ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 29, Number 4, Winter 1999

MOUFANG LOOP MULTIPLICATION GROUPS WITH TRIALITY

J.D. PHILLIPS

Introduction. In the second of his two influential papers from the mid-sixties, George Glauberman proved a fundamental theorem about the existence of a special automorphism of order three on the multiplication group of Moufang loops with trivial nucleus [**3**]. Glauberman's result motivated Stephen Doro a decade later to define a class of groups that also admit a special automorphism of order three, the so-called groups with triality [**2**]. Not surprisingly, this class of groups is intimately related to the class of Moufang loops. Doro sites Glauberman's result in showing that each Moufang loop with trivial nucleus has multiplication group that is with triality. Unfortunately, not every Moufang loop multiplication group is itself a group with triality, although each is an image of some group with triality [**2**]. Continuing the work of Glauberman and Doro, this paper enlarges the class of Moufang loop multiplication groups with known triality status. In the process, new light is shed on the fundamental importance of two signal classes of Moufang loops: the commutative Moufang loops of exponent three and the Moufang loops with trivial nucleus.

1. Basic definitions. A *quasigroup* is a set Q with a single binary operation, denoted by juxtaposition, such that in $xy = z$, knowledge of any two of x, y and z specifies the third uniquely. A *loop* is a quasigroup L with a unique two-sided identity element. A *Moufang loop* is a loop M satisfying the identity $((xy)x)z = x(y(xz))$. If there exists a smallest positive integer n such that $x^n = 1$ for every x in M, we will write $\exp(M) = n$ (M has exponent n).

The *nucleus*, $\mathrm{Nuc}\,(M)$, of a Moufang loop M is the normal subloop of all elements that associate with all pairs of elements from M. That is, $\mathrm{Nuc}\,(M) := \{x \in M : \forall\, y, z \in M (xy)z = x(yz)\}$. The *Moufang center*, $C(M)$, of a Moufang loop M is the (not necessarily normal)

Received by the editors on March 6, 1996, and in revised form on January 12, 1998.

subloop of all elements that commute with every element in M. That is, $C(M) := \{x \in M : \forall\, y \in M, xy = yx\}$. The *center*, $Z(M)$, of a Moufang loop M is the normal subloop of all central, nucleus elements. That is, $Z(M) := C(M) \cap \mathrm{Nuc}\,(M)$. An *autotopism* on a Moufang loop M is a triple (U, V, W) of bijections on M such that, for every x, y in M, $(xU)(yV) = (xy)W$.

Given a Moufang loop M, for every $m \in M$, the following two set maps are bijections:

$$R(m) : M \longrightarrow M; \quad x \mapsto xm$$
$$L(m) : M \longrightarrow M; \quad x \mapsto mx.$$

The $R(m)$ and $L(m)$ generate a subgroup of the group of all bijections on M, called the (full) *multiplication group* $MltM$ of M:

$$MltM := \langle R(m), L(m) : m \in M \rangle_{M!}.$$

Given two Moufang loops M and N with $M \leq N$, the *relative multiplication group*, $Mlt_N M$ of M in N is the subgroup of the group of all bijections on N generated by the $R(m)$ and $L(m)$ as m ranges through the subloop M:

$$Mlt_N M := \langle R(m), L(m) : m \in M \rangle_{N!}.$$

There is an involutory automorphism J on $Mlt_N M$, defined on generators by

$$R(x)^J = L(x^{-1}) \quad \text{and} \quad L(x)^J = R(x^{-1}). \tag{1.1}$$

2. Glauberman's ρ extended. Glauberman showed that if $\mathrm{Nuc}\,(M) = 1$, then $MltM$ admits an automorphism ρ of order three, defined on generators by

$$L(x)^\rho = R(x), \quad R(x)^\rho = P(x) \quad \text{and} \quad P(x)^\rho = L(x), \tag{2.1}$$

where $P(x) = R(x^{-1})L(x^{-1})$. Together with the involutory automorphism J given by (1.1), this ρ generates the symmetric group on three symbols [**3**, Theorem 6].

It is natural to attempt to extend Glauberman's result by asking whether other Moufang loop multiplication groups admit an order three automorphism ρ satisfying (2.1). The general question becomes: given two Moufang loops M and N, with $M \leq N$, does $Mlt_N M$ admit Glauberman's order three automorphism ρ satisfying (2.1)? Lemma 1 gives two necessary conditions.

