J. Group Theory **15** (2012), 775–783
DOI 10.1515/jgt-2012-0022

Metabelian groups that admit triality

Stephen M. Gagola III

Communicated by Dessislava H. Kochloukova

Abstract. A problem proposed by Grishkov asks if every metabelian triality group has a corresponding Moufang loop which is a group. Here we show that if minimal counter-examples exist, then such triality groups have to be p-groups. In fact, for any prime p, there exists a metabelian p-group that admits triality and has a corresponding Moufang loop that is not a group. Here we also determine how to strengthen the hypothesis of the original problem so that the corresponding Moufang loop is indeed a group.

1 Introduction

Suppose that G is a group and $S \leqslant \mathrm{Aut}(G)$ where $S = \langle \sigma, \rho \rangle \cong S_3$ with $|\sigma| = 2$ and $|\rho| = 3$. Here G is called a *group with triality* S if $[G, S] = G$ and for every $g \in G$

$$[g,\sigma][g,\sigma]^{\rho}[g,\sigma]^{\rho^2} = 1$$

where $[g,\sigma] = g^{-1}g^{\sigma}$. Note that if $a = [g,\sigma]$ for some $g \in G$, then it follows that $a^{\sigma} = a^{-1}$.

If G is a group with triality $S = \langle \sigma, \rho \rangle$ and $L = \{[g,\sigma] \mid g \in G\}$, then, from Doro [2], L is a Moufang loop associated with G under the new binary operation

$$\begin{aligned} a \centerdot b &= b^{-\rho^2} a b^{-\rho} \\ &= a^{-\rho} b a^{-\rho^2}. \end{aligned} \tag{1.1}$$

A *Moufang loop* is a generalization of a group that arises when the associative law is replaced with the Moufang identity $(a(bc))a = (ab)(ca)$.

A group G is called *metabelian* if its derived subgroup $G' = [G, G]$ is abelian; thus G is metabelian if and only if it has a normal abelian subgroup such that the quotient group is abelian. Likewise, a Moufang loop K is said to be metabelian if it has a normal subloop N such that both N and K/N are abelian. Grishkov asked the open problem whether every metabelian triality group has a corresponding Moufang loop which is a group. In Section 2 it is shown that if a counter-example exists, then such a triality group must contain a p-subgroup that admits triality with a corresponding Moufang loop that is nonassociative. Triality groups are then constructed in Section 3 using Latin square designs showing that for any prime p there do exist metabelian p-groups that admit triality and have corresponding Moufang loops that are not groups. However, by strengthening the hypothesis of the original problem, the following theorem is obtained.

Theorem 1.1. *Suppose that G is a finite metabelian group that admits triality. Let L be its corresponding Moufang loop and let N be the Moufang loop associated with G'. If there does not exist a prime $p \geqslant 5$ such that*

$$p^2 \mid |N| \quad \textit{and} \quad p^3 \mid |L/N|$$

and there does not exist a prime $q \in \{2, 3\}$ such that

$$q \mid |N| \quad \textit{and} \quad q^3 \mid |L/N|,$$

then L is a group.

2 Metabelian triality groups associated with groups

In this section we look at metabelian triality groups and develop tools needed to prove Theorem 1.1 along with the fact that minimal metabelian triality groups with corresponding nonassociative Moufang loops must be p-groups.

Lemma 2.1. *Suppose G is a metabelian group that admits triality S. If L is its corresponding Moufang loop then L is metabelian.*

Proof. Note that the derived subgroup G' of G is invariant under S. Let N be the subloop of L associated with G'. Since G' is an S-invariant normal subloop of G, by Doro [2], G/G' is a group with triality associated with a loop isomorphic to L/N. Since G' and G/G' are abelian groups, N and L/N are abelian groups. Hence, L is metabelian. □

Lemma 2.2. *Suppose P is a p-group that admits triality $S = \langle \sigma, \rho \rangle$ where L is its corresponding Moufang loop. Let N be the subloop of L associated with P'. If N is nontrivial, then the center of L intersects N nontrivially.*

Proof. If L is an abelian group, then $L = Z(L)$ and the lemma immediately follows. Thus, without loss, it may be assumed that L is not an abelian group.

