Abstract. An RA loop is a loop whose loop rings in characteristic different two are alternative. In this paper, we characterize Moufang loops with a unique non-identity commutator which are not associative but in which all proper subloops are associative. Surprisingly, these turn out be nearly RA.

MINIMALLY NONASSOCIATIVE MOUFANG LOOPS WITH A UNIQUE NONIDENTITY COMMUTATOR ARE NEARLY RA

ORIN CHEIN AND EDGAR G. GOODAIRE

1. Introduction

In this paper, we call a Moufang loop minimally nonassociative if it is not associative but all its proper subloops are associative. Evidently, this condition is equivalent to the statement that \( L \) is generated by any three elements which do not associate. Note also that a minimally nonassociative loop must be indecomposable because \( L = G \times H \) with \( G \) and \( H \) proper subloops implies that \( L \) is associative.

We begin with two lemmas, the first due to R. H. Bruck [?, Lemma 5.5, p. 125] and the second to the authors [?, Lemma 3].

Lemma 1.1. Let \( L \) be a Moufang loop in which \( (x, y, (y, z)) = 1 \) is an identity. Then \( (x^n, y, z) = (x, y, z)^n \) for all \( x, y, z \in L \) and all integers \( n \). Moreover, the associator \( (x, y, z) \) lies in the centre of the subloop generated by \( x, y \) and \( z \).

Lemma 1.2. Let \( L \) be a Moufang loop with a unique nonidentity commutator \( s \). Then \( s \) is central of order 2, \( x^2 \in C(L) \) for all \( x \in L \) and, for any \( x, y, z \in L \), \( (x, y, z)^3 \) is either 1 or \( s \). Moreover, \( L \) is an extra loop if and only if \( s \) is also a unique nonidentity associator in \( L \).

Our interest in minimally nonassociative Moufang loops originates in a paper written early this century by G. A. Miller and H. C. Moreno where the nonabelian groups, all of whose proper subgroups are abelian, are determined [?]. This classification, together with a construction of O. Chein leads quickly to a family of Moufang loops which are not associative, yet all of whose proper subloops are associative, that is, to a family of minimally nonassociative Moufang loops. The construction to which we refer is this [?, Theorem 1]. Let \( G \) be a group, \( u \) an element not in \( G \) and \( L = G \cup Gu \). Extending the multiplication from \( G \) to \( L \) by the rules

\[
g(hu) = (hg)u \]
\[
(gu)h = (gh^{-1})u \]
\[
(gu)(hu) = h^{-1}g
\]
makes a Moufang loop, denoted $M(G, 2)$, which is not associative if and only if $G$ is not abelian. Clearly then, if $M(G, 2)$ is minimally nonassociative, it follows that $G$ must be one of the groups arising in the work of Miller and Moreno.

Many of the loops which appear in this paper are of a type more general than $M(G, 2)$. These too were first identified by Chein [7, Theorem 2']. Let $G$ be a nonabelian group and $g \mapsto g^*$ an involution of $G$ (that is, an anti-automorphism of period two) such that $gg^*$ is in the centre of $G$ for all $g \in G$. Let $u$ be an element not in $G$ and form the set $L = G \cup Gu$. Define multiplication in $L$ by extending multiplication from $G$ with the rules

$$g(hu) = h(gu)$$

$$ (gu)h = (gh^*)u$$

$$ (gu)(hu) = g_0h^*g$$

where $g_0 = u^2$. Then $L$ is a Moufang loop, not associative, and denoted $M(G, *, g_0)$ [7, §II.5.2]. Such loops have appeared often in the literature since RA loops—Moufang loops which have alternative loop rings in characteristic different from 2—are of this form [7], [7, Theorem IV.3.1]. Curiously, the loops of interest in this paper share many of the properties of an RA loop.

2. Main Results

**Theorem 2.1.** Let $L$ be a minimally nonassociative finite Moufang loop with a unique nonidentity commutator. Then $L = M(G, *, g_0)$ for suitable $G$, * and $g_0$. Furthermore, $L$ is extra and the unique nonidentity commutator is also a unique nonidentity associator. If $g^* = sg$ for noncentral $g \in G$, then $L$ is an RA loop.

QUESTION FOR ORIN: In May, you were optimistic that a lot of our paper on CMLs could be applied to this situation. I guess the idea would be to get some sort of a converse to the above theorem.

