TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 188, Issue 2, 1974

MOUFANG LOOPS OF SMALL ORDER. I

BY

ORIN CHEIN

ABSTRACT. The main result of this paper is the determination of all nonassociative Moufang loops of orders ≤ 31. Combinatorial type methods are used to consider a number of cases which lead to the discovery of 13 loops of the type in question and prove that there can be no others. All of the loops found are isomorphic to all of their loop isotopes, are solvable, and satisfy both Lagrange's theorem and Sylow's main theorem.

In addition to finding the loops referred to above, we prove that Moufang loops of orders p, p^2, p^3 or pq (for p and q prime) must be groups.

Finally, a method is found for constructing nonassociative Moufang loops as extensions of nonabelian groups by the cyclic group of order 2.

I. **Introduction.** In studying algebraic objects, it is frequently useful to have many examples at one's fingertips. In the case of Moufang loops that are not groups, the scarcity of manageable examples is one of the difficulties that we have encountered. It is the purpose of this paper to begin to remedy this situation by finding all Moufang loops of order ≤ 31.(1) There are 13 such loops—one of order 12, five of order 16, one of order 20, five of order 24, and one of order 28. The order structures, nuclei and subloops of these loops are given (Tables 3, 4 and 5). All of the loops are G-loops (i.e. they are isomorphic to all of their loop isotopes) and they are solvable. Lagrange's theorem and Sylow's main theorem hold in all of them. In terms of the M_k-laws of Pflugfelder [10], some of the loops are M_3-loops, some are M_7-loops, and some are strictly Moufang.

In the course of studying these loops, we find a general method of constructing nonassociative Moufang loops as extensions of groups (see Theorem 1). We also prove that, for p and q being primes, Moufang loops of order pq or of order p^n for $n \leq 3$ are groups.

Presented to the Society, July 15, 1971; received by the editors November 15, 1971.

AMS (MOS) subject classifications (1970). Primary 20N05.

Key words and phrases. Moufang loop, diassociative, subloop, order, Lagrange's theorem, Sylow's theorem, center, nucleus.

(1) In order to know the Moufang loops of order n, one must know the groups of order $\leq n/2$. Since the groups of order ≤ 15 are well known, whereas the groups of order 16 and larger start getting messy, 31 was chosen as our stopping point. However, we hope to extend our work in a future paper.

We would like to thank the referee for his suggestions which led to the shortening of the proofs of Propositions 1 and 5 and of the discussion of case 3 appearing on pp. 46–47.

II. Background and notation. A Moufang loop is a loop L in which the identity

$$(ab)(ca) = [a(bc)]a \tag{1}$$

holds for all $a, b, c \in L$.

In order to study Moufang loops of order ≤ 31, we must know all groups of order ≤ 15. These groups are discussed in many books on group theory (see, for example, [1, Chapter 5, §3]), and some familarity with them will be assumed here. However, for future reference, we have included in Table 1 a list of the noncyclic groups of order ≤ 15, together with the possible orders of elements in a minimal set of generators. (Note that, slightly contrary to proper usage, we call a set of generators minimal if there is no set of generators which contains fewer elements, rather than calling it minimal if no proper subset is a set of generators.)

Table 1

Noncyclic groups and orders of their generators

Group	Order	Minimal # of generators	Order of generators in minimal sets
$C_2 \times C_2$	4	2	2 and 2
$S_3 = D_3$	6	2	2 and 3, or 2 and 2
$C_4 \times C_2$	8	2	2 and 4, or 4 and 4
$C_2 \times C_2 \times C_2$	8	3	2, 2 and 2
Q	8	2	4 and 4
D_4	8	2	2 and 4, or 2 and 2
$C_3 \times C_3$	9	2	3 and 3
D_5	10	2	2 and 5, or 2 and 2
$C_6 \times C_2$	12	2	2 and 6, or 6 and 6
A_4	12	2	2 and 3, or 3 and 3
D_6	12	2	2 and 6, or 2 and 2
G_{12}	12	2	3 and 4, 4 and 4, or 6 and 4
D_7	14	2	2 and 7, or 2 and 2

Notation. C_n is the cyclic group of order n.

D_n is the dihedral group of order $2n$.

S_n is the symmetric group on n symbols.

Q is the group of units in the quaternions.

A_n is the alternating group on n symbols.

G_{12} is the remaining nonabelian group of order 12. (It may be thought of as the group of (2×2) matrices generated by $\left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon^2 \end{smallmatrix}\right)$ where $i = \sqrt{-1}$ and $\epsilon^2 + \epsilon + 1 = 0$. Its multiplication table may be found in [1, Table 5.4, p. 155].)

In addition to this knowledge of groups, we make use of the following facts about Moufang loops:

(i) The identity (1) is equivalent to each of the identities

$$a[b(cb)] = [(ab)c]b \tag{2}$$

and

$$a[b(ac)] = [(ab)a]c \tag{3}$$

[2, Lemma 3.1, p. 115].

(ii) Moufang loops are diassociative—i.e., any two elements generate a subgroup [9, p. 421]. (Thus, in searching for nonassociative Moufang loops, one or two generator loops need not be considered.) Note that diassociativity implies the following inverse properties: If $ab = 1$ then $ba = 1$; b is denoted by a^{-1} and, for any c in L, $(ca)a^{-1} = c$, $a^{-1}(ac) = c$, and $(ac)^{-1} = c^{-1}a^{-1}$.

(iii) *Moufang's theorem.* If three elements of a Moufang loop associate in some order, then they generate a subgroup [2, p. 117].

(iv) The order of any element in a Moufang loop divides the order of the loop [2, Theorem 1.2, p. 92].

If $(L, \cdot)$ is a finite loop, the order of L will be denoted by $|L|$; and if $x \in L$, then the order of x will be denoted by $|x|$.

If $x_1, x_2, \cdots, x_k \in L$, then the subloop of L generated by $x_1, \cdots, x_k$ will be denoted by $\langle x_1, \cdots, x_k \rangle$.

If H is a subloop of L, and $x \in L$, then $\langle H, x \rangle$ will denote the smallest subloop of L which contains both H and x.

Finally, if L is a Moufang loop, we will denote its nucleus by N. (The nucleus of a Moufang loop L is the set of all elements which associate with every pair of elements of L—i.e. $a \in N$ if and only if, for every $b, c \in L$, $(ab)c = a(bc)$; $(ba)c = b(ac)$ and $b(ca) = (bc)a$.) The nucleus of a Moufang loop is a subgroup.

III. Preliminary results.

Lemma 1. *If H is a subloop of a finite Moufang loop L, and if $x \in L$ is not in H, let d be the smallest divisor > 1 of $|x|$ such that $|x|/d$ divides $|H|$. (Clearly $|x|/|x|$ divides $|H|$, so, for any x and any H, d exists.) Then $|\langle H, x\rangle| \geq d|H|$.*

Proof. Consider all elements of the form hx^i, where $h \in H$, $0 \leq i < d$. If $h_1x^i = h_2x^j$, for some $i \leq j$, then, by diassociativity, $h_1 = (h_2x^j)x^{-i} = h_2(x^{j-i})$, so $x^{j-i} = h_2^{-1}h_1 \in H$. Let $r = j - i$. Then $0 \leq r < d$, and $x^r \in H$. If the greatest common divisor $(r, |x|) = t$, then there exist integers u, v such that $ru + v|x| = t$. Thus $x^t = x^{ru+v|x|} = (x^r)^u(x^{|x|})^v = (x^r)^u \in H$. Thus $|x^t|$ divides $|H|$. However, since t divides $|x|$, $|x^t| = |x|/t$. Thus t is a divisor of $|x|$ such that $|x|/t$ divides $|H|$. But, if $r \neq 0$, then $t \leq r < d$, so that, by the way d was chosen, $t = 1$ or $r = 0$. If $t = 1$, then $x \in H$ contrary to assumption. Thus $r = 0$, so $i = j$ and $h_1 = h_2$. Thus the elements hx^i, $h \in H$, $0 \leq i < d$, are distinct, and there are $d|H|$ of them, so the lemma is proven.

Corollary 1. *If $|\langle H, x\rangle| = d|H|$, then every element of $\langle H, x\rangle$ may be uniquely expressed in the form hx^i, where $h \in H$ and $0 \leq i < d$.*

Proof. Since the elements hx^i are distinct and since there are exactly $d|H| = |\langle H, x\rangle|$ of them, they are all the elements in $\langle H, x\rangle$.