Let $Q = \langle L, L^{\rho}, L^{\rho^2} \rangle \leqslant P$ be the minimal subgroup of P that admits triality S and has L as its corresponding Moufang loop. There then exists a subgroup $Z \leqslant Z(Q)$ such that, up to isomorphism, Q/Z is the minimal triality group of L. Since L is not an abelian group, Q/Z is nonabelian. Since Q/Z is a nonabelian

p-group, $(Q/Z)'$ intersects the center of Q/Z nontrivially. By minimality of Q/Z, $(Q/Z)' \cap Z(Q/Z)$ contains nontrivial elements of $[Q/Z, \sigma] \cong L$. Such elements both commute and associate with all of the elements in the loop and are therefore in the center. Thus Q', and therefore P', contains nontrivial elements of $Z(L)$. Hence, its corresponding Moufang loop N intersects the center of L nontrivially. □

Lemma 2.3. *Let G be a group that admits triality $S = \langle \sigma, \rho \rangle$ and let L be its corresponding Moufang loop. For any $x, y \in L$, $[x^\rho, y^{\rho^2}] \in C_G(\sigma)$.*

Proof. If $x, y \in L$, then

$$\begin{aligned}
[x^\rho, y^{\rho^2}]^\sigma [x^\rho, y^{\rho^2}]^{-1} &= (x^{-\rho} y^{-\rho^2} x^\rho y^{\rho^2})^\sigma (x^{-\rho} y^{-\rho^2} x^\rho y^{\rho^2})^{-1} \\
&= x^{\rho^2} y^\rho x^{-\rho^2} y^{-\rho} y^{-\rho^2} x^{-\rho} y^{\rho^2} x^\rho \\
&= y^{-1} \centerdot y \centerdot x \centerdot x^{-1} \\
&= 1.
\end{aligned}$$

Hence, $[x^\rho, y^{\rho^2}]^\sigma = [x^\rho, y^{\rho^2}]$. □

It is known from Moufang [9] that if three elements of a Moufang loop associate in some order, then they associate in any order. For a Moufang loop L, the set of its elements that associate with all of its other elements forms a normal subloop of L called the *nucleus* of L and is often denoted by

$$\mathrm{Nuc}(L) = \{x \in L \mid x(yz) = (xy)z \text{ for all } y, z \in L\}.$$

Lemma 2.4. *Let G be a metabelian group that admits triality $S = \langle \sigma, \rho \rangle$ and let L be its corresponding Moufang loop. If an element $a \in L$ is contained in the derived subgroup of G, then $a \in \mathrm{Nuc}(L)$.*

Proof. Suppose the element $a \in L$ is contained in $[G, G]$. Then for any $x, y \in L$, the element a commutes with $[x^\rho, y^{\rho^2}]$, and therefore

$$\begin{aligned}
y \centerdot (a \centerdot x) &= y^{-\rho} x^{-\rho^2} a x^{-\rho} y^{-\rho^2} \\
&= x^{-\rho^2} y^{-\rho} [x^\rho, y^{\rho^2}]^{-\sigma} a [x^\rho, y^{\rho^2}] y^{-\rho^2} x^{-\rho} \\
&= x^{-\rho^2} y^{-\rho} [x^\rho, y^{\rho^2}]^{-1} a [x^\rho, y^{\rho^2}] y^{-\rho^2} x^{-\rho} \\
&= x^{-\rho^2} y^{-\rho} a y^{-\rho^2} x^{-\rho} \\
&= (y \centerdot a) \centerdot x.
\end{aligned}$$

Hence, $a \in \mathrm{Nuc}(L)$. □

Corollary 2.5. *Let G be a metabelian triality group and let L be its corresponding Moufang loop. If $N \leqslant L$ is the Moufang loop associated with the derived subgroup of G and $x, y \in L$, then the subloop $\langle x, y, N \rangle$ is a group.*

Proof. By Lemma 2.4, N is contained in $\mathrm{Nuc}(L)$. Thus the generators of $\langle x, y, N \rangle$ associate in any order. □

Proposition 2.6. *Let L be a Moufang loop such that $L/\mathrm{Nuc}(L)$ is a finite abelian group. If*

$$L/\mathrm{Nuc}(L) \cong \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_n^{m_n}}$$

and there do not exist indices i, j, k with $1 \leqslant i < j < k \leqslant n$ with $p_i = p_j = p_k$, then L is a group.

