JOURNAL OF ALGEBRA **164**, 409–414 (1994)

Moufang Loops of Even Order

LEONG FOOK

P. P. Sains Matematik, Universiti Sains Malaysia, 11800 Penang, Malaysia

AND

TEH PANG ENG

Sekolah Menengah Sultan Badlishah, 09000 Kulim Kedah, Malaysia

Communicated by Walter Feit

Received January 9, 1992

1. INTRODUCTION

Let L be a Moufang loop of even order $n = 2m$. For what n must L be a group?

Orin Chein has proven in [3] that for $n = 2^k$ or $n = 2p$ (k is a positive integer less than 4 and p is any prime), L is a group. Mark Purtill has shown that for $n = 2p^2$, L is also a group (unpublished result). In this paper, we extend his result for $n = 2p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with $\alpha_i \leqslant 2$, $p_j \neq 1 \bmod p_i$, $p_j^2 \neq 1 \bmod p_i$ if $\alpha_j = 2$, for all i, j ($r \geqslant 2$). We show that our problem is completely solved in the Conclusion.

Liebeck has proven in [7] that a finite nonassociative simple Moufang loop is isomorphic to $M(p^n)$, a class of Moufang loops constructed by Paige in [8]. Paige has shown that the order of $M(p^n)$ is $p^{3n}(p^{4n} - 1)/d(p)$, where $d(2) = 1$ and $d(p) = 2$ for any odd prime p. It can be demonstrated that 120 is a divisor of $|M(p^n)|$. This is the important tool we use to break through our problem.

2. DEFINITIONS

1. A loop $(L, \cdot)$ is a set L with a binary operation "$\cdot$" such that

(i) if any two of x, y, z are given as elements of L, the equation $x \cdot y = z$ uniquely determines the third as an element of L;

(ii) there exists an identity $1 \in L$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in L$.

0021-8693/94 $6.00

2. Let x, y, z be elements of a loop L. Define:

(i) the associator (x, y, z) as $xy \cdot z = (x \cdot yz)(x, y, z)$.

(ii) L_a, the associater subloop of L, as the subloop generated by all the associators (x, y, z) of L.

(iii) N, the nucleus of L, as the set of all $n \in L$ such that $(n, x, y) = (x, n, y) = (x, y, n) = 1$ for all $x, y \in L$.

(iv) Z, the centre of L, as the set of all $n \in N$ such that $(n, x) = 1$ for all $x \in L$ where $nx = xn \cdot (n, x)$.

(v) $I(L)$, the inner mapping group of L, as the group of permutations of L generated by all the permutations $R(x, y)$, $L(x, y)$, and $T(x)$ of L, where $gR(x, y) = (gx \cdot y) \cdot (xy)^{-1}$, $gL(x, y) = x^{-1}y^{-1} \cdot [y(xg)]$, and $gT(x) = x^{-1}(gx)$, for all $g \in L$.

3. If K is a subloop of L, then K is normal in L if $K\theta = K$ for all $\theta \in I(L)$.

4. L is simple if it has no proper normal subloop.

5. A loop $(L, \cdot)$ is a Moufang loop if $xy \cdot zx = (x \cdot yz)x$ for all $x, y, z \in L$.

3. Results with Moufang Loops

Let L be a Moufang loop. Then:

1. The identity $xy \cdot zy = (x \cdot yz)x$ is equivalent to each of the identities

$$y(x \cdot zx) = (yx \cdot z)x$$

$$x(y \cdot xz) = (xy \cdot x)z$$

[1, Lemma 3.1, p. 115].

2. L is diassociative, i.e., $\langle x, y \rangle$ is a group for all $x, y \in L$ [1, p. 115, Lemma 3.1].

3. If $(x, y, z) = 1$, then $\langle x, y, z \rangle$ is a group for all $x, y, z \in L$ [1, p. 117, Moufang's Theorem].

4. L_a is normal in L. In fact, L_a is the smallest normal subloop of L such that L/L_a is a group [5, p. 32, Thm. 2].

5. N and Z are normal subloops of L. Clearly, N and Z are associative [1, p. 114, Thm. 2.1].

6. $R(x^{-1}, y^{-1}) = L(x, y)$ [1, p. 124, Lemma 5.4].