Corollary 2. *If H and x are as above and $|x|$ is prime, then $|\langle H, x\rangle| \geq |x||H|$.*

Corollary 3. *If a nonassociative Moufang loop L of order ≤ 31 contains an element z of order > 3, and if $x, y \in L$, $y \notin \langle z\rangle$ and $x \notin \langle y, z\rangle$, then $L = \langle x, y, z\rangle$. (By diassociativity, since L is not a group, such x and y exist.)*

Proof. By Lemma 1,

$$|\langle x, y, z\rangle| \geq 2|y,z| \geq 4|z| \geq 16.$$

If $L \neq \langle x, y, z\rangle$, then there exists $w \in L$, $w \notin \langle x, y, z\rangle$. But then $|L| \geq |\langle w, x, y, z\rangle| \geq 2 \cdot |\langle x, y, z\rangle| \geq 32$—contradiction.

Proposition 1. *If p is a prime, then a Moufang loop L of order p^3 is a group.*

Proof. By [7, Theorem 4, p. 397] L is centrally nilpotent. Let Z be the center of L. Then $|L/Z| \mid p^2$. Thus $L/Z = \langle xZ, yZ\rangle$ for some $x, y \in L$. Therefore, $L = \langle x, y, Z\rangle = \langle x, y\rangle Z$. Every element of L may therefore be expressed in the form gz, where $g \in \langle x, y\rangle$ and $z \in Z$. Clearly, $(g_1z_1, g_2z_2, g_3z_3) = (g_1, g_2, g_3)$. Hence, by diassociativity, L is a group.

Corollary 4. *If p is prime, every Moufang loop L of order p or p^2 is a group.*

Proof. *If* $|L| = p$ then $|L \times C_{p^2}| = p^3$; if $|L| = p^2$ then $|L \times C_p| = p^3$. In either case, L is isomorphic to a subloop of the direct product which, by Proposition 1, is a group. Hence L is a group.

Proposition 2. *A Moufang loop of exponent 2 is a group.*

Proof. If $x, y \in L$, then $(xy)^2 = 1$ so $yx = x^{-1}y^{-1} = xy$. Thus L is commutative. Hence, for each x in L, x^3 is in the nucleus N of L [2, Theorem 5.5, p. 130]. However, $x^2 = 1$ is in N, and N is a group, so $x \in N$. Hence $N = L$ and L is a group.

Proposition 3. *If p and q are distinct primes, $p < q$, then every Moufang loop L of order pq is a group.*

Proof. If there exists $y \in L$ such that $|y| = q$, then choose $x \in L$ such that $x \notin \langle y \rangle$. Since $|x|$ divides $|L|$, $|x| = p$, q or pq. In any case, by Lemma 1, $|\langle x, y \rangle| \geq p\,|\langle y \rangle| = pq = |L|$. Thus $L = \langle x, y \rangle$ and hence is a group.

There are now two cases to consider.

(i) If pq is odd, then Glauberman [7, Corollary to Theorem 13, p. 411] proved that L has an element of order q, and hence the result follows.

(ii) If pq is even, then $p = 2$. Since the existence of an element of order q finishes the proof, we may assume that each element of L is of order 2. But then the result follows from Proposition 2.

IV. **Main results.** We proceed to find all Moufang loops L of order ≤ 31 by use of messy case analyses dealing with the orders of the elements in minimal sets of generators of L.

We begin with the case in which every minimal set of generators of L contains an element of order 2. We obtain

Theorem 1. *If L is a nonassociative Moufang loop for which every minimal set of generators contains an element of order 2, then there exists a nonabelian group G, and an element x of order 2 in L, such that each element of L may be uniquely expressed in the form gx^{α}, where $g \in G$, $\alpha = 0, 1$, and the product of two elements of L is given by*

$$(g_1x^{\delta})(g_2x^{\epsilon}) = (g_1^{\nu}g_2^{\mu})^{\nu}x^{\delta+\epsilon} \tag{4}$$

where $\nu = (-1)^{\epsilon}$ and $\mu = (-1)^{\epsilon+\delta}$.

Conversely, given any nonabelian group G, the loop L constructed as indicated above is a nonassociative Moufang loop.

Proof. Let $\{x, u_1, \cdots, u_n\}$ be a minimal set of generators for L containing the fewest possible elements of order 2. (By the hypothesis of the theorem, we may assume that x is of order 2.) Let $G = \langle u_1, \cdots, u_n \rangle$. If $g \in G$ then $\{gx, u_1, \cdots, u_n\}$ generate L, so that, by the way $x, u_1, \cdots, u_n$ were chosen, gx must be of order 2. Hence, $(gx)^2 = gxgx = 1$, so $gx = x^{-1}g^{-1} = xg^{-1}$. Also, by diassociativity and (1),

$$g_1(x^\epsilon g_2) = (g_2 g_2^{-1} g_1)(x^\epsilon g_2) = g_2[(g_2^{-1} g_1)x^\epsilon] g_2.$$

If $\epsilon = 0$, this is just $g_1 g_2$. If $\epsilon = 1$, then $\{g_2[(g_2^{-1}g_1)x], u_1, u_2, \cdots, u_n\}$ is a set of generators for L, so that, by the assumption made above, $(g_2[(g_2^{-1}g_1)x])^2 = 1$. Similarly, $\{(g_2^{-1}g_1)x, u_1, \cdots, u_n\}$ is a set of generators, so $[(g_2^{-1}g_1)x]^2 = 1$. Hence,

$$g_1(xg_2) = g_2[(g_2^{-1}g_1)x]g_2 = x^{-1}(g_2^{-1}g_1)^{-1} = (g_2^{-1}g_1)x = (g_1^{-1}g_2)^{-1}x.$$

Thus, if we let $\nu = (-1)^\epsilon$, we see that, regardless of the value of ϵ, $g_1(x^\epsilon g_2) = (g_1^\nu g_2)^\nu x^\epsilon$. Thus, using diassociativity and (2), we see that

$$(g_1 x^\delta)(g_2 x^\epsilon) = \{[(g_1 x^\delta)(g_2 x^\epsilon)]x^\delta\}x^{-\delta} = \{g_1[x^\delta g_2 x^{\epsilon+\delta}]\}x^{-\delta} = \{g_1(x^\epsilon g_2^\mu)\}x^{-\delta},$$

where

$$\mu = \left\{\begin{matrix} 1 \text{ if } \epsilon + \delta \equiv 0 \pmod 2 \\ -1 \quad \text{otherwise} \end{matrix}\right\} = (-1)^{\epsilon+\delta}.$$

Hence, by our previous argument,

$$(g_1 x^\delta)(g_2 x^\epsilon) = \{(g_1^\nu g_2^\mu)^\nu x^\epsilon\}x^{-\delta} = (g_1^\nu g_2^\mu)^\nu x^{\epsilon+\delta}.$$

Thus the product of two elements of the form gx^α is again of that form. Hence, the elements of the form gx^α form a subloop of L. But since $x, u_1, \cdots, u_n$ can each be expressed in the form gx^α, this subloop is all of L.

If $g_1 x^\alpha = g_2 x^\beta$, $0 \leq \alpha, \beta \leq 1$, then $x^{\alpha-\beta} = g_1^{-1}g_2 \in G$. However $u_1, \cdots, u_n$ cannot generate L, so $\alpha - \beta \neq \pm 1$; therefore $\alpha - \beta = 0$ and $\alpha = \beta$. Thus $g_1 = g_2$, and the expression is unique.

Thus, to complete the proof, we must show elements of the form gx^α, under the operation defined by (4), form a nonassociative Moufang loop if and only if G is a nonabelian group.

If L is Moufang, let $a = g_1$, $b = g_2$, $c = g_3 x$. Then

$$(ab)(ca) = (g_1 g_2)[(g_3 x)g_1] = (g_1 g_2)[(g_3 g_1^{-1})x] = [(g_3 g_1^{-1})(g_1 g_2)]x.$$

Also

$$[a(bc)]a = \{g_1[g_2(g_3 x)]\}g_1 = \{g_1[(g_3 g_2)x]\}g_1$$

$$= \{[(g_3 g_2)g_1]x\}g_1 = \{[(g_3 g_2)g_1]g_1^{-1}\}x = (g_3 g_2)x.$$

Hence, $(g_3g_1^{-1})(g_1g_2) = (g_3g_2)$, so $[(g_3g_1^{-1})(g_1g_2)]g_1^{-1} = (g_3g_2)g_1^{-1}$. Thus

$$g_3[g_1^{-1}(g_1g_2)g_1^{-1}] = g_3(g_2g_1^{-1}) = (g_3g_2)g_1^{-1}$$

for any $g_1, g_2, g_3 \in G$. Hence G is a group.

