

## Possible orders of nonassociative Moufang loops

ORIN CHEIN, ANDREW RAJAH

*Abstract.* The paper surveys the known results concerning the question: “For what values of  $n$  does there exist a nonassociative Moufang loop of order  $n$ ?”

Proofs of the newest results for  $n$  odd, and a complete resolution of the case  $n$  even are also presented.

*Keywords:* Moufang loop, order, nonassociative

*Classification:* Primary 20N05

### 1. Introduction and preliminaries

The question above and the equivalent question, “For what integers,  $n$ , must every Moufang loop of order  $n$  be associative?” have long been of interest.

Since Artin observed that the loop of units of any alternative ring is a Moufang loop ([22]), examples of finite nonassociative Moufang loops were known right from the start. For example, the non-zero Cayley numbers form a Moufang loop under multiplication, and the subloop consisting of

$$\{\pm 1, \pm i, \pm j, \pm k, \pm e, \pm ie, \pm je, \pm ke\}$$

is a nonassociative Moufang loop of order  $2^4 = 16$ .

The simplest result on nonexistence may be found in [7], where it is shown that every Moufang loop of prime order must be a group. In [4], the first author extended this result to show that Moufang loops of order  $p^2, p^3, p$  prime, must be associative. Since there are nonassociative Moufang loops of order  $2^4$  [see above] and  $3^4$  ([1] or [2]), it would seem that no extension of the results above is possible. However, in [8], Leong showed that a Moufang loop of order  $p^4$ , with  $p > 3$ , must be a group. This is the best one can do, because Wright showed in [21] that there exists a nonassociative Moufang loop of order  $p^5$ , for any prime  $p$ .

If one allows more than one prime, the first author showed that Moufang loops of order  $pq$ , where  $p$  and  $q$  are distinct primes, must be associative ([4]). M. Purtil [16] extended the result to Moufang loops of orders  $pqr$ , and  $p^2q$ , ( $p, q$  and  $r$  distinct odd 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, [14], [15], [9], [10], [11], culminating in [12], in which Leong and the second author showed the following:

---

Research of the first author was supported in part by a summer research award and a grant-in-aid of research from Temple University.

**1.1.** Any Moufang loop of order  $p^\alpha q_1^{\alpha_1} \dots q_n^{\alpha_n}$ , with  $p < q_1 < \dots < q_n$  odd primes and with  $\alpha \leq 3$ ,  $\alpha_i \leq 2$ , is a group, and the same is true with  $\alpha = 4$ , provided that  $p > 3$ .

Finally, the second author, in his doctoral dissertation [18], showed the following:

**1.2.** For  $p$  and  $q$  any odd primes, there exists a nonassociative Moufang loop of order  $pq^3$  if and only if  $q \equiv 1 \pmod{p}$ .

Since there exist nonassociative Moufang loops of order  $3^4$  and of order  $p^5$  for any prime  $p$ , and since the direct product of a nonassociative Moufang loop and a group is a nonassociative Moufang loop, the only remaining unresolved cases for  $n$  odd are the following:

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} q^\beta r_1^{\gamma_1} \dots r_s^{\gamma_s},$$

where

$$\begin{aligned} p_1 < \dots < p_k < q < r_1 < \dots < r_s \text{ are distinct odd primes;} & k \geq 1; \\ \alpha_i \leq 4 \ (\alpha_1 \leq 3 \text{ if } p_1 = 3); & 3 \leq \beta \leq 4; & \gamma_i \leq 2; \\ q \not\equiv 1 \pmod{p_i} \text{ for all } i = 1, \dots, k; \text{ and} & \\ p_j \not\equiv 1 \pmod{p_i} \text{ for all } i < j \text{ with } 3 \leq \alpha_j \leq 4. & \end{aligned}$$

For  $n$  odd, we also have the following results which will be needed below:

**1.3** ([7]). If  $L$  is a Moufang loop of odd order and if  $K$  is a subloop of  $L$ , and  $\pi$  is a set of primes which divide  $|L|$ , then

- (a)  $|K|$  divides  $|L|$ .
- (b) If  $K$  is a minimal normal subloop of  $L$ , then it is an elementary abelian group.
- (c)  $L$  contains a Hall  $\pi$ -subloop.

