, z) = (x, yn, z) = (x, y, zn) = (x, y, z)$.

Proof:

$(xn, y, z) = (xn \cdot yz)^{-1} \cdot (xny \cdot z)$

$= (n_1 x \cdot yz)^{-1} \cdot (n_1 xy \cdot z)$ for some $n_1 \in N$ since $xN = Nx$ by 1.6

$= [n_1 (x \cdot yz)]^{-1} \cdot [n_1 (xy \cdot z)]$ as $n_1 \in N$

$= (x \cdot yz)^{-1} n_1^{-1} \cdot n_1 (xy \cdot z) = (x \cdot yz)^{-1} (xy \cdot z)$.

Thus $(xn, y, z) = (x, y, z)$ ....(1).

Also,

$(x, yn, z) = (x \cdot ynz)^{-1} (x yn \cdot z)$

$= \left(x \cdot n_2 yz\right)^{-1} \left(xn_2 y \cdot z\right)$ for some $n_2 \in N$ since $yN = Ny$ by 1.6

$= (xn_2 \cdot yz)^{-1} (xn_2 y \cdot z)$ as $n_2 \in N$

$= (xn_2, y, z)$.

Thus by (1), $(x, yn, z) = (x, y, z)$ ....(2).

Similarly,

$(x, y, zn) = (x \cdot yzn)^{-1}(xy \cdot zn) = (x \cdot yn_3z)^{-1}(xy \cdot n_3z)$ for some $n_3 \in N$ by 1.6

$= (x \cdot yn_3z)^{-1}(xyn_3 \cdot z)$

$= (x, yn_3, z)$

$= (x, y, z)$ by (2).

2.1.2 Lemma: Let L be a Moufang loop of odd order such that every proper subloop of L is a group. If there exists a minimal normal Sylow subloop K in L, then L is a group.

Proof:

As K is a Sylow subloop of L, $(|K|, |L/K|) = 1$. By 1.11(e), there exists a Hall π - subloop H of order $|L/K|$ in L. By 1.11(c), $(K, K, L) = \{1\}$. Thus $K \subset N$ by 1.11(d). Since $|HK| = \frac{|H||K|}{|H \cap K|} = |H||K| = |L|$, $L = HK = HN$ by 1.6.

Now

$L_a = (L, L, L) = (HN, HN, HN) = (H, H, H)$ by 2.1.1

$= H_a = \{1\}$ since H is a group.

Thus L is a group.

2.1.3 Lemma: Let L be a Moufang loop. Suppose:

(i) Q is a commutative subloop of L; and

(ii) L_a is a cyclic group $\langle k \rangle$ which is contained in Q.

Then for all $k_0 \in L_a$, $u, v \in L$ and $y \in Q$, the following identities hold:

(a) $(u, k_0, v)^{-1} = (k_0, u, v)$;

(b) $(k_0, u, v) = (u, v, k_0)$;

(c) $(y^n, u, v) = (y, u, v)^n$ for any integer n;

(d) $(u, v, k) = k^\alpha$ for some integer $\alpha \Rightarrow k^\alpha = (k, v, u)^{\alpha-1}$;

(e) $(y, v, k) = k^\beta$ for some integer $\beta \Rightarrow k^\beta = (k, y, ky \cdot v)^{1-\beta}$.

Proof:

(a) By 1.4(g), $k_0[u(u,k_0,v)^{-1}] = (k_0u)(k_0,u,v)$.

Since $k_0 = k^r$, $(u, k_0,v)^{-1} = k^s$ and $(k_0,u,v) = k^t$ for some integers r, s and t, $(u, k_0,v)^{-1} = (k_0, u, v)$ by diassociativity of L.

(b) $(k_0,u,v) = (k_0,uv,v)$ by 1.4(c)

$= (uv, k_0,v)^{-1}$ by (a)

$= (u, v, k_0)$ by 1.4(e)

(c) $[y\,L(v, u)]^n = y^nL(v,u)$ for any integer n by 1.2. So $[y(y,u,v)^{-1}]^n$ $= y^n(y^n, u, v)^{-1}$ by 1.4(b). Then $y^n(y, u, v)^{-n} = y^n(y^n, u, v)^{-1}$ as $L_a \subset Q$ and Q is commutative. Thus $(y,u,v)^{-n} = (y^n,u,v)^{-1}$ and hence $(y^n,u,v) = (y, u, v)^n$.