4. Moufang Loops of Even Order

LEMMA 1. *Let L be a Moufang loop of order $2m$, $(2, m) = 1$. Then there exists a normal subloop M of order m in L. Hence, $L = C_2 \rtimes M$,* i.e., *$L = C_2 M$, and $C_2 \cap M = 1$.*

Proof. If L is associative, then it is true by group theory. Assume L is not associative. As 120 is not a divisor of $|L|$ and L is not associative, L is not simple. Let $K \cdot \lhd L$; i.e., K is a minimal normal subloop of L. Clearly $|K| \mid 2m$.

Case 1. $|K| = 2$. Let $K = \langle w \rangle$ and $\theta \in I(L)$. Clearly, $w\theta = w$. So $K \subset Z$. By [2, p. 44, Prop. I], there exists one subloop M of L such that $|M| = m$. Hence $L = KM$. As $K \subset Z$, $T(km) = T(m)$ and $L(k_1 m_1, k_2 m_2) = L(m_1, m_2)$ for all $k, k_1, k_2 \in K$. Thus $M\theta = M$ for all $\theta \in I(L)$. Therefore $M \lhd L$ and $L = K \times M$, a direct product of K and M.

Case 2. $|K| = 2m_0$, $1 < m_0 < m$. By induction, $K = C_2 \times M_0$ with $|M_0| = m_0$. Let $w \in M_0$ and $\theta \in I(L)$. As $K \lhd L$, $w\theta \in K$. As $|w\theta| \mid |w|$ and $M_0 \lhd K$, $w\theta \in M_0$. Thus $M_0 \lhd L$. This contradicts the minimality of K.

Case 3. $|K| = m$. Let x be an element of order 2 in L. Then $L = \langle x \rangle \rtimes K = C_2 \rtimes K$.

LEMMA 2. *Let L be a Moufang loop of order $2p^2$, $(2, p) = 1$. Then L is a group.*

Proof. Suppose L is not a group. By Lemma 1, there exists a normal subloop M of order p^2 and $L = C_2 \rtimes M$. If M is a cyclic group, then L would be a group by diassociativity. So we can assume $M = C_p \times C_p = \langle y \rangle \times \langle z \rangle$. Let $C_2 = \langle x \rangle$. By [3, Lemma 1, p. 34], if $H = \langle x, g \rangle$, then $|H| \geq 2p$ for any $g \in M$. If $M \subset H$, then $|M| = p^2 \mid |H|$ and $|H| = 2p^2 = |L|$. L would be a group by diassociativity. So $M \subset H$. If $|H| > 2p$, then $|\langle H, w \rangle| > 2p^2$ for any $w \in M - H$. So $|H| = 2p$. Clearly H cannot be a cyclic group. So H is a dihedral group D_{2p} and we have $xg = g^{-1}x$ for all $g \in M$.

Now

$$
\begin{aligned}
x \cdot y(xz) &= (xy)x \cdot z && \text{by Moufang identity} \\
&= (y^{-1}x)x \cdot z && \text{by dihedralness} \\
&= (y^{-1}x^2) \cdot z && \text{by diassociativity} \\
&= y^{-1}z && \text{by } x^2 = 1.
\end{aligned}
$$

Thus

$$\begin{aligned} y(xz) &= x^{-1}(y^{-1}z) \\ y(z^{-1}x) &= (y^{-1}z)^{-1}x^{-1} && \text{by dihedralness} \\ &= (z^{-1}y)x && \text{by } x = x^{-1} \\ &= (yz^{-1})x && \text{as } M \text{ is commutative.} \end{aligned}$$

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

By [1, Moufang Theorem, p. 117], $\langle y, z^{-1}, x\rangle = L$ is a group.