**1.4** ([12]). If  $L$  is a nonassociative Moufang loop of odd order and if all of the proper quotient loops of  $L$  are groups, then  $L_a$ , the subloop of  $L$  generated by all associators, is a minimal normal subloop of  $L$ .

**1.5** ([9]). If  $L$  is a Moufang loop of odd order and if every proper subloop of  $L$  is a group and if there exists a minimal normal Sylow subloop in  $L$ , then  $L$  is a group.

**1.6** ([11]). Let  $L$  be a Moufang loop of odd order such that every proper subloop of  $L$  is associative. Suppose that  $K$  is a minimal normal subloop which contains  $L_a$ , and that  $Q$  is a Hall subloop of  $L$  such that  $(|K|, |Q|) = 1$  and  $Q \triangleleft KQ$ . Then  $L$  is a group.

For  $n$  even, many cases are handled by a construction of the first author ([4]) which produces a nonassociative Moufang loop,  $M(G, 2)$  of order  $2m$  for any nonabelian group  $G$  of order  $m$ . Thus, if there exists a nonabelian group of order  $m$ , then there exists a nonassociative Moufang loop of order  $n = 2m$ . 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 and for which every group of order  $m$  is abelian.

The following result ([14]) will also be needed below:

**1.7.** Any Moufang loop  $L$  of order  $2m$ , with  $m$  odd must contain a (normal) subloop of order  $m$ .

Finally, we can characterize those odd  $m$  for which every group of order  $m$  is abelian. (We would like to thank Anthony Hughes for suggesting this lemma and for his helpful advice regarding its proof.)

**Lemma 1.8.** *If  $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ , with  $p_1 < \dots < p_k$  odd primes and  $\alpha_i > 0$ , for all  $i$ , then every group of order  $m$  is abelian if and only if the following conditions hold:*

- (i)  $\alpha_i \leq 2$ , for all  $i = 1, \dots, k$ ,
- (ii)  $p_j^{\alpha_j} \not\equiv 1 \pmod{p_i}$ , for any  $i$  and  $j$ .

PROOF: Note that, since the direct product of a nonabelian group with any group is a nonabelian group, if there exists a nonabelian group of order  $s$  and if  $s \mid m$ , then there exists a nonabelian group of order  $m$ . Since there exists a nonabelian group of order  $p^3$  for any prime  $p$ , (i) is necessary. Similarly, since  $|Aut(C_q)| = q - 1$ , and  $|Aut(C_q \times C_q)| = (q^2 - 1)(q^2 - q)$ , there exists a nonabelian group of order  $pq$  if  $q \equiv 1 \pmod{p}$  and one of order  $pq^2$  if  $q^2 \equiv 1 \pmod{p}$ . Thus (ii) is necessary.

To see that these conditions are sufficient, suppose that  $G$  is a group of order  $m$ , with  $m$  as above. For each  $j = 1, \dots, k$ , let  $P_j$  be a  $p_j$ -Sylow subgroup of  $G$ .

By condition (ii),  $(m, p_j^{\alpha_j} - 1) = 1$ .

Claim:  $N_G(P_j) = C_G(P_j)$ .

Suppose not. For  $g \in N_G(P_j) - C_G(P_j)$ , conjugation by  $g$  induces a non-trivial automorphism  $\theta$  of  $P_j$ . Since  $P_j$  is an abelian group,  $\theta^s$  is the identity mapping on  $P_j$ , whenever  $g^s \in P_j$ . In particular, since  $|g| \mid m$ ,  $\theta^m$  is the identity map. Hence,  $|\theta| \mid m$ . On the other hand,  $|\theta| \mid |Aut(P_j)|$ , so  $|\theta| \mid (m, |Aut(P_j)|)$ . If  $\alpha_j = 1$ ,  $|Aut(P_j)| = p_j - 1$ . But  $(m, p_j - 1) = 1$ , so  $|\theta| = 1$ , contrary to assumption. Therefore,  $\alpha_j = 2$ . If  $P_j$  is cyclic,  $|Aut(P_j)| = p_j(p_j - 1)$ ; and if  $P_j$  is elementary abelian,  $|Aut(P_j)| = p_j(p_j^2 - 1)(p_j - 1)$ . In either case, since  $(m, p_j^{\alpha_j} - 1) = 1$  and  $(p_j - 1) \mid (p_j^2 - 1)$ , we also have  $(m, (p_j^{\alpha_j} - 1)(p_j - 1)) = 1$ . Therefore  $(m, |Aut(P_j)|) = p_j$  and  $|\theta| = p_j$ . Hence  $g^{p_j} \in C_G(P_j)$ . Thus,  $\frac{N_G(P_j)}{C_G(P_j)}$  is a  $p_j$ -group contained in  $\frac{N_G(P_j)}{P_j}$ . (Recall that  $P_j$  is abelian, since  $\alpha_j = 2$ .) But then  $p_j \mid \left| \frac{N_G(P_j)}{P_j} \right|$ , and so  $p_j^3 \mid |N_G(P_j)|$ , contradicting the assumption that  $p_j^3 \nmid |G|$ . This establishes the claim.