**Proof.** Let $s$ denote the unique nonidentity commutator of $L$. By Lemma 1.2, $s$ is central of order 2. Thus $(x, y, (y, z)) = 1$ for any $x, y, z \in L$, so, by Lemma 1.1, the associator $(x, y, z)$ lies in the centre of the subloop generated by $x, y, z$. This subloop is either trivial or the entire loop $L$. It follows that associators in $L$ are central and hence that $L/Z(L)$ is an abelian group.

Now Lemma 1.2 says $(x, y, z)^6 = 1$ for any $x, y, z \in L$. By Lemma 1.1, $(x^6, y, z) = (x, y, z)^6 = 1$; in other words, $x^6 \in N(L)$ for any $x \in L$. Since $x^6 = (x^3)^2$ is also in $C(L)$, $x^6$ is central for $x$, so $L/Z(L)$ has exponent at most 6. Since $L$ is generated by 3 elements, so is $L/Z(L)$. Thus, this abelian group is the direct product $C_r \times C_s \times C_t$ of at most three cyclic groups, with $r, s, t \in \{2, 3\}$. If both $C_2$ and $C_3$ appear, then $L/Z(L)$ can be generated by two elements (since $C_2 \times C_3 \cong C_6$), and it would follow by diassociativity that $L$ is a group. Thus $r = s = t$ is either 2 or 3. If $L/Z(L) \cong C_3 \times C_3 \times C_3$, then $x^3 \in Z(L) \subseteq C(L)$ for any $x \in L$. Since also $x^2 \in C(L)$, by Lemma 1.2, it would follow that $x = x^3x^{-2} \in C(L)$ for all $x$, so $L$ would be commutative, contrary to hypothesis. It follows that $L/Z(L) \cong C_2 \times C_2 \times C_2$. In
particular, squares in $L$ are nuclear, so $L$ is extra and $s$ is a unique nonidentity associator, by Lemma 1.2.

Let the generators of $L/Z(L)$ be $Z(L)a$, $Z(L)b$ and $Z(L)u$. Thus $L = \langle Z(L), a, b, u \rangle$ is generated by $a$, $b$, $u$ and its centre. Since $L$ is not commutative, we may assume $ab \neq ba$. Let $G = \langle Z(L), a, b \rangle$ be the subloop of $L$ generated by $a$, $b$ and $Z(L)$. By diassociativity (and the properties of the centre of a loop), $G$ is a group and it is not abelian (and hence contains $s$).

Since $u^2 \in Z(L) \subseteq G$ and the map $\theta: g \mapsto u^{-1}gu$ maps $G$ to $G$—after all, $u^{-1}gu$ is either $g$ or $sg$—we may apply [?, Theorem 1] and conclude that $L = G \cup Gu$ with multiplication given by the rules

$$
g(hu) = [(g\theta)(h\theta)]\theta^{-1}u$$

$$(gu)h = [g(h\theta^{-1})]u$$

$$(gu)(hu) = [(g\theta)h]\theta^{-1}g_0$$

for $g, h \in G$. If $\theta$ is an antihomomorphism, these rules are precisely those of (1.1) and $L = M(G, \ast, g_0)$ with $\ast = \theta$. Since $G$ has a unique nonidentity central commutator and central squares, any element of $G$ can be written in the form $za^\alpha b^\beta$ where $z \in Z(G)$ and $\alpha, \beta \in \{0, 1\}$. To prove that $\theta$ is an antihomomorphism then, it suffices to show that

$$u^{-1}(xy)u = (u^{-1}yu)(u^{-1}xu)$$

for all $x, y \in G$ with $(x, y) \neq 1 \neq (x, y, u)$. Let $t = (u^{-1}yu)(u^{-1}xu)$. By the right Moufang identity,

$$tu = (u^{-1}y)[u(u^{-1}xu)u] = (u^{-1}y)(ux)^2 = (u^{-1}y \cdot x)u^2$$

and so

$$t = (u^{-1}y \cdot x)u$$

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

$$= u^{-1}(yx)u(u^{-1}, y, x)$$

$$= [u^{-1}(xy)u](x, y)(u^{-1}, y, x) = u^{-1}(xy)u$$

because $(x, y) = s = (u^{-1}, y, x)$. Indeed, $\theta$ is an antihomomorphism and $L = M(G, \ast, g_0)$.

