Mathematical Proceedings of the Cambridge Philosophical Society

VOL. 152 MARCH 2012 PART 2

Math. Proc. Camb. Phil. Soc. (2012), **152**, 193–206 © *Cambridge Philosophical Society* 2011
doi:10.1017/S0305004111000181
First published online 8 December 2011

A Moufang loop's commutant

BY STEPHEN M. GAGOLA III

Department of Mathematics, The University of Arizona,
617 *N. Santa Rita Ave, Tucson, AZ* 85721-0089*, U.S.A.*
e-mail: sgagola@math.arizona.edu

(*Received* 21 *July* 2009; *revised* 10 *February* 2011)

Abstract

The commutant of a loop is the set of elements which commute with all of the elements in the loop. The commutant of a Moufang loop is a subloop, but it has been an open problem to classify the Moufang loops for which the commutant is normal. It was S. Doro [3] who conjectured that a Moufang loop, under certain conditions, has a normal commutant. We settle this conjecture here by proving that the commutant of any Moufang loop is always a normal subloop.

1. *Introduction*

A *loop* L is a non-empty set with a closed binary operation such that L contains a 2-sided identity element and, for every $a, b \in L$, there exist unique elements $x, y \in L$ such that

$$ax = b$$

and

$$ya = b.$$

A *Moufang loop* is a loop L that satisfies the identity $(xy)(zx) = x((yz)x)$.

The *commutant* of a loop L, sometimes called the *centrum,* is the subset

$$\mathbf{C}(L) = \{a \in L \mid ag = ga \text{ for all } g \in L\}.$$

It can be shown that if L is a Moufang loop then the commutant is a subloop. It was also shown by M. Kinyon and J. D. Phillips in [**11**] that the commutant of a Bol loop of odd order

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

is a subloop. One can also see that if L is a group then $\mathbf{C}(L)$ is the center of L. But for an arbitrary loop L, the *center* of L is the set

$$\{a \in \mathbf{C}(L) \mid (ax)y = a(xy), (xa)y = x(ay), (xy)a = x(ya) \text{ for all } x, y \in L\}.$$

One can easily show that the center of L is normal in L. But is the commutant of a Moufang loop L also normal in L? In 1978, Doro [**3**] asked about conditions under which a Moufang loop's commutant is normal.

It is well known that if L is a Moufang loop and $\mathbf{C}(L)$ is of finite order relatively prime to 3 then $\mathbf{C}(L)$ is an abelian group that is normal in L. This is because the elements in $\mathbf{C}(L)$ that are of order relatively prime to 3 are contained in the center of L. However, there are Moufang loops whose commutants contain elements that do not associate. It was shown by Zassenhaus [**1**] that there does exist a commutative Moufang loop of order 81 and exponent three that is nonassociative. Another example of a nonassociative commutative Moufang loop of order 81, this one of exponent nine, was then later constructed by T. Kepka and P. Němec [**10**].

In Section six we look at the triality group $G(L)$ of a Moufang loop L, along with a triality group of $\mathbf{C}(L)$ to obtain the following theorem.

THEOREM 1·1. *For any Moufang loop L, if $\mathbf{C}(L)$ is the commutant of L then $\mathbf{C}(L) \trianglelefteq L$.*

Proof. This is proven in Section 6.

It is easy to see that one gets $\mathbf{C}(L)$ back after conjugating it by any element in L. But in order for $\mathbf{C}(L)$ to be normal in L, the following equalities must also hold for any $x, y \in L$:

$$(xy)^{-1}(x(y\mathbf{C}(L))) = \mathbf{C}(L)$$
$$((\mathbf{C}(L)x)y)(xy)^{-1} = \mathbf{C}(L).$$

2. *Moufang loops*

A set L with a binary operation is called a *loop* if there exists an identity element 1 with $1x = x = x1$ for every $x \in L$ and both left and right multiplication by any fixed element of L permutes the elements of L. A *Moufang loop* is a loop L that satisfies one (equivalently all) of the following identities:

$$(xy)(zx) = x((yz)x)$$
$$((xy)x)z = x(y(xz))$$
$$z(x(yx)) = ((zx)y)x.$$

These weaker forms of the associative law, also called the *Moufang identities*, were first introduced by Ruth Moufang. From [**2**, lemma 3·1], one can see the equivalence of the identities $(xy)(zx) = x((yz)x)$, $((xy)x)z = x(y(xz))$, and $z(x(yx)) = ((zx)y)x$.

From the definition one can see that every group is a Moufang loop. Even with the lack of associativity Moufang loops still capture many properties that hold for groups. A loop is said to be *diassociative* if any two of its elements generate a group. It was proven by Moufang [**12**] that every Moufang loop is diassociative. It was shown, in [**7**, **9**], that Lagrange's Theorem not only holds for groups but also for Moufang loops. Furthermore, it has been proven in [**4**–**8**] that Sylow's Theorems also hold for finite Moufang loops.

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

We will define permutations $R(x)$ and $L(x)$ for an arbitrary loop L in the following way:

$$aR(x) = ax$$
$$aL(x) = xa$$

for any $a \in L$. Here $R(x)$ is called the *right translation* of L by x. Similarly, $L(x)$ is called the *left translation* of L by x. The *multiplication group* of L is the group of permutations

$$\langle R(x), L(x) \mid x \in L \rangle$$

denoted by $\mathrm{Mlt}(L)$.

If L is a Moufang loop and $y \in L$ then the following map

$$\begin{aligned} f \ : \ L &\longrightarrow L \\ x &\longmapsto x^y = y^{-1}xy \end{aligned}$$

is called conjugation by y and the image of an element x will be denoted by x^y or $xT(y)$ where $T(y) = R(y)L(y^{-1})$. Note that such a map is well-defined and onto due to the fact that Moufang loops are diassociative and $(y^{-1}x)y = y^{-1}(xy)$ for all $x, y \in L$.

For any loop L the *inner mapping group* is the group of elements in $\mathrm{Mlt}(L)$ that stabilize the identity. It has been shown in [**2**] that the inner mapping group is generated by $T(x)$, $R(x, y) = R(x)R(y)R(xy)^{-1}$, and $L(x, y) = L(x)L(y)L(xy)^{-1}$. A subloop K of L is *normal* in L if it is invariant under any inner mapping. Thus we will write $K \trianglelefteq L$ if

$$KT(x) = K$$
$$KR(x, y) = K$$
$$\text{and } KL(x, y) = K,$$

for all $x, y \in L$.

3. *Groups with triality*

Here we look at the correspondence between Moufang loops and groups with triality.

Definition 3·1. Suppose G is a group, $S \leqslant Aut(G)$, $S = \langle \sigma, \rho \rangle \cong S_3$ with $|\sigma| = 2$ and $|\rho| = 3$. The pair (G, S) is called a group with triality if for every $g \in G$ the identity

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

holds.

