1992

Combinatorial triality and representation theory

Jon Douglas Phillips Jr.

Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/rtd

Part of the Mathematics Commons

Recommended Citation

https://lib.dr.iastate.edu/rtd/9946

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Retrospective Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
Combinatorial triality and representation theory

Phillips, Jon Douglas, Jr., Ph.D.
Iowa State University, 1992
Combinatorial triality
and representation theory

by

Jon Douglas Phillips, Jr.

A Dissertation Submitted to the
Graduate Faculty in Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY
Major: Mathematics

Approved:

In Charge of Major Work

Members of the Committee:

For the Major Department

For the Graduate College

Iowa State University
Ames, Iowa

1992
TABLE OF CONTENTS

INTRODUCTION 1
Explanation of Dissertation Format 2

PART I. THE ENDOCENTER AND ITS APPLICATIONS
TO QUASIGROUP REPRESENTATION THEORY 3

ABSTRACT
1. INTRODUCTION 4
2. MULTIPLICATION GROUPS 5
3. THE ENDOCENTER 8
4. A FUNCTORIAL CENTER 9
5. WHEN IS $U(G; HSP(G)) \cong \text{Mit } G$? 11
6. WHEN IS $U(G; HSP(G)) \not\cong \text{Mit } G$? 12
REFERENCES 14

PART II. MOUFANG LOOPS AND GROUPS
WITH BIALITY 15

ABSTRACT
1. INTRODUCTION 16
2. BASIC DEFINITIONS 17
3. MULTIPLICATION GROUPS 18
4. MULTIPLICATION GROUPS OF LOOPS 21
5. GROUPS WITH TRIALITY 22
6. GROUPS WITH BIALITY 24
7. GELFAND PAIRS 27
8. LOOP RINGS 26
9. THE MOUFANG LOOP CONSTRUCTION 28
10. CLASSIFICATION THEOREMS 30
REFERENCES 33
INTRODUCTION

The theory of quasigroup representations is laid out clearly and elegantly in [Sm]. It is shown there that the representations of a quasigroup $Q$ in a variety $V$ of quasigroups containing $Q$ are equivalent to the representations of quotients of group algebras of stabilizers in a particular group, namely $U(Q;V)$, the universal multiplication group of $Q$ in $V$. Thus, a large component of quasigroup representation theory is the study of these universal multiplication groups. The $U(Q;V)$ are variety dependent in the sense that, for fixed $Q$, as the variety $V$ changes, so too does $U(Q;V)$. Basically, the rule is that, "the smaller the variety, the smaller the universal multiplication group," with the caveat that "a universal multiplication group can be no smaller than the combinatorial multiplication group." Part I of this dissertation is concerned with classifying those groups $Q$ for which $U(Q;HSP(Q)) \cong \text{Mlt } Q$. The main tool in this investigation is a new subgroup, the endocenter. In addition to facilitating the identification of universal multiplication groups, the endocenter is a "functorial center".

In [Gl], Glauberman showed that if $M$ is a Moufang loop with trivial nucleus, then there is a special automorphism $\rho$ of order three defined on $\text{Mlt } M$, the combinatorial multiplication group of $M$. In [Do], Doro generalized Glauberman's result by defining the class of groups with triality. The key ingredient in a group with triality is an automorphism $\rho$ of order three that behaves as in Glauberman. There are strong relationships between groups with triality and Moufang loops. Parts III and IV of this dissertation investigate some of these relationships. Specifically, we give a partial classification of those Moufang loops whose combinatorial multiplication group is with triality. We completely characterize all groups with triality.
associated with cyclic groups. We also identify some universal multiplication groups of Moufang loops and determine their triality status. Since the class of groups with triality is not a variety, we axiomatize the variety of "triality groups", and initiate an algebraic investigation of this (and related) varieties. There are also strong geometric connections between Moufang loops and groups with triality [BS]. We investigate some of these connections.

One weakness with the theory of groups with triality is that many of the groups included in the theory are not themselves groups with triality. For instance, there are many Moufang loops whose combinatorial multiplication group is not a group with triality, even though the multiplication group is itself a natural homomorphic image of at least one group with triality. To overcome this deficiency, we define the class of groups with biality in Part II of this thesis. The class of groups with biality is a more general setting from which to study Moufang loops than is the class of groups with triality. For instance, the class of groups with biality is large enough so that it includes both the class of groups with triality and the class of multiplication groups of Moufang loops. But is it tight enough to provide a natural setting from which to study Moufang loops. This class of groups also helps in offering complete classifications of multiplication groups of various classes of inverse property loops.

Explanation of Dissertation Format

This thesis consists of four parts. Part I appeared as "The endocenter and its applications to quasigroup representation theory," in Commentationes Mathematicae Universitatis Carolinae 32, 3 (1991) 417–422. Part II of this thesis was submitted for publication in the Canadian Journal of Mathematics. Parts III and IV of this thesis are parts of larger projects that will be submitted to scholarly journals for publication. Following Part IV is a general summary. The references cited in the general Introduction and the General Summary follow the General Summary.
PART I: THE ENDOCENTER AND ITS APPLICATIONS
TO QUASIGROUP REPRESENTATION THEORY
ABSTRACT

A construction is given, in a variety of groups, of a “functorial center” called the endocenter. The endocenter facilitates the identification of universal multiplication groups of groups in the variety, addressing the problem of determining when combinatorial multiplication groups are universal.
1. INTRODUCTION

The theory of quasigroup modules, or quasigroup representation theory, is equivalent to the representation theory of quotients of group algebras of certain groups associated with quasigroups; namely, the stabilizers in the so-called universal multiplication groups (cf. [Sm, p. 56] and below). Universal multiplication groups give functors from varieties of quasigroups to the variety of groups. To help identify these universal multiplication groups we offer a construction (in varieties of groups) of a subgroup we call the endocenter. This endocenter itself gives a functor from varieties of groups to the variety of abelian groups. To a certain extent, the endocenter may be regarded as a "functorial center". We also identify some universal multiplication groups, most notably in $\text{HSP}(G)$, the variety generated by a group $G$.

2. MULTIPLICATION GROUPS

For a quasigroup $Q$ and for any $q \in Q$, the maps

$$R(q): Q \to Q; \quad x \mapsto xq$$

and

$$L(q): Q \to Q; \quad x \mapsto qx$$

are set bijections. As such, they generate a subgroup of the symmetric group $Q!$ on $Q$. This subgroup is the (combinatorial) multiplication group $\text{Mlt} Q$ of $Q$; i.e. $\text{Mlt} Q = \langle R(q), L(q) : q \in Q \rangle_{Q!}$. Unfortunately $\text{Mlt}$ (which assigns $\text{Mlt} Q$ to $Q$) does not extend suitably to homomorphisms to give a functor [Sm. p. 28]. To overcome this failure, consider the following construction.

Suppose we have a quasigroup $Q$ and an arbitrary variety $V$ of quasigroups containing $Q$. The category whose objects are quasigroups in $V$ and whose morphisms are quasigroup homomorphisms will also be denoted by $V$. As an algebraic category, $V$ is complete and co-complete [HS, 13.12, 13.14]. In $V$, form the coproduct of
Q with \( \langle x \rangle \), the free \( \mathbf{V} \)-algebra on one generator. Denote this coproduct by \( Q \ast \langle x \rangle \). Since \( Q \) may be identified with its image in \( Q \ast \langle x \rangle \) [Sm, p. 33], we can consider the subgroup of the combinatorial multiplication group of \( Q \ast \langle x \rangle \) generated by right and left multiplications by elements of \( Q \). This subgroup is the universal multiplication group \( U(Q; V) \) of \( Q \) in \( V \); i.e. \( U(Q; V) = \langle R(q), L(q) : q \in Q \rangle (Q \ast \langle x \rangle) \).

Remarks.

1. The assignment of \( U(Q; V) \) to \( Q \) gives the promised functor from the category \( V \) to the category \( \mathbf{Gp} \) of all groups [Sm, p. 34].

2. \( U(Q; V) \) is variety dependent in the sense that, for a given quasigroup \( Q \) and varieties \( V_1 \) and \( V_2 \) containing \( Q \), it is not necessarily the case that \( U(Q; V_1) = U(Q; V_2) \) [Sm, p. 36].

3. If \( V_1 \subseteq V_2 \) then there is a natural group epimorphism \( F : U(Q; V_2) \twoheadrightarrow U(Q; V_1) \) [Sm, p. 55].

4. For any variety \( V \) of quasigroups containing \( Q \), there is a natural group epimorphism \( H : U(Q; V) \twoheadrightarrow \text{Mlt} \, Q \) [Sm, p. 55].

Remark 3 can be phrased as: “The smaller the variety, the smaller the universal multiplication group”. Remark 4 can be phrased as: “A universal multiplication group can be no smaller than the combinatorial multiplication group”. Since the smallest variety containing \( Q \) is just \( \mathsf{HSP}(Q) \), it would be natural to ask whether \( U(Q; \mathsf{HSP}(Q)) \cong \text{Mlt} \, Q \), i.e. whether the combinatorial multiplication group is universal. Since lack of associativity leads to complications, we will concentrate on the “easy” case of groups. Thus, from now on \( G \) will denote a group and \( V \) an arbitrary variety of groups containing \( G \). In particular, \( V \) could be \( \mathsf{HSP}(G) \) but it is not required to be so. Theorem 5 below gives a sufficient condition for \( U(G; \mathsf{HSP}(G)) \cong \text{Mlt} \, G \). On the other hand, Theorems 6 and 7 furnish examples of groups with \( U(G; \mathsf{HSP}(G)) \not\cong \text{Mlt} \, G \).

For a group \( G \) the combinatorial multiplication group \( \text{Mlt} \, G \) is given by the exact
sequence

\[ 1 \rightarrow Z(G) \xrightarrow{\Delta} G \times G \xrightarrow{F} \text{Mlt } G \rightarrow 1, \]

where \( \Delta \) is the diagonal embedding given by \( \Delta: Z(G) \rightarrow G \times G; z \mapsto (z, z) \), and where \( F \) is the group epimorphism given by \( F: G \times G \rightarrow \text{Mlt } G; (g_1, g_2) \mapsto L(g_1^{-1})R(g_2) \). Thus,

(1) \[ \text{Mlt } G \cong (G \times G)/\hat{Z}, \]

where \( \hat{Z} = Z(g)\Delta \). Next, we define the group epimorphism \( T: G \times G \rightarrow U(G; V); \) \( (g_1, g_2) \mapsto L(g_1^{-1})R(g_2) \). Clearly

(2) \[ U(G; V) \cong (G \times G)/\text{Ker } T. \]

The map \( T \) will play a prominent role throughout, as will its kernel, \( \text{Ker } T \). By (1) and (2) it is clear that:

(3) \[ \text{If Ker } T = \hat{Z}, \text{ then } U(G; V) \cong \text{Mlt } G. \]

Thus, we note that since \( G \) embeds naturally in \( G \ast \langle x \rangle \), it is always the case the

(4) \[ \text{Ker } T \leq \hat{Z}. \]

This discussion leads to two results:

**Proposition 1.** If \( G \) is an abelian group and \( V \) is any variety of abelian groups containing \( G \), then \( \text{Ker } T = \hat{Z} \) (and hence \( U(G; V) \cong \text{Mlt } G \) by (3)).

**Proposition 2.** If \( G \) is a group such that \( Z(G) = 1 \) and \( V \) is any variety of groups containing \( G \), then \( \text{Ker } T = \hat{Z} \) (and hence \( U(G; V) \cong \text{Mlt } G \) by (3)).
3. THE ENDOCENTER

In the study of these universal multiplication groups (of groups), attention focuses on the behavior of the subgroup $\text{Ker} T$. If $\text{Ker} T = \hat{Z}$ then we have seen that $U(G; V) \cong \text{Mlt} G$. If $\text{Ker} T < \hat{Z}$, and if $G$ satisfies suitable finiteness conditions (most trivially, if $G$ is finite), then we will see that $U(G; V) \not\cong \text{Mlt} G$. An intrinsic description of $\text{Ker} T$ would clearly be beneficial. Towards that end we offer the following

**Definition.** The *endocenter*, $Z(G; V)$, of a group $G$ in a variety $V$ of groups is defined to be:

$$Z(G; V) = \bigcap_{G \leq H \in V} Z(H).$$

The relevance of this definition to representation theory, especially to the study of universal multiplication groups, is seen in

**Theorem 3.** $Z(G; V)\Delta = \text{Ker} T$.

**Proof.** First note that $Z(G; V) \leq Z(G * (x))$ since $G * (x) \in V$ and $G \leq G * (x)$. This means that if $g \in Z(G; V)$, then for every $t \in G * (x)$ we have $g^{-1}tg = t$, i.e. $(g, g) \in \text{Ker} T$. Therefore, $Z(G; V)\Delta \leq \text{Ker} T$.