To see if L is associative, let $a = g_1x^{\alpha}$, $b = g_2x^{\beta}$, $c = g_3x^{\gamma}$. Then

$$(ab)c = [(g_1^{\nu_1}g_2^{\mu_1})^{\nu_1}x^{\alpha+\beta}](g_3x^{\gamma}) = [(g_1^{\nu_1}g_2^{\mu_1})^{\nu_1\nu_2}g_3^{\mu_2}]^{\nu_2}x^{\alpha+\beta+\gamma},$$

where $\nu_1 = (-1)^{\beta}$, $\mu_1 = (-1)^{\alpha+\beta}$, $\nu_2 = (-1)^{\gamma}$, $\mu_2 = (-1)^{\alpha+\beta+\gamma}$;

$$a(bc) = (g_1x^{\alpha})[(g_2^{\nu_3}g_3^{\mu_3})^{\nu_3}x^{\beta+\gamma}] = [g_1^{\nu_4}(g_2^{\nu_3}g_3^{\mu_3})^{\nu_3\mu_4}]^{\nu_4}x^{\alpha+\beta+\gamma},$$

where $\nu_3 = (-1)^{\gamma} = \nu_2$, $\mu_3 = (-1)^{\beta+\gamma}$, $\nu_4 = (-1)^{\beta+\gamma} = \mu_3$, $\mu_4 = (-1)^{\alpha+\beta+\gamma} = \mu_2$. Thus L is associative if and only if

$$[(g_1^{\nu_1}g_2^{\mu_1})^{\nu_1\nu_2}g_3^{\mu_2}]^{\nu_2} = [g_1^{\mu_3}(g_2^{\nu_2}g_3^{\mu_3})^{\nu_2\mu_2}]^{\mu_3}.$$

Taking $\alpha = \beta = 0$, $\gamma = 1$, $g_3 = 1$, this becomes $[(g_1g_2)^{-1}]^{-1} = [g_1^{-1}(g_2^{-1})]^{-1}$, or $g_1g_2 = g_2g_1$. So if L is associative then G is abelian. Conversely, if G is abelian, then

$$[(g_1^{\nu_1}g_2^{\mu_1})^{\nu_1\nu_2}g_3^{\mu_2}]^{\nu_2} = g_1g_2^{\mu_1\nu_1}g_3^{\mu_2\nu_2}$$

and

$$[g_1^{\mu_3}(g_2^{\nu_2}g_3^{\mu_3})^{\nu_2\mu_2}]^{\mu_3} = g_1g_2^{\mu_2\mu_3}g_3^{\nu_2\mu_2}.$$

However, $\mu_1\nu_1 = (-1)^{\alpha} = \mu_2\mu_3$, so L is associative.

The final step in the proof is to show that if G is a group then L is Moufang. This involves a straightforward, although somewhat messy computation.

We must check the Moufang law (1). Let $a = g_1x^{\alpha}$, $b = g_2x^{\beta}$, $c = g_3x^{\gamma}$. Then

$$(ab)(ca) = [(g_1^{\nu_1}g_2^{\mu_1})^{\nu_1}x^{\alpha+\beta}][(g_3^{\nu_2}g_1^{\mu_2})^{\nu_2}x^{\alpha+\gamma}] = [(g_1^{\nu_1}g_2^{\mu_1})^{\nu_1\nu_3}(g_3^{\nu_2}g_1^{\mu_2})^{\nu_2\mu_3}]^{\nu_3}x^{\beta+\gamma}$$

and

$$\begin{aligned}[a(bc)]a &= \{(g_1x^{\alpha})[(g_2^{\nu_4}g_3^{\mu_4})^{\nu_4}x^{\beta+\gamma}]\}(g_1x^{\alpha}) \\ &= \{[g_1^{\nu_5}(g_2^{\nu_4}g_3^{\mu_4})^{\nu_4\mu_5}]^{\nu_5}x^{\alpha+\beta+\gamma}\}(g_1x^{\alpha}) \\ &= \{[g_1^{\nu_5}(g_2^{\nu_4}g_3^{\mu_4})^{\nu_4\mu_5}]^{\nu_5\nu_6}g_1^{\mu_6}\}^{\nu_6}x^{\beta+\gamma},\end{aligned}$$

where

$$\mu_1 = (-1)^{\alpha+\beta}, \qquad \nu_1 = (-1)^{\beta},$$
$$\mu_2 = (-1)^{\alpha+\gamma}, \qquad \nu_2 = (-1)^{\alpha},$$
$$\mu_3 = (-1)^{\beta+\gamma}, \qquad \nu_3 = (-1)^{\alpha+\gamma} = \mu_2,$$
$$\mu_4 = (-1)^{\beta+\gamma} = \mu_3, \qquad \nu_4 = (-1)^{\gamma},$$
$$\mu_5 = (-1)^{\alpha+\beta+\gamma}, \qquad \nu_5 = (-1)^{\beta+\gamma} = \mu_3,$$
$$\mu_6 = (-1)^{\beta+\gamma} = \mu_3, \qquad \nu_6 = (-1)^{\alpha} = \nu_2.$$

Therefore, we need

$$[(g_1^{\nu_1} g_2^{\mu_1})^{\nu_1\nu_3}(g_3^{\nu_2} g_1^{\mu_2})^{\nu_2\mu_3}]^{\nu_3} = \{[g_1^{\nu_5}(g_2^{\nu_4} g_3^{\mu_4})^{\nu_4\mu_5}]^{\nu_5\nu_6} g_1^{\mu_6}\}^{\nu_6}.$$

There are eight cases that need be considered, depending on the values of α, β and γ. These are exhibited in Table 2.

Thus L is Moufang, and the proof is complete. Q.E.D.

If G is a nonabelian group of order n, then the Moufang loop L formed as in the theorem with be denoted by $M_{2n}(G, 2)$.

Corollary 5. *The only nonassociative Moufang loops of order* ≤ 31 *in which every minimal set of generators contains an element of order* 2 *are*

A. $M_{12}(S_3, 2)$ (2)
B. $M_{16}(Q, 2)$
C. $M_{16}(D_4, 2)$ (2)
D. $M_{20}(D_5, 2)$ (2)
E. $M_{24}(A_4, 2)$
F. $M_{24}(D_6, 2)$ (2)
G. $M_{24}(G_{12}, 2)$
H. $M_{28}(D_7, 2)$.(2)

Proof. The corollary follows directly from Theorem 1, by use of Table 1.

As a result of Theorem 1, we may now restrict our attention to nonassociative Moufang loops having a minimal set of generators, each element of which is of order greater than 2. Thus, in particular, for every $y, z \in L$, there exists an $x \notin \langle y, z\rangle$ such that $|x| > 2$.

Proposition 4. *A nonassociative Moufang loop* L *which contains an element* x *of order* > 7 *must be of order* > 31.

(2) The loops $M_{4k}(D_k, 2)$ were actually discussed in [3] (see Example 4), where they were denoted by $L_4(k)$. The isomorphism between $M_{4k}(D_k, 2)$ and $L_4(k)$ may be given by $x \to a$, $y \to b$, $z \to c$, where $D_k = \langle y, z\rangle$, $y^2 = z^k = (yz)^2 = 1$, and every element of $M_{4k}(D_k, 2)$ is expressed in the form $(z^\alpha y^\beta)x^\gamma$, $0 \leq \alpha < k$, $0 \leq \beta, \gamma \leq 1$. $M_{12}(S_3, 2)$ is the smallest Moufang loop [4, Main theorem].

Table 2

α	β	γ	$(ab)(ca)$	$[a(bc)]a$
0	0	1	$[(g_1g_2)^{-1}(g_3g_1^{-1})^{-1}]^{-1} = g_3g_2$	$[g_1^{-1}(g_2^{-1}g_3^{-1})]^{-1}g_1^{-1} = g_3g_2$
0	1	0	$(g_1^{-1}g_2^{-1})^{-1}(g_3g_1)^{-1} = g_2g_3^{-1}$	$[g_1^{-1}(g_2g_3^{-1})^{-1}]^{-1}g_1^{-1} = g_2g_3^{-1}$
0	1	1	$[(g_1^{-1}g_2^{-1})(g_3g_1^{-1})]^{-1} = g_1g_3^{-1}g_2g_1$	$[g_1(g_2^{-1}g_3)^{-1}]g_1 = g_1g_3^{-1}g_2g_1$
1	0	0	$[(g_1g_2^{-1})^{-1}(g_3^{-1}g_1^{-1})^{-1}]^{-1} = g_3^{-1}g_2^{-1}$	$\{[g_1(g_2g_3)^{-1}]^{-1}g_1\}^{-1} = g_3^{-1}g_2^{-1}$
1	0	1	$[(g_1g_2^{-1})(g_3^{-1}g_1)] = g_1g_2^{-1}g_3^{-1}g_1$	$\{[g_1^{-1}(g_2^{-1}g_3^{-1})^{-1}]g_1^{-1}\}^{-1} = g_1g_2^{-1}g_3^{-1}g_1$
1	1	0	$[(g_1^{-1}g_2)(g_3^{-1}g_1^{-1})]^{-1} = g_1g_3g_2^{-1}g_1$	$[g_1^{-1}(g_2g_3^{-1})g_1^{-1}]^{-1} = g_1g_3g_2^{-1}g_1$
1	1	1	$[(g_1^{-1}g_2)^{-1}(g_3^{-1}g_1)^{-1}] = g_2^{-1}g_3$	$\{[g_1(g_2^{-1}g_3)]^{-1}g_1\}^{-1} = g_2^{-1}g_3$
0	0	0	$(g_1g_2)(g_3g_1) = g_1g_2g_3g_1$	$[g_1(g_2g_3)]g_1 = g_1g_2g_3g_1$

Proof. There must exist $y, z \in L$ such that $y \notin \langle x \rangle$ and $z \notin \langle x, y \rangle$. By Lemma 1,

$$|L| \geq |\langle x, y, z \rangle| \geq 2|\langle x, y \rangle| \geq 4|\langle x \rangle| \geq 32.$$

Proposition 5. *The only nonassociative Moufang loops L of order ≤ 31 which contain an element z of order 5 or 7 are $M_{20}(D_5, 2)$ and $M_{28}(D_7, 2)$.*

Proof. If every minimal set of generators of L contains an element of order 2, then the result follows easily from Corollary 5 and a knowledge of the groups in Table 1.

