Publ. Math. Debrecen
55 / 3-4 (1999), 501–507

Moufang loops of order $2m$, m odd

By ORIN CHEIN (Philadelphia)

Abstract. We first show that every Moufang loop L which contains an abelian associative subloop M of index two and odd order must, in fact, be a group. We then use this to address the question "For what value of $n = 2m$, m odd, must a Moufang loop of order n be associative?"

1. Introduction

This paper is motivated by a question asked by Rajah and Jamal in [19]: If L is a Moufang loop of order $2m$ with an abelian associative subloop M of order m, must L be a group? Generalizing a result of Leong and Teh [13], which gives an affirmative answer in the case that $m = p^2$, p an odd prime, Rajah and Jamal prove that the answer is also affirmative if $m = p_1^2 \dots p_k^2$, or if $M \cong C_p \times C_{p^n}$. We will show that the answer is affirmative for any M of odd order.

Actually, the question raised above stems from other work done by Fook Leong and his students which investigated the question, "For what integers, n, must every Moufang loop of order n be associative?" The first result in this direction may be found in [6], where it is shown that every Moufang loop of prime order must be a group. In [3], the author extended this result to show that Moufang loops of order p^2, p^3, and pq, where p and q are distinct primes, must be associative. Since there are well known nonassociative Moufang loops of order 2^4 and 3^4, it would seem that no extension of the results above is possible. However, in [7], Leong showed that a Moufang loop of order p^4, with $p > 3$, must be a group.

Mathematics Subject Classification: 20N05.
Key words and phrases: Moufang loop, normal subloops, abelian group.

M. Purtill [16] extended the result to Moufang loops of orders pqr, and p^2q, (p, q and r distinct primes), although the proof of the latter result has a flaw in the case $q < p$; see [17]. Then Leong and his students produced a spate of papers, [13], [14], [8], [9], [10], culminating in [11], in which Leong and Rajah show that any Moufang loop of order $p^\alpha q_1^{\alpha_1} \dots q_n^{\alpha_n}$, with $p < q_1 < \cdots < q_n$ odd primes and with $\alpha \leq 3$, $\alpha_i \leq 2$, is a group, and that the same is true with $\alpha = 4$, provided that $p > 3$. Since there exist nonassociative Moufang loops of order 3^4 [1] and of order p^5 for $p > 3$ [20], and since the direct product of a nonassociative Moufang loop and a group is a nonassociative Moufang loop, this result goes a long way toward resolving the problem for odd n. The only remaining cases are $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} q^\beta r_1^{\gamma_1} \dots r_m^{\gamma_m}$, where $p_1 < \cdots < p_k < q < r_1 < \cdots < r_m$, $k \geq 1$, $\alpha_i \leq 4$ $(\alpha_1 \leq 3$ if $p_1 = 3)$, $3 \leq \beta \leq 4$, and $\gamma_i \leq 2$. Rajah, in his doctoral dissertation [18] showed that, for p and q any odd primes, there exists a nonassociative Moufang loop of order pq^3 if and only if $q \equiv 1 \pmod{p}$, so that there exist nonassociative Moufang loops of order n, for n of the form above, provided that $q \equiv 1 \pmod{p_i}$, for at least one i, or $p_j \equiv 1 \pmod{p_i}$, for some i, j with $i < j$ and $3 \leq \alpha_j \leq 4$.

For n even, many cases are handled by a construction of the author [3] which produces a nonassociative Moufang loop, $M(G,2)$ of order $2m$ for any nonabelian group G of order m. In particular, since the dihedral group D_r is not abelian, we get a nonassociative Moufang loop of order $4r$, for each $r \geq 3$. This leaves the case $n = 2m$, for m odd. Since there exist nonabelian groups of order p^3 and of order pq for primes $p < q$, with $q \equiv 1 \pmod{p}$, there exist nonassociative Moufang loops of orders $2p^3$ and $2pq$ for p and q as above. For $n < 64$, these account for the only nonassociative Moufang loops of order $2m$, with m odd.[1]). As a result, the only the values $n = 2m$ which still need be considered, are those for which $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, with $p_1 < \cdots < p_k$ odd primes such that no p_j is congruent to 1 modulo any p_i, and with $0 \leq \alpha_i \leq 2$, for all i.