Conversely, if $(g, g) \in \text{Ker} T$ and $H \in V$ with $G \leq H$ we need to show that $g \in Z(H)$. So given $h \in H$, we need to show $g^{-1}hg = h$. If we let $f: G \rightarrow H$ be the inclusion map, and $k: (x) \rightarrow H$ be determined by mapping $x \mapsto h$, then since $G^*(x)$ is a $V$-coproduct, there exists a unique group homomorphism $F: G^*(x) \rightarrow H$ such
that the following diagram commutes:

\[
\begin{array}{ccc}
G & \xrightarrow{f} & G * \langle x \rangle \\
\downarrow & & \uparrow \\
H & \xleftarrow{k} & H
\end{array}
\]

Since \((g, g) \in \text{Ker} \, T\), we have \(g^{-1}xg = x\). Thus,

\[
F(g^{-1}xg) = F(x), \quad \text{which implies}
\]

\[
F(g^{-1})F(x)F(g) = F(x), \quad \text{which implies}
\]

\[
f(g^{-1})k(x)f(g) = k(x), \quad \text{and so}
\]

\[
g^{-1}hg = h,
\]

as desired. Therefore, \(\text{Ker} \, T \leq Z(G; V)\Delta\); and hence, \(\text{Ker} \, T = Z(G; V)\Delta\). \(\square\)

**Remark.** In light of Theorem 3, we can recast (3) in the following form:

\[(5) \quad \text{If } Z(G, V) = Z(G), \text{ then } U(G; V) \cong \text{Mlt } G.\]

4. **A FUNCTORIAL CENTER**

The usual center of a group is not a functorial construction. By contrast, the endocenter is natural:

**Theorem 4.** \(Z(\ ; V)\) is a functor from \(V\) to \(\text{Gp}\).

**Proof.** Given a group homomorphism \(f: G \to H\), define \(Z(f; V)\) to be the restriction of \(f\) to \(Z(G; V)\). So if \(g \in Z(G; V)\), we must show that \(f(g) \in Z(H; V)\),
i.e. we must show that for a group $K \in \mathbb{V}$ with $H \leq K$ we have $f(g) \in Z(K)$. Hence, given $k \in K$, we must show that $f(g)^{-1}k f(g) = k$. Towards that end, define $h: \langle x \rangle \to K$ to be the unique group homomorphism determined by mapping $x \mapsto k$. Let $i: H \to K$ be the inclusion map. Since $G * \langle x \rangle$ is a $\mathbb{V}$-coproduct, there exists a unique group homomorphism $F: G * \langle x \rangle \to K$ such that the following diagram commutes:

\[
\begin{array}{ccc}
G & \longrightarrow & G * < x > \\
\downarrow f & & \downarrow \text{F} \\
H & \longrightarrow & \langle x \rangle \\
i & \downarrow & h \\
K & & \\
\end{array}
\]

Now $g \in Z(G; \mathbb{V})$ implies that $g \in Z(G * \langle x \rangle)$, so that

\[
g^{-1}xg = x, \quad \text{which implies} \quad F(g^{-1}xg) = F(x), \quad \text{which implies} \quad F(g^{-1})F(x)F(g) = F(x), \quad \text{which implies} \quad f(g^{-1})h(x)f(g) = h(x), \quad \text{which implies} \quad f(g)^{-1}kf(g) = k.
\]

Thus $f(g) \in Z(K)$, and hence $f(g) \in Z(H; \mathbb{V})$. It is now easy to check that $Z(f; \mathbb{V}): Z(G; \mathbb{V}) \to Z(H; \mathbb{V})$ is a group homomorphism and that $Z(\cdot; \mathbb{V})$ is a functor. □

**Corollary.** $Z(G; \mathbb{V})$ is fully invariant in $G$. 
Proof. Suppose \( f : G \to G \) is a group endomorphism. By functorality, \( Z(f; V) \) is a group homomorphism from \( Z(G; V) \) to \( Z(G; V) \). But \( Z(f; V) = f|_{Z(G; V)} \), so that \( f \) maps \( Z(G; V) \) to \( Z(G; V) \). □

5. WHEN IS \( U(G; HSP\{G\}) \cong \text{Mlt} \ G \)?

Anticipating the next theorem, we recall the definition of a verbal subgroup: a subgroup \( H \) of a group \( G \) is verbal if there exists a set \( W \) of words such that \( H = \langle w(g_1, \ldots) : g_i \in G, w \in W \rangle \) [Ne, p. 5]. In the event that \( V = HSP\{G\} \), Propositions 1 and 2 are special cases of

Theorem 5. If the center \( Z(G) \) of a group \( G \) is verbal, then \( Z(G; HSP\{G\}) = Z(G) \). Thus, by (5), \( U(G; HSP\{G\}) \cong \text{Mlt} \ G \).

Proof. Since \( Z(G) \) is a verbal subgroup, there exists a set \( W \) of words such that \( Z(G) = \langle w(g_1, \ldots) : g_i \in G, w \in W \rangle \). Thus, for every \( w \in W \),

\[(6) [y, w(x_1, \ldots)] = 1\]

is an identity in \( G \). By Birkhoff's Theorem (6) is an identity in every group \( H \) in \( HSP\{G\} \), in particular in those \( H \) for which \( G \leq H \). So, given \( g \in Z(G) \), since \( g = w_g(g_1, \ldots) \) for some \( g_i \in G, w_g \in W \), and since \( [y, w_g(x_1, \ldots)] = 1 \) is an identity in \( H \), we know that \( [y, g] = [y, w_g(g_1, \ldots)] = 1 \) for every \( y \in H \). Thus, \( g \in Z(H) \), i.e. \( g \in Z(G; HSP\{G\}) \). Hence, \( Z(G) \leq Z(G; HSP\{G\}) \) and we have \( Z(G) = Z(G; HSP\{G\}) \), as desired. □

Many familiar groups have verbal centers. For instance abelian groups, simple groups, free groups, symmetric groups, and dihedral groups all have verbal centers. Such groups constitute a fairly large class of groups, and in light of Cayley's theorem and the fact that every group is the homomorphic image of a free group, one might be tempted to think that perhaps \( U(G; HSP\{G\}) \cong \text{Mlt} \ G \) for every group \( G \).
Before dispelling this notion, we recall the definition of Hopfian: a group \( G \) is said to be **Hopfian** if it is not isomorphic to a proper quotient of itself [Rb, p. 159].

6. WHEN IS \( U(G; \text{HSP}\{G\}) \not\approx \text{Mlt } G \)?

**Theorem 6.** If \( G \) is a group such that:

(a) \( 1 < Z(G) < G \);

(b) \( \text{HSP}\{G\} = \text{Gp} \); and

(c) \( G \times G \) is Hopfian,

then \( \text{Mlt } G \not\approx U(G; \text{HSP}\{G\}) \).

**Proof.** Here we use a fact proved in [Sm, p. 35]. Namely, \( U(G; \text{Gp}) \cong G \times G \). So suppose on the contrary that \( U(G; \text{HSP}\{G\}) \cong \text{Mlt } G \). Then

\[
G \times G \cong U(G; \text{Gp})
= U(G; \text{HSP}\{G\}) \quad \text{[by (b)]}
\cong \text{Mlt } G \quad \text{[by assumption]}
\cong (G \times G)/\hat{Z} \quad \text{by (1)}.
\]

This contradicts the Hopfian property of \( G \times G \). Therefore, \( U(G; \text{HSP}\{G\}) \not\approx \text{Mlt } G \). \( \square \)

To see that there are groups which satisfy the hypotheses of Theorem 6, consider the following

**Example.** Let \( G = \langle x, y, z : [x, z] = [y, z] = 1 \rangle \); i.e \( G \) is the direct product of the free group \( \langle x, y \rangle \) on two generators with the free (abelian) group \( \langle z \rangle \) on one generator.

We note that:

(a) \( 1 < Z(G) < G \) (since \( Z(G) = \langle z \rangle \)).

(b) \( \text{HSP}\{G\} = \text{Gp} \) (since \( \langle x, y \rangle \) is clearly a homomorphic image of \( G \), and
\( \text{HSP}\{\langle x, y \rangle\} = \text{Gp} \) [MKS, p. 413]). And
(c) $G \times G$ is Hopfian (since $G$ is residually finite [MKS, pp. 116, 152] and finitely generated, so too is $G \times G$; and thus $G \times G$ is also Hopfian [MKS, p. 415]). Applying Theorem 6 yields $U(G; HSP(G)) \neq \text{Mlt } G$.

Clearly, groups satisfying the hypotheses of Theorem 6 belong to a restricted class. For instance, such groups must be infinite. The following theorem provides finite groups for which the combinatorial multiplication group is not universal.

**Theorem 7.** If $G$ is a group such that $Z(G)$ is not fully invariant, then $Z(G; V) < Z(G)$. Suppose further that for normal subgroups $N_1, N_2$ of $G$, the proper containment $N_1 < N_2$ implies that $(G \times G)/N_1 \neq (G \times G)/N_2$. Then $U(G; V) \neq \text{Mlt } G$.

**Proof.** By the corollary to Theorem 4, $Z(G; V)$ is fully invariant in $G$. Since we are assuming that $Z(G)$ is not fully invariant, and since $Z(G; V) \leq Z(G)$, we have that $Z(G; V) < Z(G)$ is desired. The final statement follows from the first with $N_1 = Z(G; V)$ and $N_2 = Z(G)$. □

**Example.** The group $G = A_4 \times Z_2$ (the direct product of the alternating group of order 12 with the cyclic group of order two) has center that is not fully invariant [Rb, p. 30]. Being finite, it also satisfies the further hypothesis of the theorem. Thus, $U(G; HSP(G)) \neq \text{Mlt } G$.

**Corollary.** If $G$ is a group with center that is cyclic of prime order, but not fully invariant, and if $V$ is any variety of groups containing $G$, then $Z(G; V) = 1$. Thus by (2) and Theorem 3, $U(G; V) \cong G \times G$.

**Example.** Let $G = \langle a, b, c : a^2 = b^2 = c^2 = 1, [a, b] = [b, c] = 1 \rangle$. Then $G$ is a group with simple, non-fully invariant center $Z(G) = Z_2$ (the cyclic group of order two). Hence $U(G; HSP(G)) \cong G \times G \neq \text{Mlt } G$. 


REFERENCES


PART II: MOUFGANG LOOPS AND GROUPS WITH BIALITY
ABSTRACT

We define the class of groups with biality. This class of groups contains the class of groups with triality [Do], and the class of those groups that are the multiplication group of some Moufang loop. Given a group $G$ with biality, we construct a Moufang loop $T$ on a transversal to a stabilizer subgroup in $G$ such that $\text{Mlt } T$, the multiplication group of $T$, is a homomorphic image of $G$. Conversely, every Moufang loop arises in this fashion from some group with biality. We offer an abstract characterization of multiplication groups of various classes of loops: (right) inverse property loops, (commutative) Moufang loops, Moufang loops of some finite exponent, groups. We also show that if $G$ is a group with biality, then $G$ and the stabilizer subgroup of $G$ form a Gelfand pair, and this leads to a decomposition theorem for the loop ring $C(T)$ and its center.
1. INTRODUCTION

There have been many attempts to understand classes of loops by studying various classes of groups. Barlotti and Strambach [BS] investigate groups associated with the geometry of (Moufang) loops. Scimemi [Sc] and Joyce [Jo] realize (loops principally isotopic) to quasigroups as "loop transversals" [S2] to certain subgroups of special types of groups.

