Math. Proc. Camb. Phil. Soc. (1978), **83**, 377
Printed in Great Britain

Simple Moufang loops

BY STEPHEN DORO
Michigan State University, East Lansing, Michigan 48824

(*Received* 7 *March* 1977, *revised version* 11 *November* 1977)

Introduction. If H is a Moufang loop, and $x \in H$, there are defined permutations of H, $L(x): y \mapsto xy$ and $R(x): y \mapsto yx$. The group $\mathrm{Gr}(H)$, generated by these permutations for all choices of x, is called the multiplication group of H. It has a close connexion with the structure of H, as shown, for instance, in the papers of Albert(1). The purpose of this paper is to investigate the correspondence between groups and loops, so that group theoretic results may be applied to determine the structure of Moufang loops.

Glauberman(6) points out that for Moufang loops M with trivial nucleus, the multiplication group $\mathrm{Gr}(M)$ admits a certain dihedral group D of automorphisms, with $|D| = 6$. For fixed generators $\sigma, \rho \in D$ with $|\sigma| = 2$, $|\rho| = 3$, the following equation holds for any x in $\mathrm{Gr}(M)$:

$$[x, \sigma][x, \sigma]^{\rho}[x, \sigma]^{\rho^2} = 1. \tag{1}$$

We shall call groups G with such automorphisms, and satisfying the condition $[G, D] = G$, groups with triality, since the most striking example is $D_4(q)$ with its graph automorphisms.

From any group with triality G, there is a uniform construction of a Moufang loop M on which the group G has a permutation representation isomorphic to $\mathrm{Gr}(M)$. Conversely, every Moufang loop arises in this way from a group with triality. This correspondence is not quite unique; it is possible for two groups to give rise to the same loop, but the two groups must then be isomorphic modulo certain factors in their centres. Associative Moufang loops correspond to wreath products or to closely related constructions, while simple non-associative Moufang loops correspond to simple groups with triality.

Thus any theorem about finite groups with triality whose hypotheses have an easily stated interpretation for the corresponding loops, yields a theorem about Moufang loops. For example, Glauberman's Z^* theorem implies immediately Glauberman's result on the solvability of Moufang loops without involutions; the Fischer–Aschbacher classification of groups generated by odd transpositions yields a classification of simple Moufang loops of odd type; that is, those for which every element has either odd order or else is an involution.

Let $M(q)$ denote the finite, simple Moufang loop which consists of the units in an eight-dimensional composition algebra over $GF(q)$, modulo the centre. These are the only known examples of simple, non-associative Moufang loops. Every $M(q)$ contains elements of order 3, which leads to the conjecture that the same is valid for all finite, simple, non-associative Moufang loops. In the last section of this paper we reduce this problem to a purely group-theoretic question, but in this case the requisite result in

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

group theory is not known; it is the analogue of the Glauberman Z^*-theorem for elements of order 3. If we could show 3′ non-associative Moufang loops did not exist, the result would be, in a sense, the best possible; in $M(2)$ and $M(3)$ every element has order 1, 2 or 3. We shall show $M(2)$ and $M(3)$ are the only finite, simple Moufang loops with just three conjugacy classes of elements.

The following construction is used throughout the paper. Define a composition on M by $x.y = xy^{-1}x$. Then

$$x.x = x, \tag{2}$$

$$x.(x.y) = y, \tag{3}$$

$$x(y.z) = xy.xz, \tag{4}$$

$$(y.z)x = yx.zx. \tag{5}$$

Using (4) and (5), $x(y.z)^{-1}x = x(y^{-1}.z^{-1})x = xy^{-1}x.xz^{-1}x$

$$x.(y.z) = (x.y).(x.z). \tag{6}$$

In (5) we study systems satisfying (2), (3) and (6), called symmetric spaces. (4) and (5) assert that $R(x)$, $L(x)$ and hence $\mathrm{Gr}(M)$ act as automorphisms of the symmetric space M. It is not true that every symmetric space may be embedded in a group, however all the symmetric spaces which are treated in this paper are so embedded. Nevertheless, it is convenient to use the notation and some elementary results about symmetric spaces; these are treated in a brief introductory section.