Here $[g, \sigma] = g^{-1}g^{\sigma}$ for all $g \in G$. So 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 [**3**] and [**9**], L is a Moufang loop associated with G under the binary operation

$$\begin{aligned} a \centerdot b &= (a^{-1})^{\rho}b(a^{-1})^{\rho^2} \\ &= a^{-\rho}ba^{-\rho^2}. \end{aligned} \tag{1}$$

It was shown by Doro [**3**] that for any Moufang loop L there exists a group G with triality S such that L is the corresponding Moufang loop. However, such a group is not necessarily unique.

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

LEMMA 3·2 (Doro). *If L is a Moufang loop and G is a triality group of L then L^{ρ^2} is a right transversal of $C_G(\sigma)$ in G. So every element in G can be written uniquely as xg^{ρ^2} where $x \in C_G(\sigma)$ and $g \in L$ and $|G| = |C_G(\sigma)| \cdot |L|$. Similarly, every element in G can be written uniquely as yh^{ρ} where $y \in C_G(\sigma)$ and $h \in L$.*

Proof. This was proven by Doro in [**3**, lemma 1].

Definition 3·3. 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 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 particular details are given in the following example.

Example 3·4. Let the point set be 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 $x \in L$ we will let $f_x = L(x)$, $g_x = R(x)$, and $h_x = R(x^{-1})L(x^{-1})$. Now let G be the following subgroup of $H = \mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$:

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

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

$$(f, g, h)^{\rho} = (g, h, f)$$

and

$$(f, g, h)^{\sigma} = (g', f', h')$$

where $g'(a) = g(a^{-1})^{-1}$, $f'(a) = f(a^{-1})^{-1}$ and $h'(a) = h(a^{-1})^{-1}$ for all $(f, g, h) \in G$. Also note that

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

Under the binary operation $\cdot$ defined by equation (1), $[G, \sigma]$ is isomorphic to L.

Suppose that G is a group with triality S where L is the corresponding Moufang loop. If G is isomorphic to the previous example, namely the smallest triality group associated with L, then we will denote such a group by $G(L)$. If K is a subloop of L then, from [**7**] and [**9**], there is a subgroup

$$G_L(K) = \left\langle K, K^{\rho}, K^{\rho^2} \right\rangle$$

of $G(L)$, which is also invariant under S, such that K is the Moufang loop associated with the triality group $G_L(K)$.

LEMMA 3·5. *Let G be a group with triality $S = \langle \sigma, \rho \rangle$ where L is its corresponding Moufang loop. If $x \in C_G(\sigma)$ and $g \in L$ then*:

(i) $x^{-\rho} g x^{\rho^2}, x^{-\rho^2} g x^{\rho} \in L$;
(ii) $g^x \in L$; *and*
(iii) $g^{-\rho} g^{\rho^2} \in C_G(\sigma)$.

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

Proof. For any $x \in C_G(\sigma)$ and $g \in L$ we get

$$\begin{aligned} x^{-\rho} g x^{\rho^2} &= x^{-\rho} g^{-\rho} g^{-\rho^2} x^{\rho^2} \\ &= [g^\rho x^\rho, \sigma] \in L, \\ x^{-\rho^2} g x^\rho &= x^{-\rho^2} g^{-\rho} g^{-\rho^2} x^\rho \\ &= \left[g^\rho x^{\rho^2}, \sigma\right] \in L \end{aligned}$$

and

$$\begin{aligned} g^x &= x^{-1} g^{-\rho} g^{-\rho^2} x \\ &= [g^\rho x, \sigma] \in L. \end{aligned}$$

Furthermore, $(g^{-\rho} g^{\rho^2})^\sigma = g^{\rho^2} g^{-\rho} = g^{-\rho} g^{\rho^2}$.

LEMMA 3·6. *Let G be a group with triality $S = \langle \sigma, \rho \rangle$ where L is its corresponding Moufang loop. If $g, h \in L$ then $ghg = g \cdot h \cdot g$ and $g \cdot h = h^{-\rho^2} g h^{-\rho}$.*

Proof. See [**4**].

LEMMA 3·7. *If L is an abelian group then $G(L)$ is abelian.*

Proof. Since L is both commutative and associative, by definition of $G(L)$ and Example 3·4, the elements of the set $\left\{g, g^\rho, g^{\rho^2} \mid g \in L\right\} \subseteq G(L)$ commute. Hence, $G(L) = \left\langle g, g^\rho, g^{\rho^2} \mid g \in L \right\rangle$ is abelian.

LEMMA 3·8. *Suppose L is a Moufang loop with $g, h \in L$ where $g \cdot h \neq h \cdot g$. Then $gh \neq hg$ in $G(L)$ and in fact $ghN \neq hgN$ in $\mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ where $N = 1 \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$.*

Proof. The permutation $gh \in G(L) \leqslant \mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ maps the point 1_R to $1_R L(g) L(h)$ whereas the permutation hg maps the point 1_R to $1_R L(h) L(g)$. Since $g \cdot h \neq h \cdot g$ in $(L, \cdot)$, $gh \neq hg$ in $G(L)$ and $ghN \neq hgN$ in $\mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$.

4. *Properties of $R(x)R(y)R(x)^{-1}R(y)^{-1}$*

In this section we look at certain properties that hold for the map

$$F(x, y) = R(x)R(y)R(x)^{-1}R(y)^{-1}$$

when working with a Moufang loop L. Note that if either x or y is in the commutant of L then $F(x, y)$ is in the inner mapping group of L.

LEMMA 4·1. *If L is a Moufang loop with $g \in L$ and $a \in \mathbf{C}(L)$ then the map*

$$\begin{aligned} L &\longrightarrow L \\ h &\longmapsto hF(g, a) \end{aligned}$$

is an automorphism.