Finally, note that $Z(G) = Z(L)$ and $G/Z(G) \cong C_2 \times C_2$. Thus $G$ has the so-called “LC property” [?, pp. 305-306], [?, Proposition III.3.6]. The final statement now follows immediately from [?, Corollary III.3.4].

**Proposition 2.2.** Let $L = M(G, \ast, g_0)$ for some finite nonabelian group $G$, involution $g \mapsto g^*$ of $G$ and $g_0 \in Z(G)$. Suppose $H^* \subseteq H$ for all nonabelian subgroups of $G$. If $L$ is minimally nonassociative, then $G = \langle a, b, g_0 \rangle$ for any noncommuting elements $a, b \in G$. The converse holds if $G$ is a 2-group.

**Proof.** Suppose $L$ is minimally nonassociative and $a, b \in G$ do not commute. Then $H = \langle a, b, g_0 \rangle$ is a nonabelian group and $L_1 = M(H, \ast, g_0)$ is a subloop of $L$ which is not associative. Thus $L_1 = L$, so $H = G$. Conversely, let $G$ be a 2-group and
suppose $G = \langle a, b, g_0 \rangle$ for any noncommuting elements $a, b \in G$. Let $x, y$ and $z$ be any three elements of $L$ which do not associate. We prove that $\langle x, y, z \rangle = L$. For this, we may assume that $x, y, z$ are of the form $x = g, y = h, z = ku$, with $g, h, k \in G$. For example, $\langle gh, hu, ku \rangle = \langle g, (hu)(ku) \rangle$ and $(hu)(ku) \in G$. We compute the associator $a = (g, h, ku)$, recalling that this element is defined by the equation $\langle gh \rangle \langle ku \rangle = g \langle h \rangle \langle ku \rangle$. The rules for multiplication in $L$ give $a \in G$, and $\langle gh \rangle \langle ku \rangle = \langle kgh \rangle u = (kgh) u$ imply $a = (g, h)^*$. Since $(x, y, z) \neq 1$, it follows that $(g, h) \neq 1$ and, by hypothesis, that $G = \langle g, h, g_0 \rangle$. Writing $k = w g_0^\gamma$ with $w$ a work in $g$ and $h$, we have

$$\langle g, h, ku \rangle = \langle g, h, g_0^\gamma u \rangle = \langle g, h, u^{2\gamma + 1} \rangle$$

(remembering that $g_0 = u^2$). Since $u^2 \in G$ and $G$ is 2-group, $u^n = 1$ for some $n$, a power of 2. Writing $m + j(2\gamma + 1) = 1$ for integers $i$ and $j$, we have $u = u^{m+j(2\gamma+1)} = (u^{2\gamma+1})^i$ and so $\langle g, h, ku \rangle = \langle g, h, u \rangle$. But $g_0 = u^2 \in \langle g, h, u \rangle$, hence $G = \langle g, h, g_0 \rangle \subseteq g, h, u \rangle$, so $L = G \cup Gu \subseteq \langle g, h, u \rangle$, giving equality and the desired result.

**Corollary 2.3.** A finite RA loop $L = M(G, *, g_0)$ is minimally nonassociative if and only if it is indecomposable and $G = \langle a, b, g_0 \rangle$ for any noncommuting elements $a, b \in G$.

**Proof.** An RA loop $L$ has a unique nonidentity commutator $s$ which is necessarily an element of the nonabelian group $G$. Since $g^* = g$ or $g^* = sg$ for $g \in G$, it follows that $H^* \subseteq H$ for any nonabelian subgroup $H$ of $G$. At the beginning of this paper, we remarked that a minimally nonassociative loop is indecomposable. Thus one direction follows immediately from Proposition 2.2, and so does this other because in the case that $L$ is indecomposable, it is known that $G$ is a 2-group [?, Theorem 6], [?, Corollary V.1.4].

**Remark 2.4.** Finite indecomposable RA loops fall into seven categories which have been denoted $L_1, \ldots, L_7$ [?], [?, §V.3]. Direct application of Corollary 2.3 shows that the loops in classes $L_2, L_4$ and $L_6$ are the minimally nonassociative ones.

**Temple University, Philadelphia, PA 19122 U.S.A.**

**E-mail address:** orin@math.temple.edu

**Memorial University of Newfoundland, St. John’s, Newfoundland, Canada A1C 5S7**

**E-mail address:** edgar@math.mun.ca