Assume there exists a minimal set S of generators each of which is of order greater than 2.

Let $a, b \in S$. (We may assume $\langle a, b \rangle$ is not cyclic otherwise S would not be minimal.) Since L is not associative, $L \neq \langle a, b \rangle$, and so, by Lemma 1, $\langle a, b \rangle \leq 15$. If $z \in \langle a, b \rangle$, a survey of Table 1 implies that $\langle a, b \rangle = D_5$ or D_7. But then either a or b would be of order 2, contrary to assumption. Thus, $z \notin \langle a, b \rangle$. By Corollary 2, $L = \langle z, a, b \rangle$ and $\langle a, b \rangle \leq 6$. But this is incompatible with the fact that neither a nor b is of order 2. Thus the assumption must be false, and the proposition follows.

From this point on, a familiarity with the groups listed in Table 1 is important.

The remainder of our argument is divided into three cases depending on the orders of the elements in L.

Case 1. L contains an element z of order 6. If $x \notin \langle z \rangle$, then, since L cannot be generated by two elements, there exists a $y \notin \langle x, z \rangle$. By Lemma 1,

$$31 \geq |L| \geq |\langle x, y, z\rangle| \geq 2|\langle x, z\rangle|,$$

so $|\langle x, z\rangle| \leq 15$. Since $\langle x, z\rangle$ is a group containing an element of order 6, a quick survey of Table 1 shows that $\langle x, z\rangle \cong C_6 \times C_2$, $\langle x, z\rangle \cong D_6$ or $\langle x, z\rangle \cong G_{12}$. A knowledge of these groups tells us that $|x| \neq 3$.

We now consider several subcases:

1(a) There exist x, y both of order 6 in L, such that $y \notin \langle z\rangle$ and $x \notin \langle y, z\rangle$. Then $\langle x, y\rangle \cong \langle x, z\rangle \cong \langle y, z\rangle \cong C_2 \times C_6$. By replacing x and/or y by their inverses if necessary, we may assume that $x^2 = y^2 = z^2$. Since $\langle x, y\rangle \cong C_2 \times C_6$, and $x^2 = y^2$, $|xy| = 6$. But then $\langle xy, z\rangle \cong C_2 \times C_6$ so that $(xy)z = z(xy)$. However,

$$[(xy)z]y = x(yzy) = x(y^2z) = xz^3 = (xz)z^2 = (xz)y^2$$

so that

$$z(xy) = (xy)z = [(xz)y^2]y^{-1} = (xz)y = (zx)y.$$

Thus L is a group, so case 1(a) cannot occur.

1(b) There exists $y \notin \langle z\rangle$ such that $|y| = 6$, but, for every $x \notin \langle y, z\rangle$, $|x| \neq 6$. Since $\langle x, z\rangle \cong C_2 \times C_6$, D_6 or G_{12}, $|x| = 2$ or 4. However, if $|x| = 2$ for each $x \notin \langle y, z\rangle$, then every minimal set of generators of L contains an element of order 2; hence $|x| = 4$ for some $x \notin \langle y, z\rangle$.

$\langle y, z\rangle \cong C_2 \times C_6$, and, as we did before, we may assume that $y^2 = z^2$. Also $\langle x, z\rangle \cong \langle x, y\rangle \cong G_{12}$, so that $x^2 = z^3$ and $x^2 = y^3$. Thus $y^3 = z^3$. But then $y = z$, contrary to assumption. Hence case 1(b) cannot occur.

1(c) For each $w \notin \langle z\rangle$, $|w| < 6$. Again, since $\langle w, z\rangle \cong C_2 \times C_6$, D_6, or G_{12}, $|w| = 2$ or 4. Hence, since not every minimal set of generators of L contains an element of order 2, there exist $x, y \in L$ such that $|x| = |y| = 4$, and, by Corollary 3, $L = \langle x, y, z\rangle$.

$$\langle x, z\rangle \cong \langle y, z\rangle \cong G_{12}, \text{ and } \langle x, y\rangle \cong C_2 \times C_4, Q, \text{ or } G_{12} \text{ (see Table 1).}$$

However, if $\langle x, y\rangle \cong G_{12}$, then there exists, contrary to assumption, an element of order 6 which is not in $\langle z\rangle$. Thus $\langle x, y\rangle \cong C_2 \times C_4$ or Q. In either case $x^2 = y^2 = z^3$ and $zx = xz^{-1}$ and $zy = yz^{-1}$. If $\langle x, y\rangle \cong C_2 \times C_4$, then $(xy)^2 = 1$, so $\langle xy, z\rangle \cong C_2 \times C_6$ or D_6. In the former case $(xy)z$ is of order 6, contrary to assumption; thus $\langle xy, z\rangle \cong D_6$ and $z(xy) = (xy)z^{-1}$.

If $\langle x, y\rangle \cong Q$, then $|xy| = 4$ and so $\langle xy, z\rangle \cong G_{12}$ and $z(xy) = (xy)z^{-1}$. Thus in either case $z(xy) = (xy)z^{-1}$.

Consider the elements of L of the form $(x^\alpha y^\beta)z^\gamma$. Since $x^2 = y^2$ and $y^2 = z^3$, we may assume that $0 \leq \alpha, \beta \leq 1$, $0 \leq \gamma \leq 5$, e.g.,

$$(x^3y)z^5 = (xx^2y)z^5 = (xy^3)z^5 = [(xy)z^3]z^5 = (xy)z^2.$$

If we can show that the product of two elements of this form is again of this form, then, since x, y and z are of this form and $L = \langle x, y, z\rangle$ every element of L is expressible in this form. Also, since there are at most 24 distinct elements of this form and $|L| = |\langle x, y, z\rangle| \geq 2\,|\langle y, z\rangle| = 24$, every element of L is uniquely expressible in the form $(x^{\alpha}y^{\beta})z^{\gamma}$, where $0 \leq \alpha, \beta \leq 1$, $0 \leq \gamma \leq 5$.

To investigate the multiplication of $(x^{\alpha}y^{\beta})z^{\gamma}$ by $(x^{\sigma}y^{\tau})z^{\rho}$, let $u = x^{\alpha}y^{\beta}$ and $v = x^{\sigma}y^{\tau}$. If $v \neq 1$ (i.e. $v = x, y$ or xy), then $zv = vz^{-1}$; thus

$$[(uz^{\gamma})(vz^{\rho})]z^{\gamma} = u(z^{\gamma}vz^{\gamma+\rho}) = \begin{cases} uz^{2\gamma+\rho} & \text{if } v = 1 \\ u(vz^{\rho}) & \text{otherwise} \end{cases}.$$

If $v \neq 1$ but $u = 1$, this is just vz^{ρ}; and if $u = v \neq 1$, we get u^2z^{ρ}. If $u^2 \neq 1$ then $u^2 = z^3$. Hence, if $u \neq 1$, $v \neq 1$, $u \neq v$, and $\theta = 0$ if $u^2 = 1$, $= 3$ otherwise,

$$u(vz^{\rho}) = u(z^{-\rho}v) = u[(z^{\theta-\rho}u^{-2})v] = u[(u^{-1}z^{\rho-\theta}u^{-1})v]$$

$$= u\{u^{-1}[z^{\rho-\theta}(u^{-1}v)]\} = z^{\rho-\theta}(u^{-1}v) = (u^{-1}v)z^{\theta-\rho} = (uz^{-\theta})v]z^{\theta-\rho} = (uv)z^{-\rho}.$$

(The last step follows since $z^{\theta} \in \langle v\rangle$, as $z^3 = x^2 = y^2$.) Putting this all together, we find that

$$(uz^{\gamma})(vz^{\rho}) \overset{!}{=} \begin{cases} uz^{\gamma+\rho} & \text{if } v = 1 \\ vz^{\rho-\gamma} & \text{if } v \neq 1,\ u = 1 \\ u^2z^{\rho-\gamma} & \text{if } u = v \neq 1 \\ (uv)z^{-\rho-\gamma} & \text{otherwise} \end{cases}.$$

Setting

$$\mu = \begin{cases} 1 & \text{if } v = 1 \\ -1 & \text{otherwise} \end{cases} \quad \text{and} \quad \nu = \begin{cases} 1 & \text{if } u = 1, \text{ or } v = 1, \text{ or } u = v \\ -1 & \text{otherwise} \end{cases},$$

this becomes $(uz^{\gamma})(vz^{\rho}) = (uv)\,z^{\mu\gamma+\nu\rho}$.