Niemenmaa and Kepka [NK], on the other hand, understand loops (and loop transversals) as special "$H$-connected" transversals to some subgroup $H$ of a group $G$. Griess's [Gr] Moufang loops of exponent two (code loops) arise from doubly even codes (i.e. certain abelian groups). Doro [Do] realizes Moufang loops as transversals to certain subgroups of groups he calls "groups with triality".

In this paper, we offer a generalization of Doro's work. This generalization provides a natural setting from which to study Moufang loops and takes the form of a construction in the spirit of Niemenmaa-Kepka [NK] and Doro [Do]. And (at least for the "odd order case") this construction can be considered from within the context of Scimemi's [Sc] and Joyce's [Jo] constructions.

Specifically, we define the class of "groups with biality." Given any group $G$ in this class, there is a binary operation $+$ on a transversal $T$ to a certain subgroup in $G$, making $(T, +)$ a Moufang loop. Further, the multiplication group $\text{Mlt } T$, of $T$, is a natural homomorphic image of $G$. This leads to an abstract characterization of those groups that are the multiplication group of some Moufang loop. We prove similar results for (right) inverse property loops, commutative Moufang loops, Moufang loops of some fixed finite exponent, and groups. Along the way, we show that groups with biality (and the appropriate subgroups) are natural examples of Gelfand pairs, and this leads to a decomposition theorem about the loop ring $C(T)$ and its center.

2. BASIC DEFINITIONS

Quasigroups. A quasigroup is a set $Q$ with a single binary operation $\cdot$ such that in $x \cdot y = z$, knowledge of any two of $x$, $y$ and $z$ specifies the third uniquely. A loop
is a quasigroup \( L \) with an identity element 1 such that \( \forall x \in L, x \cdot 1 = 1 \cdot x = x \). A loop \( L \) is a right inverse property loop if \( \forall x \in L, \exists \mu \in L, \forall y \in L, (y \cdot x) \cdot \mu = y \) (similarly for left inverse property loop). A loop \( L \) is an inverse property loop if \( \forall x \in L, \exists x^{-1} \in L, \forall y \in L, x^{-1} \cdot (x \cdot y) = (y \cdot x) \cdot x^{-1} = y \). A Moufang loop is a loop \( M \) such that \( \forall x, y, z \in M, (\langle z \cdot x \rangle \cdot y) \cdot x = z \cdot (x \cdot (y \cdot x)) \). Given \( a, b \) and \( c \) in a Moufang loop \( M \), if \( (a \cdot b) \cdot c = a \cdot (b \cdot c) \), then the subloop of \( M \) generated by \( a, b \) and \( c \) is actually a group [Mo], [B2, p. 117]. A weaker version of this statement is that Moufang loops are diassociative, i.e., subloops generated by pairs of elements are actually groups. Thus, Moufang loops are inverse property loops.

Loop Transversals. A subset \( T \) of a group \( G \) is said to be a (right) transversal to a subgroup \( S \) of \( G \) if

\[
G = \bigcup_{t \in T} St.
\]

An action of \( G \) on \( T \), restricting to a binary operation \(+\) on \( T \), is defined by

\[
(2.1) \quad t + g = w, \quad \text{where } Stg = Sw.
\]

\( \forall t, u \in T \), the equation \( x + t = u \) has a unique solution \( x \) [S2, §1]. Thus, \( (T, +, 1) \) is a right loop. If the equation \( t + y = u \) also has a unique solution \( y \), then \( T \) is said to be a loop transversal, since in this case, \( (T, +, 1) \) is a loop. If \( (T, +, 1) \) is a Moufang loop, then \( T \) is said to be a Moufang loop transversal.

3. MULTIPLICATION GROUPS

Given a quasigroup \( Q \), for every \( q \in Q \), the following two set maps are bijections:

\[
R(q) : Q \to Q; \quad x \mapsto x \cdot q
\]

\[
L(q) : Q \to Q; \quad x \mapsto q \cdot x.
\]

The \( R(q) \) and \( L(q) \) generate a subgroup of the group of all bijections on \( Q \) called
the *combinatorial multiplication group* \( \text{Mlt} \, Q \), of \( Q \), or more informally, the multiplication group of \( Q \):

\[
\text{Mlt} \, Q := \langle R(q), L(q) : q \in Q \rangle.
\]

The **Universal Multiplication Group**. Let \( Q \) be a quasigroup and let \( V \) be a variety of quasigroups containing \( Q \). The category whose objects are quasigroups in \( V \) and whose morphisms are quasigroup homomorphisms will also be denoted by \( V \). As an algebraic category, \( V \) is complete and co-complete [HS, 13.12, 13.14]. In \( V \), form the coproduct of \( Q \) with \( \langle X \rangle \), the free \( V \)-algebra on one generator. Denote this coproduct by \( Q[X] \). Since \( Q \) may be identified with its image in \( Q[X] \) [S1, p. 33], we consider the subgroup of the combinatorial multiplication group of \( Q[X] \) generated by right and left multiplications by elements of \( Q \). This subgroup is the **universal multiplication group** \( U(Q; V) \) of \( Q \) in \( V \):

\[
U(Q; V) := \langle R(q), L(q) : q \in Q \rangle_{\langle Q[X] \rangle}.
\]

Note that \( \text{Mlt} \, Q \) is a natural homomorphic image of \( U(Q; V) \) via the restriction mapping. Thus, \( U(Q; V) \) has a natural action on \( Q \). The modules of certain quotients of group algebras of stabilizers in \( U(Q; V) \) are exactly the modules of \( Q \) [S1]. Thus, universal multiplication groups play a central role in (quasi)group representation theory [PS]. For instance, [PS] examines situations when \( \text{Mlt} \, M \) is a universal multiplication group, and situations when \( \text{Mlt} \, M \) is not a universal multiplication group. □

Given an inverse property loop \( M \), there is an involutory automorphism

\( J : \text{Mlt} \, M \to \text{Mlt} \, M; \alpha \mapsto J \alpha J \), operating on the generators by \( J : R(x) \mapsto L(x^{-1}), L(x) \mapsto R(x^{-1}) \). If the loop \( M \) is Moufang, there is such a \( J \) defined on \( M[X] \), considered in any variety \( V \) of Moufang loops containing \( M \). The resulting \( J \) restricts to \( U(M; V) \). Thus, when no confusion will arise, when \( M \) is a Moufang
loop we will use $J$ to denote both the involutory automorphism on $\text{Mlt } M$ and the involutory automorphism on $U(M; V)$. Similarly, in either setting let $I = C_G(J)$, and let $T = \{R(x): x \in M\}$.

**Theorem 1.** If $G$ represents either $\text{Mlt } M$ or $U(M; V)$, where $V$ is any variety of Moufang loops containing $M$, then:

(3.1) $T$ is a Moufang loop transversal to $I$ in $G$,

(3.2) $[T, T^{-J}] \leq I$,

(3.3) $\forall g \in T, [g, g^{-J}] = 1$,

(3.4) $\forall g, h \in T, ghg \in T$,

(3.5) $\langle T, T^{-J} \rangle = G$, and

(3.6) $I = \text{Stab}_G(1)$.

**Proof.** (3.2) and (3.3) are direct consequences of the diassociativity of $M$. (3.4) follows from the Moufang law. (3.5) follows by definition. (3.6) is trivial [Cf, (5.8) and Prop. 4]. To prove (3.1) we first prove that $T$ is a loop transversal. By comments after (2.1) is suffices to show that $(T, +)$ is a left loop. So assume $R(x) + R(a) = R(x) + R(b)$.

$$\Rightarrow R(x)R(a)R(b^{-1})R(x^{-1}) \in I$$

$$\Rightarrow ((xa)b^{-1})x^{-1} = 1$$

$$\Rightarrow a = b.$$ 

Now observe that $(T, +)$ is a Moufang loop: by [B2, p. 61] and [S1, p. 40], $R(a) + R(b) = R(ab)$; and so, $((R(x) + R(y)) + R(x)) + R(z) = R(((xy)x)z) = R(x(y(xy)))) = R(x) + (R(y) + (R(x) + R(z)))$. $\square$
4. MULTIPLICATION GROUPS OF LOOPS

In [NK], Niemenmaa and Kepka prove the following:

**Theorem 2.** [NK, Thm. 4.1]) A group $G$ is the multiplication group of a loop iff there is a subgroup $H$ of $G$ with $\text{core}_G(H) = 1$ and with two transversals, $A$ and $B$, to $H$ in $G$ satisfying

\begin{align}
(4.1) & & [A, B] \leq H, \\
(4.2) & & \langle A, B \rangle = G.
\end{align}

Further, Niemenmaa and Kepka implicitly prove (although they don’t formally state) the following:

**Theorem 3.** If $G$ is a group with subgroup $H$ and with two transversals $A$ and $B$ to $H$ in $G$ such that (4.1) and (4.2) hold, then $A$ is a loop transversal. Further, $\text{Mlt} A$ is a natural homomorphic image of $G$.

**Proof.** The multiplication on $A$ is given by (2.1) and the details of showing that this makes $A$ a loop are given in [NK, Thm. 4.1]. □

These two theorems help to put the results from the rest of this paper, especially §6, Theorem 16 and Remark 17, into context. They also lead to classification theorems about multiplication groups of (right) inverse property loops.

**Theorem 4.** A group $G$ is the multiplication group of a right inverse property loop iff there is a subgroup $H$ of $G$ with $\text{core}_G(H) = 1$ and with two transversals, $A$ and $B$, to $H$ in $G$ satisfying (4.1) and (4.2) and such that $A^{-1} = A$.

**Proof.** Define a loop operation $+$ on $A$ by (2.1). So given $a \in A$, we need to find a $\mu \in A$ such that for every $c \in A$, $(c + a) + \mu = c$. Take $\mu = a^{-1}$. The rest of the proof is routine. □
Theorem 5. A group $G$ is the multiplication group of an inverse property loop iff there is a subgroup $H$ of $G$ with $\text{core}_G(H) = 1$ and with two transversals, $A$ and $B$, to $H$ in $G$ satisfying (4.1) and (4.2) and such that $A^{-1} = A$ and $B^{-1} = B$.

Proof. The only nontrivial thing to show is that given $a \in A$, for every $c \in A$, $a^{-1} + (a + c) = c$. First note that there is a $b \in B$ such that $Ha = Hb$ and $Ha^{-1} = Hb^{-1}$. Thus, $ba^{-1} \in H$ and $b^{-1}a \in H$. Let $a + c = d$. So $a cd^{-1} \in H$. Thus, $b cd^{-1} = (ba^{-1})(a cd^{-1}) \in H$. And since $[A, B] \leq H$, we have $cbd^{-1} = (cbc^{-1}b^{-1})(bcd^{-1}) \in H$. Now let $f = a^{-1} + d$. So $a^{-1}df^{-1} \in H$. Thus, $b^{-1}df^{-1} = (b^{-1}a)(a^{-1}df^{-1}) \in H$. And again, since $[A, B] \leq H$, we have $db^{-1}f^{-1} = (db^{-1}d^{-1}b)(b^{-1}df^{-1}) \in H$. Thus, $c f^{-1} = (cbd^{-1})(db^{-1}f^{-1}) \in H$, and hence $Hc = Hf$. But $A$ is a tranversal to $H$, so $c = f$. And this completes the proof since we have shown $a^{-1} + (a + c) = a^{-1} + d = f = c$. □

5. GROUPS WITH TRIALITY

Glauberman [Gl] showed that if $M$ is a Moufang loop with trivial nucleus, then there is an automorphism $\rho$ of order three on $\text{Mlt} M$ such that $\rho$ combined with the $J$ from §3 satisfy (5.1)-(5.4) below. Doron's groups with triality [Do] generalize Glauberman's work. A group $G$ is said to be a triality group if there exist automorphisms $J$ and $\rho$ on $G$ such that

\begin{align*}
(5.1) & \quad \rho^3 = 1, \\
(5.2) & \quad J^2 = 1, \\
(5.3) & \quad \rho J \rho J = 1, \quad \text{and} \\
(5.4) & \quad \forall g \in G, \ g^{-1}g^Jg^{-\rho}g^J\rho g^{-\rho^2}g^\rho J = 1.
\end{align*}