Remark. This result was first obtained by Mark Purtill as mentioned in [9]. Allthough our proof is somehow different and shorter, the essential steps are the same. We record our appreciation here.

LEMMA 3. *Let L be a Moufang loop of order $2pq$; p and q are distinct primes; $p < q$ and $q \neq 1 \bmod(p)$. Then L is a group.*

Proof. By Lemma 1, there exists a normal subloop M in L such that $|M| = pq$. So $L = C_2 \rtimes M$. As $q \neq 1 \bmod(p)$, $M = C_p \times C_q = C_{pq}$. Then L can be generated by two elements. By diassociativity, L is a group.

LEMMA 4. *Let L be a Moufang loop of odd order n such that*

(i) $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_i \leqslant 2$ *and* p_i *are distinct odd primes.*

(ii) $p_i \neq 1 \bmod(p_j)$ *for all* i, j.

(iii) $p_i^2 \neq 1 \bmod(p_j)$ *if* $\alpha_i = 2$, *for all* i, j.

Then L is an Abelian group.

Proof. Let $m = \alpha_1 + \cdots + \alpha_r$. We prove by induction on m.

Step 1. $m = 1 \Rightarrow n = p_i$, $m = 2 \Rightarrow n = p_j^2$ or $p_j p_k$. These cases are obvious.

Step 2. $m = 3 \Rightarrow n = p_j^2 p_k$ or $p_j p_k p_l$. As n is odd, L is solvable [6, p. 413, Thm. 16]. Let $K \cdot \lhd L$. Then K is an elementary Abelian group [6, p. 402, Thm. 7].

(a) $n = p_j^2 p_k$. If $|K| = p_j^2$ or p_k, then $K \subset N$, the nucleus of L by [6, p. 402, Thm. 7 and p. 405, Thm. 10]. There exists a Hall subloop H such that $(|K|, |H|) = 1$ by [6, p. 409, T. 12(a)]. Then $L = NH$. So $L_a = (NH, NH, NH) = (H, H, H) = 1$ and L is a group. It is an Abelian group by using Sylow's theorem with conditions (ii) and (iii).

If $|K| = p_j$, then L/K is an Abelian group of order $p_j p_k$. Then $L/K = P_j/K \times P_j/K$ with $|P_j| = p_j^2$, $|P_k| = p_k p_j$. But $P_k = Q_k \times K$ by Step 1. Let $\theta \in I(L)$. $Q_k \lhd P_k \lhd L \Rightarrow Q_k\theta \subset P_k\theta = P_k \Rightarrow Q_k \lhd L$. Thus $L = P_j \times Q_k$ is an Abelian group.

(b) $n = p_j p_k p_l$. We may assume $|K| = p_k$. As before, using Step 1, $L/K = P_j/K \times P_l/K$, $P_j = K \times Q_j$ and $P_l = K \times Q_l$. So $L = K \times Q_j \times Q_l$ is an Abelian group. In fact L is a cyclic group C_n.

Step 3. We assume the proposition is true for all $m \leqslant k$. Now let $m = \alpha_1 + \cdots + \alpha_r = k+1$. Let $K \cdot \lhd L$. Then L/K is an Abelian group by induction. Without loss of generality, we may assume

$$|K| = p_1^{\beta_1}, \qquad 1 \leqslant \beta_1 \leqslant \alpha_1.$$

(a) Let $|K| = p_1 < \alpha_1$. Now $m = (\alpha_1 - 1) + \alpha_2 + \cdots + \alpha_r = k$. Then $L/K = P_1/K \times Q_2/K \times \cdots \times Q_r/K$ where $|P_1| = p_1^{\alpha_1}$ and $|Q_j/K| = p_j^{\alpha_j}$ or $|Q_j| = p_1 p_j^{\alpha_j}$, $2 \leqslant j \leqslant r$. Clearly $Q_j = K \times P_j$ where P_j is a subloop of order $p_j^{\alpha_j}$. As $Q_j \lhd L$, $P_j \lhd L$ for $j = 2, 3, ..., r$. Thus $L = P_1 \times P_2 \times \cdots \times P_r$ is an Abelian group.