Proof. One can easily see that the map is one-to-one and onto. Let $g \in L$ and $a \in \mathbf{C}(L)$. Note that

$$hF(g, a) = a^{\rho^2} g^{\rho^2} a^{-\rho^2} g^{-\rho^2} h g^{-\rho} a^{-\rho} g^\rho a^\rho.$$

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

We will first show that $x = g^{-\rho}a^{-\rho}g^{\rho}a^{\rho}$ is stabilized by S. Here

$$\begin{aligned}\left[g^{-\rho}a^{-\rho}g^{\rho}a^{\rho}, \sigma\right] &= a^{-\rho}g^{-\rho}a^{\rho}g^{-1}a^{\rho^2}g^{-\rho^2}a^{-\rho^2} \\ &= a \,.\, g \,.\, a^{-1} \,.\, g^{-1} \\ &= 1\end{aligned}$$

and

$$\begin{aligned}\left[\left(g^{-\rho}a^{-\rho}g^{\rho}a^{\rho}\right)^{\rho}, \sigma\right] &= a^{-\rho^2}g^{-\rho^2}a^{\rho^2}g^{-1}a^{\rho}g^{-\rho}a^{-\rho} \\ &= g^{-1} \,.\, a^{-1} \,.\, g \,.\, a \\ &= 1.\end{aligned}$$

Hence x is stabilized by S. Thus, for any $h_1, h_2 \in L$ we get

$$\begin{aligned}(h_1 \,.\, h_2)F(g,a) &= x^{-\sigma}(h_1^{-\rho}h_2h_1^{-\rho^2})x \\ &= x^{-\sigma}h_1^{-\rho}xx^{-1}h_2xx^{-1}h_1^{-\rho^2}x \\ &= x^{-\rho}h_1^{-\rho}x^{\rho}x^{-1}h_2xx^{-\rho^2}h_1^{-\rho^2}x^{\rho^2} \\ &= (x^{-1}h_1x) \,.\, (x^{-1}h_1x) \\ &= h_1F(g,a) \,.\, h_2F(g,a).\end{aligned}$$

COROLLARY 4·2. *If L is a Moufang loop with $g \in L$ and $a \in \mathbf{C}(L)$ then $\mathbf{C}(L)F(g,a) = \mathbf{C}(L)$.*

LEMMA 4·3. *Suppose L is a Moufang loop. If $g \in L$ and $a, b \in \mathbf{C}(L)$ then there exists an element $c \in \mathbf{C}(L)$ such that*

$$(g \,.\, a) \,.\, b = g \,.\, c.$$

Proof. For any $g \in L$ and $a, b \in \mathbf{C}(L)$ we get that

$$\begin{aligned}(g \,.\, a) \,.\, b &= (a \,.\, g) \,.\, b \\ &= (((((a \,.\, g) \,.\, b) \,.\, g^{-1}) \,.\, b^{-1}) \,.\, b) \,.\, g \\ &= (aF(g,b) \,.\, b) \,.\, g \\ &\in (\mathbf{C}(L) \,.\, b) \,.\, g = \mathbf{C}(L) \,.\, g = g \,.\, \mathbf{C}(L).\end{aligned}$$

LEMMA 4·4. *If L is a Moufang loop with $g, h \in L$ and $a \in \mathbf{C}(L)$ then*

$$(g \,.\, a^3) \,.\, h = (g \,.\, h) \,.\, a^3$$

and

$$h \,.\, \left(a^3 \,.\, g\right) = a^3 \,.\, (h \,.\, g)$$

hold.

Proof. Since $a \in \mathbf{C}(L)$ we get

$$\begin{aligned}(g \,.\, a^3) \,.\, h &= (a \,.\, (a \,.\, g) \,.\, a) \,.\, h \\ &= a \,.\, ((a \,.\, g) \,.\, (a \,.\, h)) \\ &= a \,.\, ((a \,.\, g) \,.\, (h \,.\, a)) \\ &= a^2 \,.\, (g \,.\, h) \,.\, a \\ &= (g \,.\, h) \,.\, a^3\end{aligned}$$

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

and

$$\begin{aligned} h \cdot (a^3 \cdot g) &= h \cdot (a \cdot (g \cdot a) \cdot a) \\ &= ((h \cdot a) \cdot (g \cdot a)) \cdot a \\ &= ((a \cdot h) \cdot (g \cdot a)) \cdot a \\ &= a \cdot (h \cdot g) \cdot a^2 \\ &= a^3 \cdot (h \cdot g). \end{aligned}$$

LEMMA 4·5. *If L is a Moufang loop then for any $g \in L$ and $a \in \mathbf{C}(L)$ $F(g,a) = L(g)L(a)L(g^{-1})L(a^{-1})$.*

Proof. From the proof of Lemma 4·1 we know that $x = g^{-\rho}a^{-\rho}g^{\rho}a^{\rho}$ is stabilized by S. Thus for any $h \in L$ we get

$$\begin{aligned} hF(g,a) &= a^{\rho^2}g^{\rho^2}a^{-\rho^2}g^{-\rho^2}hg^{-\rho}a^{-\rho}g^{\rho}a^{\rho} \\ &= x^{-\sigma}hx \\ &= x^{-\sigma\rho^2}hx^{\rho} \\ &= a^{\rho}g^{\rho}a^{-\rho}g^{-\rho}hg^{-\rho^2}a^{-\rho^2}g^{\rho}a^{\rho^2} \\ &= hL(g)L(a)L(g^{-1})L(a^{-1}). \end{aligned}$$

5. *The image $hR(g)R(a)R(g)^{-1}R(a)^{-1}$*

Our aim in this section is to show that for any Moufang loop L with $h, g \in L$ and $a \in \mathbf{C}(L)$ the image of h under $F(g,a)$ is contained in the coset $\mathbf{C}(L) \cdot h$. Notice that showing that $hF(g,a) \in \mathbf{C}(L) \cdot h$ is equivalent to showing that $(hF(g,a) \cdot h^{-1}) \cdot a \in \mathbf{C}(L)$. Also note that the element

$$(hF(g,a) \cdot h^{-1}) \cdot a = (((((h \cdot g) \cdot a) \cdot g^{-1}) \cdot a^{-1}) \cdot h^{-1}) \cdot a$$

is the image of a under the map

$$\begin{aligned} \varphi \;:\; L &\longrightarrow L \\ x &\longmapsto ((((x \cdot (h \cdot g)) \cdot g^{-1}) \cdot a^{-1}) \cdot h^{-1}) \cdot a. \end{aligned}$$

Without loss we may assume that $G(L) \leqslant \mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ as defined in section three using a Latin square design. Furthermore $L = [G(L), \sigma] \subseteq G(L)$ where b will be our notation for the element $(f_b, g_b, h_b) \in L = [G(L), \sigma]$. If K is a subloop of L and $b \in K$ then we will denote the projection of b onto $\mathrm{Sym}(K_R) \times \mathrm{Sym}(K_C) \times \mathrm{Sym}(K_E)$ by $\pi_K(b)$.

We will start off by extending the map φ to the triality group $G(L)$ in the following way:

$$\begin{aligned} \varphi \;:\; G(L) &\longrightarrow G(L) \\ x &\longmapsto a^{-\rho^2}h^{\rho^2}a^{\rho^2}g^{\rho^2}(h \cdot g)^{-\rho^2}x(h \cdot g)^{-\rho}g^{\rho}a^{\rho}h^{\rho}a^{-\rho}. \end{aligned}$$

In fact, φ can be extended to the entire group $\mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$.

PROPOSITION 5·1. *This map φ is an automorphism of* $\mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$.