Replacing u and v by their expressions in terms of x and y, we get

$$[(x^{\alpha}y^{\beta})z^{\gamma}][(x^{\sigma}y^{\tau})z^{\rho}] = (x^{\alpha}y^{\beta}x^{\sigma}y^{\tau})z^{\mu\gamma+\nu\rho} \tag{5}$$

where

$$\mu = \begin{cases} 1 & \text{if } \sigma = \tau = 0 \\ -1 & \text{otherwise} \end{cases} = (-1)^{\sigma+\tau+\sigma\tau}$$

and

$$\nu = \begin{cases} 1 & \text{if } \alpha = \beta = 0, \text{ or } \sigma = \tau = 0, \text{ or } \alpha = \sigma, \beta = \tau \\ -1 & \text{otherwise} \end{cases} = (-1)^{\alpha\tau+\beta\sigma}.$$

We now consider two subcases.

Case $1(c_1)$. If $\langle x, y\rangle \cong C_2 \times C_4$, then $xy = yx$, and $x^{\alpha}y^{\beta}x^{\sigma}y^{\tau} = x^{\alpha+\sigma}y^{\beta+\tau}$. Thus (5) becomes

$$[(x^{\alpha}y^{\beta})z^{\gamma}][(x^{\sigma}y^{\tau})z^{\rho}] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho}, \tag{6}$$

where μ and ν are as defined above.

This product is of the desired form, so that, as stated previously, every element of L is expressible in this form, and (6) gives the rule for multiplying two elements of L. Thus L has the following presentation:

$$L = \langle x, y, z: x^2 = y^2 = z^3,\ z^6 = 1,\ [(x^{\alpha}y^{\beta})z^{\gamma}][(x^{\sigma}y^{\tau})z^{\rho}] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho},$$

where μ and ν are as defined above$\rangle$.

To see that a Moufang loop having this presentation actually exists, let $a = (x^{\alpha}y^{\beta})z^{\gamma}$, $b = (x^{\sigma}y^{\tau})z^{\rho}$, $c = (x^{\delta}y^{\epsilon})z^{\eta}$. We then check the Moufang identity (1).

$$(ab)(ca) = (x^{2\alpha+\sigma+\delta}y^{2\beta+\tau+\epsilon})z^{\mu_3(\mu_1\gamma+\nu_1\rho)+\nu_3(\mu_2\eta+\nu_2\gamma)}$$

$$[a(bc)]a = (x^{2\alpha+\sigma+\delta}y^{2\beta+\tau+\epsilon})z^{\mu_6[\mu_5\gamma+\nu_5(\mu_4\rho+\nu_4\eta)]+\nu_6\gamma};$$

where

$$\mu_1 = (-1)^{\sigma+\tau+\sigma\tau}, \qquad \nu_1 = (-1)^{\alpha\tau+\beta\sigma},$$

$$\mu_2 = (-1)^{\alpha+\beta+\alpha\beta}, \qquad \nu_2 = (-1)^{\alpha\epsilon+\beta\delta},$$

$$\mu_3 = (-1)^{\alpha+\delta+\beta+\epsilon+(\alpha+\delta)(\beta+\epsilon)}, \qquad \nu_3 = (-1)^{(\alpha+\sigma)(\beta+\epsilon)+(\beta+\tau)(\alpha+\delta)},$$

$$\mu_4 = (-1)^{\delta+\epsilon+\delta\epsilon}, \qquad \nu_4 = (-1)^{\sigma\epsilon+\tau\delta},$$

$$\mu_5 = (-1)^{\delta+\sigma+\epsilon+\tau+(\delta+\sigma)(\epsilon+\tau)}, \qquad \nu_5 = (-1)^{\alpha(\tau+\epsilon)+\beta(\sigma+\delta)},$$

$$\mu_6 = \mu_2, \qquad \nu_6 = (-1)^{\alpha(\beta+\tau+\epsilon)+\beta(\alpha+\sigma+\delta)}.$$

For the Moufang identity to hold, we need the coefficients of γ, ρ and η in $(ab)(ca)$ to be congruent modulo 6 to those in $[a(bc)]a$. The coefficients of γ are $\mu_1\mu_3 + \nu_2\nu_3$ and $\mu_5\mu_6 + \nu_6$ respectively. Since $(-1)^{2k} = 1$, we find

$$\mu_1\mu_3 + \nu_2\nu_3 = (-1)^{\alpha+\beta+\sigma+\tau+\delta+\epsilon+\sigma\tau+\alpha\beta+\alpha\epsilon+\beta\delta+\delta\epsilon} + (-1)^{\beta\sigma+\sigma\epsilon+\tau\delta+\alpha\tau},$$

$$\mu_5\mu_6 + \nu_6 = (-1)^{\alpha+\beta+\alpha\beta+\sigma+\delta+\tau+\epsilon+\delta\epsilon+\delta\tau+\sigma\epsilon+\sigma\tau} + (-1)^{\alpha\tau+\alpha\epsilon+\beta\sigma+\beta\delta}.$$

Thus

$$\mu_1\mu_3 + \nu_2\nu_3 = (-1)^{\sigma\epsilon+\delta\tau-\alpha\epsilon-\beta\delta}(\mu_5\mu_6 + \nu_6).$$

If $(-1)^{\sigma\epsilon+\delta\tau-\alpha\epsilon-\beta\delta} = (-1)^{\delta(\tau-\beta)+\epsilon(\sigma-\alpha)} \neq 1$, then $\delta = 0$, $\epsilon = 1$ and $\alpha + \sigma \equiv 1 \pmod 2$, or $\delta = 1$, $\epsilon = 0$ and $\beta + \tau \equiv 1 \pmod 2$, or $\delta = \epsilon = 1$ and $\alpha + \beta + \sigma + \tau \equiv 1 \pmod 2$. However, in any of these cases, $\mu_1\mu_3 + \nu_2\nu_3 = 0 = \mu_5\mu_6 + \nu_6$. Thus the coefficients of γ check.

In a similar way, the coefficients of ρ and of η check, so that L is Moufang.

To see that L is not a group, $x(yz) = (xy)z^{-1} = (xy)z^5 \neq (xy)z$.

For future reference, we will denote this nonassociative Moufang loop found in case $1(c_1)$ by $M_{24}(G_{12}, C_2 \times C_4)$.

Case $1(c_2)$. $\langle x, y\rangle \cong Q$, so that $yx = xy^3 = (xy)y^2 = (xy)z^3$, and hence, $x^\alpha y^\beta x^\sigma y^\tau = (x^{\alpha+\sigma}y^{\beta+\tau})z^{3\beta\sigma}$.

Thus (5) becomes

$$[(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{3\beta\sigma+\mu\gamma+\nu\rho}, \tag{7}$$

where μ and ν are again as defined above.

Thus (7) gives the rule of multiplication for L, and L has the presentation

$$L = \langle x, y, z: x^2 = y^2 = z^3;\ z^6 = 1,\ [(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{3\beta\sigma+\mu\gamma+\nu\rho},\ \text{where } \mu = (-1)^{\sigma+\tau+\sigma\tau} \text{ and } \nu = (-1)^{\alpha\tau+\beta\sigma}\rangle.$$

It is again a straightforward, although somewhat tedious, matter to check that L is a nonassociative Moufang loop, and the details will be omitted. (Acutally, since $z^3 = z^{-3}$, the only difference between the check here and the check for $M_{24}(G_{12}, C_2 \times C_4)$ is in the exponents of z which are not a coefficient of η, γ or ρ. These are $3\beta\sigma + 3\alpha\epsilon + 3(\beta+\tau)(\alpha+\delta)$ for $(ab)(ca)$, and $3\tau\delta + 3\beta(\sigma+\delta) + 3(\beta+\tau+\epsilon)\alpha$ for $[a(bc)]a$, which are clearly equal.)

The Moufang loop found in case $1(c_2)$ will henceforth be denoted by $M_{24}(G_{12}, Q)$.