[1] See [4] for a discussion of all nonassociative Moufang loops of order < 64. Table 16 on page 81 contains all three loops of either of the forms above, $M_{42}(G_{21},2)$, $M_{54}(B_3,2)$, and $M_{54}(G_{27},2)$, although the former is inexplicably absent from Table 28 on page 129, where it is mistakenly counted as a loop of order 40 rather than 42. Also, while I am on the subject of noting corrections to [4], I would like to thank E.G. Goodaire for observing that the loop $M_{12}(S_3,2) \times C_3$ is missing (the error can be traced to the argument on the bottom of page 91) and that $M_{48}(5,5,5,3,6,0) \cong M_{48}(5,5,5,3,3,0)$ and $M_{48}(5,5,5,6,3,6) \cong M_{48}(5,5,5,3,3,6)$.

Leong and Teh [12] showed that any Moufang loop L of order $2pq$ with $p < q$ odd primes such that $p \nmid (q-1)$ must in fact be a group. This is not surprising since a group of order pq, for p and q as above, must be cyclic and hence, if L contains a subloop of order pq, then L would be a group, since Moufang loops are diassociative. Of course, this in itself is not a proof, since Cauchy's Theorem does not always hold for Moufang loops (for example, Paige's simple Moufang loop of order 120 [15] does not contain an element of order 5), and so L might not contain an element of order p or one of order q, and thus it might not contain a subloop of order pq. In a subsequent work [13], Leong and Teh show that, in fact, a Moufang loop of order $2m$, with m odd, must contain a normal subloop of order m (and so the argument above could now be applied). This fact will be needed in order to prove Corollary 1, below.

2. The main results

Suppose that L is a Moufang loop of order $2m$, m odd, and that L contains a normal abelian subgroup M of order m.

Let u be an element of $L - M$. Then $L = \langle u, M\rangle$, and every element of L can be expressed in the form mu^α, where $m \in M$ and $0 \le \alpha \le 1$. Let T_u denote the inner mapping of L corresponding to conjugation by u. That is, for x in L, $xT_u = u^{-1}xu$. Since M is a normal subloop, T_u maps M to itself. Let θ be the restriction of T_u to M. That is, for every m in M, $m\theta = u^{-1}mu$, and $mu = u(m\theta)$. By diassociativity, $m^2\theta = u^{-1}m^2u = u^{-1}muu^{-1}mu = (m\theta)^2$. Also, since u^2 must be in M, and since M is abelian, u^2 is in the center of M. Thus, $m\theta^2 = u^{-1}(u^{-1}mu)u = u^{-2}mu^2 = m$; so θ^2 is the identity mapping and $\theta^{-1} = \theta$.

By Lemma 3.2 on page 117 of [2] , T_u is a semiautomorphism of L. That is, for x, y in L, $(xyx)T_u = (xT_u)(yT_u)(xT_u)$. In particular, for m_1, m_2 in M, $(m_1m_2m_1)\theta = (m_1\theta)(m_2\theta)(m_1\theta)$. But M is abelian, so $(m_1^2m_2)\theta = (m_1\theta)^2(m_2\theta) = (m_1^2\theta)(m_2\theta)$. Since M is of odd order and since the order of an element of a finite Moufang loop must divide the order of the loop, every element of M is of odd order and hence has a square root. (That is, if $|m| = 2k+1$, then $(m^{k+1})^2 = m$.) Thus, for any m, m' in M, $(mm')\theta = [(m'')^2m']\theta = [(m'')^2\theta](m'\theta) = (m\theta)(m'\theta)$, where m'' is the square root of m. Thus θ is an automorphism of M.

For m_1 and m_2 in M, let $x = (m_1u)m_2$, let $y = m_1(m_2u)$, and let $z = (m_1u)(m_2u)$. Then, by the Moufang identities and the fact that M is an abelian group, $xu = [(m_1u)m_2]u = m_1(um_2u) = m_1[u^2(m_2\theta)] = m_1[(m_2\theta)u^2] = [m_1(m_2\theta)]u^2$, so that

$$(m_1u)m_2 = x = [m_1(m_2\theta)]u.$$

Similarly,

$$\begin{aligned} uy &= u[m_1(m_2u)] = u[m_1(u(m_2\theta))] = (um_1u)(m_2\theta) \\ &= [u^2(m_1\theta)](m_2\theta) = u^2[(m_1\theta)(m_2\theta)]. \end{aligned}$$

so that

$$m_1(m_2u) = y = u[(m_1\theta)(m_2\theta)] = [(m_1\theta)(m_2\theta)]\theta u.$$