(d) Since $(u, v, k) \in \langle k \rangle$, we can write $(u, v, k) = k^\alpha$ for some integer α.

Now $uv \cdot k = (u \cdot vk)(u, v, k)$

$= (u \cdot vk)k^\alpha$.

So $uv \cdot k^{1-\alpha} = u \cdot vk$ by diassociativity of L.

Thus $v[uv \cdot k^{1-\alpha}] = v[u \cdot vk] = vuv \cdot k$ by 1.7.

Then $(vuv \cdot k^{1-\alpha})(v,uv,k^{1-\alpha})^{-1} = vuv \cdot k$. Since $(v, uv, k^{1-\alpha})^{-1}$ lies in $\langle k \rangle$, we can write $vuv \cdot \left[k^{1-\alpha}\left(v,uv,k^{1-\alpha}\right)^{-1}\right] = vuv \cdot k$ by diassociativity of L. Thus $k^{1-\alpha}(v, uv, k^{1-\alpha})^{-1} = k$.

Hence $k^{\alpha} = (v,\ uv,\ k^{1-\alpha})^{-1}$

$= (k,\ v,\ uv)^{\alpha-1}$ by (b) and (c)

$= (k,\ v,\ u)^{\alpha-1}$ by 1.4(d).

(e) If $(y,\ v,\ k) = k^{\beta}$, then $k^{\beta} = (k,\ v,\ y)^{\beta-1}$ by (d). So

$k^{\beta} = (v,\ y,k)^{\beta-1}$ by (b)

$= (v,y,ky)^{\beta-1}$ by 1.4(d)

$= (v,y,ky\cdot v)^{\beta-1}$ by 1.4(f)

$= ((ky)^{-1}(ky\cdot v)\ ,\ y,\ ky\cdot v)^{\beta-1}$

$= ((ky)^{-1},\ ky\cdot v,\ y)^{1-\beta}$ by 1.4(e)

$= (ky,ky\cdot v,y)^{\beta-1}$ by (c) as $ky \in Q$

$= (k,\ y,\ ky\cdot v)^{1-\beta}$ by 1.4(e).

2.1.4 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:

(a) Suppose L/K is a group. Then $xKyK\cdot zK = xK\cdot yKzK$ for each $x,\ y,\ z \in L$.

So $(xy\cdot z)K = (x\cdot yz)K$ as $K \lhd L$. Thus $(x\cdot yz)^{-1}(xy\cdot z) = (x,\ y,\ z) \in K$.

Hence $L_a \subset K$.

(b) Suppose L/K is a commutative loop. Then $xKyK = yKxK$ for each $x,\ y \in L$.

So $(xy)K = (yx)K$ as $K \lhd L$. Thus $(yx)^{-1}(xy) = [x,\ y] \in K$. Hence $L_c \subset K$.

2.1.5 Theorem: Let L be a Moufang loop of odd order pq^2 where p and q are distinct primes. Then L is a group.

Proof:

Suppose $q < p$. Then L would be a group by 1.18. So we can assume that $p < q$. By 1.11(a), L is solvable. So there exists a minimal normal subloop K in L. By 1.11(c), K is elementary abelian. Thus $|K| = p$, q or q^2 by 1.11(b).

Suppose $|K| = p$ or q^2. Then L would be a group by 2.1.2. So we can assume that $|K| = q$. By 1.9, L/K is a group of order pq. Since $p < q$, there exists a subgroup Q/K of order q normal in L/K by 1.23. Then Q is a subloop of order q^2 normal in L.

Since L/K is a group, by 2.1.4(a), $L_a \subset K$. Since L_a is a subloop of K, by 1.11(b), $|L_a| = 1$ or q. If $|L_a| = 1$ then L would be a group. So we can assume that $|L_a| = q$ and $L_a = K$. In other words, we suppose that L is not a group.

We write $K = \langle k \rangle$. Let $y \in Q\text{-}K$ and $w \in L\text{-}Q$. So $Q = \langle y, k \rangle$. Let $H = \langle y, w, k \rangle$. Then $|H| > |Q| = q^2$. By 1.11(b), $|H|$ divides pq^2. Thus $H = L = \langle y, w, k \rangle$.

