Math. Proc. Camb. Phil. Soc. (2021), **170**, 609–614 © *Cambridge Philosophical Society* 2020
doi:10.1017/S0305004119000549
First published online 10 January 2020

Moufang loops with nonnormal commutative centre

BY ALEXANDER N. GRISHKOV
Departamento de Matemática, Universidade de São Paulo, Caixa Postal 66281, *São Paulo-SP,* 05311-970, *Brazil.*
e-mail: grishkov@ime.usp.br

AND ANDREI V. ZAVARNITSINE†
Sobolev Institute of Mathematics, 4, *Koptyug av., Novosibirsk,* 630090, *Russia.*
e-mail: zav@math.nsc.ru

(*Received* 29 *November* 2017; *accepted* 07 *October* 2019)

Abstract

We construct two infinite series of Moufang loops of exponent 3 whose commutative centre (i. e. the set of elements that commute with all elements of the loop) is not a normal subloop. In particular, we obtain examples of such loops of orders 3^8 and 3^{11} one of which can be defined as the Moufang triplication of the free Burnside group B(3, 3).

2010 Mathematics Subject Classification: 20N05

1. *Introduction*

A Moufang loop is a loop in which the identity

$$(xy)(zx) = (x(yz))x \tag{1·1}$$

holds. Moufang loops are known to be *diassociative*, i. e. their subloops generated by a pair of elements are groups. In particular, elements of Moufang loops have unique inverses and $(xy)^{-1} = y^{-1}x^{-1}$ for all x, y.

The *commutative centre* (also known as the *Moufang centre* or the *commutant*[1]) of a Moufang loop M is the set

$$\mathrm{C}(M) = \{c \in M \mid cx = xc \text{ for all } x \in M\}.$$

It is known [**7**, theorem IV·3·10] that $\mathrm{C}(M)$ is a subloop of M which is characteristic.

Officially raised by A. Rajah at *Loops* '03 conference in Prague, the following problem has been open for quite a while.

†Supported by the program of fundamental scientific research of SB RAS No. I.1.1., project No. 0314-2016-0001 and by FAPESP, process 2017/14489-2.

[1]We avoid using the term 'commutant' due to the unfortunate collision with the term 'derived subgroup' as both are translated into Russian as 'КОММУТАНТ'.

Problem 1·1. Is $\mathrm{C}(M)$ a normal subloop of M?

It was stated in [2] that the answer to this question is affirmative. Here we show that the answer is in fact generally negative by constructing two series of examples of Moufang loops whose commutative centre is not normal. The first series is given by an explicit multiplication formula over any field of characteristic 3. This series contains a finite loop of order 3^{11}. The second series is a particular case of the triplication of Moufang loops of exponent 3. We show that, for any Moufang loop M of exponent 3 that does not satisfy the identity $[[x, y], z] = 1$, there is a Moufang loop $\mathrm{M}(M, 3)$ whose commutative centre is not normal. In particular, we have the example $\mathrm{M}(\mathrm{B}(3, 3), 3)$ of order 3^8, where $\mathrm{B}(3, 3)$ is the free 3-generator Burnside group of exponent 3. As proposed by the referee, we state:

CONJECTURE 1·2. *The minimal order of a Moufang loop with nonnormal commutative centre is* 3^8.

Recall that the *nucleus* of a Moufang loop M is

$$\mathrm{Nuc}(M) = \{a \in M \mid (ax)y = a(xy) \text{ for all } x, y \in M\}.$$

Our results reopen the following conjecture by S. Doro [1]:

CONJECTURE 1·3. *If* $\mathrm{Nuc}(M) = 1$ *then* $\mathrm{C}(M)$ *is normal in* M.

2. *Motivation*

For elements x, y, z of a Moufang loop M, we denote by $[x, y]$ the unique element $s \in M$ such that $xy = (yx)s$ and by (x, y, z) the unique element $t \in M$ such that $(xy)z = (x(yz))t$.

The idea behind the construction is the following straightforward observation.

LEMMA 2·1. *If* $\mathrm{C}(M)$ *is normal in* M *then, for every* $a \in \mathrm{C}(M)$ *and every* $b, c, d \in M$, *we have* $[(a, b, c), d] = 1$.