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

Proof. The map φ is certainly one-to-one and onto. So one just has to show that φ is a homomorphism. First note that

$$\begin{aligned}(h \cdot g)^{-\rho} g^{\rho} a^{\rho} h^{\rho} a^{-\rho}\ a^{-\rho^2}\ h^{\rho^2} a^{\rho^2} g^{\rho^2} (h \cdot g)^{-\rho^2} &= (h \cdot g)^{-\rho} g^{\rho} a^{\rho} h^{\rho} a h^{\rho^2} a^{\rho^2} g^{\rho^2} (h \cdot g)^{-\rho^2} \\ &= (h \cdot g)^{-\rho} g^{\rho} a^{\rho} (h^{-1} \cdot a) a^{\rho^2} g^{\rho^2} (h \cdot g)^{-\rho^2} \\ &= (h \cdot g)^{-\rho} g^{\rho} (a^{-1} \cdot (h^{-1} \cdot a)) g^{\rho^2} (h \cdot g)^{-\rho^2} \\ &= (h \cdot g)^{-\rho} g^{\rho} h^{-1} g^{\rho^2} (h \cdot g)^{-\rho^2} \\ &= (h \cdot g)^{-\rho} (g^{-1} \cdot h^{-1}) (h \cdot g)^{-\rho^2} \\ &= (h \cdot g) \cdot (g^{-1} \cdot h^{-1}) \\ &= 1.\end{aligned}$$

Thus, for any $x, y \in \mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ we get that

$$\begin{aligned}\varphi(x)\varphi(y) &= a^{-\rho^2} h^{\rho^2} a^{\rho^2} g^{\rho^2} (h \cdot g)^{-\rho^2} x\ \ 1\ \ y (h \cdot g)^{-\rho} g^{\rho} a^{\rho} h^{\rho} a^{-\rho} \\ &= \varphi(xy).\end{aligned}$$

If K is a subloop of L then we will let ψ_K be an embedding from $\mathrm{Sym}(K_R) \times \mathrm{Sym}(K_C) \times \mathrm{Sym}(K_E)$ into $\mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ which extends a permutation of $K_R \cup K_C \cup K_E$ to a permutation of $L_R \cup L_C \cup L_E$ by fixing pointwise the points of $(L_R \setminus K_R) \cup (L_C \setminus K_C) \cup (L_E \setminus K_E)$.

LEMMA 5·2. *Let* $N = 1 \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$. *If* $b, z \in L$, $A = \langle b, z \rangle \leqslant (L, \cdot)$, *and* $B = \langle \varphi(b), \varphi(z) \rangle \leqslant (L, \cdot)$ *then*

$$\begin{aligned}&\varphi\,(\psi_A\,(\pi_A(b)))\,N = \psi_B\,(\pi_B(\varphi(b)))\,N, \\ &\varphi\,(\psi_A\,(\pi_A(z)))\,N = \psi_B\,(\pi_B(\varphi(z)))\,N, \text{ and thus} \\ &\varphi\,(\psi_A\,(\langle \pi_A(b), \pi_A(z) \rangle))\,N = \psi_B\,(\langle \pi_B(\varphi(b)), \pi_B(\varphi(z)) \rangle)\,N.\end{aligned}$$

Proof. From the proof of Proposition 5·1 we see that $\varphi(x) = p^{-1}xp$ for some $p = (p_1, p_2, p_3) \in \mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$. Let $S_R = p_1(A_R) \subseteq L_R$. By definition of p, we see that $1_R = p_1(1_R) \in S_R$. Note that for any element $x \in \psi_A(\langle \pi_A(b), \pi_A(z) \rangle)$, $\varphi(x)$ leaves all of the points in $L_R \setminus S_R$ fixed. Also note that for any element $y \in A$, $\varphi(y) \in L$. Thus $\varphi(y)$, and therefore $\varphi(\psi_A(\pi_A(y)))$, permutes the elements of S_R by multiplying elements on the left by $\varphi(y)_R$. So to prove the lemma we must show that $S_R = B_R$.

Since $\varphi(b)_R S_R \subseteq S_R$, $\varphi(z)_R S_R \subseteq S_R$, $1_R \in S_R$, and the subloop $B_R = \langle \varphi(b)_R, \varphi(z)_R \rangle \subseteq L_R$ is associative, $B_R \subseteq S_R$. Similarly, since φ^{-1} is an automorphism of $\mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ with $\varphi^{-1}(L) = L$ and $p_1^{-1}(1_R) = 1_R$, $A_R \subseteq p_1^{-1}(B_R)$. Hence $B_R = p_1(A_R) = S_R$. This completes the proof.

PROPOSITION 5·3. *The map* φ *stabilizes* $\mathbf{C}(L)$.

Proof. Since $\varphi(L) = L$, the map φ stabilizes the subgroup $\langle L \rangle \leqslant G(L)$. Suppose $b \in L$. By Lemmas 3·7 and 3·8, $b \in \mathbf{C}(L)$ if and only if, for every $z \in L$, $\pi_A(b)\pi_A(z) = \pi_A(z)\pi_A(b)$ in the triality group $G(A)$ where $A = \langle b, z \rangle \leqslant (L, \cdot)$. Let z be an arbitrary element of L, $A = \langle b, z \rangle \leqslant (L, \cdot)$, and $B = \langle \varphi(b), \varphi(z) \rangle \leqslant (L, \cdot)$. Also let $N = 1 \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)$ and $N_B = 1 \times \mathrm{Sym}(B_C) \times \mathrm{Sym}(B_E)$. Thus,

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

$b \in \mathbf{C}(L)$

$$\begin{aligned}
&\Longrightarrow \pi_A(b)\pi_A(z) = \pi_A(z)\pi_A(b)\\
&\Longrightarrow \psi_A(\pi_A(b)\pi_A(z)) = \psi_A(\pi_A(z)\pi_A(b))\\
&\Longrightarrow \varphi(\psi_A(\pi_A(b)\pi_A(z))) = \varphi(\psi_A(\pi_A(z)\pi_A(b)))\\
&\Longrightarrow \varphi(\psi_A(\pi_A(b)))\varphi(\psi_A(\pi_A(z))) = \varphi(\psi_A(\pi_A(z)))\varphi(\psi_A(\pi_A(b)))\\
&\Longrightarrow \varphi(\psi_A(\pi_A(b)))\varphi(\psi_A(\pi_A(z)))N = \varphi(\psi_A(\pi_A(z)))\varphi(\psi_A(\pi_A(b)))N\\
&\Longrightarrow \psi_B(\pi_B(\varphi(b)))\psi_B(\pi_B(\varphi(z)))N = \psi_B(\pi_B(\varphi(z)))\psi_B(\pi_B(\varphi(b)))N\\
&\qquad \text{by Lemma 5·2,}\\
&\Longrightarrow \pi_B(\varphi(b))\pi_B(\varphi(z))N_B = \pi_B(\varphi(z))\pi_B(\varphi(b))N_B\\
&\Longrightarrow \varphi(b) \cdot \varphi(z) = \varphi(z) \cdot \varphi(b) \text{ by Lemma 3·8.}
\end{aligned}$$

Since z is arbitrary, if $b \in \mathbf{C}(L)$ then $\varphi(b) \in \mathbf{C}(L)$. By the same argument, if $b \in \mathbf{C}(L)$ then $\varphi^{-1}(b) \in \mathbf{C}(L)$. Hence, φ stabilizes $\mathbf{C}(L)$.