Recall that a symmetric space is a set $S$ together with a binary operation $\cdot$ such that $\forall x, y, z \in S, x \cdot x = x, x \cdot (x \cdot y) = y$, and $x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$. The
sets $T_\pi = \{[x, J]: x \in G\}$, $T_\mu = \{[x, J\rho]: x \in G\}$, and $T_\lambda = \{[x, \rho J]: x \in G\}$ are isomorphic symmetric spaces (embedded) in $G$. Let $S$ be an abstract symmetric space isomorphic to $T_\pi$, $T_\mu$ and $T_\lambda$. Let $P$ be a symmetric space isomorphism from $S$ to $T_\pi$. Let $L(x) = (P(x))^\rho$ and let $R(x) = (L(x))^\rho$. Let $T = \{R(x): x \in S\}$ and let $I = C_G(J)$. Then $T$ is a (right) transversal to $I$ in $G$, and $G$ has a natural action on $S$ given by

\[(5.5)\quad xg = y, \quad \text{where } IR(x)g = IR(y),\]

Moreover,

\[(5.6)\quad T \text{ is a Moufang loop transversal to } I \text{ in } G,\]
\[(5.7)\quad [T, T^{-J}] \leq I,\]
\[(5.8)\quad \forall g \in T, \ [g, g^{-J}] = 1, \quad \text{and}\]
\[(5.9)\quad \forall g, h \in T, \ ghg \in T.\]

Since by (5.6), $T$ can be viewed as a Moufang loop, so too can $S$, via the bijection $R$. Thus, there is a "1" in $S$ and so the next result makes sense:

\[(5.10)\quad I = \text{Stab}_G(1).\]

Finally, a triality group $G$ is said to be a group with triality if

\[(5.11)\quad \langle T, T^{-J} \rangle = G.\]

And since, for each $x \in S$, the action of $R(x)$ on $S$ given by (5.5) is exactly the same as the action on $S$ of $R(x)$ viewed as an element of $\text{Mlt } S$ (and since the analogous statement for $L(x)$ also holds), $G$ has $\text{Mlt } S$ as a natural homomorphic image. Unfortunately, not all Moufang loops $S$ have $\text{Mlt } S$ with triality [Ph]. Thus, it is not always possible to recover $S$ from $\text{Mlt } S$ via Doro's method. The class of groups with biality and the construction in §9 and §10 overcome this apparent deficiency.
6. GROUPS WITH BIALITY

Let $G$ be a group with an involutory automorphism $J$, and let $I = C_G(J)$. We say that the triple $(G, T, J)$ is a group with biality, or more informally, that $G$ is a group with biality, if $T$ is a transversal to $I$ in $G$ such that:

1. $[T, T^{-J}] \leq I$,
2. $\forall g \in T, [g, g^{-J}] = 1$,
3. $\forall g, h \in T, ghg^{-T}$,
4. $(T, T^{-J}) = G$.

By (5.6)-(5.9) and (5.11), a group with triality is easily seen to be a group with biality. Also, if $M$ is a Moufang loop, then by (3.2)-(3.5) $M$ and the $U(M; V)$ are groups with biality. Thus, the class of groups with biality includes the class of groups with triality, the class of multiplication groups of Moufang loops and the class of universal multiplication groups of Moufang loops in some variety of Moufang loops.

Let $G$ be a group acting on a set $X$. A subset $T$ of $G$ is said to be sharply transitive if for every $a, b$ in $X$, there is a unique $t$ in $T$ such that $at = b$. Baer showed that a subset $T$ of $G$ is sharply transitive iff $T$ is a transversal to $S$ in $G$, where $S$ is the stabilizer of a singleton [Ba, p. 113]. Thus, if $(G, T, J)$ is a group with biality, then $T$ is sharply transitive.

Let $(G, T, J)$ be a group with biality. Then $G$ has a natural action on $T$ given by

$$T(x) = L(x)^{-1}R(x), \quad R(x) = R(x)R(y)R(xy)^{-1}, \quad L(x, y) = L(x)L(y)L(xy)^{-1}.$$ 

**Proposition 6.** If $(G, T, J)$ is a group with biality, then

i) $I = Stab_G(1)$, and (Cf. (3.6) and (5.8))

ii) $I = \langle T(x), R(x, y), L(x, y): x, y \in T \rangle$. 

Proof.

i) Let \( h \in I \). Then, \( I \, 1 \, h = I \, h = I \). Thus, \( h \in \text{Stab}_G(1) \). Conversely, let \( h \in \text{Stab}_G(1) \). Then, \( I \, h = I \, 1 \, h = I \, 1 = I \). Thus, \( h \in I \).

ii) (Cf. [Do, Cor. 3, p. 382], [SI, Thm. 244, p. 40], [B2, Lemma IV.1.2, p. 61]). □

7. GELFAND PAIRS

Let \( G \) be a finite group acting transitively on a set \( T \). Let \( I \) be the stabilizer in \( G \) of some point in \( T \). Let \( C(T) \) be the vector space of all functions from \( T \) into the set of complex numbers. The action of \( G \) on \( T \) induces a representation \( \rho \) of \( G \) in \( C(T) \);

\[
\rho: G \to \text{Aut} \left( C(T) \right); \quad g \mapsto (f(t) \mapsto f(g^{-1}t)).
\]

\( \rho \) decomposes into a direct sum of irreducible representations. If this decomposition is multiplicity free then \((G, I)\) is called a Gelfand pair. Since it is sometimes quite difficult to determine the decomposition of \( C(T) \), the following lemma is often useful.

Lemma 7. [Di, p. 59] (Gelfand's Lemma) Let \( J: G \to G \) be a monomorphism such that \( \forall \, g \in G, \, g^{-1} \in I \, g \, J \, I \). Then \((G, I)\) is a Gelfand pair.

We use Gelfand's Lemma to prove the following:

Theorem 8. If \((G, T, J)\) is a group with biality, and if \( G \) is finite, then \((G, I)\) is a Gelfand pair.
Proof. Let \( g = ht \), where \( h \in I \), and \( t \in T \). We observe that

\[
\begin{align*}
gg^{-J}h &= h \cdot (ht)^{-J}h \\
&= h \cdot t^{-J}h^{-1}h \\
&= h \cdot t^{-J}h^{-1}h \\
&= h \cdot t^{-J}h \\
&= h \cdot (t^{-J}h^{-1})(ht) \\
&= h \cdot g^{-J}g.
\end{align*}
\]

Thus, \( g^{-J}h \cdot g^{-1} = g^{-1}h \cdot g^{-J} \)

\[
\begin{align*}
&\implies g^{-J}h \cdot g^{-1} = k, \text{ some } k \in I. \\
&\implies g^{-1} = h^{-1}g^Jk \in Ig^JI. \quad \square
\end{align*}
\]

We note that Theorem 8 and its proof are also valid if \( G \) is finite and is interpreted as a group with triality, as the multiplication group of some Moufang loop or as a universal multiplication group of a Moufang loop. In fact, the formal aspects of the proof of Theorem 8 require no finiteness assumptions on the group \( G \), even though the statement of Theorem 6 does.

If \( (G, T, J) \) is a group with biality, then by Theorem 6, the representation of \( G \) given in (7.1) decomposes into a direct sum of distinct irreducible \( I \)-modules. This generalizes [S1, Theorem 532], where the decomposition is shown to hold when \( G \) is taken to be \( \text{Mlt } T \).

8. LOOP RINGS

If \( T \) is a loop and \( R \) is any commutative, associative ring with identity element, the loop ring \( R(T) \) is the \( R \)-module of all finitely supported functions from \( T \) to \( R \), together with a multiplication obtained by extending the multiplication on \( T \)
via linearity and distributivity. Traditionally, \( R(T) \) is thought of as the set of all formal, finite sums

\[
\sum_{x \in T} r_x x, \quad r_x = 1
\]

with the following rules for addition and multiplication

\[
\left( \sum_{x \in T} r_x x \right) + \left( \sum_{x \in T} s_x x \right) = \sum_{x \in T} \left( r_x + s_x \right) x,
\]

and

\[
\left( \sum_{x \in T} r_x x \right) \left( \sum_{x \in T} s_x x \right) = \sum_{x \in T} \left( \sum_{y \in T} r_y s_x \right) x.
\]

If \( T \) is a group then \( R(T) \) is the familiar group ring. If \( T \) is a proper loop (i.e. not a group), then \( R(T) \) is not an associative ring. Chein and Goodaire have studied the combinatorial properties of these general loop rings. For instance, in [CG] they describe a class of Moufang loops whose loop rings satisfy the alternative laws:

\[(yx)x = yx^2, \text{ and } x(xy) = x^2 y.\]

If \( I \) is the stabilizer of 1 in \( Mlt T \), then under the decomposition of \( C(T) \) as a direct sum of distinct irreducible \( I \)-modules, \( Z(C(T)) \), the center of the loop algebra, decomposes as a direct sum of \( h \) one dimensional \( I \)-modules, where \( h \) is the number of distinct conjugacy classes of \( T \) \([S1, \S 5.2]\). Recall that given \( x \) in \( T \), the conjugacy class of \( x \) is the set \( \{xh : h \in I\} \).

This result generalizes to arbitrary groups with biality. So let \( (G, T, J) \) be a group with biality. Under the decomposition of \( C(T) \) as a direct sum of distinct irreducible \( I \)-modules, \( Z(C(T)) \) decomposes as a sum of \( h \) one-dimensional \( I \)-modules, where \( h \) is the number of conjugacy classes of \( T \) \([B1, \text{Thm. I.12B}]\). One possible program of study is to investigate further the (multiplicative properties of) the loop ring \( C(T) \) and its relationship to the group ring \( C(G) \).
9. THE MOUFANG LOOP CONSTRUCTION

Given a group \((G, T, J)\) with biality, we endow \(T\) with a Moufang loop structure \((T, +)\) as follows:

**Theorem 9.** \(\forall a, b \in T, a^Jb^{-1}b^Ja^{-1} = b^{-1}a^{-1}a^Jb^J\).

**Proof.**

\[
\begin{align*}
a^{-1}b^Ja^{-1}b^{-1} & \in I, \quad \text{(by (6.1))} \\
\implies a^{-1}b^Ja^{-1}b^{-1} & = a^{-1}b^Ja^{-1}b^{-1}, \\
\implies a^Jb^{-1}b^Ja^{-1} & = b^{-1}a^{-1}b^Ja^{-1}b^J = b^{-1}a^{-1}a^Jb^J. \quad \text{(by (6.2)).}
\end{align*}
\]

**Lemma 10.** \(\forall a, b \in T, [a, J] = [b, J] \implies a = b.\)

**Proof.** \([a, J] = [b, J]

\[
\begin{align*}
& \implies a^{-1}a^J = b^{-1}b^J, \\
& \implies ba^{-1} = b^Ja^{-1}, \\
& \implies ba^{-1} \in I, \\
& \implies Ib = Ia, \\
& \implies a = b. \quad \Box
\end{align*}
\]

**Lemma 11.** \(T\) has a binary operation \(+\) that makes \(T\) a loop.

**Proof.** By comments in (2.1), \(T\) has a binary operation \(+\) that makes \((T, +, 1)\) a
right loop. We must show \((T, +, 1)\) is a left loop. So assume \(t + a = t + b\).

\[
\begin{align*}
\implies & t a b^{-1} t^{-1} = t^J a^J b^{-J} t^{-J} \\
\implies & t^{-J} t a b^{-1} t^{-1} t^J = a^J b^{-J} \\
\implies & t t^{-J} a b^{-1} t^{-1} t^J = a^J b^{-J} \quad \text{(by (6.2))} \\
\implies & t^{-1} a^J = t^{-J} a b^{-1} t^{-1} t^J b^J \\
\implies & t^{-1} a^J t a^{-J} = t^{-J} a(b^{-1} t^{-1} t^J b^J) t a^{-J} \quad \text{(by Thm. 9)} \\
\implies & t^{-J} a t^J a^{-1} = t^{-J} a(t^J b^{-1} b^J t^{-1}) t a^{-J} \quad \text{(by Thm. 9)} \\
\implies & a^{-1} = b^{-1} b^J a^{-J} \\
\implies & [a, J] = [b, J] \\
\implies & a = b \quad \text{(by Lemma 10)}.
\end{align*}
\]

Thus, \((T, +, 1)\) is a left loop, and so it is a loop. \(\square\)

Lemma 12. \(\forall a, b \in T, [a + b, J] = [ab, J] = a^J[b, J]a^{-1} = b^{-1}[a, J]b^J\).