Proof. Since $\mathrm{C}(M)$ is normal and $a \in \mathrm{C}(M)$, we have $(a, b, c) \in \mathrm{C}(M)$, because this associator is mapped by the natural homomorphism $^- : M \to M/\mathrm{C}(M)$ to $(\overline{a}, \overline{b}, 1) = 1$ and hence must lie in its kernel.

Therefore, for any Moufang loop L, if there is $a \in \mathrm{C}(L)$ such that $[(a, b, c), d] \neq 1$ for some $b, c, d \in L$ then $\mathrm{C}(L)$ is not a normal subloop in view of Lemma 2·1. Examples of such loops are constructed in the next sections.

Recall that *the centre* $\mathrm{Z}(M)$ of a Moufang loop M consists of all $x \in \mathrm{C}(M)$ such that $(a, x, b) = 1$ for every $a, b \in M$. It is known that $\mathrm{Z}(M)$ is a normal subloop of M. The following classical result explains why the search for Moufang loops with nonnormal commutative centre may be started by looking at 3-loops. It implies that if $c \in \mathrm{C}(M)$ has finite order coprime to 3 then $c \in \mathrm{Z}(M)$.

LEMMA 2·2. *If* M *is a Moufang loop and* $c \in \mathrm{C}(M)$ *then* $c^3 \in \mathrm{Z}(M)$.

Proof. For $a, b \in M$, we have

$$(ac^3)b = (c.ac.c)b = c(ac.cb) = (ac.cb)c = a(c.cb.c) = a(c^3b),$$

https://doi.org/10.1017/S0305004119000549 Published online by Cambridge University Press

hence $c^3 \in \mathrm{Z}(M)$, where we have used diassociativity and the identities $((xy)x)z = x(y(xz))$ and $((zx)y)x = z(x(yx))$ which are equivalent to the Moufang identity (1·1).

3. *Algebraic loop*

The underlying set of the loop is an 11-dimensional vector space V over a field F of characteristic 3. An element $x \in V$ will be written as a tuple $x = (x_1, x_2, \ldots, x_{11})$, $x_i \in F$. We introduce a new operation '$\circ$' on V which is given, for $x, y \in V$, by

$$x \circ y = x + y + f, \tag{3·1}$$

where $f = (f_1, \ldots, f_{11})$ and f_k are polynomials in x_i, y_j explicitly given below.

$$\begin{aligned}
f_1 &= f_2 = f_3 = f_4 = 0,\\
f_5 &= -x_3y_2,\ \ f_6 = -x_4y_2,\ \ f_7 = -x_4y_3,\\
f_8 &= \ \ x_1x_3y_2 - x_1y_2y_3 - x_2x_3y_1 + x_2y_1y_3,\\
f_9 &= \ \ x_1x_4y_2 - x_1y_2y_4 - x_2x_4y_1 + x_2y_1y_4,\\
f_{10} &= \ \ x_1x_4y_3 - x_1y_3y_4 - x_3x_4y_1 + x_3y_1y_4,\\
f_{11} &= -x_1x_2x_4y_3 + x_1x_2y_3y_4 + x_1x_3y_2y_4 + x_1x_4y_2y_3 + x_2x_3y_1y_4 + x_2x_4y_1y_3\\
&\quad - x_2y_1y_3y_4 + x_3x_4y_1y_2 - x_4y_1y_2y_3 - x_1x_5y_4 + x_1x_6y_3 - x_1x_7y_2 + x_1y_2y_7\\
&\quad - x_1y_3y_6 + x_1y_4y_5 + x_2x_7y_1 - x_2y_1y_7 - x_3x_6y_1 + x_3y_1y_6 + x_4x_5y_1 - x_4y_1y_5\\
&\quad + x_8y_4 - x_9y_3 + x_{10}y_2.
\end{aligned}$$

It can be checked that $L = (V, \circ)$ is a loop in which the Moufang identity (1·1) holds. We omit the heavily technical verification. The identity element of L is the zero vector of V and, for $x \in L$, we have

$$x^{-1} = -x + h, \tag{3·2}$$

where $h = (h_1, \ldots, h_{11})$ and the polynomials h_k are as follows:

$$\begin{aligned}
h_1 &= h_2 = h_3 = h_4 = h_8 = h_9 = h_{10} = 0,\\
h_5 &= -x_2x_3,\ \ h_6 = -x_2x_4,\ \ h_7 = -x_3x_4,\\
h_{11} &= \ \ x_2x_{10} - x_3x_9 + x_4x_8.
\end{aligned}$$