THEOREM 5·4. *Let L be a Moufang loop. If $h, g \in L$ and $a \in \mathbf{C}(L)$ then $hF(g,a) \in \mathbf{C}(L) \cdot h$.*

Proof. By Proposition 5·3, if

$$\begin{aligned}
\varphi \;:\; G(L) &\longrightarrow G(L)\\
x &\longmapsto a^{-\rho^2}h^{\rho^2}a^{\rho^2}g^{\rho^2}(h \cdot g)^{-\rho^2}x(h \cdot g)^{-\rho}g^{\rho}a^{\rho}h^{\rho}a^{-\rho}
\end{aligned}$$

then $\varphi(a) \in \mathbf{C}(L)$. Therefore,

$$\begin{aligned}
&\varphi(a) \in \mathbf{C}(L)\\
&\qquad \Longrightarrow ((((a \cdot (h \cdot g)) \cdot g^{-1}) \cdot a^{-1}) \cdot h^{-1}) \cdot a \in \mathbf{C}(L)\\
&\qquad \Longrightarrow (((((h \cdot g) \cdot a) \cdot g^{-1}) \cdot a^{-1}) \cdot h^{-1}) \cdot a \in \mathbf{C}(L)\\
&\qquad \Longrightarrow (hF(g,a) \cdot h^{-1}) \cdot a \in \mathbf{C}(L)\\
&\qquad \Longrightarrow hF(g,a) \cdot h^{-1} \in \mathbf{C}(L)\\
&\qquad \Longrightarrow hF(g,a) \in \mathbf{C}(L) \cdot h.
\end{aligned}$$

6. *Proof of Theorem* 1·1

Let L be any Moufang loop and $\mathbf{C}(L)$ be the commutant of L. We will define a subset, N, of $G(L)$ in the following way:

$$N = \left\{ xg^{\rho} \in G(L) \;\middle|\; \begin{array}{l} x \in C_{G(L)}(\sigma),\ g \in \mathbf{C}(L),\ \text{there exists an element } c \in \mathbf{C}(L)\\ \text{such that } x^{-\rho}x^{\rho^2} = c^3,\ \text{and for any } z \in L \text{ there exists}\\ \text{an element } b_z \in \mathbf{C}(L) \text{ such that } \left[z^{\rho}x, \sigma\right] = x^{-1}zx = z \cdot b_z \end{array} \right\}$$

Here we will prove that the set N is a group with triality S.

THEOREM 6·1. *If L is a Moufang loop then the set N is a group with triality S where $\mathbf{C}(L)$ is its corresponding Moufang loop.*

Proof. We will first show that N is invariant under S. For any $xg^{\rho} \in N$ where $x \in C_{G(L)}(\sigma)$ and $g \in \mathbf{C}(L)$,

$$\begin{aligned}
(xg^{\rho})^{\sigma} &= xg^{-\rho^2}\\
&= \left(xg^{-\rho^2}g^{\rho}\right)(g^{-1})^{\rho}
\end{aligned}$$

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

where $xg^{-\rho^2}g^{\rho} \in C_{G(L)}(\sigma)$. Here

$$\begin{aligned}\left(xg^{-\rho^2}g^{\rho}\right)^{-\rho}\left(xg^{-\rho^2}g^{\rho}\right)^{\rho^2} &= g^{-\rho^2}gx^{-\rho}x^{\rho^2}g^{-\rho}g\\ &= gg^{-\rho^2}c^3g^{-\rho}g \text{ for some } c \in \mathbf{C}(L)\\ &= g \centerdot c^3 \centerdot g \centerdot g\\ &= (g \centerdot c)^3.\end{aligned}$$

Also, for any $z \in L$ we get that

$$\begin{aligned}\left[z^{\rho}xg^{-\rho^2}g^{\rho}, \sigma\right] &= g^{-\rho}g^{\rho^2}x^{-1}zxg^{\rho}g^{-\rho^2}\\ &= g \centerdot (x^{-1}zx) \centerdot g^{-1}\\ &= g \centerdot g^{-1} \centerdot (x^{-1}zx)\\ &= x^{-1}zx \in z \centerdot \mathbf{C}(L).\end{aligned}$$

Therefore, $(xg^{\rho})^{\sigma} \in N$. Similarly,

$$\begin{aligned}(xg^{\rho})^{\rho} &= x^{\rho}g^{\rho^2}\\ &= x^{\rho}g^{\rho^2}\left[x^{\rho}g^{\rho^2}, \sigma\right]^{-\rho}\left[x^{\rho}g^{\rho^2}, \sigma\right]^{\rho}\\ &= (x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g)(g^{-\rho^2}x^{-\rho}x^{\rho^2}g^{-\rho})^{\rho}\\ &= (x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g)(c^3 \centerdot g)^{\rho} \text{ for some } c \in \mathbf{C}(L).\end{aligned}$$

Here $x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g \in C_{G(L)}(\sigma)$ with

$$\begin{aligned}\left(x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g\right)^{-\rho}&\left(x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g\right)^{\rho^2}\\ &= \left(\left(x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g\right)^{\sigma}\right)^{-\rho}\left(x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g\right)^{\rho^2}\\ &= g^{\rho}x^{-\rho^2}x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}xg^{\rho}g^{\rho}x^{-\rho^2}x^{\rho}g^{\rho^2}\\ &= g^{\rho}\left(x^{-\rho}x^{\rho^2}\right)^{-1}g^{-2}\left(x^{-\rho}x^{\rho^2}\right)^{-1}g^{\rho^2}\\ &= g^{\rho}c^{-3}g^{-2}c^{-3}g^{\rho^2}\\ &= g^{-1} \centerdot c^{-3} \centerdot g^{-2} \centerdot c^{-3}\\ &= (c^{-2} \centerdot g^{-1})^3.\end{aligned}$$