Proof. By the hypothesis on the indices, $L/\mathrm{Nuc}(L)$ is a direct product of two cyclic subgroups. Hence, L can be generated by $\mathrm{Nuc}(L)$ along with two other elements of L, making L a group. □

Theorem 2.7. *Suppose L is a finite Moufang loop where $L/\mathrm{Nuc}(L)$ is an abelian group. If L is not a group, then L contains a nonassociative Sylow p-subloop for some prime p.*

Proof. Since $L/\mathrm{Nuc}(L)$ is a finite abelian group,

$$L/\mathrm{Nuc}(L) \cong \mathbb{Z}_{p_1^{m_1}} \times \mathbb{Z}_{p_2^{m_2}} \times \cdots \times \mathbb{Z}_{p_n^{m_n}}$$

for some primes $p_1, \dots, p_n$. Let $g_1, \dots, g_n$ be elements of L such that $\bar{g}_1, \dots, \bar{g}_n$ are generators of $L/\mathrm{Nuc}(L)$ with $|\bar{g}_i| = p_i^{m_i}$. If the elements $g_1, \dots, g_n$ all associate in L, then $L = \langle g_1, \dots, g_n, \mathrm{Nuc}(L) \rangle$ must be a group. Since L is nonassociative, there exist g_i, g_j, g_k which do not associate. Assume that p_i, p_j, and p_k are not all equal. Then by Proposition 2.6, $\langle g_i, g_j, g_k, \mathrm{Nuc}(L) \rangle$ is a group which contradicts the fact that g_i, g_j and g_k do not associate. Thus $p_i = p_j = p_k$ and $\langle \bar{g}_i, \bar{g}_j, \bar{g}_k \rangle$ is a p-group where $p = p_i$. Since L does not contain any composition factors that are nonassociative, from [3], there exists a Sylow p-subloop of $\langle g_i, g_j, g_k, \mathrm{Nuc}(L) \rangle$, say P. Since $\langle P, \mathrm{Nuc}(L) \rangle = \langle g_i, g_j, g_k, \mathrm{Nuc}(L) \rangle$ is nonassociative, P itself is nonassociative. Hence, from [3], P is embedded inside of a nonassociative Sylow p-subloop of L. □

Theorem 2.8. *If there exist finite metabelian groups that admit triality with corresponding Moufang loops that are nonassociative, then minimal such groups must be p-groups.*

Proof. Let G be a minimal such group and let L be its corresponding Moufang loop. If $N \leqslant L$ is the loop associated with G', then, by Lemma 2.4, $N \leqslant \mathrm{Nuc}(L)$. Furthermore, from Lemma 2.1, L/N is an abelian group. It then follows from Theorem 2.7 that L contains a nonassociative Sylow p-subloop, say P. By minimality of G, $L = P$. It is known from [4] that if K is a Moufang p-loop, then a minimal triality group associated with it must be a p-group. Hence, G itself is a p-group. □

The following lemma, originally proven by Hsu [7, Theorem A], is a useful tool needed to prove Theorem 1.1.

Lemma 2.9. *If L is a finite Moufang loop with an order that is coprime to* 6 *and* $L/Z(L)$ *is abelian, then L is a group.*

Proof. Assume that this is not true and let L be a minimal counter-example. Since $L/Z(L)$ is abelian with an order coprime to 6, L contains a normal subloop of index p, say H, such that p is a prime greater than three and $Z(L) \leqslant H$. By minimality of L, H is a group. Let $u \in L \setminus H$ be an element of order a power of p and define $\varphi : H \to H$ by

$$g \to u^{-1}gu.$$

Now let $x, y \in H$ be arbitrary elements. Since $2 \nmid |L|$, x has a unique square root in L which will be denoted by $x^{1/2}$. Thus, since $L/Z(L)$ is abelian, there exists an element $c \in Z(L)$ such that

$$xy = x^{1/2}x^{1/2}y = x^{1/2}yx^{1/2}c = x^{1/2}ycx^{1/2}.$$

Moreover, there exist elements $a, b \in Z(L)$ such that

$$\varphi(x^{1/2}) = x^{1/2}a \quad \text{and} \quad \varphi(y) = yb.$$

It is known from Bruck [1] that φ is a semi-automorphism of H, namely,

$$\varphi(ghg) = \varphi(g)\varphi(h)\varphi(g) \quad \text{for any } g, h \in H.$$