Proof. Let \(c = a + b\). Then

\[
\begin{align*}
I a b &= I c, \\
\implies & a b c^{-1} = a^J b^J c^{-J} \\
\implies & c^{-1} c^J = b^{-1} a^{-1} a^J b^J \\
\implies & [a + b, J] = [c, J] = c^{-1} c^J = b^{-1} a^{-1} a^J b^J = [a b, J] = b^{-1} a^{-1} a^J b^J \\
&= a^J b^{-1} b^J a^{-1} = a^J [b, J] a^{-1} = b^{-1} a^J a^{-1} b^J = b^{-1} [a, J] b^J. \quad \square
\end{align*}
\]

Lemma 13. \((T, +)\) is a Moufang loop.
Proof. Let $y + x = a$, $x + a = b$, $z + b = c$, $z + x = d$, $d + y = e$, $e + x = f$. Then

$$[c, J] = b^{-1}z^{-1}z^Jb^J$$

$$= z^J[b, J]z^{-1}$$

(by Lemma 9)

$$= z^Jx^J[a, J]x^{-1}z^{-1}$$

(by Lemma 12, since $b = x + a$)

$$= z^Jx^Jy^J[x, J]y^{-1}x^{-1}z^{-1}$$

(by Lemma 12, since $a = y + x$)

$$= z^Jx^Jy^Jx^Jx^{-1}y^{-1}x^{-1}z^{-1}$$

(by (6.2))

$$= z^J(xy)x^{-1}(xy)x^Jz^{-1}$$

(by (6.2) and (6.3))

$$= (xy)^{-1}z^{-1}z^J(xy)x^J$$

(by (6.3) and Lemma 9)

$$= x^{-1}y^{-1}[zx, J]y^Jx^J$$

(by Lemma 12, since $d = z + x$)

$$= x^{-1}y^{-1}[d, J]y^Jx^J$$

(by Lemma 12)

$$= x^{-1}[e, J]x^J$$

(by Lemma 12)

$$= [ex, J]$$

(by Lemma 12)

$$= [f, J]$$

(by Lemma 12).

And so by Lemma 10, $c = f$. Thus, $z + (x + (y + x)) = z + (x + a) = z + b = c = f = e + x = (d + y) + x = ((z + x) + y) + x$. This proves the following:

**Theorem 14.** If $(G, T, J)$ is a group with biality, then $(T, +)$ is a Moufang loop.

If $(G, T, J)$ is a group with biality such that $\forall a, b \in T, (a^{-1}a^J)^2 = (b^{-1}b^J)^2 \implies a^{-1}a^J = b^{-1}b^J$ (in particular, if $|G|$ is odd), then the Scimemi-Joyce construction summarized in §3, Thm 1 is applicable to $(G, T, J)$. The resulting loop is precisely the Moufang loop constructed in our Thm. 14.

10. CLASSIFICATION THEOREMS

The next theorem shows the relationship between $G$ and Mlt $T$. 
Theorem 15. If \((G, J, T)\) is a group with biality, then Mlt \(T\) is a natural homomorphic image of \(G\).

Proof. For mnemonic purposes, given \(x \in T\), let \(R(x) = x\) and let \(L(x) = x^{-J}\). The similarity with \(R(x)\) and \(L(x)\) in Mlt \(T\) is apparent. In light of (6.4), it is sufficient to show that in \(G\), \(R(x)\) and \(L(x)\) act on \(T\) exactly as they do in Mlt \(T\). First note that by (2.1), \(tR(x) = t + x\). Now show \(tL(x) = x + t\). By (6.1) we have 

\[
x^{-1}t^Jxt^{-J} = x^{-J}tx^Jt^{-1},
\]

\[
\implies xt^{-J}tx^{-J} = t^{-J}xx^{-J}t = t^{-J}x^{-J}xt,
\]

by (6.2),

\[
\implies tx^{-J}t^{-1}x^{-1} = t^Jx^{-1}t^{-J}x^{-J},
\]

\[
\implies tx^{-J}t^{-1}x^{-1} \in I,
\]

\[
\implies Itx^{-J} = Ixt,
\]

\[
\implies ItL(x) = Ixt,
\]

\[
\implies tL(x) = x + t.
\]

Thus, Mlt \(T\) is a homomorphic image of \(G\). \(\Box\)

The kernel of this homomorphism is the set of elements that induce the trivial permutation on \(T\), or equivalently, on cosets of \(I\). This kernel is \(\text{core}_G(I)\). This proves the following

Theorem 16. A group \(G\) is the multiplication group of some Moufang loop iff \(G\) is a group with biality and \(\text{core}_G(I) = 1\).

The next comments are similar in spirit to Theorem 16, and so are stated without proof as

Remark 17.

i) A group \(G\) is the multiplication group of some commutative Moufang loop iff \(G\) is a group with biality, \(\text{core}_G(I) = 1\), and \(\forall x \in T, x^{-J} = x\). (Cf [NK, Cor. 4.2])
ii) A group $G$ is the multiplication group of some Moufang loop of finite exponent $n$ iff $G$ is a group with biality, $\text{core}_G(I) = 1$, and $\forall x \in T, x^n \in I$.

iii) A group $G$ is the multiplication group of some group iff $G$ is a group with biality, $\text{core}_G(I) = 1$ and $T$ is a subgroup of $G$. 
REFERENCES


PART III: GROUPS WITH TRIALITY AND MULTIPLICATION GROUPS OF MOUFANG LOOPS
ABSTRACT

In the first section we determine the triality status of multiplication groups of a large class of Moufang loops. In the second section, we present classes of Moufang loops whose universal multiplication groups are with triality. We also address the conjecture from Part I of this thesis, by enlarging the class of quasigroups whose universal multiplication group is known to be combinatorial. In the third section we completely determine all groups with triality associated with cyclic groups.
1. AN EXTENSION OF A RESULT OF GLAUBERMAN

In [Gl], Glauberman showed that if \( M \) is a Moufang loop with trivial nucleus, then \( \text{Mlt} \ M \) is a group with triality. We will address the question as to whether other Moufang loops have multiplication group with triality.

We begin by letting \( M \) be a Moufang loop. A subloop \( N \) of \( M \) is normal if \( N \) is the kernel of some loop homomorphism on \( M \). A subloop \( N \) is characteristic if \( N \) is invariant under all automorphisms on \( M \). The nucleus of \( M \) is the normal subloop of \( M \) consisting of all elements that associate with all pairs of elements, i.e. \( \text{Nuc}(M) := \{ x \in M : \forall y, z \in M, (xy)z = x(yz) \} \). The center of \( M \) is the normal subloop of \( M \) consisting of all nucleus elements that commute with all elements of \( M \), i.e. \( \text{Z}(M) := \{ x \in \text{Nuc}(M) : \forall y \in M, xy = yx \} \). The Moufang center of \( M \) is the (not necessarily normal) subloop of \( M \) consisting of all elements that commute with every element of \( M \), i.e. \( \text{C}(M) := \{ x \in M : \forall y \in M, xy = yx \} \). Finally, an autotopy of \( M \) is a triple \((U, V, W)\) such that each of \( U, V \) and \( W \) is a bijection of \( M \) and such that for every \( x, y \) in \( M \), \((xU)(yV) = (xy)W\).

Let \( J \) be the involutory automorphism given in §3 of Part II, i.e. \( J: \text{Mlt} \ M \to \text{Mlt} \ M; \alpha \mapsto J \alpha J \). Note that \( J \) operates on the generators by \( J: R(x) \mapsto L(x^{-1}), L(x) \mapsto R(x^{-1}) \). Let \( I = \text{C}_G(J) \), let \( T = \{ R(x) : x \in M \} \), and let \( P(x) = R(x^{-1})L(x^{-1}) \).

If there is an automorphism \( \rho \) on \( \text{Mlt} \ M \), such that \( \rho^3 = 1 \) and defined on generators (and \( P \)) by

\[
(1.1) \quad L(x)^\rho = R(x), \quad R(x)^\rho = P(x), \quad (P(x)^\rho = L(x)),
\]

then it is routine to check that \( \rho \) together with \( J \) makes \( \text{Mlt} \ M \) a group with triality. Although there could be other automorphisms of order three making \( \text{Mlt} \ M \) a group with triality in conjunction with \( J \), we are interested only in the automorphism given
by (1.1). In this case we will say that such a $\rho$ acts "as in Doro" and that $\operatorname{Mlt} M$ is with triality "as in Doro". We will attempt to classify those Moufang loops $M$ such that $\operatorname{Mlt} M$ is with triality as in Doro.

Given a Moufang loop $M$, define a map $\rho$ on the generators of $\operatorname{Mlt} M$ as in (1.1). We must decide if it is possible to extend $\rho$ to all of $\operatorname{Mlt} M$. Clearly it is sufficient to show that $Q_1(x_1) \cdots Q_n(x_n) = 1$ implies that $Q_1(x_1)^\rho \cdots Q_n(x_n)^\rho = 1$ (here each $Q_i$ is either $R$ or $L$). This task is simplified by a result from elementary autotopy theory, namely if $Q_1(x_1) \cdots Q_n(x_n) = 1$, then $Q_1(x_1)^\rho \cdots Q_n(x_n)^\rho = R(c)$, for some $c \in \operatorname{Nuc}(M)$ [Gl, p. 400], [Br, p. 112]. Thus, it is clear that if $\operatorname{Nuc}(M) = 1$, then $\rho$ extends to all of $\operatorname{Mlt} M$. This is the result of Glauberman mentioned in the title of this section.

Theorem 1. If $M$ is a commutative Moufang loop of exponent three, then $\operatorname{Mlt} M$ is with triality.

Proof. Let $\rho = 1$. Then since for every $x$ in $M$, $R(x) = L(x) = P(x)$, $\rho$ is as in Doro, and $\operatorname{Mlt} M$ is a group with triality as in Doro. \hfill \square

Theorem 2. If $M \cong Z(M) \times L$, where $\exp(Z(M)) = 3$ and $L$ is a subloop of $M$ such that $\operatorname{Mlt} L$ is with triality as in Doro, then $\operatorname{Mlt} M$ is with triality as in Doro.

Proof. Clearly every element in $\operatorname{Mlt} M$ can be written as $R(z_1) \cdots R(z_m)Q_1(x_1) \cdots Q_n(x_n)$, where each $z_j$ is in $Z(M)$ and each $x_i$ is in $L$. So $R(z_1) \cdots R(z_m)Q_1(x_1) \cdots Q_n(x_n) = 1$ implies that $R(z_1 \cdots z_m)Q_1(x_1) \cdots Q_n(x_n) = 1$, which in turn implies that $z_1 \cdots z_m$ is in $L$. Thus $z_1 \cdots z_m = 1$. So $Q_1(x_1) \cdots Q_n(x_n) = 1$, which implies that $Q_1(x_1)^\rho \cdots Q_n(x_n)^\rho = R(c)$, for some $c \in \operatorname{Nuc}(M)$. But notice that in $\operatorname{Mlt} L$ we also have $Q_1(x_1) \cdots Q_n(x_n) = 1$, and so since $\operatorname{Mlt} L$ is with triality as in Doro, in $\operatorname{Mlt} L$, $Q_1(x_1)^\rho \cdots Q_n(x_n)^\rho = 1$. That is for every $a$ in $L$, $aQ_1(x_1)^\rho \cdots Q_n(x_n)^\rho = a$. Thus, given $a$ in $L$, in $\operatorname{Mlt} M$ we have $a = aQ_1(x_1)^\rho \cdots Q_n(x_n)^\rho = aR(c) = ac$. And so $c = 1$. Hence, in $\operatorname{Mlt} M$, $Q_1(x_1)^\rho \cdots Q_n(x_n)^\rho = 1$. Thus, $R(z_1)^\rho \cdots$
Let $R(z_m) \rho Q_1(z_1) \rho \cdots Q_n(z_n) \rho = R(z_1) \rho \cdots R(z_n) \rho = R(z_1) \cdots R(z_n) = R(z_1 \cdots z_m) = 1$, and Mlt $M$ is with triality as in Doro. $\square$

If $L$ is a Moufang loop with trivial nucleus and if $A$ is an abelian group of exponent three then $M = A \times L$ satisfies the hypotheses of Theorem 2, and so Mlt $M$ is with triality as in Doro.