Since $(y, w, k) \in L_a = K$, we can write

$$(y, w, k) = k^{\alpha} \qquad \ldots.(1)$$

for some integer α where $1 \leq \alpha < q$. (Our assumption that L is not a group eliminates the possibility $\alpha = q$).

By 2.1.3(e),

$$k^{\alpha} = (k, y, ky \cdot w)^{1-\alpha} \qquad \ldots.(2).$$

Suppose there exists an element u of order q^2 in L. Then take $v \in L - \langle u \rangle$. Now $q^2 < |\langle u, v \rangle| \leq pq^2 = |L|$. So $|\langle u, v \rangle| = pq^2$ by 1.11(b). Then L would be a group by diassociativity. This is a contradiction. So there exists no element of order q^2 in L. Similarly, we can show that there exists no element of order pq in L.

Since $ky \in Q$, $|ky| = q$.

Suppose $|w| \neq p$. Then by 1.5, $|w| = q$. Since $w \notin Q$ and $Q \triangleleft L$, $|\langle w \rangle Q| = q^3 > pq^2 = |L|$. This is a contradiction. Hence $|w| = p$.

Let $S = \langle ky, w \rangle$. S is a group by disassociativity. Since $|w| = p$ and $|ky| = q$, pq divides $|S|$. Since L is not a group, $L \neq S$. Thus $|S| = pq$ by 1.11(b). So $\langle ky \rangle$, the Sylow q - subloop of S, is normal in S by 1.23. Thus $ky \cdot w = w(ky)^{\gamma}$ for some integer γ.

Substituting in (2) we get:

$$
\begin{aligned}
k^{\alpha} &= \left(k,\, y,\, w(ky)^{\gamma}\right)^{1-\alpha} \\
&= \left(y,\, w(ky)^{\gamma},\, k\right)^{1-\alpha} && \text{by 2.1.3(b)} \\
&= \left(y,\, w(ky)^{\gamma}, ky\right)^{1-\alpha} && \text{by 1.4(f)} \\
&= (y,\, w,\, ky)^{1-\alpha} && \text{by 1.4(c) repeatedly} \\
&= (y,\, w,\, k)^{1-\alpha} && \text{by 1.4(f).}
\end{aligned}
$$

So by (1), $(y, w, k) = (y, w, k)^{1-\alpha}$. Then $(y, w, k)^{\alpha} = 1$. Thus $|(y, w, k)|$ must divide α. But $(y, w, k) \in L_a - \{1\} \Rightarrow |(y, w, k)| = q$. Hence q must divide α. This is a contradiction by (1).

Thus $|L_a| \neq q$. Hence L is a group.

2.2 Moufang Loops of Odd Order $p_1^2 p_2^2 \cdots p_n^2$

Motivation

We proved in 2.1 that all Moufang loops of odd order pq^2 are groups for distinct primes p and q. Now, we extend that result to Moufang loops of odd order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ where p_i are distinct primes and $\alpha_i \leq 2$.

Results

2.2.1 Lemma: Let L be a Moufang loop of odd order and M a normal subloop of L. If H is a Hall π-subloop of M such that H is normal in M, then H is normal in L.

Proof:

Take $h \in H$. Since $H \triangleleft M \triangleleft L$, $H\theta \subset M\theta = M$ for all $\theta \in I(L)$. So $(h\theta)H \in M/H$. Thus by 1.5, $|(h\theta)H|$ divides $|M/H|$. Also,

$$\begin{aligned} [(h\theta)H]^{|H|} &= (h\theta)^{|H|} H = (h^{|H|}\theta)H && \text{by 1.2} \\ &= (1\theta)H && \text{by 1.5} \\ &= 1H && \text{the identity element of } M/H. \end{aligned}$$

Hence, by 1.5, $|(h\theta)H|$ divides $|H|$. As $(|M/H|, |H|) = 1$, $(h\theta)H = 1H$. Thus $h\theta \in H$. Therefore $H \triangleleft L$.

2.2.2 Lemma: Let G be a group of odd order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ where $1 \leq \alpha_i \leq 2$ and each p_i is a prime such that $p_1 < p_2 < \ldots < p_n$. Then there exists a subgroup Q of order $p_n^{\alpha_n}$ normal in G.