Hence

$$\begin{aligned}\varphi(xy) &= \varphi(x^{1/2}ycx^{1/2}) = \varphi(x^{1/2})\varphi(yc)\varphi(x^{1/2}) = x^{1/2}aybcx^{1/2}a \\ &= x^{1/2}yx^{1/2}ca^2b = xya^2b = x^{1/2}ax^{1/2}ayb = \varphi(x^{1/2})\varphi(x^{1/2})\varphi(y) \\ &= \varphi(x)\varphi(y).\end{aligned}$$

Since φ is an automorphism of H and u has order coprime to 3, by [5, Proposition 4.3 and Lemma 4.4], u associates with all of the elements in H. Therefore $L = \langle u, H \rangle$ is a group, and this contradicts the assumption. □

Proof of Theorem 1.1. Suppose that L is not a group. Then by Theorem 2.7, L contains a nonassociative Sylow p-subloop, say P, for some prime p. By Lemma 2.1, L/N is an abelian group. Thus $p \mid |N|$, since otherwise P would be isomorphic to a Sylow p-subgroup of L/N. Moreover, by Proposition 2.6, in order for P to be nonassociative, p^3 must divide $|L/N|$. Furthermore, if $p > 3$, then, by Lemma 2.9, N is not contained in $Z(P)$, since otherwise P would be a group. Also, by Lemma 2.2, N intersects the center of P nontrivially. Hence, the order of N is at least p^2. □

3 Creating minimal counter-examples using Latin square designs

In this section we show that for any prime p there exists a metabelian p-group that admits triality and has a corresponding Moufang loop that is not a group. We do so by creating such a group using a Latin square design that is associated with the Cayley table of a nonassociative Moufang p-loop.

Definition 3.1. A Latin square design $\mathcal{D}$ is a pair $\mathcal{D} = (P, A)$ of points $P = P(\mathcal{D})$ and lines $A = A(\mathcal{D})$ (subsets of P) such that

(i) P is the disjoint union of three parts R, C, E with $|R| = |C| = |E|$,

(ii) every line $l \in A$ contains exactly three points, meeting each of R, C, E exactly once,

(iii) any pair of points from different parts belong to exactly one line.

Suppose that L is a Moufang loop. A Latin square design may be constructed using the loop L. This design can then be used to construct a triality group whose corresponding Moufang loop is isomorphic to L. The details are given in the following example.

Example 3.2. Let the point set consist of three disjoint copies of L,

$$P = L_R \cup L_C \cup L_E,$$

and let the line set A be the set of triples $\{a_R, b_C, c_E\}$ with $(ab)c = 1$ in L. For any $x \in L$ define the permutations f_x, g_x, h_x of L by

$$f_x : a \to xa, \quad g_x : a \to ax, \quad h_x : a \to x^{-1}ax^{-1}.$$

Now let $H = \mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ and define G to be the following subgroup of H:

$$G = \langle (f_x, g_x, h_x), (g_x, h_x, f_x), (h_x, f_x, g_x) \in H \mid x \in L \rangle.$$

Note that the group G contains permutations of the point set P that take lines to lines. Moreover, the group G is a group with triality $S = \langle \sigma, \rho \rangle$ with

$$(f, g, h)^{\rho} = (g, h, f) \quad \text{and} \quad (f, g, h)^{\sigma} = (g', f', h')$$

where

$$g'(a) = g(a^{-1})^{-1}, \quad f'(a) = f(a^{-1})^{-1} \quad \text{and} \quad h'(a) = h(a^{-1})^{-1}$$

for all $(f, g, h) \in G$.

Note that if $(f, g, h) \in G$ where $c = h(1)$, then for any $x \in L$, $g(x^{-1})$ must equal $f(x)^{-1}c^{-1}$ in order for (f, g, h) to take the line $\{x_R, x_C^{-1}, 1_E\}$ to another line. Using the fact that $g(x^{-1}) = f(x)^{-1}c^{-1}$ for all $x \in L$ it then follows that $(f, g, h)^{-1}(f, g, h)^{\sigma} = (f_c, g_c, h_c)$. Hence,

$$[G, \sigma] = \{(f_x, g_x, h_x) \in G \mid x \in L\}.$$

Under the binary operation $\centerdot$ defined by equation (1.1), $[G, \sigma]$ is isomorphic to L.