Lemma 1. *$Mlt_N M$ admits Glauberman's ρ only if both*

(a) $\exp[M \cap C(N)] = 3$ *and*

(b) $[M \cap \mathrm{Nuc}\,(N)] \leq C(M)$.

Proof. (a) Let $x \in [M \cap C(N)]$. This means that $L(x) = R(x)$. Since Glauberman's ρ is defined on $Mlt_N M$, we must have $L(x)^\rho = R(x)^\rho$. That is, we must have $R(x) = P(x)$. This in turn implies $x^3 = 1$.

(b) Let $x \in [M \cap \mathrm{Nuc}\,(N)]$. Then, for every $y \in M$, we have $L(x)L(y) = L(yx)$. Since Glauberman's ρ is defined on $Mlt_N M$, we have $L(x)^\rho L(y)^\rho = L(yx)^\rho$. That is, we must have $R(x)R(y) = R(yx)$. This implies that $xy = yx$. Thus, $x \in C(M)$.

One consequence of Lemma 1 is that Glauberman's ρ is defined on the full multiplication group $MltM$ only if both $\exp[C(M)] = 3$ and $\mathrm{Nuc}\,(M) = Z(M)$. In particular, if M is a group, $MltM$ admits Glauberman's ρ only if M is abelian of exponent 3.

In view of Lemma 1, we will restrict our attention to those multiplication groups $Mlt_N M$ with $\exp[M \cap C(N)] = 3$ and with $[M \cap \mathrm{Nuc}\,(N)] \leq C(M)$. In this case define a map ρ^* on the generators of $Mlt_N M$ by

$$(2.2) \qquad L(x)^{\rho^*} = R(x), \quad R(x)^{\rho^*} = P(x) \quad \text{and} \quad P(x)^{\rho^*} = L(x).$$

(Note: to define ρ^*, $\exp[M \cap C(N)] = 3$ is the only necessary condition.) We must decide if ρ^* extends homomorphically to all of $Mlt_N M$. Note that ρ^* extends homomorphically if and only if

$$(2.3) \qquad Q_1(x_1)Q_2(x_2)\cdots Q_n(x_n) = 1$$

implies

$$Q_1(x_1)^{\rho^*} Q_2(x_2)^{\rho^*} \cdots Q_n(x_n)^{\rho^*} = 1$$

where each $Q_i(x_i)$ is either $R(x_i)$ or $L(x_i)$. Applying Lemma 2.1 in Section 7 of [**1**] to the following autotopism on N,

$$[Q_1(x_1)Q_2(x_2)\cdots Q_n(x_n), Q_1(x_1)^{\rho^*}Q_2(x_2)^{\rho^*}\cdots Q_n(x_n)^{\rho^*}, \\ Q_1(x_1)^{J\rho^*}Q_2(x_2)^{J\rho^*}\cdots Q_n(x_n)^{J\rho^*}]$$

yields

$$Q_1(x_1)Q_2(x_2)\cdots Q_n(x_n) = 1 \tag{2.4}$$

implies

$$Q_1(x_1)^{\rho^*}Q_2(x_2)^{\rho^*}\cdots Q_n(x_n)^{\rho^*} = R(c)$$

for some $c \in [\mathrm{Nuc}\,(N) \cap \langle x_1, x_2, \ldots, x_n\rangle]$. Thus, ρ^* extends homomorphically to all of $Mlt_N M$ if and only if $c = 1$ in (2.4). This proves

Theorem 2. *If* $[M \cap \mathrm{Nuc}\,(N)] = 1$, *then* ρ^* *extends to Glauberman's* ρ *on* $Mlt_N M$. (*Of course, the special case* $M = N$ *yields precisely Theorem* 6 *in* [**3**].)

Not surprisingly, Moufang central elements of exponent three are also of special interest.

Theorem 3. *If* $M \le C(N)$ *and if* $\exp(M) = 3$, *then* ρ^* *extends to Glauberman's* ρ *on* $Mlt_N M$. (*So, in particular, if* M *is a commutative Moufang loop of exponent three, then* $MltM$ *is with triality.*)

Proof. In this case, ρ^* acts trivially and so extends to $\rho = 1$ in (2.1).

Theorems 2 and 3 suggest the following.

Theorem 4. *If Glauberman's* ρ *is defined on* $Mlt_N L$ *for some subloop* L *of* M (*for instance, if* $L \cap \mathrm{Nuc}\,(N) = 1$), *and if* $M \approx H \times L$, *for some subloop* $H \le [M \cap Z(N)]$ *with* $\exp(H) = 3$, *then* ρ^* *extends to Glauberman's* ρ *on* $Mlt_N M$. (*Note that if* $M = N$, $H = Z(M)$ *and*

$M \approx H \times L$, a situation we will be interested in later, we must have Nuc$(L) = 1$*, by Lemma* 1.)