(b) Let $|K| = p_1^{\alpha_1}$. Now $m = \alpha_2 + \cdots + \alpha_r = k - 1$. Then $L/K = Q_2/K \times \cdots \times Q_r/K$. As before, we obtain a normal subloop P_j of L for $j = 2, 3, ..., r$. Then $L = K \times P_2 \times P_3 \times \cdots \times P_r$ is an Abelian group.

THEOREM. *Let L be a Moufang loop of order $2m$ where*

(i) $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_i \leqslant 2$, *p_i are distinct odd primes*;

(ii) $p_i \neq 1 \bmod p_j$ *for all i and j. Then L is a group.*

(iii) $p_i^2 \neq 1 \bmod p_j$ *if $\alpha_i = 2$, for all i, j.*

Proof. We prove by induction on r. By Lemma 1, there exists a normal subloop M of order m. So $L = C_2 \rtimes M$. By Lemma 4, M is an Abelian group. If $m = p_1^2$, then we are through by Lemma 2. Assume that the theorem is true for m when m is a product of less than r primes, with restrictions as stated in (i), (ii), and (iii) above.

Now, let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $r \geqslant 2$. Let P_i be a Sylow p_i-subgroup of M for $i = 1, 2$. Then $P_i \lhd M$. As $M \lhd L$, we have $P_i \lhd L$. L/P_i is a group by induction. So $L_a \subset P_i$ for $i = 1, 2$. Thus $L_a \subset P_1 \cap P_2 = \{1\}$. Thus L is a group.

5. CONCLUSION

There exist nonabelian groups of orders p^3, pq ($q \neq 1 \bmod p$), and pq^2 ($q^2 \neq 1 \bmod p$) where p and q are odd primes with $p < q$. Then nonassociative Moufang loops of orders $2p^3$, $2pq$, and $2pq^2$ can be constructed by [3, p. 35, Thm. 1]. Given any odd integer $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where m is different from (i), (ii), or (iii) as stated in the Theorem, a nonassociative Moufang loop of order $2m$ can be obtained by using the direct product. So

conditions (i), (ii), and (iii) in the Theorem are necessary and sufficient conditions for all Moufang loops of order $2m$ to be groups.

Since there exist nonassociative Moufang loops of orders 2^4 and $2^2 \times 3$, our problem is completely solved.

ACKNOWLEDGMENT

We thank Professor Orin Chein for pointing out the existence of a non-associative Moufang loop of order $2 \times 3 \times 5^2$. He suggested that condition (iii) be included in the Theorem. This inclusion makes the proof perfect.

REFERENCES

1. R. H. BRUCK, "A Survey of Binary Systems," Springer-Verlag, Berlin, 1971.
2. R. H. BRUCK AND LEONG FOOK, Schur's splitting theorems for Moufang loops, *Nanta math.* **II**, No. 1 (1978), 44–54.
3. O. CHEIN, Moufang loops of small order, I, *Trans. Amer. Math. Soc.* **188**, No. 2 (1974), 31–51.
4. O. CHEIN, Moufang loops of small order, *Memoirs of the Amer. Math. Soc.* **13** (1), No. 197 (1978).
5. LEONG FOOK, The devil and the angel of loops, *Proc. Amer. Math. Soc.* **54** (1976), 32–34.
6. G. GLAUBERMAN, On loops of odd order II, *J. Algebra* **8** (1968), 393–414.
7. M. W. LIEBECK, The classification of finite simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* **102** (1987), 33–47.
8. L. J. PAIGE, A class of simple Moufang loops, *Proc. Amer. Math. Soc.* **7** (1956), 471–482.
9. M. PURTILL, On Moufang loops of order the product of three odd primes, *J. Algebra* **112** (1988), 122–128.