Example 3.2 can then be used to create minimal metabelian groups that admit triality and have corresponding nonassociative Moufang loops. If p is either 2 or 3, then there are exactly five nonassociative Moufang loops of order p^4 which can be retrieved in GAP [6] as `MoufangLoop(p^4,i)` with $1 \leqslant i \leqslant 5$. Using GAP, a triality group associated with such a Moufang loop $L = \langle x, y, u \rangle$ can then be generated by

$$\{(f_c, g_c, h_c), (g_c, h_c, f_c) \mid c \in \{x, y, u\}\}$$

as a subgroup of $\mathrm{Sym}(p^4) \times \mathrm{Sym}(p^4) \times \mathrm{Sym}(p^4)$ as in Example 3.2. For every nonassociative Moufang loop of order 16, the minimal triality group associated with it is metabelian of order 2^{11}, of exponent 4, and has a derived subgroup that is an elementary abelian 2-group of order 32. For the two nonassociative Moufang loops of order 81 and exponent 3, the minimal corresponding triality group is metabelian of order 3^7, of exponent 3, and has a derived subgroup that is an elementary abelian 3-group of order 81. Likewise, for the three nonassociative Moufang loops of order 81 and exponent 9, the minimal corresponding triality group is metabelian of order 3^8, of exponent 9, and has a derived subgroup that is an elementary abelian 3-group of order 81.

Proposition 3.3. *For any prime $p \geqslant 5$ there exists a metabelian group that admits triality and is associated with a nonassociative Moufang loop of order p^5.*

Proof. For primes $p \geqslant 5$, it is known from Leong [8] and from Nagy and Valsecchi [10] that all Moufang loops of order p^4 are groups and that there are exactly four nonassociative Moufang loops of order p^5 each with a nilpotency class equal to 3. Let L be a nonassociative Moufang loop of order p^5. From Nagy and Valsecchi [10, Theorem 3.2], the nilpotency class of the multiplication group of L, $\mathrm{Mlt}(L)$, is also 3. Since the nilpotency class of $\mathrm{Mlt}(L)$ is 3, the derived length of $\mathrm{Mlt}(L)$ is bounded above by $\log_2(3) + 1$ and is therefore equal to 2. From Example 3.2, a triality group associated with L, say G, can be generated by

$$\{(f_x, g_x, h_x), (g_x, h_x, f_x), (h_x, f_x, g_x) \mid x \in L\}$$

as a subgroup of $\mathrm{Mlt}(L) \times \mathrm{Mlt}(L) \times \mathrm{Mlt}(L)$. Since $\mathrm{Mlt}(L)$ is metabelian, so is $\mathrm{Mlt}(L) \times \mathrm{Mlt}(L) \times \mathrm{Mlt}(L)$ and thus G is a metabelian group. □

From these cases, it follows that for any prime p there are metabelian p-groups that admit triality with corresponding Moufang loops that are not groups.

Acknowledgments. The author would like to thank the referee for suggestions that improved the proof of Proposition 3.3.

Bibliography

[1] R. H. Bruck, Pseudo-automorphisms and Moufang loops, *Proc. Amer. Math. Soc.* **3** (1952), 66–72.

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

[3] S. M. Gagola III, The development of Sylow p-subloops in finite Moufang loops, *J. Algebra* **322** (2009), 2804–2810.

[4] S. M. Gagola III, The number of Sylow p-subloops in finite Moufang loops, *Comm. Algebra* **38** (2010), 1436–1448.

[5] S. M. Gagola III, Abelian by cyclic groups resulting in Moufang loops, *J. Group Theory* **15** (2012), 1–7.

[6] The GAP Group, *GAP-Groups, Algorithms, and Programming,* Version 4.4.12, 2008, `http://www.gap-system.org`.

[7] T. Hsu, Moufang loops of class 2 and cubic forms, *Math. Proc. Cambridge Philos. Soc.* **128** (2000), 197–222.

[8] F. Leong, Moufang loops of order p^4, *Nanta Math.* **7** (1974), 33–34.

[9] R. Moufang, Zur Struktur von Alternativkörpern, *Math. Ann.* **110** (1934), 416–430.

[10] G. Nagy and M. Valsecchi, On nilpotent Moufang loops with central associators, *J. Algebra* **307** (2007), 547–564.

Received February 24, 2012; revised July 8, 2012.

Author information

Stephen M. Gagola III, Department of Algebra, Charles University,
Sokolovská 83, 186 75 Prague 8, Czech Republic.
E-mail: gagola@karlin.mff.cuni.cz