Proof. Each element in $Mlt_N M$ can be written as $R(z_1)R(z_2)\cdots R(z_m)Q_1(x_1)Q_2(x_2)\cdots Q_n(x_n)$, where each $z_i \in H$ and each $x_i \in L$. So here the antecedent in (2.3) translates to $R(z_1)R(z_2)\cdots R(z_m)Q_1(x_1) \times Q_2(x_2)\cdots Q_n(x_n) = 1$. This can be rewritten as $R(z_1z_2\cdots z_m)Q_1(x_1) \times Q_2(x_2)\cdots Q_n(x_n) = 1$. Since H and L intersect trivially, we must have $z_1z_2\cdots z_m = 1$. And so we have $Q_1(x_1)Q_2(x_2)\cdots Q_n(x_n) = 1$. Since Glauberman's ρ is defined on $Mlt_N L$ we must have $Q_1(x_1)^{\rho^*}Q_2(x_2)^{\rho^*} \cdots Q_n(x_n)^{\rho^*} = 1$. Finally, since $\exp(H) = 3$, we have $R(z_1)^{\rho^*}R(z_2)^{\rho^*}\cdots R(z_m)^{\rho^*}Q_1(x_1)^{\rho^*}Q_2(x_2)^{\rho^*}\cdots Q_n(x_n)^{\rho^*} = R(z_1)R(z_2)\cdots R(z_m) = R(z_1z_2 \cdots z_m) = 1$.

There is a general relationship between the existence of Glauberman's ρ on $MltM$ and the existence of Glauberman's ρ on the relative multiplication groups involving M.

Theorem 5. *The following are equivalent.*

(a) *Glauberman's ρ is defined on $MltM$.*

(b) *Glauberman's ρ is defined on $Mlt_N M$ for every Moufang loop N with $M \leq N$.*

(c) *Glauberman's ρ is defined on $Mlt_M L$ for every subloop L of M.*

Proof. (a) $\rightarrow$ (b). We must show $c = 1$ in (2.4). Note that if $Q_1(x_1)Q_2(x_2)\cdots Q_n(x_n) = 1$ in $Mlt_N M$, then $Q_1(x_1)Q_2(x_2)\cdots Q_n(x_n) = 1$ in $MltM$ also. And, since Glauberman's ρ is defined on $MltM$, we must have $Q_1(x_1)^{\rho^*}Q_2(x_2)^{\rho^*}\cdots Q_n(x_n)^{\rho^*} = 1$ in $MltM$. This means that, for every $m \in M$, we have

$$mQ_1(x_1)^{\rho^*}Q_2(x_2)^{\rho^*}\cdots Q_n(x_n)^{\rho^*} = m. \tag{2.5}$$

By (2.4), $Q_1(x_1)^{\rho^*}Q_2(x_2)^{\rho^*}\cdots Q_n(x_n)^{\rho^*} = R(c)$ in $Mlt_N M$, for some

$c \in [\mathrm{Nuc}\,(N) \cap \langle x_1, x_2, \dots, x_n \rangle]$. Thus,

$$\begin{aligned} c &= 1R(c) \\ &= 1Q_1(x_1)^{\rho^*} Q_2(x_2)^{\rho^*} \cdots Q_n(x_n)^{\rho^*} && \text{(considered in } Mlt_N M) \\ &= 1Q_1(x_1)^{\rho^*} Q_2(x_2)^{\rho^*} \cdots Q_n(x_n)^{\rho^*} && \text{(considered in } MltM) \\ &= 1 && \text{(by (2.5)).} \end{aligned}$$

(b) $\to$ (c). Take $N = M$, so that Glauberman's ρ is defined on $MltM$. Glauberman's ρ on $Mlt_M L$ is simply the restriction of Glauberman's ρ on $MltM$ to $Mlt_M L$.

(c) $\to$ (a). Take $L = M$.