Furthermore, for any $z \in L$ we get that

$$\begin{aligned}\left[z^{\rho}x^{\rho}g^{\rho^2}g^{\rho^2}x^{-1}x^{\rho^2}g, \sigma\right] &= g^{-1}x^{-\rho^2}xg^{-\rho^2}g^{-\rho^2}x^{-\rho}zx^{\rho^2}g^{-\rho}g^{-\rho}x^{-1}x^{\rho}g^{-1}\\ &= g^{-1} \centerdot ((c^3)^{\rho}((c^3 \centerdot (x^{-1}zx)) \centerdot g^2)(c^3)^{\rho^2}) \centerdot g^{-1}\\ &= g^{-1} \centerdot ((c^3)^{\rho}((c^3 \centerdot (x^{-1}zx)) \centerdot g^2)(c^3)^{\rho^2}) \centerdot g^{-1}\\ &= g^{-1} \centerdot (c^{-3} \centerdot ((c^3 \centerdot (x^{-1}zx)) \centerdot g^2)) \centerdot g^{-1}\\ &= g^{-2} \centerdot (c^{-3} \centerdot (c^3 \centerdot (g^2 \centerdot (x^{-1}zx)))) \text{ by Lemma 4·4}\\ &= g^{-2} \centerdot (g^2 \centerdot (x^{-1}zx))\\ &= x^{-1}zx \in \mathbf{C}(L).\end{aligned}$$

So for any $xg^{\rho} \in N$ we have that $(xg^{\rho})^{\sigma}, (xg^{\rho})^{\rho} \in N$. Hence N is invariant under S.

We will now show that N is closed under multiplication. It is enough to show that for any $x, y \in N \cap C_{G(L)}(\sigma)$ and $a, b \in \mathbf{C}(L)$, the elements xy, $a^{\rho}y$, and $a^{\rho}b^{\rho}$ are contained in N.

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

Let $x, y \in N \cap C_{G(L)}(\sigma)$. Clearly $xy \in C_{G(L)}(\sigma)$ with

$$\begin{aligned}(xy)^{-\rho}\,(xy)^{\rho^2} &= y^{-\rho}x^{-\rho}x^{\rho^2}y^{\rho^2}\\ &= y^{-\rho}yy^{-1}\left(x^{-\rho}x^{\rho^2}\right)yy^{-1}y^{\rho^2}\\ &= \left(y^{-\rho}y^{\rho^2}\right)^{-\rho^2}y^{-1}c^3y\left(y^{-\rho}y^{\rho^2}\right)^{-\rho}\\ &= (c'^3)^{-\rho^2}(y^{-1}cy)^3(c'^3)^{-\rho}\\ &= (y^{-1}cy)^3 \centerdot c'^3\\ &= ((y^{-1}cy) \centerdot c')^3.\end{aligned}$$

Moreover, for any $z \in L$ we get that

$$\begin{aligned}[z^\rho xy, \sigma] &= y^{-1}x^{-1}zxy\\ &= y^{-1}(z \centerdot b_z)y\\ &= (z \centerdot b_z) \centerdot b' \text{ for some } b' \in \mathbf{C}(L)\\ &= z \centerdot b''_z \in z \centerdot \mathbf{C}(L) \text{ by Lemma 4·3.}\end{aligned}$$

Therefore, $xy \in N$.

Now let $y \in N \cap C_{G(L)}(\sigma)$ and $a \in \mathbf{C}(L)$. First note that $[a^\rho y, \sigma] = y^{-1}ay \in \mathbf{C}(L)$. Moreover, $a^\rho y = a^\rho yy^{-\rho}a^{-\rho}y^\rho(y^{-1}ay)^\rho$ where $a^\rho yy^{-\rho}a^{-\rho}y^\rho \in C_{G(L)}(\sigma)$. Here

$$\begin{aligned}(a^\rho yy^{-\rho}a^{-\rho}y^\rho)^{-\rho}(a^\rho yy^{-\rho}a^{-\rho}y^\rho)^{\rho^2} &= ((a^\rho yy^{-\rho}a^{-\rho}y^\rho)^\sigma)^{-\rho}(a^\rho yy^{-\rho}a^{-\rho}y^\rho)^{\rho^2}\\ &= y^{-1}a^{-1}yy^{-\rho}aay^{\rho^2}y^{-1}a^{-1}y\\ &= (y^{-1}a^{-1}y)\left(y^{-\rho}y^{\rho^2}\right)^{-\rho^2}(y^{-1}ay)(y^{-1}ay)\left(y^{-\rho}y^{\rho^2}\right)^{-\rho}(y^{-1}a^{-1}y)\\ &= (y^{-1}a^{-1}y)(c'^3)^{-\rho^2}(y^{-1}ay)(y^{-1}ay)(c'^3)^{-\rho}(y^{-1}a^{-1}y)\\ &= (y^{-1}ay)^{-1}(c'^3)^{-\rho^2}(y^{-1}ay)(y^{-1}ay)(c'^3)^{-\rho}(y^{-1}ay)^{-1}\\ &= (y^{-1}ay)^{-1} \centerdot (y^{-1}ay)^2 \centerdot c'^3 \centerdot (y^{-1}ay)^{-1}\\ &= c'^3\end{aligned}$$

and for any $z \in L$ we get

$$\begin{aligned}\left[z^\rho a^\rho yy^{-\rho}a^{-\rho}y^\rho, \sigma\right] &= y^{-\rho}a^\rho y^\rho y^{-1}a^{-\rho}za^{-\rho^2}yy^{-\rho^2}a^{\rho^2}y^{\rho^2}\\ &= (y^{-1}ay)^\rho y^{-1}(a \centerdot z)y(y^{-1}ay)^{\rho^2}\\ &= (y^{-1}ay)^\rho\left((a \centerdot z) \centerdot b'\right)(y^{-1}ay)^{\rho^2} \text{ for some } b' \in \mathbf{C}(L)\\ &= (y^{-1}ay)^{-1} \centerdot \left((a \centerdot z) \centerdot b'\right)\\ &\in z \centerdot \mathbf{C}(L) \text{ by Lemma 4·3.}\end{aligned}$$

Thus $a^\rho y \in N$.

Next we will let $a, b \in \mathbf{C}(L)$. Here $[a^\rho b^\rho, \sigma] = b^{-\rho}ab^{-\rho^2} = b \centerdot a \in \mathbf{C}(L)$. Thus

$$\begin{aligned}a^\rho b^\rho &= a^\rho b^\rho ba^{-\rho}b^{\rho^2}(b^{-\rho}ab^{-\rho^2})^\rho\\ &= a^\rho b^{-\rho^2}a^{-\rho}b^{\rho^2}(b^{-\rho}ab^{-\rho^2})^\rho\end{aligned}$$

where $a^\rho b^{-\rho^2}a^{-\rho}b^{\rho^2} \in C_{G(L)}(\sigma)$. Since

$$\begin{aligned}\left(a^\rho b^{-\rho^2}a^{-\rho}b^{\rho^2}\right)^{-\rho}\left(a^\rho b^{-\rho^2}a^{-\rho}b^{\rho^2}\right)^{\rho^2} &= \left(\left(a^\rho b^{-\rho^2}a^{-\rho}b^{\rho^2}\right)^\sigma\right)^{-\rho}\left(a^\rho b^{-\rho^2}a^{-\rho}b^{\rho^2}\right)^{\rho^2}\\ &= b^{\rho^2}a^{-1}b^{-\rho^2}aab^{-\rho}a^{-1}b^\rho\\ &= a^{-1} \centerdot a^2 \centerdot b \centerdot a^{-1} \centerdot b^{-1}\\ &= 1^3\end{aligned}$$