Proof:

By Sylow's theorem, there exists a subgroup P_1 of order $p_1^{\alpha_1}$ in G. Since p_1 is the smallest prime dividing $|P_1|$ and $1 \leq \alpha_1 \leq 2$, by 1.23, P_1 has a normal p_1 – complement H_2 of order $p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_n^{\alpha_n}$ in G. By similar argument, we can get $H_3, H_4, \ldots, H_n$ such that $H_n \lhd H_{n-1} \lhd \ldots \lhd H_2 \lhd G$ and $|H_i| = p_i^{\alpha_i} p_{i+1}^{\alpha_{i+1}} \ldots p_n^{\alpha_n}$.

Since H_n is normal Hall in H_{n-1} and $H_{n-1} \lhd H_{n-2}$, $H_n \lhd H_{n-2}$ by 2.2.1. Now H_n is normal Hall in H_{n-2} and $H_{n-2} \lhd H_{n-3}$. Thus $H_n \lhd H_{n-3}$ by 2.2.1. In this manner, by using 2.2.1 repeatedly, we can show that $H_n \lhd G$ where $|H_n| = p_n^{\alpha_n}$.

2.2.3 Lemma: Let L be a Moufang loop of odd order $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ where $1 \leq \alpha_n \leq 2$ and each p_i is a prime such that $p_1 < p_2 < \ldots < p_n$. Suppose:

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

(ii) the Sylow p_n- subloop is normal in L.

Then L is a group.

Proof:

Let Q be the Sylow p_n -subloop described in (ii). Now, L/Q is a group by (i). So $L_a \subset Q$ by 2.1.4(a). By 1.11(a), L is solvable. Let K be a minimal normal subloop of L. Then K is elementary abelian by 1.11(c). So by 1.11(b), $|K| = p_j^{\beta}$ where $1 \leq \beta \leq \alpha_j$. Now L/K is a group by (i). Thus $L_a \subset K$ by 2.1.4(a).

Suppose $p_j \neq p_n$. Then $L_a \subset K \cap Q = \{1\}$,i.e., $L_a = \{1\}$. Thus L would be a group.

So we can assume that $p_j = p_n$. Thus $|K| = p_n^{\beta}$.

Suppose $\beta = \alpha_n$. Then K would be a Sylow subloop of L and L would be a group by 2.1.2.

So we can assume that $\beta < \alpha_n$, that is, $\beta = 1$ and $\alpha_n = 2$. Thus $|K| = p_n$ and $|Q| = p_n^2$. Since $L_a \subset K$, $|L_a| = 1$ or p_n. If $|L_a| = 1$, then L would be a group. So we can assume that $|L_a| = p_n$ and $L_a = K$. We write $K = \langle k \rangle$.

Let $y \in Q\text{-}K$ and $w \in L\text{-}Q$. Since the associator $(y, w, k) \in K$, we can write $(y, w, k) = k^\theta$ for some integer θ.

Case 1: Suppose $k^\theta = (y, w, k) = 1$ for all $w \in L\text{-}Q$.

We want to show that $(Q, Q, L) = \{1\}$.

Suppose Q is cyclic. Then we are through by diassociativity of L. So we can assume that Q is not cyclic. Since $|Q| = p_n^2$, it is elementary abelian. So we can write $Q = \langle k \rangle \langle y \rangle$. Thus any element in Q can be written as $k_i y_j$ where $k_i \in \langle k \rangle$ and $y_j \in \langle y \rangle$.

Take an element $(g_1, g_2, w) \in (Q, Q, L\text{-}Q)$. Write $g_1 = k_1 y_1$ and $g_2 = k_2 y_2$. We aim to prove:

(a) $(g_2, y_1, w) = 1$;

(b) $(g_2, k_1, w) = 1$;

(c) $(g_1, g_2, w) = 1$.

Now $(k_2 y_2) L(w, y_1) \cdot c_1 = (k_2 L(w, y_1)) \cdot (y_2 L(w, y_1) \cdot c_1)$, where $c_1 = [w^{-1}, y_1^{-1}]$, by 1.3. So by 1.4(b), $(k_2 y_2)(k_2 y_2, y_1, w)^{-1} \cdot c_1 = (k_2 (k_2, y_1, w)^{-1}) \cdot (y_2 (y_2, y_1, w)^{-1} \cdot c_1)$. Since $Q \lhd L$ and $y_1 \in Q$, $c_1 \in Q$. Also, since $\langle y, w \rangle$ is a group by diassociativity, $(y_2, y_1, w) = 1$. Clearly all the terms in the above equality lie in the abelian group Q. Thus we get

$(k_2y_2, y_1, w) = (k_2, y_1, w)$. So by the assumption in Case 1, $(k_2y_2, y_1, w) = 1$. This proves (a).