Since  $N_G(P_j) = C_G(P_j)$  for all  $j$ , by Burnside's Theorem ([20, p.137]), each  $P_j$  has a normal  $p_j$ -complement, which we denote by  $N_j$ .

$\left| \frac{G}{N_j} \right| = |P_j| = p_j^{\alpha_j}$ , where  $\alpha_j \leq 2$ , so  $\frac{G}{N_j}$  is abelian. Let  $\varphi : G \rightarrow \frac{G}{N_1} \times \frac{G}{N_2} \times \dots \times \frac{G}{N_k}$  be defined by  $g\varphi = (gN_1, gN_2, \dots, gN_k)$ . Clearly  $\varphi$  is a homomorphism, and  $\ker(\varphi) = \{g \mid gN_j = N_j, \text{ for all } j\} = N_1 \cap N_2 \cap \dots \cap N_k$ .

Therefore,  $\frac{G}{N_1 \cap N_2 \cap \dots \cap N_k} \cong G\varphi \subseteq \frac{G}{N_1} \times \frac{G}{N_2} \times \dots \times \frac{G}{N_k}$ . But, for each  $j$ ,  $N_1 \cap N_2 \cap \dots \cap N_k \subseteq N_j \subseteq G$ , so  $|N_1 \cap N_2 \cap \dots \cap N_k| \mid |G| = m$ , and yet, for each  $j$ ,  $|N_1 \cap N_2 \cap \dots \cap N_k| \mid |N_j|$ , which is  $p_j$ -free. This implies that  $|N_1 \cap N_2 \cap \dots \cap N_k| = 1$ . Thus  $G \cong G\varphi \subseteq \frac{G}{N_1} \times \frac{G}{N_2} \times \dots \times \frac{G}{N_k}$ , which is abelian, as required.  $\square$

### 2. New results

We divide this section into two parts:  $n$  odd, and  $n = 2m$ ,  $m$  odd.

**$n$  odd.**

**Theorem 2.1.** *If  $L$  is a Moufang loop of order  $p_1 p_2 \dots p_k q^3$ , with  $p_1, p_2, \dots, p_k$  and  $q$  distinct odd primes, and if  $q \not\equiv 1 \pmod{p_1}$  and, for each  $i > 1$ ,  $q^2 \not\equiv 1 \pmod{p_i}$ , then  $L$  is a group.*

PROOF: Suppose not. Let  $k$  be the smallest positive integer for which there exists a nonassociative Moufang loop of order  $p_1 p_2 \dots p_k q^3$ , with  $p_1, p_2, \dots, p_k$  and  $q$  distinct odd primes, and with  $q \not\equiv 1 \pmod{p_1}$  and  $q^2 \not\equiv 1 \pmod{p_i}$  for each  $i > 1$ ; and let  $L$  be such a loop. By 1.2,  $k \geq 2$ .