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

and for all $z \in L$

$$\begin{aligned}\left[z^{\rho}a^{\rho}b^{-\rho^2}a^{-\rho}b^{\rho^2},\sigma\right] &= b^{-\rho^2}a^{\rho}b^{\rho^2}a^{-\rho}za^{-\rho^2}b^{\rho}a^{\rho^2}b^{-\rho}\\ &= (a^{-1}\,.\,((a\,.\,z)\,.\,b^{-1}))\,.\,b\\ &= (((z\,.\,a)\,.\,b^{-1})\,.\,a^{-1})\,.\,b\\ &= zF(a,b^{-1})\\ &\in z\,.\,\mathbf{C}(L) \text{ by Theorem 5·4,}\end{aligned}$$

$a^{\rho}b^{\rho} \in N$. Therefore, N is closed under multiplication. Hence N is a group with triality S where $\mathbf{C}(L)$ is its corresponding Moufang loop.

We are now ready to prove Theorem 1·1.

Proof of Theorem 1·1. It is clear that for any $h \in L$ and any $a \in \mathbf{C}(L)$, $aT(h) = h^{-1}ah = a$ and thus $\mathbf{C}(L)T(h) = \mathbf{C}(L)$. We now want to show that for any $h, g \in L$, $\mathbf{C}(L)R(h,g) = \mathbf{C}(L)$ and $\mathbf{C}(L)L(h,g) = \mathbf{C}(L)$.

We will start off by showing that the triality group N is normal in $G(L)$. Let $h \in L$ and $a \in \mathbf{C}(L)$. Then $\left[h^{\rho}a^{\rho}h^{-\rho},\sigma\right] = h^{\rho}a^{-\rho}ha^{-\rho^2}h^{\rho^2} = h^{-1}\,.\,a\,.\,h = a \in \mathbf{C}(L)$ and $h^{\rho}a^{\rho}h^{-\rho} = \left(h^{\rho}a^{\rho}h^{-\rho}a^{-\rho}\right)a^{\rho}$ with $h^{\rho}a^{\rho}h^{-\rho}a^{-\rho} \in C_{G(L)}(\sigma)$. From the proof of Lemma 4·1, we know that $h^{\rho}a^{\rho}h^{-\rho}a^{-\rho}$ is stabilized by S. Therefore,

$$\left(h^{\rho}a^{\rho}h^{-\rho}a^{-\rho}\right)^{-\rho}\left(h^{\rho}a^{\rho}h^{-\rho}a^{-\rho}\right)^{\rho^2} = 1 = 1^3.$$

Since

$$\begin{aligned}\left[z^{\rho}h^{\rho}a^{\rho}h^{-\rho}a^{-\rho},\sigma\right] &= a^{\rho}h^{\rho}a^{-\rho}h^{-\rho}zh^{-\rho^2}a^{-\rho^2}h^{\rho^2}a^{\rho^2}\\ &= a^{-1}\,.\,(h^{-1}\,.\,(a\,.\,(h\,.\,z)))\\ &= zF(h,a) \text{ by Lemma 4·5}\\ &\in z\,.\,\mathbf{C}(L) \text{ by Theorem 5·4}\end{aligned}$$

for any $z \in L$, $h^{\rho}a^{\rho}h^{-\rho} \in N$. Now let $h \in L$ and $x \in N \cap C_{G(L)}(\sigma)$. Note that $[h^{\rho}xh^{-\rho},\sigma] = h^{\rho}x^{-1}hxh^{\rho^2} = h^{-1}\,.\,(x^{-1}hx) = h^{-1}\,.\,h\,.\,b_h = b_h \in \mathbf{C}(L)$. Thus

$$\begin{aligned}h^{\rho}xh^{-\rho} &= h^{\rho}xh^{-\rho}\,(b_h)^{-\rho}\,(b_h)^{\rho}\\ &= h^{\rho}xh^{-\rho}\left(h^{\rho}x^{-1}hxh^{\rho^2}\right)^{-\rho}(b_h)^{\rho}\\ &= \left(h^{\rho}xh^{-\rho}h^{-1}x^{-\rho}h^{-\rho}x^{\rho}h^{-\rho^2}\right)(b_h)^{\rho}\\ &= \left(h^{\rho}xh^{\rho^2}x^{-\rho}h^{-\rho}x^{\rho}h^{-\rho^2}\right)(b_h)^{\rho}\end{aligned}$$

where $h^{\rho}xh^{\rho^2}x^{-\rho}h^{-\rho}x^{\rho}h^{-\rho^2} \in C_{G(L)}(\sigma)$. Here

$$\begin{aligned}&\left(h^{\rho}xh^{\rho^2}x^{-\rho}h^{-\rho}x^{\rho}h^{-\rho^2}\right)^{-\rho}\left(h^{\rho}xh^{\rho^2}x^{-\rho}h^{-\rho}x^{\rho}h^{-\rho^2}\right)^{\rho^2}\\ &\quad= \left(\left(h^{\rho}xh^{\rho^2}x^{-\rho}h^{-\rho}x^{\rho}h^{-\rho^2}\right)^{\sigma}\right)^{-\rho}\left(h^{\rho}xh^{\rho^2}x^{-\rho}h^{-\rho}x^{\rho}h^{-\rho^2}\right)^{\rho^2}\\ &\quad= h^{-\rho^2}x^{-1}h^{-1}xh^{\rho^2}x^{-\rho}hhx^{\rho^2}h^{\rho}x^{-1}h^{-1}xh^{-\rho}\\ &\quad= h^{-\rho^2}(x^{-1}h^{-1}x)h^{\rho^2}\left(x^{-\rho}x^{\rho^2}\right)^{-\rho^2}x^{-1}h^2x\left(x^{-\rho}x^{\rho^2}\right)^{-\rho}h^{\rho}(x^{-1}h^{-1}x)h^{-\rho}\\ &\quad= h^{-\rho^2}(x^{-1}h^{-1}x)h^{\rho^2}(c^3)^{-\rho^2}(x^{-1}hx)^2(c^3)^{-\rho}h^{\rho}(x^{-1}h^{-1}x)h^{-\rho}\\ &\quad= ((x^{-1}h^{-1}x)\,.\,(((x^{-1}hx)^2\,.\,c^3)\,.\,h^{-1})\,.\,(x^{-1}h^{-1}x))\,.\,h\\ &\quad= (((x^{-1}h^{-1}x)\,.\,((x^{-1}hx)^2\,.\,h^{-1})\,.\,(x^{-1}h^{-1}x))\,.\,h)\,.\,c^3 \text{ by Lemma 4·4}\end{aligned}$$