**Theorem 3.** If $M$ is a Moufang loop with $\exp(C(M)) \neq 3$, then Mlt $M$ is not with triality as in Doro.

*Proof.* There must be an $x$ in $C(M)$ with $x^3 \neq 1$. And since $L(x) = R(x)$, if $\rho$ were defined as in Doro, we would have $R(x) = L(x)^\rho = R(x) = P(x)$. But this implies that $x^3 = 1$. This is a contradiction. $\square$

**Corollary 4.** If $\text{Nuc}(M) = 1$, then $\exp(C(M)) = 3$.

**Theorem 5.** If $M$ is a Moufang loop such that $\text{Nuc}(M)$ is not contained in $C(M)$ then Mlt $M$ is not with triality as in Doro.

*Proof.* By assumption there is an $x$ in $\text{Nuc}(M)$ and a $y$ in $M$ such that $xy \neq yx$. Since $x$ is in $\text{Nuc}(M)$, we have $L(x)L(y) = L(yx)$. But then if $\rho$ were defined as in Doro, we would have $R(x)R(y) = R(yx)$. And thus $xy = yx$. This is a contradiction. $\square$

Theorems 1, 2, 3, and 5 combine to determine the triality status of Mlt $M$ for all Moufang loops not in the following class $H$ of Moufang loops:

$H := \{M : 1 < \text{Nuc}(M) \leq C(M) < M, \exp(C(M)) = 3, \text{and} \ Z(M) \text{ does not appear as a direct factor in some decomposition of } M\}$.

Finishing the classification theorem, i.e. determining the triality status of Mlt $M$ for $M \in H$, is a difficult problem. It is part of the author's ongoing research project and includes a development of the appropriate cohomology theory for (Moufang) loops.
2. UNIVERSAL MULTIPLICATION GROUPS WITH TRIALITY

The next four theorems describe classes of Moufang loops whose universal multiplication groups are with triality.

**Theorem 6.** If $\text{Mlt } M$ is a group with triality, then so too is $U(M; V)$, where $V$ is any variety of Moufang loops containing $M$.

**Proof.** Let $G = U(M; V)$. Define $\rho$ on the generators of $G$. We show that $\rho$ extends to all of $G$. Assume $Q_1(x_1)\ldots Q_n(x_n) = 1$, in $G$. Then $Q_1(x_1)\rho \ldots Q_n(x_n)\rho = R(c)$, for some $c$ in $\text{Nuc}(M[X])$. But $Q_1(x_1)\ldots Q_n(x_n) = 1$, in $\text{Mlt } M$ also. And since $\text{Mlt } M$ is with triality, $Q_1(x_1)\rho \ldots Q_n(x_n)\rho = 1$, in $\text{Mlt } M$. This means that $c = 1c = 1Q_1(x_1)\rho \ldots Q_n(x_n)\rho = 1$. Hence $\rho$ is well defined and $U(M; V)$ is a group with triality. □

Before proving the next theorem, we need a technical lemma.

**Lemma 7.** If $M$ is a cyclic group, then $M \cap C(M[X]) = 1$. (Here the coproduct $M[X]$ is in any category of Moufang loops containing all groups).

**Proof.** $M$ embeds in some group $G$ so that $Z(G) \cap M = 1$. (If $M$ is infinite, take $G$ free on two or more generators, if the order of $M$ is $n$, take $G = \langle x, y : x^n = 1 \rangle$.) Say $f : M \to G$ is such an embedding. Then given $y \in M$, $\exists g \in G$ such that $f(y)g \neq gf(y)$. Let $h : \langle x \rangle \to G$ be determined by $x \mapsto g$. Thus, there is a unique $F : M[X] \to G$ such that the following diagram commutes

```
M ----宏伟-- M[X] ← ------<x>
    |                        |       |
    V                        V       V
    G                       h      f
```

The diagram commutes, implying $F$ is well defined.
If \( yx = xy \) then

\[
    F(yx) = F(xy) \quad \text{which implies}
\]

\[
    F(y)F(x) = F(x)F(y) \quad \text{which implies}
\]

\[
    f(y)h(x) = h(x)f(y) \quad \text{which implies}
\]

\[
    f(y)g = g f(y) \quad \text{which is a contradiction.}
\]

Hence \( yx \neq xy \) and \( y \notin C(M[X]) \). We conclude the \( M \cap C(M[X]) = 1 \). \( \square \)

**Theorem 8.** If \( M \) is a cyclic group, and \( M \) is any variety of Moufang loops containing \( M \) and all groups, then \( U(M; M) = M \times M \), and \( U(M; M) \) is with triality.

**Proof.** Let \( R(M) = \langle R(x): x \in M \rangle_{U(M; M)} \) and let \( L(M) = \langle L(x): x \in M \rangle_{U(M; M)} \).

Since \( M \) is cyclic, \( M[X] \) is generated by two elements, and so by Moufang's Theorem, \( M[X] \) is a group. Thus

\[
    (2.1) \quad R(M) = \{R(x): x \in M\} \triangleleft U(M; M)
\]

\[
    (2.2) \quad L(M) = \{L(x): x \in M\} \triangleleft U(M; M)
\]

Thus, by Lemma 7,

\[
    (2.3) \quad R(M) \cap L(M) = 1.
\]

(2.1)–(2.3) combine with

\[
    (2.4) \quad U(M; M) = \langle R(M), L(M) \rangle
\]

to give

\[
    U(M; M) \cong R(M) \times L(M) \cong M \times M.
\]

Define \( \rho \) on \( U(M; M) \) as follows

\[
    (R(w)L(y))^\rho = R(w^{-1}y)L(y^{-1}).
\]
By (2.1), (2.2) and (2.4) \( \rho \) is well-defined. Also

\[
[(R(w_1)L(y_1))(R(w_2)L(y_2))]^\rho \\
= [R(w_1w_2)L(y_1y_2)]^\rho \\
= R(w_2^{-1}w_1^{-1}y_1y_2)L(w_2^{-1}w_1^{-1}) \\
= R(w_1^{-1}w_2^{-1}y_1y_2)L(w_2^{-1}w_1^{-1}) \quad \text{(since } M \text{ is abelian)} \\
= R(w_1^{-1}y_1L(w_1^{-1})R(w_2^{-1}y_2)L(w_2^{-1}) \quad \text{(since } M[X] \text{ is a group)} \\
= [R(w_1)L(y_1)]^\rho [R(w_2)L(y_2)]^\rho.
\]

Thus, \( \rho \) is a well-defined homomorphism. Clearly, \( \rho \) is as in Doro so that \( U(M; M) \) is with triality as in Doro. \( \square \)

**Theorem 9.** If \( A = \prod_{i \in I} A_i \) and if each \( U(A_i; V) \) is a group with triality, then so too is \( U(A; V) \), where \( V \) is any variety of Moufang loops containing each \( A_i \).

**Proof.** We will use vector notation, \( \underline{z} \), to denote elements of \( A \). So, \( Q_1(\underline{z}_1) \ldots Q_n(\underline{z}_n) = 1 \), implies that \( Q_1^\rho(\underline{z}_1) \ldots Q_n^\rho(\underline{z}_n) = R(\underline{e}) \), for some \( \underline{e} \in \text{Nuc}(A) \). Now in each \( U(A_i; V) \) we have \( Q_1(x_1) \ldots Q_n(x_n) = 1 \). But since each \( U(A_i; V) \) is with triality \( Q_1^\rho(x_1) \ldots Q_n^\rho(x_n) = 1 \). Thus, \( \underline{e} = 1R(\underline{e}) = 1Q_1^\rho(\underline{z}_1) \ldots Q_n^\rho(\underline{z}_n) = 1Q_1^\rho(x_1) \ldots Q_n^\rho(x_n) = 1 \). Thus, \( A \) is a group with triality. \( \square \)

Theorems 8 and 9 combine to give

**Corollary 10.** If \( A \) is a finitely generated abelian group, then \( U(A; V) \) is a group with triality.

Next we consider the conjecture on page 4 of Part I of this thesis by enlarging the class of quasigroups whose universal multiplication groups are known to be combinatorial.

**Theorem 11.** If \( M \) is a commutative Moufang loop of exponent three, if \( V \) is
any variety of commutative Moufang loops of exponent three containing $M$, and if $Z(U(M; V)) \cap I = 1$, then $U(M; V) \cong \text{Mlt } M$.

Proof. $U(M; V)$ is a group with triality as in Doro with $\rho = 1$. Let $G = U(M; V)$. By [Do, Thm. 1] $G/\text{core}_G(I) \cong \text{Mlt } M$. Let $k$ be in $\text{core}_G(I)$. Thus, for every $g$ in $G$, $k = g^{-1} g^I k (g^{-1})^I g$. Taking $g = R(x)$, for any $x$ in $M$, we get $k = P(x^{-1}) k P(x)$. But $M[X]$ is a commutative Moufang loop of exponent three, so $R(x) = L(x) = P(x)$. And since $x$ was arbitrary, $k$ is in $Z(G)$. Thus $k$ is in $Z(G) \cap I = 1$, and so $k = 1$. And here, $\text{core}_G(I) = 1$. So we conclude that $U(M; V) \cong \text{Mlt } M$. □

If $M$ is an infinitely generated free commutative Moufang loop of exponent three and if $V$ is any variety of commutative Moufang loops of exponent three containing $M$, then $Z(U(M; V)) \cap I = 1$. Hence by Theorem 1, $U(M; V) \cong \text{Mlt } M$.

3. CYCLIC GROUPS AND GROUPS WITH TRIALITY

Given a Moufang loop $M$, there may be many groups $G$ with triality such that Doro’s construction on $G$ yields $M$. Doro showed that among these there is a largest. Specifically, given $M$, there is a group $G(M)$ with triality such that the Moufang loop constructed from $G(M)$ is $M$, and such that for any other group $G$ with triality that gives rise to $M$, $G$ is a natural homomorphic image of $G(M)$. Similarly, there is a smallest group with triality associated with $M$. This group, $G_0(M)$ has the properties that the Moufang loop constructed from it is $M$, and that any other group with triality that gives rise to $M$ has $G_0(M)$ as a natural homomorphic image.

Theorem 12. If $M$ is a cyclic group, then $G(M) \cong M \times M$.

Proof. Let $M = \langle a \rangle$. Two trivial induction arguments show that for every pair of
positive integers \( m, n \) we have

\[(3.1) \quad R_a^m R_a^n = R_a^{m+n}\]
\[(3.2) \quad L_a^m L_a^n = L_a^{m+n}.\]

We prove (3.3) by induction on \( m + n \)

\[(3.3) \quad R_a^m L_a^n = L_a^n R_a^m.\]

The cases \( m + n = 1 \), and either \( m = 0 \) or \( n = 0 \) are trivial. The nontrivial instance of \( m + n = 2 \) is proved by noting

\[(3.4) \quad R_a L_a = R_a P_1 L_a = P_{a-1} = L_a P_1 R_a = L_a R_a.\]

So assume (3.3) is true for all \( m+n < k \). Consider the nontrivial cases of \( m+n = k \):

\[
R_a^m L_a^n = R_a R_a^{m-1} L_a^{n-1} L_a \quad \text{(by (3.5) and (3.6))}
= R_a L_a^{n-1} R_a^{m-1} L_a \quad \text{(by induction hypothesis)}
= L_a^{n-1} R_a L_a R_a^{m-1} \quad \text{(by induction hypothesis)}
= L_a^{n-1} L_a R_a R_a^{m-1} \quad \text{(by (3.8))}
= L_a^n R_a^m \quad \text{(by (3.5) and (3.6)).}
\]

Thus (3.3) is valid, and the following map is onto:

\[F: M \times M \to G(M); (a^m, a^n) \mapsto R_a^m L_a^n.\]

By (3.1)–(3.3) \( F \) is a homomorphism. Finally, \( U(M; M) \cong M \times M \) is a homomorphic image of \( G(M) \), and so \( F \) is one-to-one. \( \Box \)

For a finite cyclic group \( M \) we have a complete description of \( G_0(M) \). First, we need a technical lemma.
Lemma 13. If $D$ is the $S_3$ group of automorphisms acting on $G(M)$, and if $S$ is the subset of elements of $G(M)$ fixed by $\rho$, then $C_{G(M)}(G(M)D) \cong (I \cap S \cap Z(G(M)))$.