Let  $H$  be a proper subloop of  $L$ . By 1.3 (a),  $|H| = p_{j_1} p_{j_2} \dots p_{j_s} q^\beta$ , where either  $\beta < 3$ , or  $s < k$ . If  $\beta < 3$ , then  $H$  is a group by 1.1; and if  $s < k$ , then  $H$  is a group by the minimality of  $k$ . Thus, every proper subloop of  $L$  is a group. The same applies to any proper quotient loop of  $L$ . Therefore, by 1.4 and 1.3 (b),  $L_a$  is a minimal normal subloop of  $L$  and is an elementary abelian group. By 1.5, if  $L$  is not a group, then  $L_a$  cannot be a Sylow subloop of  $L$ , and so  $|L_a| \neq q^3$ , and  $|L_a| \neq p_i$ , for any  $i$ . But, by 1.3 (a),  $|L_a|$  must divide  $|L|$ , so, since  $L_a$  is an elementary abelian group,  $|L_a| = q$  or  $q^2$ . Therefore, by 1.3 (c),  $L$  contains a subgroup  $X_j$  of order  $p_j$ . Let  $n_k$  denote the number of  $p_k$ -Sylow subgroups of  $L_a X_k$ . By the Sylow theorems,  $n_k \equiv 1 \pmod{p_k}$ , so  $(n_k, p_k) = 1$ . Also  $n_k$  divides  $|L_a X_k|$ . But, since  $L_a \triangleleft L$ ,  $|L_a X_k| = p_k q$  or  $p_k q^2$ , so, in either case,  $n_k \mid q^2$ . If  $n_k \neq 1$ , then  $n_k = q$  or  $q^2$  and so, in either case,  $q^2 \equiv 1 \pmod{p_k}$ , contrary to assumption. Therefore,  $n_k = 1$ , and so  $X_k \triangleleft L_a X_k$ . But  $X_k$  is a Hall subloop of  $L$ , and  $(|L_a|, |X_k|) = 1$ . Therefore, by 1.6,  $L$  is a group, contrary to assumption. The theorem now follows.  $\square$

This leaves us with the question: What happens if  $q^2 \equiv 1 \pmod{p_i}$  for some  $i$ ? If  $q \equiv 1 \pmod{p_i}$ , then, by 1.2, there exists a nonassociative Moufang loop of order  $p_i q^3$ . Thus, we may assume that, for all  $i$ ,  $q \not\equiv 1 \pmod{p_i}$ , but that

$q \equiv -1 \pmod{p_i}$ , for some  $i$ . If there is only one such  $i$ , then, by reordering if necessary, we can assume that it is  $p_1$ , and we have a group, by Theorem 2.1. Therefore, we are left with the case  $k \geq 2$ ,  $q \equiv -1 \pmod{p_1}$ , and  $q \equiv -1 \pmod{p_k}$  (with no assumption about the relationship between  $q$  and  $p_i$  for  $1 < i < k$ , other than  $q \not\equiv 1 \pmod{p_i}$ ). The smallest such open case is  $n = 3 \cdot 5 \cdot 29^3$ .

$n = 2m$ ,  $m$  **odd**.

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  $mu^\alpha$ , where  $m \in M$  and  $0 \leq \alpha \leq 1$ . 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  $\theta$  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  $\theta^2$  is the identity mapping and  $\theta^{-1} = \theta$ .

By Lemma 3.2 on page 117 of [3],  $T_u$  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  $\theta$  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 [5], we can summarize these results as follows: For  $0 \leq \alpha, \beta \leq 1$ ,

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

But  $\theta$  is an endomorphism of  $M$ , and  $\theta^2$  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 2.2.** *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 2.3.** *Every Moufang loop of order  $2m$  is associative if and only if every group of order  $m$  is abelian.*

PROOF: We may assume that  $m \geq 6$ , since there are no nonabelian groups of order less than 6, and no nonassociative Moufang loops of order less than 12 ([6]).

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 takes care of all even values of  $m$ , since the dihedral group of order  $m$  is not abelian.

Now consider  $n = 2m$ ,  $m$  odd, and suppose that every group of order  $m$  is abelian. By 1.7, 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 1.1. Furthermore, since all groups of order  $m$  are abelian,  $M$  is an abelian group. But then, by the theorem,  $L$  is a group.  $\square$

Applying Lemma 1.8, we obtain the following:

**Corollary 2.4.** *Every Moufang loop of order  $2m$  is associative if and only if*

$m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ , where  $p_1 < \dots < p_k$  are odd primes and where

- (i)  $\alpha_i \leq 2$ , for all  $i = 1, \dots, k$ ,
- (ii)  $p_j \not\equiv 1 \pmod{p_i}$ , for any  $i$  and  $j$ ,
- (iii)  $p_j^2 \not\equiv 1 \pmod{p_i}$ , for any  $i$  and any  $j$  with  $\alpha_j = 2$ .