Now, by 1.3, $(k_2y_2)L(w,k_1)\cdot c_2 = \left(k_2L(w,k_1)\right)\cdot\left(y_2L(w,k_1)\cdot c_2\right)$ where $c_2 = \left[w^{-1}, k_1^{-1}\right]$. Then by 1.4(b), $(k_2y_2)(k_2y_2, k_1, w)^{-1}\cdot c_2 = \left(k_2(k_2, k_1, w)^{-1}\right)\cdot\left(y_2(y_2, k_1, w)^{-1}\cdot c_2\right)$. As in the previous paragraph, $(k_2y_2, k_1, w) = (y_2, k_1, w) = 1$. This proves (b).

Now $(k_1y_1)L(w,g_2)\cdot c_3 = \left(k_1L(w,g_2)\right)\cdot\left(y_1L(w,g_2)\cdot c_3\right)$ where $c_3 = \left[w^{-1}, g_2^{-1}\right]$ by 1.3. So by 1.4(b), $(k_1y_1)(k_1y_1, g_2, w)^{-1}\cdot c_3 = \left(k_1(k_1, g_2, w)^{-1}\right)\cdot\left(y_1(y_1, g_2, w)^{-1}\cdot c_3\right)$. As in the previous paragraphs, $(k_1y_1, g_2, w) = (k_1, g_2, w)\cdot(y_1, g_2, w) = 1$ by (a), (b) and Moufang's Theorem. This proves (c).

Hence by (c), $(Q, Q, L\text{-}Q) = \{1\}$. Also $(Q, Q, Q) = Q_a = \{1\}$ as Q is a group. Thus $(Q, Q, L) = \{1\}$. Since $\left(|Q|, |L/Q|\right) = 1$, $Q \subset N$ by 1.11(d). By 1.11(e), there exists a Hall subloop H of order $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{n-1}^{\alpha_{n-1}}$ in L. So $L=HQ=HN$ and $L= (L, L, L) = (HN, HN, HN) = (H, H, H)$ by 2.1.1. Then $L_a = H_a = \{1\}$ as H is a group by (i). Thus L is a group.

Case 2: Suppose $k^\theta = (y, w, k) \neq 1$ for some $w \in L\text{-}Q$.

Clearly $\langle y, w, k\rangle$ is not a group. Since every proper subloop of L is a group by (i), $\langle y, w, k\rangle = L$. By 2.1.3(e),

$$k^\theta = (k, y, ky\cdot w)^{1-\theta} \qquad \ldots.(*).$$

Let $S = \langle w, ky\rangle$. By diassociativity, S is a group.

Suppose p_n^2 divides $|S|$. Then by 1.11(e) and 1.11(b), we can show that $Q \subset S$. Thus $k \in S$. So $k^{-1} \cdot ky = y \in S$. Hence $\langle y, w, k \rangle = 1$ as S is a group. This contradicts our assumption in Case 2. So p_n^2 does not divide $|S|$. Since $ky \in S$, p_n divides $|S|$. Thus by 1.11(b), $|S| = p_1^{\beta_1} p_2^{\beta_2} \ldots p_{n-1}^{\beta_{n-1}} p_n$ where $0 \leq \beta_i \leq \alpha_i$.

Suppose $\langle ky \rangle$ is not normal in S. Then there exists $\langle y_1 \rangle$ another Sylow p_n-subgroup in S. Since $ky, y_1 \in Q$, they commute. Thus $|\langle ky, y_1 \rangle| = p_n^2$. This is a contradiction as $\langle ky, y_1 \rangle \subset S$ but p_n^2 does not divide $|S|$. So $\langle ky \rangle$, the Sylow p_n-subgroup of S, is normal in S. Thus $ky \cdot w = w(ky)^\gamma$ for some integer γ. Substituting in $(*)$, we get:

$$
\begin{aligned}
(y,\ w,\ k) &= \left(k, y, w(ky)^\gamma\right)^{1-\theta} \\
&= \left(y, w(ky)^\gamma, k\right)^{1-\theta} && \text{by 2.1.3(b)} \\
&= \left(y, w(ky)^\gamma, ky\right)^{1-\theta} && \text{by 1.4(f)} \\
&= \left(y, w,\ ky\right)^{1-\theta} && \text{by 1.4(c) several times} \\
&= \left(y, w, k\right)^{1-\theta} && \text{by 1.4(f).}
\end{aligned}
$$