Proof.

$$C_{G(M)}(G(M)D) = \{(g, 1): \forall h \in G(M), \forall \theta \in D, (g, 1)(h, \theta) = (h, \theta)(g, 1)\}$$

$$= \{(g, 1): \forall h \in G(M), \forall \theta \in D, (gh, \theta) = (hg^{\theta^{-1}}, \theta)\}.$$ 

Taking $h = 1$ and $\theta = J (\theta = \rho^2, \theta = 1, \text{respectively})$ yields

$$C_{G(M)}(G(M)D) \subset I \quad (\subset S, Z(G(M)) \text{respectively}).$$

The converse is now trivial. $\square$

Theorem 14. If $M$ is a finite cyclic group of order $n$, then $G_0(M) \cong M \times M$ if 3 does not divide $n$, and $G_0(M) \cong (M \times M)/C_3$ if 3 divides $n$ (here $C_3$ is the three element cyclic group) (cf. [Do, Prop. 1]).

Proof. Let $\langle x \rangle = M$. Doro shows that $G_0(M) \cong G(M)/C_{G(M)}(G(M)D)$ [Do, p. 384]. Thus, by Lemma 13, $G_0(M) \cong G(M)/(I \cap S \cap Z(G(M)))$.

In $G(M)$, $R(x^k)L(x^m)$ is in $I$ iff $R(x^{k+m})L(x^{k+m}) = 1$. But since by Theorems 8 and 12, $G(M)$ is really just $U(M;M)$, and since $U(M;Gp)$ is a homomorphic image of $U(M;M)$, the proof of [Sm, Thm. 235] assures us that $|x|$ divides $m + k$. But clearly we are assuming that $|x|$ is greater than or equal to both $m$ and $k$. Thus, $|x| = m + k$.

On the other hand, in $G(M)$, $R(x^k)L(x^m)$ is in $S$ iff $|x|$ divides $3k$. So if 3 does not divide $n$ (and note that $n = |x|$), we must have, that $|x|$ divides $k$. And since $|x| = m + k$, this means that $m = 0$ and $n = k$. Thus, $R(x^k)L(x^m) = 1$, and so $I \cap S = 1$. Thus, $(I \cap S \cap Z(G(M))) = 1$. And hence, $G_0(M) \cong G(M)/(I \cap S \cap Z(G(M))) \cong G(M) \cong M \times M$. This proves the first part of the theorem.
If 3 does divide \( n \), say \( n = 3s \), then it is easy to check that \( I \cap S = \{1, R(x^s)L(x^{n-s})\} = C_3 \). And since \( Z(G(M)) = G(M), I \cap S = (I \cap S \cap Z(G(M))) \). And hence, \( G_0(M) \cong G(M)/(I \cap S \cap Z(G(M))) \cong (M \times M)/C_3 \). This completes the proof of the theorem. □

**Theorem 15.** If \( M \) is the infinite cyclic group, then \( G_0(M) \cong M \times M \).

**Proof.** In \( G(M), R(x^k)L(x^m) \) is in \( I \) iff \( R(x^{k+m})L(x^{k+m}) = 1 \). But since by Theorems 8 and 12, \( G(M) \) is really just \( U(M;M) \), and since \( U(M;Gp) \) is a homomorphic image of \( U(M;M) \), the proof of [Sm, Thm. 235] assures us that \( |x| \) divides \( m + k \). Thus \( x = 1 \) and hence \( I = 1 \). Thus, \( G_0(M) \cong G(M)/(I \cap S \cap Z(G(M))) \cong G(M) \cong M \times M \). □

If \( M \) is a cyclic group such that 3 does not divide \( M \), then Theorems 12, 14 and 15 show that there is really only one group with triality that gives rise to \( M \), namely \( M \times M \). If 3 does divide \( M \), then the same theorems show that there are precisely two groups with triality giving rise to \( M \), namely \( M \times M \) and \((M \times M)/C_3\).
REFERENCES


PART IV: THE VARIETY OF TRIALITY GROUPS, GEOMETRY AND MISCELLANEA
ABSTRACT

The class of groups with triality is not a variety. But the class of triality groups is a variety, and so we initiate an algebraic investigation of this variety. We also study the geometry of quasigroups and Moufang loops, and consider geometric connections with triality groups. In the final section we offer some miscellaneous results.
1. THE VARIETY OF TRIALITY GROUPS

Consider a group $G$ with triality as a universal algebra $\langle G, F \rangle$ with operations $F = \{\cdot, -1, 1, J, \rho\}$ such that $\langle G; -1, 1 \rangle$ is a group and such that $J$ and $\rho$ are the obvious unary operations on $G$. Clearly the class $\text{GT}$ of all groups with triality, considered as universal algebras, is closed under the taking of homomorphic images and under the formation of products. But $\text{GT}$ is not closed under the taking of subalgebras. To see this, let $G$ be the multiplication group of a not associative commutative Moufang loop of exponent three. Then $G$ is with triality, $I$ is a subalgebra, but $[I, D] = 1 < I$ (where $D$ is the group of triality automorphisms). And so $I$ is not a group with triality. Thus, $\text{GT}$ is not a variety. By the above comments, the variety it generates is $\text{HSP} (\text{GT}) = \text{HS} (\text{GT})$.

However, the class $\text{TG}$ of triality groups (Part II, §5) is a variety. To see this, note that each triality group $G$ can be considered as an algebra of type $F = \{\cdot, -1, 1, J, \rho\}$ such that $\langle G; -1, 1 \rangle$ is a group and such that $\langle G; F \rangle$ further satisfies

\begin{align*}
(x y)^J &= x^J y^J, \\
(x y)^\rho &= x^\rho y^\rho, \\
x^{J J} &= x, \\
x^{\rho \rho \rho} &= x, \\
x^{J \rho J \rho} &= x, \\
x^{-1} x^J x^{-\rho} x^J \rho x^{-\rho^2} x^\rho J &= 1.
\end{align*}

Conversely, each such algebra is a triality group. So by Birkhoff’s Theorem, $\text{TG}$ is a variety. Clearly $\text{HS} (\text{GT}) \subseteq \text{TG}$.

Given a triality group $G$, the term operations $F = \{\cdot, -1, 1, J, \rho\}$ are really just those demanding that $\langle G; -1, 1 \rangle$ be a group together with two unary operations (automorphisms) $J$ and $\rho$. Thus, it may be helpful to think of a triality group as a
traditional "group with operators."

We begin our investigation of triality groups by identifying the largest group with triality contained as a subalgebra in a given triality group $G$. Recall that there is a transversal $T$ to $I$ in $G$, and a symmetric space, $S$, bijective with $T$. Returning to the notation of Part II, §5, $T = \{R(x): x \in S\}$, $T^{-J} = \{L(x): x \in S\}$.


Proof. The generators of $[G, D]$ are $\{g^{-1}g^\theta: g \in G, \theta \in D\}$. So

(1.7) $g^{-1}g^\rho J = \left((g^\rho)^{-1}g^\rho J\right)^\rho \in T^{-J},$

(1.8) $g^{-1}g^J\rho = ((g^\rho)^{-1}g^\rho J)^{\rho^2} \in T,$

(1.9) $g^{-1}g^J = g^{-J\rho^2}g^{\rho^2}g^{-J^\rho g^\rho}$ (by (1.6))

$= \left((g^{-1}g^J)^{\rho^2}\right)^{-1} \left[(g^{-1}g^J)^{\rho}\right]^{-1} \in T^{-1} \cdot T^J \subset (T, T^{-J}),$

(1.10) $g^{-1}g^\rho J = (g^{-1}g^\rho J)(g^{-J^\rho g^J^\rho}) \in (T, T^{-J})$

(by (1.8) and (1.9)),

(1.11) $g^{-1}g^\rho = (g^{-1}g^\rho^2)(g^{-\rho^2}g^{\rho^2}) \in (T, T^{-J})$

(by (1.10)).

(1.7)-(1.11) imply that $[G, D] \leq (T, T^{-J})$.

Conversely, the generators of $(T, T^{-J})$ are $\{g^{-\rho^i}g^{J^\rho^i}: g \in G, i = 1, 2\}$. So

(1.12) $g^{-\rho^3}g^{J^\rho^3} = g^{-J^\rho g^\rho g^{-J^\rho}}$ (by (1.6))

$= \left((g^\rho)^{-1}(g^\rho)^{J^\rho}\right)^{-1} \left(g^{-1}g^J\right)^{-1} \in [G, D],$

(1.13) $g^{-\rho}g^{J^\rho} = (g^\rho)^{-1}(g^\rho)^{J^\rho} \in [G, D].$

(1.12) and (1.13) show that $(T, T^{-J}) \leq [G, D]$. And so, $[G, D] = (T, T^{-J})$. □
Thus, given a triality group $G$, it contains a largest group with triality $[G, D] = \langle T, T^{-J} \rangle$ as a subalgebra. And so an investigation of Moufang loops can take place from the universal algebraic context of the variety of triality groups.

In the class of groups with triality, Doro identified "free" objects [Do, Thm. 2]. The situation is more complex for triality groups, but the varietal setting lends itself to the powerful tools of universal algebra. We begin by identifying $1\text{TG}$, the free algebra on one generator in the variety. Let $n\text{Gp}$ denote the free group on $n$ generators.

**Theorem 2.** $1\text{TG} \cong 5\text{Gp}/H^{5\text{Gp}}$, where $H = \langle y^{-1}y^Jy^{-\rho}y^Jy^{-\rho^3}, y \in 5\text{Gp} \rangle$ and $H^{5\text{Gp}}$ denotes the normal closure of $H$ in $5\text{Gp}$.

Clearly, this description of $1\text{TG}$ is complicated. To better understand $1\text{TG}$ we consider free algebras in a subvariety of $\text{TG}$, namely the subvariety of triality groups with $\rho = 1$. Denote this subvariety by $\text{TG}_\rho$. Even in this subvariety, identification of (free) algebras is a difficult problem. Let $G \in \text{TG}_\rho$ and let $B = [G, D]$ be the largest group with triality contained as a subalgebra in $G$. Let $\tilde{B} = \langle y^{-1}y^J : y \in G \rangle$. Since $\rho = 1$, $B = \langle \tilde{B} \rangle_G$ and Doro's Moufang loop constructed from $B$ is commutative of exponent three [Do, Lemma 2]. Also, by (1.6), for every $b \in \tilde{B}$, $b^3 = 1$. Thus, $B$ is generated by elements of order three.

A large component of the author's ongoing research program is an investigation of these two varieties, $\text{TG}$ and $\text{TG}_\rho$.

2. **THE GEOMETRY OF MOUFANG LOOPS**

A $k$-net ($k \geq 3$) is a structure consisting of a set $\Phi$ of points and a set of lines, which is partitioned into $k$ disjoint families $L_i$ ($i = 1, \ldots, k$) such that

i) every point is incident with exactly one line of every $L_i$ ($i = 1, \ldots, k$);

ii) two lines of different families have exactly one point in common;
iii) there exist \( k \) lines belonging to \( k \) different \( L_i \) and which are not incident with the same point.