Finally, $zu = [(m_1u)(m_2u)]u = m_1(um_2u^2) = m_1[u(m_2u^2)]$, so that $uzu = u\{m_1[u(m_2u^2)]\} = (um_1u)(m_2u^2) = [u^2(m_1\theta)](m_2u^2) = [(m_1\theta)m_2]u^4$. Thus, $(z\theta)u^2 = u^2(z\theta) = uzu = [(m_1\theta)m_2]u^4$, so $z\theta = [(m_1\theta)m_2]u^2$, and

$$(m_1u)(m_2u) = z = [(m_1\theta)m_2]\theta u^2.$$

As in [4] , we can summarize these results as follows: For $0 \le \alpha, \beta \le 1$,

$$(m_1u^\alpha)(m_2u^\beta) = [(m_1\theta^\beta)(m_2\theta^{\alpha+\beta})]\theta^\beta \cdot u^{\alpha+\beta}.$$

But θ is an endomorphism of M, and θ^2 is the identity, so

$$\begin{aligned} (m_1u^\alpha)(m_2u^\beta) &= [(m_1\theta^\beta)(m_2\theta^{\alpha+\beta})]\theta^\beta u^{\alpha+\beta} \\ &= [(m_1\theta^{2\beta})(m_2\theta^{\alpha+2\beta})]u^{\alpha+\beta} = [m_1(m_2\theta^\alpha)]u^{\alpha+\beta}. \end{aligned}$$

But then, for any $m_1u^\alpha, m_2u^\beta, m_3u^\gamma$ in L,

$$\begin{aligned} [(m_1u^\alpha)(m_2u^\beta)](m_3u^\gamma) &= \{[m_1(m_2\theta^\alpha)]u^{\alpha+\beta}\}(m_3u^\gamma) \\ &= \{[m_1(m_2\theta^\alpha)]m_3\theta^{\alpha+\beta}\}u^{\alpha+\beta+\gamma}, \end{aligned}$$

and

$$\begin{aligned}(m_1u^\alpha)[(m_2u^\beta)(m_3u^\gamma)] &= (m_1u^\alpha)\{[m_2(m_3\theta^\beta)]u^{\beta+\gamma}\}\\ &= \{m_1[m_2(m_3\theta^\beta)]\theta^\alpha\}u^{\alpha+\beta+\gamma}\\ &= \{m_1[(m_2\theta^\alpha)(m_3\theta^{\alpha+\beta})]\}u^{\alpha+\beta+\gamma}\\ &= \{[m_1(m_2\theta^\alpha)](m_3\theta^{\alpha+\beta})\}u^{\alpha+\beta+\gamma}.\end{aligned}$$

Thus L is associative.

We have proved the following:

Theorem. *Every Moufang loop L of order $2m$, m odd, which contains a normal abelian subgroup M of order m is a group.*

We can now settle the question of for which values of $n = 2m$ must every Moufang loop of order n be a group.

Corollary 1. *Every Moufang loop of order $2m$ is associative if and only if every group of order m is abelian.*

Proof. If there exists a nonabelian group G of order m, then the loop $M_n(G,2)$ is a nonassociative Moufang loop of order $n = 2m$.

As shown above, this covers all even values of m, $m \geq 6$. (There are no nonabelian groups of order less than 6, and there are no nonassociative Moufang loops of order less than 12.)

Now consider $n = 2m$, and suppose that every group of order m is abelian. If $m < 6$, then the result follows from [5], since there are no nonassociative Moufang loops of order less than 12. On the other hand, if $m \geq 6$, then m must be odd (since the dihedral group of order $2k$ is not abelian), and so, by the result of Leong and Teh discussed above [13], any Moufang loop L of order n must contain a normal subloop M of order m. Since there exists a nonabelian group of order p^3, for any prime p, m cannot be divisible by p^3 for any prime p. But then, M must be associative, by [11]. Furthermore, since all groups of order m are abelian, M is an abelian group. But then, by the Theorem, L is a group.

3. Some questions

We might wonder whether all of the hypotheses of the Theorem are really necessary.

Clearly it is necessary that M be abelian, since the $M(G, 2)$ construction of [3] provides examples of nonassociative Moufang loops when M is not abelian.

The proof of the Theorem clearly uses the fact that m is odd, but might there be a different proof which gives us the result for m even as well? We thank E.G. Goodaire for noting that the loop $M_{32}(D_4 \times C_2, 2)$ provides a counterexample. This nonassociative Moufang loop contains an abelian normal subgroup of index two which is isomorphic to $C_2 \times C_2 \times C_2 \times C_2$.