So $(y,\ w,\ k)^\theta = 1$. Thus $|(y, w, k)|$ divides θ. Since $(y,\ w,\ k) \neq 1$, $|(y, w, k)| = p_n$. So $\theta = cp_n$ for some integer c. Then we get $k^\theta = k^{cp_n} = 1$ which is a contradiction by our assumption in Case 2.

2.2.4 Theorem: Let L be a Moufang loop of odd order $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ where p_i are distinct primes and $\alpha_i \leq 2$. Then L is a group.

Proof:

Let L be a smallest counter example. By 1.11(b), every proper subloop and quotient loop of L is a group. Without loss of generality, $p_1 < p_2 < \ldots < p_n$ and $\alpha_i \neq 0$. By 1.11(a), L is solvable. Let K be a minimal normal subloop of L. Then by 1.11(c), K is elementary abelian. Suppose $|K| = p_j^{\alpha_j}$. Then by 2.1.2, L would be a group as K would be a Sylow p_j-subloop of L. So we can assume that $|K| = p_j$ and $\alpha_j = 2$.

Case 1: Suppose $p_j \neq p_n$.

Then, the quotient loop L/K is a group of order $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{j-1}^{\alpha_{j-1}} p_j p_{j+1}^{\alpha_{j+1}} \ldots p_n^{\alpha_n}$.

By 2.2.2, there exists a subgroup $\hat{Q}/K$ of order $p_n^{\alpha_n}$ normal in L/K. So $\hat{Q}$ is a subloop of order $p_j p_n^{\alpha_n}$ normal in L.

Since $\hat{Q}$ is a group, there exists a subgroup Q of order $p_n^{\alpha_n}$ normal in $\hat{Q}$ by 2.2.2. Since Q is a Hall subloop of $\hat{Q}$, it is normal in L by 2.2.1. Now by 2.2.3, L is a group.

Case 2: Suppose $p_j = p_n$. Then, the quotient loop L/K is a group of order $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{n-1}^{\alpha_{n-1}} p_n$. By 2.2.2, there exists a subgroup Q/K of order p_n normal in L/K. So Q is a subloop of order $p_n^2 = p_n^{\alpha_n}$ and Q is normal in L. Again, L is a group by 2.2.3.

2.3 Moufang Loops of Odd Order $p^4q_1\cdots q_n$

Motivation

It has been proven in [25] that all Moufang loops of odd order $p^\alpha q_1\cdots q_n$ are associative when $p, q_1, \ldots, q_n$ are distinct odd primes with $p < q_i$ and $\alpha \leq 3$. Following that, an open question was raised there: "Are all Moufang loops of odd order $p^4q_1\cdots q_n$ associative?" For $p = 3$, the answer is no since there exist nonassociative Moufang loops of order 3^4[4]. We give an affirmative answer for $p \geq 5$.

Results

2.3.1 Lemma: Let L be a Moufang loop of odd order such that every proper subloop of L is a group. Suppose H is a Hall subloop of L such that $H \subset N$. Then L is a group.

Proof:

Since $(|H|, |L|/|H|) = 1$, by 1.11(e), there exists a Hall subloop M of order $|L|/|H|$ in L. Write $S = \langle M, H\rangle$, i.e., the loop generated by all the elements in M and H. By 1.11(b), $|S|$ is odd. Then by 1.11(b) again, $|M|$ and $|H|$ divides $|S|$. Since $(|M|,|H|) = 1$, $|M||H| = |L|$ divides $|S|$. Thus $L = S$. Then $L = \langle M, H\rangle = \langle M, N\rangle$ as $H \subset N$. Hence $L = MN$ as $N \lhd L$ by 1.6.

Thus $L_a = (L, L, L) = (MN, MN, MN)$

$= (M, M, M)$ by 2.1.1

$= M_a = \{1\}$ as M is a group.

Hence L is a group.