We have now completed the discussion of Case 1, in which L contains an element of order 6. By Proposition 5, L cannot contain an element of order 5 (since we are restricting attention to Moufang loops not of the form $M_{2n}(G, 2)$), so we now consider

Case 2. L contains an element x of order 4, but no element of larger order. If L also contains an element y of order 3, then, from Table 1 and a knowledge of cyclic groups, either $|\langle x, y\rangle| > 15$, or $\langle x, y\rangle \cong C_{12}$ or G_{12}. If $|\langle x, y\rangle| > 15$, then $|L| > 31$, contrary to assumption; and if $\langle x, y\rangle \cong C_{12}$ or G_{12}, then L contains an element of order greater than 4, again contrary to assumption. Thus L can contain no element of order 3, and so each nonidentity element of L must be of order 2 or 4. Since, by assumption, not every minimal set of generators of L contains an element of order 2, there exist (by Corollary 3) x, y, z in L, each of order 4, such that $L = \langle x, y, z\rangle$. Since each element of L is of order a power of 2, $|L| = 2^k$ for some k [8, p. 415]. Since $|L| \leq 31$, we have $|L| \leq 16$, so

$$16 \geq |L| = |\langle x, y, z\rangle| \geq 2|\langle x, y\rangle| \geq 4|x| = 16.$$

Thus $|L| = 16$, and $|\langle x, y\rangle| = 8$. (Similarly for any $u, v \in L$, $|\langle u, v\rangle| = 8$ if $|u| = 4$ and $v \notin \langle u\rangle$.)

Thus $\langle x, y\rangle \cong C_2 \times C_4$ or Q. In either case, $x^2 = y^2$, and, by analogous reasoning $x^2 = y^2 = z^2$. Every element of L may be uniquely expressed in the form $(x^\alpha y^\beta)z^\gamma$, $0 \le \alpha, \beta \le 1$, $0 \le \gamma \le 3$, since $|L| = 16$, and there are 16 elements of this form which are easily seen to be distinct. Thus, as in case 1, we need only determine how to multiply two elements of this form.

If $w \in L$, then $\langle w, x\rangle \cong C_2 \times C_4$, D_4, Q or C_4. In any of these cases $wx^2 = x^2w$, so x^2 is in the Moufang center of L (i.e. it commutes with every element of L). Since $(x^2)^2 = x^4 = 1$, x^2 is in the center of L (the intersection of the nucleus and the Moufang center) [8, Lemma 1].

Also, for each $w \in L$, either $w^2 = x^2$ or $w^2 = 1$.

As mentioned previously, $\langle x, y\rangle \cong C_2 \times C_4$ or Q. Similarly for $\langle x, z\rangle$ and $\langle y, z\rangle$. By symmetry, there are thus four cases that need be considered:

2(a) $\langle x, y\rangle \cong \langle x, z\rangle \cong \langle y, z\rangle \cong C_2 \times C_4$,

2(b) $\langle x, y\rangle \cong Q$, $\langle x, z\rangle \cong \langle y, z\rangle \cong C_2 \times C_4$,

2(c) $\langle x, y\rangle \cong C_2 \times C_4$, $\langle x, z\rangle \cong \langle y, z\rangle \cong Q$,

2(d) $\langle x, y\rangle \cong \langle x, z\rangle \cong \langle y, z\rangle \cong Q$.

In cases 2(a) and 2(b),

$$z(xy) = [z(xy)z]z^3 = [(zx)(yz)]z^3 = [(xz)(yz)]z \cdot z^2 = [x(zyz^2)]z^2$$

$$= [x(yz^3)]z^2 = x(yz) \quad (\text{since } z^2 \in \text{center of } L).$$

But L is not a group, so $x(yz) \neq (xy)z$ and hence $z(xy) \neq (xy)z$.

In 2(a), $|xy| = 2$, so $\langle xy, z\rangle \cong C_2 \times C_4$ or D_4. But $z(xy) \neq (xy)z$, so $\langle xy, z\rangle \cong D_4$ and $z(xy) = (xy)z^{-1}$.

Similarly, in case 2(b), $|xy| = 4$ so $\langle xy, z\rangle \cong C_2 \times C_4$ or Q. But $z(xy) \neq (xy)z$, so $\langle xy, z\rangle \cong Q$ and again $z(xy) = (xy)z^{-1}$.

Thus, in either case,

$$z^\eta(x^\delta y^\epsilon) = \begin{cases} (x^\delta y^\epsilon)z^{-\eta} & \text{if } \delta \equiv \epsilon \equiv 1 \pmod 2 \\ (x^\delta y^\epsilon)z^\eta & \text{otherwise} \end{cases}.$$

Defining μ, ϕ, ψ and ν respectively by

$$\mu = (-1)^{\sigma\tau}, \quad \phi = (-1)^{\alpha\beta}, \quad \psi = (-1)^{(\alpha+\sigma)(\beta+\tau)}, \quad \nu = (-1)^{\alpha\tau+\beta\sigma},$$

and recalling that x^2 and y^2 are in the center of L, we obtain

$$(x^\alpha y^\beta)([x^\sigma y^\tau)z^\rho] = (x^\alpha y^\beta)[z^{\mu\rho}(x^\sigma y^\tau)]. \tag{8}$$

In case 2(a), this is equal to

$$(x^\alpha y^\beta)[z^{\mu\rho}\{(x^\alpha y^\beta)(x^{\sigma-\alpha} y^{\tau-\beta})\}] = [(x^\alpha y^\beta)z^{\mu\rho}(x^\alpha y^\beta)](x^{\sigma-\alpha} y^{\tau-\beta})$$

$$= (z^{\phi\mu\rho} x^{2\alpha} y^{2\beta})(x^{\sigma-\alpha} y^{\tau-\beta}) = z^{\phi\mu\rho}(x^{\alpha+\sigma} y^{\beta+\tau}) = (x^{\alpha+\sigma} y^{\beta+\tau})z^{\psi\phi\mu\rho}.$$

But $\psi\phi\mu = (-1)^{\alpha\tau+\beta\sigma} = \nu$, so $(x^\alpha y^\beta)[(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma} y^{\beta+\tau})z^{\nu\rho}$. Thus

$$[(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = \{(x^\alpha y^\beta)[z^\gamma(x^\sigma y^\tau)z^{\rho+\gamma}]\}z^{-\gamma}$$

$$= \{(x^\alpha y^\beta)[(x^\sigma y^\tau)z^{\rho+\gamma+\mu\gamma}]\}z^{-\gamma} = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\nu(\rho+\gamma+\mu\gamma)-\gamma} = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho}.$$

[Note $z^{2\gamma} = z^{-2\gamma}$ so that the value of ν does not effect the coefficient of γ.] Thus

$$L = \langle x, y, z: x^2 = y^2 = z^2;\ z^4 = 1;\ [(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho},$$
$$\text{where } \mu = (-1)^{\sigma\tau} \text{ and } \nu = (-1)^{\alpha\tau+\beta\sigma}\rangle.$$

The check that L is a nonassociative Moufang loop is again tedious but straightforward, and will be omitted. (Note that, since $z^4 = 1$, we only need the exponents of z in $(ab)(ca)$ and $[a(bc)]a$ to be congruent mod 4.)

In case 2(b), recalling that $yx = xy^3 = (xy)y^2 = (xy)z^2$, and that z^2 is in the center of L, we see that (8) becomes

$$(x^\alpha y^\beta)[(x^\sigma y^\tau)z^\rho] = (x^\alpha y^\beta)[z^{\mu\rho}\{(x^\alpha y^\beta)[(x^{\sigma-\alpha}y^{\tau-\beta})z^{2\beta(\sigma-\alpha)}]\}]$$

$$= [(x^\alpha y^\beta)z^{\mu\rho}(x^\alpha y^\beta)][(x^{\sigma-\alpha}y^{\tau-\beta})z^{2\beta(\sigma-\alpha)}]$$

$$= [z^{\phi\mu\rho}(x^{2\alpha}y^{2\beta}z^{2\alpha\beta})][(x^{\sigma-\alpha}y^{\tau-\beta})z^{2\beta(\sigma-\alpha)}]$$

$$= z^{\phi\mu\rho}(x^{\alpha+\sigma}y^{\beta+\tau})z^{2\beta(\sigma-\alpha)+2\alpha\beta+4\beta(\sigma-\alpha)} = z^{\phi\mu\rho}(x^{\alpha+\sigma}y^{\beta+\tau})z^{2\beta\sigma}$$

$$= (x^{\alpha+\sigma}y^{\beta+\tau})z^{\psi\phi\mu\rho+2\beta\sigma} = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\nu\rho+2\beta\sigma}.$$

Thus, in a manner similar to case 2(a), we find that

$$[(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho+2\beta\sigma}.$$

[Note again that $z^{2\nu\beta\sigma} = z^{2\beta\sigma}$ regardless of the value of ν.] Thus

$$L = \langle x, y, z: x^2 = y^2 = z^2;\ z^4 = 1;\ [(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho+2\beta\sigma},$$
$$\text{where } \mu = (-1)^{\sigma\tau} \text{ and } \nu = (-1)^{\alpha\tau+\beta\sigma}\rangle.$$

Again the verification that L is a nonassociative Moufang loop will be omitted.