3. Groups with triality. Motivated by Glauberman's work, Doro [**2**] calls a group G a *group with triality* if it admits two automorphisms J and ρ such that

(3.1) $\quad J^2 = 1,$

(3.2) $\quad \rho^3 = 1,$

(3.3) $\quad \rho J \rho J = 1,\quad$ (that is, ρ and J generate the symmetric group on three symbols)

(3.4) $\quad \forall\, g \in G, \quad g^{-1} g^J g^{-\rho} g^{J\rho} g^{-\rho\rho} g^{\rho J} = 1,$

and

(3.5) $\quad \langle g^{-1} g^{\theta} : g \in G, \theta \in \langle J, \rho \rangle \rangle = G.$

Equations (3.1)–(3.3) are obvious generalizations of Glauberman's work. Though less obvious, (3.4) and (3.5) are also generalizations of Glauberman's work. In any event, Doro's groups with triality are related to the class of Moufang loops by virtue of their status as progeny of Glauberman's work. This relationship is even more fundamental. Doro showed that each Moufang loop is realizable as the loop transversal to the stabilizer subgroup of the automorphism J of some group with triality. Conversely, from each group with triality, Doro showed that a unique Moufang loop is so realizable.

If Glauberman's ρ is defined on $Mlt_N M$, then it is routine to check that ρ together with J make $Mlt_N M$ a group with triality. Although there could be other automorphisms defined on $Mlt_N M$ making it a group with triality, we are concerned here only with J and ρ. Hence, since $Mlt_N M$ automatically admits the involutory J, see Section 1, we will abuse the language and say that $Mlt_N M$ is with or without triality, according to whether it does or does not admit precisely the automorphism ρ given by (2.1). Doro [**2**, Corollary 5] noted that $MltM$ is with triality in the event that $\mathrm{Nuc}\,(M) = 1$. But, unfortunately, not all Moufang loop multiplication groups are with triality. The results from Section 2 give general conditions under which $Mlt_N M$ is (or is not) a group with triality. For instance, Theorem 2 tells us that if $[M \cap \mathrm{Nuc}\,(N)] = 1$, then $Mlt_N M$ is a group with triality, while Lemma 1 tells us that if there is an $x \in [M \cap C(N)]$ with $x^3 \neq 1$, then $Mlt_N M$ is not with triality.

4. Conclusion. We have enlarged the class of Moufang loop multiplication groups $Mlt_N M$ with known triality status by considering which of them admit Glauberman's special automorphism ρ. In particular, we have generalized Corollary 5 in [**2**] by determining the triality status of $MltM$ for a rather general and large class of Moufang loops. To wit, let $\mathbf{K}$ be the class of Moufang loops, M, such that

$$1 < Z(M) \leq C(M) < M, \tag{4.1}$$

$$\exp[C(M)] = 3, \tag{4.2}$$

and

$$M \not\approx Z(M) \times L, \quad \text{some subloop } L. \tag{4.3}$$

Let $\underline{\mathbf{K}}$ be the (rather general and large) class of those Moufang loops that are not members of $\mathbf{K}$.

Theorem 6. *For a Moufang loop M belonging to $\underline{\mathbf{K}}$, $MltM$ is with triality if and only if*

$$Z(M) = \mathrm{Nuc}\,(M), \tag{4.4}$$

$$\exp[C(M)] = 3, \tag{4.5}$$

and

$$M \approx Z(M) \times L, \quad \textit{for some subloop } L \\ \textit{with} \quad \mathrm{Nuc}\,(L) = 1; \quad \textit{or} \quad C(M) = M. \tag{4.6}$$

Proof. If $C(M) = M$, Theorem 3 establishes sufficiency. If $\mathrm{Nuc}\,(L) = 1$, then Theorems 2 and 4 establish sufficiency. Lemma 1 establishes the necessity of both (4.4) and (4.5). This, together with restriction to $\underline{\mathbf{K}}$, establishes the necessity of $Z(M)$ appearing as a direct factor of M in some factorization (in the event that $C(M) < M$). This in turn implies that $\mathrm{Nuc}\,(L) \leq \mathrm{Nuc}\,(M)$. But $\mathrm{Nuc}\,(M) = Z(M)$, which intersects L trivially. This establishes the necessity of $\mathrm{Nuc}\,(L) = 1$.

Theorem 6 underscores the fundamental roles played by commutative Moufang loops of exponent three and by Moufang loops with trivial nucleus in the general theory of Moufang loops.

REFERENCES

1. R.H. Bruck, *A survey of binary systems*, Springer-Verlag, Heidelberg, 1958.

2. S. Doro, *Simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **83** (1978), 377–392.

3. G. Glauberman, *On loops of odd order* II, J. of Algebra **8** (1968), 383–414.

Department of Mathematical Sciences, St. Mary's College, Moraga, California 94575
E-mail address: phillips@stmarys-ca.edu