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

$$= ((x^{-1}hx) \cdot h^{-1} \cdot (x^{-1}h^{-1}x) \cdot h) \cdot c^3$$
$$= ((b_h \cdot h) \cdot h^{-1} \cdot (h \cdot b_h)^{-1} \cdot h) \cdot c^3$$
$$= c^3$$

and for any $z \in L$

$$\begin{aligned}
\left[z^{\rho}h^{\rho}xh^{-\rho}b_h^{-\rho}, \sigma\right] &= b_h^{\rho}h^{\rho}x^{-1}h^{-\rho}zh^{-\rho}xh^{\rho^2}b_h^{\rho^2} \\
&= b_h^{\rho}h^{\rho}x^{-1}(h \cdot z)xh^{\rho^2}b_h^{\rho^2} \\
&= b_h^{\rho}h^{\rho}(b' \cdot (h \cdot z))h^{\rho^2}b_h^{\rho^2} \text{ for some } b' \in \mathbf{C}(L) \\
&= b_h^{-1} \cdot (h^{-1} \cdot (b' \cdot (h \cdot z))) \\
&= b_h^{-1} \cdot (b' \cdot (b'^{-1} \cdot (h^{-1} \cdot (b' \cdot (h \cdot z))))) \\
&= b_h^{-1} \cdot (b' \cdot (zF(h, b'))) \text{ by Lemma 4·5} \\
&= b_h^{-1} \cdot (b' \cdot (z \cdot b'')) \text{ for some } b'' \in \mathbf{C}(L), \text{ by Theorem 5·4} \\
&\in z \cdot \mathbf{C}(L) \text{ by Lemma 4·3.}
\end{aligned}$$

Hence for any $h \in L$, any $x \in N \bigcap C_{G(L)}(\sigma)$, and any $a \in \mathbf{C}(L)$, we get that

$$h^{\rho}xh^{-\rho} \in N$$

and

$$h^{\rho}a^{\rho}h^{-\rho} \in N.$$

Therefore $h^{-\rho}$, and likewise h^{ρ}, are in the normalizer of N in $G(L)$. Since N is invariant under S, h and h^{ρ^2} are also contained in the normalizer of N in $G(L)$ for any $h \in L$. Hence $N \trianglelefteq G(L)$.

Since $N \trianglelefteq G(L)$, for any $h, g \in L$ and any $a \in \mathbf{C}(L)$ we get that

$$\begin{aligned}
aR(h, g) &= ((a \cdot h) \cdot g) \cdot (g^{-1} \cdot h^{-1}) \\
&= (g^{\rho}h^{-1}g^{\rho^2})^{-\rho^2}g^{-\rho^2}h^{-\rho^2}a^{-\rho^2}a^{-\rho}h^{-\rho}g^{-\rho}(g^{\rho}h^{-1}g^{\rho^2})^{-\rho} \\
&= g^{-\rho}h^{\rho^2}g^{\rho}h^{-\rho^2}a^{-\rho^2}a^{-\rho}h^{-\rho}g^{\rho^2}h^{\rho}g^{-\rho^2} \\
&= \left[g^{-\rho}h^{\rho^2}g^{\rho}h^{-\rho^2}a^{\rho^2}h^{\rho^2}g^{-\rho}h^{-\rho^2}g^{\rho}, \sigma\right] \\
&\in [N, \sigma] = \mathbf{C}(L)
\end{aligned}$$

and

$$\begin{aligned}
aL(h, g) &= (h^{-1} \cdot g^{-1}) \cdot (g \cdot (h \cdot a)) \\
&= (g^{\rho^2}h^{-1}g^{\rho})^{-\rho}g^{-\rho}h^{-\rho}a^{-\rho}a^{-\rho^2}h^{-\rho^2}g^{-\rho^2}(g^{\rho^2}h^{-1}g^{\rho})^{-\rho^2} \\
&= g^{-\rho^2}h^{\rho}g^{\rho^2}h^{-\rho}a^{-\rho}a^{-\rho^2}h^{-\rho^2}g^{\rho}h^{\rho^2}g^{-\rho} \\
&= \left[g^{-\rho^2}h^{\rho}g^{\rho^2}h^{-\rho}a^{\rho}h^{\rho}g^{-\rho^2}h^{-\rho}g^{\rho^2}, \sigma\right] \\
&\in [N, \sigma] = \mathbf{C}(L).
\end{aligned}$$

This completes the proof of Theorem 1·1.

Acknowledgements. I thank J. D. Phillips for bringing this open problem to my attention at the 2nd Mile High Conference on Nonassociative Mathematics.

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press

REFERENCES

[**1**] G. BOL. Gewebe und Gruppen. *Math. Ann.* **114** (1937), no. 1, 414–431.
[**2**] R. H. BRUCK. *A Survey of Binary Systems* (Springer-Verlag, 1971).
[**3**] S. DORO. Simple Moufang loops. *Math. Proc. Camb. Phil. Soc.* **83** (1978), no. 3, 377–392.
[**4**] S. M. GAGOLA III. The development of Sylow p-subloops in finite Moufang loops. *J. Algebra* **322** (2009), no. 5, 1565–1574.
[**5**] S. M. GAGOLA III. The existence of Sylow 2-subloops in finite Moufang loops. *J. Algebra* **322** (2009), no. 4, 1029–1037.
[**6**] S. M. GAGOLA III. The number of Sylow p-subloops in finite Moufang loops. *Comm. Algebra* **38** (2010), no. 4, 1436–1448.
[**7**] S. M. GAGOLA III and J. I. HALL. Lagrange's theorem for Moufang loops. *Acta Sci. Math. (Szeged)* **71** (2005), 45–64.
[**8**] A. GRISHKOV and A. ZAVARNITSINE. Sylows theorem for Moufang loops. *J. Algebra* **321** (2009), no. 7, 1813–1825.
[**9**] A. GRISHKOV and A. ZAVARNITSINE. Lagrange's theorem for Moufang loops. *Math. Proc. Camb. Phil. Soc.* **139** (2005), no. 1, 41–57.
[**10**] T. KEPKA and P. NĚMEC. Commutative Moufang loops and distributive groupoids of small orders. *Czechoslovak Math. J.* **31 (106)** (1981), no. 4, 633–669.
[**11**] M. KINYON and J. D. PHILLIPS. Commutants of Bol loops of odd order. *Proc. Amer. Math. Soc.* **132** (2004), no. 3, 617–619.
[**12**] R. MOUFANG. Zur Struktur von Alternativ *Körpern. Math. Ann.* **110** (1935), 416–430.

https://doi.org/10.1017/S0305004111000181 Published online by Cambridge University Press