In case 2(c), since $\langle x, z\rangle \cong Q$, $|xz| = 4$ and $\langle x, xz\rangle \cong Q$. As in case 2(a), $\langle xy, z\rangle$ must be $C_2 \times C_4$ or D_4, and

$$z(xy) = [z(xy)z]z^3 = [(zx)(yz)]z^3 = [(xz^3)(yz)]z^3 = x(z^3y) = x(yz) \neq (xy)z.$$

Thus $z(xy) = (xy)z^3$. Consider $\langle y, xz\rangle$.

$$y(xz) = zz^3[y(z^3x)] = z[(z^3yz^3)x] = z(yx) = z(xy) = (xy)z^3.$$

Also

$$(xz)y = [(xz)y]z \cdot z^3 = [x(zyz)]z^3 = (xy)z^3,.$$

so $y(xz) = (xz)y$. Thus $\langle y, xz\rangle \cong C_2 \times C_4$. If we now choose x, xz, y as our set of generators for L, we have $\langle x, xz\rangle \cong Q$, $\langle x, y\rangle \cong \langle xz, y\rangle \cong C_2 \times C_4$, so case 2(c) is really the same as case 2(b). [If we do not realize that 2(c) is the same as 2(b), and if we approach 2(c) in a manner similar to the way we did 2(a) and 2(b), we find that the loop in 2(c) is presented by

$$L = \langle x, y, z: x^2 = y^2 = z^2;\ z^4 = 1;\ [(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho},$$
$$\text{where } \mu = (-1)^{\sigma+\tau+\sigma\tau} \text{ and } \nu = (-1)^{\alpha\tau+\beta\sigma}\rangle.$$

The isomorphism between the loops in 2(c) and 2(b) may be given by f: 2(c) $\to$ 2(b), where $f(x) = y$, $f(y) = z$, $f(z) = xy$, but the verification that f is an isomorphism is quite messy. As this verification is not needed, it will be omitted. However, the fact that the loops in 2(b) and 2(c) are isomorphic, leads us to ask whether any of the other loops we found are also isomorphic. This question will be answered in the next section.]

The details of case 2(d) are very similar to those of cases 2(a) and 2(b) and will for the most part be omitted. We again find that $z(xy) = (xy)z^{-1}$, but this time

$$z^\eta(x^\delta y^\epsilon) = \begin{cases} (x^\delta y^\epsilon)z^\eta & \text{if } \delta \equiv \epsilon \equiv 0 \pmod 2 \\ (x^\delta y^\epsilon)z^{-\eta} & \text{otherwise} \end{cases}.$$

Following through in a manner similar to the previous cases, we then obtain

$$[(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho+2\beta\sigma},$$

where $\nu = (-1)^{\alpha\tau+\beta\sigma}$ as before, but now $\mu = (-1)^{\sigma+\tau+\sigma\tau}$. Thus

$$L = \langle x, y, z: x^2 = y^2 = z^2;\ z^4 = 1;\ [(x^\alpha y^\beta)z^\gamma][(x^\sigma y^\tau)z^\rho] = (x^{\alpha+\sigma}y^{\beta+\tau})z^{\mu\gamma+\nu\rho+2\beta\sigma},$$
$$\text{where } \mu = (-1)^{\sigma+\tau+\sigma\tau} \text{ and } \nu = (-1)^{\alpha\tau+\beta\sigma}\rangle.$$

Again it may be verified that L is a nonassociative Moufang loop.

It is worthwhile noting that the loop found in 2(d) is just the loop of units in the Cayley numbers.

This completes Case 2, but for future reference let us give the loops we found names. The loop in 2(a) will be denoted by $M_{16}(C_2 \times C_4)$; the one found in 2(b) and 2(c) will be denoted by $M_{16}(C_2 \times C_4, Q)$; and the one found in 2(d) will be denoted by $M_{16}(Q)$.

All that remains to be done now in order to find all nonassociative Moufang loops of order ≤ 31 is to consider

Case 3. L contains no element of order greater than 3. Since we are assuming that not all minimal sets of generators of L contain an element of order 2, L must contain a minimal set of generators, each element of which is of order 3.

From Lemma 1 and its corollaries, such a set of generators must contain exactly 3 elements x, y and z.

Let $K = \{g \mid g \in L, |g| = 3\}$. Let $g_1, g_2 \in K$. By Table 1, $\langle g_1, g_2\rangle \cong A_4$ or $C_3 \times C_3$. We can assume that $x \notin \langle g_1, g_2\rangle$. If $\langle g_1, g_2\rangle \cong A_4$, then, by Corollary 2, $|\langle g_1, g_2, x\rangle| \geq 36$, contrary to assumption. Therefore $\langle g_1, g_2\rangle \cong C_3 \times C_3$ and $|g_1 g_2| = 3$. Thus, K is a commutative Moufang loop of exponent 3. Since $x, y, z \in K$, $K = L$. By [2, Theorem 10.1, p. 157], L is centrally nilpotent of order 3^3. By Proposition 1, L is therefore a group.

Thus Case 3 gives rise to no nonassociative Moufang loops.

Having considered all possible cases, we may summarize our results in the following theorem.

Theorem 2. *The only nonassociative Moufang loops of order* ≤ 31 *are those given in Corollary* 4, *and the following*:

I. $M_{16}(C_2 \times C_4)$ L. $M_{24}(G_{12}, C_2 \times C_4)$.

J. $M_{16}(C_2 \times C_4, Q)$ M. $M_{24}(G_{12}, Q)$

K. $M_{16}(Q)$

V. **Some properties.** In studying cases 2(b) and 2(c) above, we raised the question of whether any of the loops are isomorphic. The answer is no. This is most easily seen by considering the order structure of each of the loops. Table 3 summarizes these results, giving the number of elements of each order in each loop.

Since isomorphisms preserve the order structure, the only possible isomorphism that could exist is between $M_{16}(Q, 2)$ and $M_{16}(C_2 \times C_4)$. However, every set of generators of $M_{16}(Q, 2)$ contains an element of order 2, while this is not true for $M_{16}(C_2 \times C_4)$, so none of the loops in question are isomorphic. [Note that there are 5 nonisomorphic nonassociative Moufang loops of order 16, and not only 2 as had been previously suggested by the author [3, final paragraph].]

In fact, since isotopy of Moufang loops preserves order of elements, none of the loops, with the exception of $M_{16}(Q, 2)$ and $M_{16}(C_2 \times C_4)$, could be isotopic. Thus each of the other loops is a G-loop (i.e. each loop is isomorphic to all its loop-isotopes). (Actually $M_{16}(Q, 2)$ and $M_{16}(C_2 \times C_4)$ are also G-loops. This will be shown later.)

We now turn our attention to which of the M_k-laws each of our loops satisfies. A loop is said to satisfy the M_k-law for some positive integer k if, for all $a, b, c \in L$,

$$(ab)(ca^k) = [a(bc)]a^k.$$

Table 3

Loop	Number of elements of order					
	2	3	4	5	6	7
$M_{12}(S_3, 2)$	9	2	–	–	–	–
$M_{16}(Q, 2)$	9	–	6	–	–	–
$M_{16}(D_4, 2)$	13	–	2	–	–	–
$M_{20}(D_5, 2)$	15	–	–	4	–	–
$M_{24}(A_4, 2)$	15	8	–	–	–	–
$M_{24}(D_6, 2)$	19	2	–	–	2	–
$M_{24}(G_{12}, 2)$	13	2	6	–	2	–
$M_{28}(D_7, 2)$	21	–	–	–	–	6
$M_{16}(C_2 \times C_4)$	9	–	6	–	–	–
$M_{16}(C_2 \times C_4, Q)$	5	–	10	–	–	–
$M_{16}(Q)$	1	–	14	–	–	–
$M_{24}(G_{12}, C_2 \times C_4)$	7	2	12	–	2	–
$M_{24}(G_{12}, Q)$	1	2	18	–	2	–

Pflugfelder proved that a loop L satisfies the M_k-law if and only if L is Moufang and x^{k-1} is in the nucleus of L for each x in L [10, Theorem 3]. She also proved that if L satisfies the M_r-law and also the M_s-law, then L satisfies the M_d-law, where $d = 1 + (r - 1, s - 1)$, and hence that the set of all k for which L satisfies the M_k law is determined by the smallest such k which is greater than 1 [10, Theorem 1].

If d is the smallest such k, and if the M_d-law is satisfied in a nontrivial way (i.e. if $x^{d-1} \neq 1$ for at least one x in L), then L is called an M_d-loop. Otherwise, M is said to be strictly Moufang. We would like to investigate the M_k-law for the loops we found. We begin by finding their nuclei.