How about the fact that M is of index two? In the proof of the Theorem, we do not really need u^2 to be an element of M. All that is needed is that u^2 commutes with every element of M and that it associates with every pair of elements of M. That is, what is needed is that u^2 is in the center of $\langle u^2, M\rangle$. We could therefore prove the following:

Corollary 2. *If a Moufang loop L contains a normal abelian subgroup M of odd order m, such that L/M is cyclic, and if $u^2 \in Z(\langle u^2, M\rangle)$, for uM some generator of L/M, then L is a group.*

Can we dispose with the assumption that $u^2 \in Z(\langle u^2, M\rangle)$? That is,

Question 1. If a Moufang loop L contains a normal abelian subgroup M of odd order m, such that L/M is cyclic, must L be a group?

Returning to the question of whether M must be of odd order, in the counterexample above, M is of order 16 and $|L/M| = 2$. This suggests the following question:

Question 2. If a Moufang loop L contains a normal abelian subgroup M such that L/M is is cyclic and such that $(|L/M|, |M|) = 1$, must L be a group?

References

[1] R. H. Bruck, Contributions to the theory of loops, *Trans. Amer. Math Soc.* **60** (1946), 245–354, (MR 8, p. 134).

[2] R. H. Bruck, A Survey of Binary Systems, Ergeb. Math. Grenzgeb., vol. 20, *Springer Verlag*, 1968, (MR 20 #76).

[3] O. Chein, Moufang loops of small order I, *Trans. Amer. Math. Soc.* **188** (1974), 31–51, (MR 48 # 8673).

[4] O. Chein, Moufang loops of small order, *Mem. Amer. Math. Soc., 197,* **13** Issue 1 (1978), 1–131, (MR 57 #6271).

[5] O. Chein and H. O. Pflugfelder, The smallest Moufang loop, *Archiv der Mathematik* **22** (1971), 573–576, (MR 45 #6966).

[6] G. Glauberman, On loops of odd order II, *J. Algebra* **8** (1968), 393–414, (MR 36 #5250).

[7] F. Leong, Moufang loops of order p^4, *Nanta Math.* **7** (1974), 33–34, (MR 51 #5826).

[8] F. Leong and A. Rajah, On Moufang loops of odd order pq^2, *J. Algebra* **176** (1995), 265–270, (MR 96i #20082).

[9] F. Leong and A. Rajah, Moufang loops of odd order $p_1^2 p_2^2 \dots p_m^2$, *J. Algebra* **181** (1996), 876–883, (MR 97i #20083).

[10] F. Leong and A. Rajah, Moufang loops of odd order $p^4 q_1 \dots q_n$, *J. Algebra* **184** (1996), 561–569, (MR 97k #20118).

[11] F. Leong and A. Rajah, Moufang loops of odd order $p^\alpha q_1^2 \dots q_n^2 r_1 \dots r_m$, *J. Algebra* **190** (1997), 474–486, (MR 98b #20115).

[12] F. Leong and P. E. Teh, Moufang loops of orders $2pq$, *Bull. of the Malaysian Math. Soc.* **15** (1992), 27–29, (MR 93j #20142).

[13] F. Leong and P. E. Teh, Moufang loops of even order, *J. Algebra* **164** (1994), 409–414, (MR 95b #20097).

[14] F. Leong, P. E. Teh and V. K. Lim, Moufang loops of odd order $p^m q_1 \dots q_n$, *J. Algebra* **168** (1994), 348–352, (MR 95g #20068).

[15] L. J. Paige, A class of simple Moufang loops, *Proc. Amer. Math. Soc.* **7** (1956), 471–482, (MR 18 (1957), p. 110).

[16] M. Purtill, On Moufang loops of order the product of three primes, *J. Algebra* **112** (1988), 122–128, (MR 89c # 20120).

[17] M. Purtill, Corrigendum, *J. Algebra* **145** (1992), 262, (MR 92j # 20066).

[18] A. Rajah, Which Moufang loops are associative?, doctoral dissertation, *University Sains Malaysia*, 1996.

[19] A. Rajah and E. Jamal, Moufang loops of order $2m$, *Publ. Math. Debrecen* **55** (1–2) (1999), 47–51.

[20] C. R. B. Wright, Nilpotency conditions for finite loops, *Illinois J. Math.* **9** (1965), 399–409, (MR 31 # 5918).

ORIN CHEIN
DEPARTMENT OF MATHEMATICS
TEMPLE UNIVERSITY
1805 NORTH BROAD STREET
PHILADELPHIA, PA 19122
USA

(Received June 12, 1998; revised September 18, 1998)