Let $e_1, \ldots, e_{11}$ be the standard basis of V, i. e., $e_i = (\ldots, 0, 1, 0, \ldots)$ with '1' at the ith place. Define

$$a = e_1, \quad b = e_2, \quad c = e_3, \quad d = e_4.$$

LEMMA 3·1. *$a \in \mathrm{C}(L)$.*

Proof. This is true because using the multiplication formula (3·1) one can check that, for an arbitrary $x \in L$, both $a \circ x$ and $x \circ a$ equal

$$x + a + (0, 0, 0, 0, 0, 0, 0, 0, -x_2x_3, -x_2x_4, -x_3x_4, x_2x_7 - x_3x_6 + x_4x_5).$$

LEMMA 3·2. *$[(a, b, c), d] \neq 1$ in L.*

https://doi.org/10.1017/S0305004119000549 Published online by Cambridge University Press

Proof. Using (3·1) it can be shown that the following equalities hold in L:

$$e_5 = [b, c],\ e_6 = [b, d],\ e_7 = [c, d],$$
$$e_8 = (a, b, c),\ e_9 = (a, b, d),\ e_{10} = (a, c, d),$$
$$e_{11} = [(a, b, c), d].$$

Since $e_{11} \neq 0$ in V, it follows that $[(a, b, c), d]$ is not the identity element of L.

Therefore, Lemma 2·1 implies:

COROLLARY 3·3. *$\mathrm{C}(L)$ is not a normal subloop of L.*

The following properties of L are worth mentioning. L has exponent 3 and satisfies the identity $[[x, y], z] = 1$. $\mathrm{C}(L) = \langle e_1, e_5, e_6, e_7, e_{11}\rangle_F$ is associative, where $\langle\ \rangle_F$ denotes the F-linear span in V, and is close to being normal — it has a subloop N of index 3 which is normal in L. We have $N = \langle e_5, e_6, e_7, e_{11}\rangle_F$ and L/N is commutative. Also, $\mathrm{Nuc}(L) = \langle e_8, e_9, e_{10}, e_{11}\rangle_F$ and $\mathrm{Z}(L) = \mathrm{Nuc}(L) \cap \mathrm{C}(L) = \langle e_{11}\rangle_F$.

In particular, if $F = \mathbb{F}_3$, we obtain an example of order 3^{11}.

4. *Triplication of Moufang loops of exponent* 3

In this section, we revisit the construction from [4] which allows us, given a Moufang loop M of exponent 3, to obtain a larger one that contains M as a normal subloop of index 3.

A group G possessing automorphisms ρ and σ that satisfy $\rho^3 = \sigma^2 = (\rho\sigma)^2 = 1$ is called a *group with triality* $S = \langle \rho, \sigma\rangle$ if

$$(x^{-1}x^{\sigma})(x^{-1}x^{\sigma})^{\rho}(x^{-1}x^{\sigma})^{\rho^2} = 1$$

for every x in G. In such a group, the set

$$\mathcal{M}(G) = \{x^{-1}x^{\sigma} \mid x \in G\}$$

is a Moufang loop with respect to the multiplication

$$m.n = m^{-\rho}nm^{-\rho^2} \tag{4·1}$$

for all $n, m \in \mathcal{M}(G)$. Conversely, every Moufang loop arises so from a suitable group with triality. Observe that taking powers or inverses of elements of $\mathcal{M}(G)$ is the same, whether considered under the loop or group operation. We will also require the following properties.

LEMMA 4·1 ([5, lemma 2·1]). *Let G be a group with triality $S = \langle \rho, \sigma\rangle$. Then, for all $m, n \in \mathcal{M}(G)$, we have:*

(i) $m^{\sigma} = m^{-1}$;
(ii) m, m^{ρ}, m^{ρ^2} *pairwise commute*;
(iii) $m^{-\rho}nm^{-\rho^2} = n^{-\rho^2}mn^{-\rho}$;
(iv) $m.n.m = mnm$.

For more details on groups with triality, see [1, 3].