It is known that to every quasigroup \( Q \) we can associate a 3-net \([BS]\). The full collineation group \( \Sigma \) of \( Q \) is the full collineation group of the associated 3-net, that is, the group of permutations of the points of the 3-net that map lines to lines. \( \Sigma \) has a normal subgroup \( \Gamma \) of index \( \leq 6 \) which maps each class of parallel lines into itself. This subgroup is called the group of direction preserving collineations of \( Q \).

Define the group of inner autotopies of a Moufang loop \( M \) to be the subset of the group of all autotopies of \( M \) whose components are multiplication group elements.

That is

\[
\text{InAtp } M := \{(U, V, W) \in \text{Atp } M : U \in \text{Mlt } M\}.
\]

**Theorem 3.** \( \Gamma \cong \text{Atp } M \).

**Proof.** Define \( F: \text{Atp } M \to \Gamma; (U, V, W) \mapsto ((x, y) \mapsto (xU, yV)) \). It is easy to check that \( F \) is a bijection. \( \square \)

**Theorem 4.** There is a set-bijection \( F: \text{Mlt } M \times \text{Nuc}(M) \to \text{InAtp } M \).

**Proof.** Define \( F: \text{Mlt } M \times \text{Nuc}(M) \to \text{InAtp } M; (E, c) \mapsto (E, E^\rho R(c), E^{J^\rho} R(c)) \).

Define \( G: \text{InAtp } M \to \text{Mlt } M \times \text{Nuc}(M); (U, V, W) \mapsto (U, c) \), where

\[
(U^{-1}, (U^{-1})^\rho, (U^{-1})^{J^\rho})(U, V, W) = (1, R(c), R(c)) \quad \text{for some } c \in \text{Nuc}(M) \quad \text{[Br, p. 112]}.\]

Here \( E^\rho \) is given by \( Q_1^\rho(x_1) \ldots Q_n^\rho(x_n) \) where \( E = Q_1(x_1) \ldots Q_n(x_n) \), with each \( Q_i \) either \( R \) or \( L \). Similarly for \( E^{J^\rho}, U^\rho \) and \( U^{J^\rho} \). Clearly \( F \) and \( G \) are inverses of each other. \( \square \)

**Corollary 5.** If \( \text{Nuc}(M) \leq C(M) \), then \( \text{InAtp } M \cong \text{Mlt } M \times \text{Nuc}(M) \). So if \( \text{Nuc}(M) = 1 \), then \( \text{InAtp } M \cong \text{Mlt } M \).

**Proof.** If \( \text{Nuc}(M) \leq C(M) \), then the \( F \) of Theorem 4 is a homomorphism. \( \square \)

Much has been written about Moufang loops with transitive automorphism group \([BS]\). For such Moufang loops with trivial nucleus, the situation is trivial.
Theorem 6. If $\text{Nuc}(M) = 1$ and if $\text{Aut}(M)$ is transitive, then $M = 1$.

Proof. By [BS, Thm. 10.11], $\Gamma = \{(x, y) \mapsto (x^\alpha, y^\alpha) : \alpha \in \text{Aut} M\}$. Thus, by Theorem 3, $\text{Atp} M = \{(\alpha, \alpha, \alpha) : \alpha \in \text{Aut} M\}$. Since for every $x$ in $M$, $(L(x), R(x), P(x^{-1}))$ is in $\text{Atp} M$, this means that $L(x) = P(x^{-1})$. Thus, $x = 1$. Hence, $M = 1$. \ \qed

The next theorem shows that the geometry of a Moufang loop can be studied from the algebraic context of the variety of triality groups.

Theorem 7. $\Gamma_{(1,1)}$, the stabilizer of $(1,1)$ in $\Gamma$, is a triality group.

Proof. Let

$J : \Sigma \to \Sigma; \ (x, y) \mapsto (xy, y^{-1})$

$\rho : \Sigma \to \Sigma; \ (x, y) \mapsto (y^{-1}x^{-1}, x)$.

Then conjugation by $J$ and conjugation by $\rho$ are both automorphisms on $\Gamma$, of orders two and three respectively. Together, they generate a group of automorphisms on $\Gamma_{(1,1)}$ such that $\Gamma_{(1,1)}$ becomes a triality group (cf. [Do, Thm. 10.3]). \ \qed

And since $\text{Aut} M \cong \Gamma_{(1,1)}$ [BS, Thm. 10.2], $\text{Aut} M$ is a triality group.

(Here $\text{Aut} M$ is the group of automorphisms on $M$).

3. MISCELLANEA

Here we give three miscellaneous theorems.

Theorem 8. If $M$ is a Moufang loop that is not commutative of exponent two, then $M[X]$ is not commutative. (Here the coproduct $M[X]$ is in the variety of all Moufang loops.)

Proof. If $M$ is not commutative, then there is nothing to show. So assume $M$ is commutative. Let $M \to M'; \ x \mapsto x^{-1}$. Form the semidirect product $M(J)$.
Select $y \in M$ such that $y^{-1} \neq y$. Let $1_M : M \to M\langle J \rangle; y \mapsto (y, 1)$. Let $h : (x) \to M\langle J \rangle$ be determined by sending $x \mapsto (1, J)$. Then there exists a unique $F : M[X] \to M\langle J \rangle$ such that the following diagram commutes.

\[
\begin{array}{c}
M \\
\downarrow 1_M
\end{array}
\begin{array}{c}
\xrightarrow{F} \\
\downarrow h
\end{array}
\begin{array}{c}
M[X] \\
\downarrow F
\end{array}
\begin{array}{c}
\xleftarrow{F} \\
\downarrow h
\end{array}
\begin{array}{c}
M\langle J \rangle
\end{array}
\]

If $yx = xy$ then

\[
F(yx) = F(xy)
\]
which implies

\[
F(y)F(x) = F(x)F(y)
\]
which implies

\[
(y, 1)(1, J) = (1, J)(y, 1)
\]
which implies

\[
(y, J) = (y^{-1}, J)
\]
which implies

\[
y = y^{-1}.
\]

This is a contradiction, so $yx \neq xy$ and $M[X]$ is not commutative.

Before proving the next theorem we need a technical lemma.

**Lemma 9.** If $M$ is a Moufang loop such that Mlt $M$ is with triality as in Doro, then $C_{\text{Mlt}} M(\text{Mlt } M \ D) = 1$.

**Proof.** By proof of Part III, Lemma 13, $C_{\text{Mlt}} M(\text{Mlt } M \ D) = I \cap S \cap Z(\text{Mlt } M)$. So if $h \in Z(\text{Mlt } M)$, then $h = R(c)$, for some $c \in \text{Nuc}(M)$ [Al, Thm. 11]. But $h$ is also in $I$, so $c = 1$, and hence $h = 1$. Thus, $I \cap S \cap Z(\text{Mlt } M) = 1$.

The next theorem is a generalization of [Do, Corollary 5]. It is offered here because the proof in Doro is incorrect.
Theorem 10. If $M$ is a Moufang loop such that $\text{Mlt } M$ is with triality as in Doro, then $\text{Mlt } M \cong G_0(M)$.

Proof.

\[
G_0 \cong \text{Mlt } M/C_{\text{Mlt } M}(\text{Mlt } M D) \quad \text{(by [Do, Corollary 4])}
\]

\[
\cong \text{Mlt } M \quad \text{(by Lemma 9).}
\]

Finally, we recall that there is a collection of theorems about the relationship between a loop $L$, its multiplication group $\text{Mlt } L$ and its inner mapping group $I$. For instance, $I$ is trivial iff $L$ is an abelian group. Niemenmaa and Kepka prove that if $I$ is cyclic and if $L$ is finite then $L$ is an abelian group [NK, Thm. 4.3]. (They are currently working on a theorem that says if $I$ is abelian then $\text{Mlt } L$ is solvable.)

We close this thesis by pointing out that these theorems have natural analogues in the setting of groups with biality. That is, if $M$ is a Moufang loop, if $G$ is a group with biality giving rise to $M$, and if $I = C_G(I)$ then we have

Theorem 11.

a) If $I$ is trivial then $M$ is an abelian group.

b) If $I$ is cyclic and if $G$ is finite, then $G'' = 1$.

c) Conjecture: If $I$ is abelian then $G$ is solvable.

Proof.

a) Trivial.

b) [NK, Thm. 3.6].
REFERENCES


GENERAL SUMMARY

This thesis consists of four parts. Part I is an investigation of quasigroup modules via a new subgroup, the endocenter.

Part II offers a natural context from which to study Moufang loops, the class of groups with biality. This class generalizes Doro's groups with triality and provides a setting from which to classify multiplication groups of various classes of inverse property loops.

Part III includes a partial classification of those Moufang loops whose multiplication group is with triality, a short list of universal multiplication groups that are with triality, and a complete description of all groups with triality associated with cyclic groups.

Part IV initiates an algebraic investigation of triality groups, considers some of the geometry associated with Moufang loops, and describes some groups with triality with abelian stabilizer subgroups.

Throughout the thesis, various open problems are mentioned, and components of the author's ongoing research projects are outlined.
BIBLIOGRAPHY


ACKNOWLEDGEMENTS

This thesis would not have been possible without the support and encouragement of a variety of people. Chief among them is my wife, Cathy. Her patience and grace during the writing of this thesis (and during all of my graduate school years) were inspiring. The support she gives me is evident on every page of this thesis. To her, whom I owe so much, I simply say, "Thanks."

My mother, Donna, my father, Jon, and his wife Mary, together with my brothers, David and Peter, have given me more than I can hope to return. They've provided me with a warm, supportive emotional and intellectual environment. Their unconditional acceptance and love is a continual source of strength. My gratitude to them is enormous.

I offer my thanks to the faculty of Briar Cliff College, from whom I first learned about the life of the mind. In particular, I would like to thank Professors Norine Ryan, Craig Kalicki and Bill Cooney (and Rev. Victor Raemaker from Heelan High School) for inspiring me as a scholar and for caring about me as a human being. Their influence on me was tremendous.

I am indebted to my graduate school friends for offering the kind of support and encouragement that only "fellow sufferers" can provide. The ordeals of qualifying exams, classroom competition, and a neverending succession of deadlines, were made bearable largely through the friendship and compassion of my peers. Although there are many to whom I am grateful, the following deserve special mention: Mike Millar, Kirk Jones, Xiaorong Shen, Paul Hertzel, Monthy Fuad, Anand Medapalli and Sundar Athreya.

I am indebted to the professors in the mathematics department at Iowa State University for teaching me mathematics. There are five faculty members to whom
I would like to give special thanks: Alexander Abian, Clifford Bergman, Elgin Johnston, Jonathan Smith and Anne Steiner. These five mathematicians catalyzed my development as a mathematician and a scholar.

Professor Smith deserves singular thanks. As my thesis advisor, he worked with me more closely than anyone else. He consoled me and encouraged me during the hard times. He focused my energies during the good times. But most of all he taught me, not only the mathematics that I now pursue, but also the scholar's outlook on life. The care and consideration he shows for students, both in the classroom and as a thesis advisor, are inspirational.

It's been a great pleasure to work with the secretaries and the staff of the mathematics department. In particular; Madonna Blanshan, Ruth DeBoer and Jan Nyhus have been great friends over the past six years. I offer special thanks to Jan for typing this thesis.

As a mathematician I am most interested in aesthetics. I view mathematics as I view art, literature, philosophy and music. That is to say, I view mathematics as a monument to man's creative powers. Perhaps utility has its place in mathematics, but it is peripheral to beauty and elegance. And so I would like to thank some of the creators whose works have comforted and inspired me: Albert Camus, Ayn Rand, Fyodor Dostoyevsky, Wolfgang Amadeus Mozart, Franz Schubert, Johan Sebastian Bach, Benjamin Britten, Dmitri Shostakovich, Antonin Dvorak, Claude Monet, Vincent Van Gogh, Paul Cezanne, Kurt Godel, Everiste Galois, Georg Cantor and Ruth Moufang.

In this same spirit of recognizing the creators, I would like to dedicate this thesis to my youngest brother, Peter. His integrity to the creative ideal is unwavering. His singleness of purpose and his dedication to his art are truly epic. As a creator and as an artist, he is an inspiration. I hope the work in this thesis conforms to his high standards of creativity.