### 3. Some questions

We might wonder whether all of the hypotheses of Theorem 2.2 are really necessary.

Clearly it is necessary that  $M$  be abelian, since the  $M(G, 2)$  construction of [4] 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 3.1.** *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, 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?

The answer in general is no. When  $q \equiv 1 \pmod{3}$ , there exists a nonassociative Moufang loop  $L$  of order  $3q^3$ , constructed in [18], which contains a normal abelian subgroup  $M$  of order  $q^3$ , with  $L/M \cong C_3$ . (Note also that, in this example,  $(|M|, |L/M|) = 1$ , so that even this additional condition would not suffice to guarantee that  $L$  is a group.) However, if  $p > 3$ , the subgroup of order  $q^3$  in the nonassociative Moufang loop of order  $pq^3$ ,  $q \equiv 1 \pmod{p}$ , is not abelian, so the question is still open for  $|L/M| > 3$ .

### REFERENCES

- [1] Bol G., *Gewebe und Gruppen*, Math. Ann. **114** (1937), 414–431.
- [2] Bruck R.H., *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354. (MR 8, p. 134).
- [3] Bruck R.H., *A Survey of Binary Systems*, Ergeb. Math. Grenzgeb., vol. 20, Springer Verlag, 1968. (MR 20 # 76).

- [4] Chein O., *Moufang loops of small order. I*, Trans. Amer. Math. Soc. **188** (1974), 31–51. (MR 48 # 8673).
- [5] Chein O., *Moufang loops of small order*, Mem. Amer. Math. Soc. **197**, Vol 13, Issue 1 (1978), 1–131. (MR 57 # 6271).
- [6] Chein O., Pflugfelder H.O., *The smallest Moufang loop*, Archiv der Mathematik **22** (1971), 573–576. (MR 45 # 6966).
- [7] Glauberman G., *On loops of odd order II*, J. Algebra **8** (1968), 393–414. (MR 36 # 5250).
- [8] Leong F., *Moufang loops of order  $p^4$* , Nanta Math. **7** (1974), 33–34. (MR 51 # 5826).
- [9] Leong F., Rajah A., *On Moufang loops of odd order  $pq^2$* , J. Algebra **176** (1995), 265–270. (MR 96i # 20082).
- [10] Leong F., Rajah A., *Moufang loops of odd order  $p_1^2 p_2^2 \dots p_m^2$* , J. Algebra **181** (1996), 876–883 (MR 97i # 20083).
- [11] Leong F., Rajah A., *Moufang loops of odd order  $p^4 q_1 \dots q_n$* , J. Algebra **184** (1996), 561–569. (MR 97k # 20118).
- [12] Leong F., Rajah A., *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).
- [13] Leong F., Teh P.E., *Moufang loops of orders  $2pq$* , Bull. of the Malaysian Math. Soc. **15** (1992), 27–29. (MR 93j # 20142).
- [14] Leong F., Teh P.E., *Moufang loops of even order*, J. Algebra **164** (1994), 409–414. (MR 95b # 20097).
- [15] Leong F., Teh P.E., Lim V.K., *Moufang loops of odd order  $p^m q_1 \dots q_n$* , J. Algebra **168** (1994), 348–352. (MR 95g # 20068).
- [16] Purtill M., *On Moufang loops of order the product of three primes*, J. Algebra **112** (1988), 122–128. (MR 89c # 20120).
- [17] Purtill M., *Corrigendum*, J. Algebra **145** (1992), p. 262. (MR 92j # 20066).
- [18] Rajah A., *Which Moufang loops are associative*, Doctoral Dissertation, University Sains Malaysia, 1996.
- [19] Rajah A., Jamal E., *Moufang loops of order  $2m$* , Publ. Math. Debrecen **55** (1999), 47–51.
- [20] Scott W.R., *Group Theory*, Prentice Hall, Englewood Cliffs, NJ, 1964.
- [21] Wright C.R.B., *Nilpotency conditions for finite loops*, Illinois J. Math. **9** (1965), 399–409. (MR 31 # 5918).
- [22] Zorn M., *The theory of alternative rings*, Hamb. Abhandl. **8** (1930), 123–147.

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

SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY SAINS MALAYSIA, 11800 USM PENANG,  
MALAYSIA

(Received October 18, 1999)