In the loop $(\mathcal{M}(G), .)$, we write $[\![x, y]\!] = x^{-1}.y^{-1}.x.y$ instead of $[x, y] = x^{-1}y^{-1}xy$ to make a distinction between the loop and group commutator.

https://doi.org/10.1017/S0305004119000549 Published online by Cambridge University Press

Let G be a group with triality $S = \langle \rho, \sigma \rangle$ and let $M = \mathcal{M}(G)$. It was observed in [4, lemma 3] that the natural semidirect product $\widetilde{G} = G \rtimes \langle \rho \rangle$ is also a group with triality S if and only if M has exponent 3. In this case, we will denote the corresponding Moufang loop $\mathcal{M}(\widetilde{G})$ by $\mathrm{M}(M, 3)$ and call it the *triplication* of M. It contains M as a normal subloop of index 3 and coincides as a subset of $\widetilde{G}$ with

$$M \cup \rho M \rho \cup \rho^2 M \rho^2.$$

LEMMA 4·2. *Let M be a Moufang loop of exponent 3 and let $L = \mathrm{M}(M, 3)$. Then:*

(i) *L has exponent 3;*
(ii) *The multiplication rule of L is as given in Table I;*
(iii) $\rho \in \mathrm{C}(L)$;
(iv) $(\rho, m, n) = [\![n^{-1}, m^{-1}]\!]$ *for all $m, n \in M$;*
(v) *L is associative iff M is an abelian group.*

Proof. We will use Lemma 4·1 and the fact that M has exponent 3 implicitly throughout the proof.

(i) Let $m \in L$. If $m \in M$ then $m^3 = 1$. If $m = \rho n \rho$ then $m^3 = \rho n \rho^2 n \rho^2 n \rho = n^{\rho^2} n n^{\rho} = 1$. If $n = \rho^2 n \rho^2$ then $n^3 = \rho^2 n \rho n \rho n \rho^2 = n^{\rho} n n^{\rho^2} = 1$. Hence, L has exponent 3.

(ii) Let $m, n \in M$. Then the product rules are

$$\begin{aligned}
&m.\rho n \rho = m^{-\rho} \rho n \rho m^{-\rho^2} = \rho m^{-\rho^2} n m^{-\rho} \rho = \rho(n.m)\rho,\\
&\rho m \rho.n = n^{-\rho^2} \rho m \rho n^{-\rho} = \rho n^{-1} m n^{-1} \rho = \rho(n^{-1}.m.n^{-1})\rho = \rho(m^{-1}.n.m^{-1})\rho,\\
&\rho m \rho.\rho n \rho = (\rho m \rho)^{-\rho} \rho n \rho (\rho m \rho)^{-\rho^2} = \rho m^{-1} \rho n \rho m^{-1} \rho = \rho^2 m^{-\rho} n m^{-\rho^2} \rho^2 = \rho^2 (m.n) \rho^2,\\
&\rho^2 m \rho^2.\rho n \rho = (\rho^2 m \rho^2)^{-\rho} \rho n \rho (\rho^2 m \rho^2)^{-\rho^2} = \rho m^{-\rho} \rho^2 n \rho^2 m^{-\rho^2} \rho = m^{-1} n m^{-1}\\
&\qquad\qquad = m^{-1}.n.m^{-1},
\end{aligned}$$

and similarly for other choices of the factors.

(iii) Let $m \in M$. Using (ii), we have

$$\begin{aligned}
\rho.n &= \rho^2 \rho^2.n = \rho^2 n \rho^2, & n.\rho &= n.\rho^2 \rho^2 = \rho^2 n^{-2} \rho^2 = \rho^2 n \rho^2,\\
\rho.\rho n \rho &= \rho^2 \rho^2.\rho n \rho = n, & \rho n \rho.\rho &= \rho n \rho.\rho^2 \rho^2 = n,\\
\rho.\rho^2 n \rho^2 &= \rho^2 \rho^2.\rho^2 n \rho^2 = \rho n \rho, & \rho^2 n \rho^2.\rho &= \rho^2 n \rho^2.\rho^2 \rho^2 = \rho n \rho.
\end{aligned}$$

Therefore, $\rho \in \mathrm{C}(L)$.

(iv) By (ii), we have

$$\begin{aligned}
(\rho, m, n) &= (\rho.(m.n))^{-1}.((\rho.m).n) = (\rho^2 (m.n) \rho^2)^{-1}.(\rho^2 m \rho^2.n)\\
&= (\rho (m.n)^{-1} \rho).(\rho^2 (n.m) \rho^2) = n.m.(m.n)^{-1} = [\![n^{-1}, m^{-1}]\!].
\end{aligned}$$

(v) If M is not associative then neither is L, since M is a subloop of L. By (iv), L is not associative if M is not commutative. Conversely, if M is a commutative group then Table I turns into the multiplication rule of the direct product $M \times \langle \rho \rangle$, hence L is associative in this case (an elementary abelian 3-group, in fact).