Theorem 3. *If $L = M(G, 2)$, then the nucleus of L is equal to the center of G.*

Proof. In the proof of Theorem 1, we saw that $a = g_1x^{\alpha}$, $b = g_2x^{\beta}$, $c = g_3x^{\gamma}$ associate if and only if

$$[(g_1^{\nu_1}g_2^{\mu_1})^{\nu_1\nu_2}g_3^{\mu_2}]^{\nu_2} = [g_1^{\mu_3}(g_2^{\nu_2}g_3^{\mu_3})^{\nu_2\mu_2}]^{\mu_3},$$

where $\nu_1 = (-1)^{\beta}$, $\mu_1 = (-1)^{\alpha+\beta}$, $\nu_2 = (-1)^{\gamma}$, $\mu_2 = (-1)^{\alpha+\beta+\gamma}$, $\mu_3 = (-1)^{\beta+\gamma}$.

If g_2 is in the center of G, this becomes

$$g_2^{\mu_1\nu_1}[g_1^{\nu_2}g_3^{\mu_2}]^{\nu_2} = g_2^{\mu_2\mu_3}[g_1^{\mu_3}g_3^{\mu_3\nu_2\mu_2}]^{\mu_3}.$$

Since $\mu_1\nu_1 = \mu_2\mu_3 = (-1)^{\alpha}$, $\mu_3\nu_2^{-1} = \mu_3\nu_2 = \nu_1$, this becomes

$$g_1^{\nu_2}g_3^{\mu_2} = (g_1^{\mu_3}g_3^{\nu_1\mu_2})^{\nu_1}.$$

If $\beta = 0$, then $\nu_1 = 1$, and $\nu_2 = \mu_3$, so we have equality. Thus if g_2 is in the center of G and $\beta = 0$, then g_2x^{β} is in the middle nucleus and hence the nucleus of L.

Conversely, if g_2x^{β} is in the middle nucleus of L, taking $g_3 = 1$, $\gamma = 1$ and $\alpha = \beta$, we see that $\mu_3 = -\nu_1$ and $\mu_1 = -\mu_2 = 1$ so that we must have

$$(g_1^{\nu_1}g_2) = (g_1^{-\nu_1}g_2^{-1})^{-1} = g_2g_1^{\nu_1},$$

and thus g_2 must be in the center of G.

But then, as in the first part of the proof, we must have

$$(g_1^{\nu_2}g_3^{\mu_2}) = (g_1^{\mu_3}g_3^{\nu_1\mu_2})^{\nu_1}.$$

If $\beta = 1$, then $\nu_1 = -1$ and $\nu_2 = -\mu_3$, so that

$$(g_1^{\nu_2}g_3^{\mu_2}) = (g_1^{-\nu_2}g_3^{-\mu_2})^{-1} = g_3^{\mu_2}g_1^{\nu_2}.$$

But, since G is not abelian, this will not hold for all g_1 and g_3. Hence $\beta = 0$.

Thus the theorem is proven.

Table 4 lists the loops of order ≤ 31, their nuclei (which in each case turns out to be identical with the center, although this will not be true in general), and the value of d for which L is an M_d-loop (if L is strictly Moufang, we write $d = 1$).

Note that all the loops of order 16 are M_3-loops, and hence extra loops [5, Corollary 2]. Thus in particular they are G-loops ([3, Theorem, 1], or [6, Theorem 4]), so that $M_{16}(Q, 2)$ and $M_{16}(C_2 \times C_4)$ are not isotopic.

Note also that $M_{24}(D_6, 2)$ gives an example of a strictly Moufang loop with a nontrivial nucleus.

As a final consideration, Table 5 lists the prototypes of all possible subloops of our loops. (These were found by considering the subloops generated by each possible collection of elements.)

Using this table, we see that all of our loops satisfy Lagrange's theorem, and they all have Sylow subloops for each prime dividing their order. Also, all are seen to be solvable but only those of order 16 are centrally nilpotent [8, p. 415].

Note that $M_{16}(Q)$ is hamiltonian (see [2, Theorem 7.2, p. 87]).

Table 4

loop	nucleus (center) (3)	M_d-loop
$M_{12}(S_3, 2)$	1	1
$M_{16}(Q, 2)$	$\langle y^2\rangle = \langle z^2\rangle \cong C_2$	3
$M_{16}(D_4, 2)$	$\langle y^2\rangle \cong C_2$	3
$M_{20}(D_5, 2)$	1	1
$M_{24}(A_4, 2)$	1	1
$M_{24}(D_6, 2)$	$\langle y^3\rangle \cong C_2$	1
$M_{24}(G_{12}, 2)$	$\langle y^3\rangle = \langle z^2\rangle \cong C_2$	7
$M_{28}(D_7, 2)$	1	1
$M_{16}(C_2 \times C_4)$	$\langle x^2\rangle = \langle y^2\rangle = \langle z^2\rangle \cong C_2$	3
$M_{16}(C_2 \times C_4, Q)$	$\langle x^2\rangle = \langle y^2\rangle = \langle z^2\rangle \cong C_2$	3
$M_{16}(Q)$	$\langle x^2\rangle = \langle y^2\rangle = \langle z^2\rangle \cong C_2$	3
$M_{24}(G_{12}, C_2 \times C_4)$	$\langle x^2\rangle = \langle y^2\rangle = \langle z^3\rangle \cong C_2$	7
$M_{24}(G_{12}, Q)$	$\langle x^2\rangle = \langle y^2\rangle = \langle z^3\rangle \cong C_2$	7

Table 5

loop	subloops	
	normal	not normal
$M_{12}(S_3, 2)$	S_3, C_3	$C_2 \times C_2, C_2$
$M_{16}(Q, 2)$	$Q, D_4, C_4, C_2 \times C_2, C_2$	C_2
$M_{16}(D_4, 2)$	$D_4, C_2 \times C_2 \times C_2, C_4, C_2 \times C_2, C_2$	C_2
$M_{20}(D_5, 2)$	D_5, C_5	$C_2 \times C_2, C_2$
$M_{24}(A_4, 2)$	$A_4, C_2 \times C_2$	$C_2 \times C_2 \times C_2, C_2 \times C_2, C_3, C_2, S_3$
$M_{24}(D_6, 2)$	$D_6, M(S_3, 2), C_6, S_3, C_3, C_2$	$C_2 \times C_2 \times C_2, C_2 \times C_2, C_2$
$M_{24}(G_{12}, 2)$	G_{12}, D_6, C_3, C_2	$D_4, S_3, C_4, C_2 \times C_2$
$M_{28}(D_7, 2)$	D_7, C_7	$C_2 \times C_2, C_2$
$M_{16}(C_2 \times C_4)$	$C_2 \times C_4, D_4, C_4, C_2$	$C_2 \times C_2, C_2$
$M_{16}(C_2 \times C_4, Q)$	$Q, D_4, C_2 \times C_4, C_4, C_2 \times C_2, C_2$	C_2
$M_{16}(Q)$	Q, C_4, C_2	none
$M_{24}(G_{12}, C_2 \times C_4)$	$G_{12}, D_6, S_3, C_6, C_3, C_2$	$C_2 \times C_4, C_2 \times C_2, C_4, C_2$
$M_{24}(G_{12}, Q)$	G_{12}, C_6, C_3, C_2	Q, C_4

(3) In $M_{2n}(G, 2)$, $\{y, z\}$ denotes a minimal set of generators of G, in which y is of maximal possible order. In the other loops, x, y and z refer to the presentation given when the loop was first discussed.

REFERENCES

1. B. Baumslag and B. Chandler, *Theory and problems of group theory*, Schaum's Outline Series, McGraw-Hill, New York, 1968.

2. R. H. Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, N. F., Heft 20, Springer-Verlag, Berlin, 1958. MR 20 #76.

3. O. Chein and H. O. Pflugfelder, *On maps* $x \longrightarrow x^n$ *and the isotopy-isomorphy property of Moufang loops*, Aequationes Math. 6 (1971), 157–161. MR 45 #2067.

4. ———, *The smallest Moufang loop*, Arch. Math. 22 (1971), 573–576.

5. O. Chein and D. A. Robinson, *An "extra" law for characterizing Moufang loops*, Proc. Amer. Math. Soc. 33 (1972), 29–32. MR 45 #2068.

6. F. Fenyves, *Extra loops*. I, Publ. Math. Debrecen 15 (1968), 235–238. MR 38 #5976.

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

8. G. Glauberman and C. R. B. Wright, *Nilpotence of finite Moufang 2-loops*, J. Algebra 8 (1968), 415–417. MR 36 #5251.

9. R. Moufang, *Zur Struktur von Alternativkörpern*, Math. Ann. 110 (1935), 416–430.

10. H. O. Pflugfelder, *A special class of Moufang loops*, Proc. Amer. Math. Soç. 26 (1970), 583–586.

DEPARTMENT OF MATHEMATICS, TEMPLE UNIVERSITY, PHILADELPHIA, PENNSYLVANIA 19122