Lemma 4·2(ii) shows that up to isomorphism $\mathrm{M}(M, 3)$ does not depend on the group G as long as $\mathcal{M}(G) \cong M$ (such a group is not unique). In other words, we can construct $\mathrm{M}(M, 3)$

https://doi.org/10.1017/S0305004119000549 Published online by Cambridge University Press

Table I. The product $x.y$ in $\mathrm{M}(M, 3)$

$x \setminus y$	n	$\rho n\rho$	$\rho^2 n\rho^2$
m	$m.n$	$\rho(n.m)\rho$	$\rho^2(m^{-1}.n.m^{-1})\rho^2$
$\rho m\rho$	$\rho(m^{-1}.n.m^{-1})\rho$	$\rho^2(m.n)\rho^2$	$n.m$
$\rho^2 m\rho^2$	$\rho^2(n.m)\rho^2$	$m^{-1}.n.m^{-1}$	$\rho(m.n)\rho$

by adjoining to M an outer element $\rho = \rho^2\rho^2$ and use Table I to define multiplication on formal elements of the shape m, $\rho m\rho$, $\rho^2 m\rho^2$ with $m \in M$.

PROPOSITION 4·3. *Let M be a Moufang loop of exponent* 3 *that does not satisfy the identity* $[[x, y], z] = 1$. *Then the commutative centre of* $\mathrm{M}(M, 3)$ *is not a normal subloop.*

Proof. Denote $L = \mathrm{M}(M, 3)$. By Lemma 4·2(iii), $\rho \in \mathrm{C}(L)$. By assumption, there are $x, y, z \in M$ such that $[[y^{-1}, x^{-1}], z] \neq 1$. We have $(\rho, x, y) = [y^{-1}, x^{-1}]$ by Lemma 4·2(iv). Therefore, $\mathrm{C}(L)$ is not normal by Lemma 2·1.

It is known [**6**, section 18·2] that the free r-generator Burnside group $\mathrm{B}(3, r)$ of exponent 3 has nilpotency class 3 for $r \geqslant 3$. In particular, it does not satisfy the identity $[[x, y], z] = 1$. Hence, we obtain

COROLLARY 4·4. *The commutative centre of the Moufang triplication* $\mathrm{M}(\mathrm{B}(3, r), 3)$ *is not a normal subloop if* $r \geqslant 3$.

The minimal example in this series is the loop $\mathrm{M}(\mathrm{B}(3, 3), 3)$ of order 3^8.

Finally, observe that the loops from Section 3 cannot be obtained by an application of Proposition 4·3, because they satisfy the identity $[[x, y], z] = 1$.

Acknowledgements. We are thankful to the anonymous referee for suggesting a number of improvements to the original text.

Remark. In a personal communication with the first author on November 15, 2017, S. Gagola noted the following regarding his paper [**2**]: "Is it best to mention to the editor that I have spotted a mistake in the proof of Lemma 5.2 and, due to the mistake, Proposition 5.3 is actually false."

REFERENCES

[1] S. DORO. Simple Moufang loops. *Math. Proc. Camb. Phil. Soc.* **83**, N3 (1978), 377–392.
[2] S. M. GAGOLA III. A Moufang loop's commutant. *Math. Proc. Camb. Phil. Soc.* **152**, N2 (2012), 193–206.
[3] A. N. GRISHKOV & A. V. ZAVARNITSINE. Groups with triality. *J. Algebra Appl.* **5**, N4 (2006), 441–463.
[4] A. N. GRISHKOV & A. V. ZAVARNITSINE. Sylow's theorem for Moufang loops. *J. Algebra*. **321**, N7 (2009), 1813–1825.
[5] A. N. GRICHKOV & A. V. ZAVARNITSINE. Multiplication formulas in Moufang loops. *Internat. J. Algebra Comput.* **26**, N4 (2016), 705–725.
[6] M. HALL JR. *The Theory of Groups*. The Macmillan Co., New York, N.Y, (1959), 434 pp.
[7] H. O. PFLUGFELDER. *Quasigroups and loops: introduction*. Sigma Series in Pure Mathematics, 7 (Berlin: Heldermann Verlag, 1990), 147 pp.