Symmetric spaces. We shall define a symmetric space to be a set S with a binary composition such that for all $x, y, z \in S$ the equations (2), (3) and (6) are satisfied. We are concerned with two types of examples.

Let $C = \mathrm{ccl}_G e$ be the collection of all involutions in a group G conjugate to a particular involution e. For $x, y \in C$ define $x.y = xyx$. This is a symmetric space.

Let G be a group with an involutory automorphism C and let $D = \{[x, e] : x \in G\}$. If $x, y \in D$, then define $x.y = xy^{-1}x$. D is a symmetric space since

$$(x^{-1}exe)(ey^{-1}ey)(x^{-1}exe) = (x^{-1}exy^{-1})e(yx^{-1}ex)e.$$

In fact, this example is isomorphic to one of the first type. In the semidirect product, $G\langle e\rangle$, let $C = \mathrm{ccl}_G(e)$. Since $e^g = [g, e]e$, the map $\phi : C \to D$, $x \mapsto xe$ is a one-to-one correspondence of C with D. It is a symmetric space isomorphism since

$$(x.y)e = xyxe = (xe)(ye)^{-1}(xe) = (xe).(ye).$$

Define a pointed symmetric space to be a symmetric space with a distinguished element e. In a pointed symmetric space we may define powers and inverse of an element inductively. $x^0 = e$, $x^1 = x, x^{n+2} = x.(e.x^n)$, $x^{-n} = e.x^n$. The map $x \mapsto x^{-1}$ is an automorphism of a symmetric space. In the space D, if 1 is chosen as the base point, then this definition of powers coincides with that obtained by taking powers in the group G. D is closed under symmetric compositions in G; that is, if $x, y \in D$, $xyx \in D$.

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

Groups with triality. In the rest of this paper, the letter D will always represent a dihedral group of order 6 and ρ and σ will represent fixed elements of D with $|\rho| = 3$ and $|\sigma| = 2$.

Let G be a group admitting D as a group of automorphisms. In the semidirect product GD, there are three isomorphic symmetric spaces σ^G, $(\rho\sigma)^G$ and $(\sigma\rho)^G$ and hence the sets $T_\pi = \{[x, \sigma] : x \in G\}$, $T_\mu = \{[x, \sigma\rho] : x \in G\}$ and $T_\lambda = \{[x, \rho\sigma] : x \in G\}$ are isomorphic symmetric spaces embedded in G. Choose an abstract symmetric space S isomorphic to these and an isomorphism P of S with T_π. Then define $L(x) = (P(x))^\rho$ and $R(x) = (L(x))^\rho$ so $P(x) = (R(x))^\rho$. $L(x) \in T_\lambda$ and $R(x) \in T_\mu$, so that P, L, R are each isomorphisms of S with T_π, T_λ and T_μ respectively. Furthermore, $P(x) = u^{-1}u^\sigma$ for some $u \in G$ so $(P(x))^\sigma = P(x)^{-1}$. $(L(x)\rho\sigma)^\sigma = (P(x)\sigma)^{\rho\sigma} = (P(x)\sigma)^{\sigma\rho^{-1}} = R(x)^{-1}\sigma\rho$. In summary,

$$\left.\begin{aligned} P(x)^\rho &= L(x), \\ L(x)^\rho &= R(x), \\ R(x)^\rho &= P(x), \end{aligned}\right\} \tag{7}$$

$$\left.\begin{aligned} P(x)^\sigma &= P(x)^{-1}, \\ L(x)^\sigma &= R(x)^{-1}, \\ R(x)^\sigma &= L(x)^{-1}. \end{aligned}\right\} \tag{8}$$

Fixing σ, $\sigma\rho$, and $\rho\sigma$ as the base points in their respective symmetric spaces, we have

$$P(x)^{-1} = P(x^{-1}), \quad L(x)^{-1} = L(x^{-1}) \quad \text{and} \quad R(x)^{-1} = R(x^{-1}). \tag{9}$$

Now assume G is a group with triality. Since $P(x) = [u, \sigma]$ for some u, we have

$$P(x)\,L(x)\,R(x) = 1$$

or

$$P(x) = R(x)^{-1}L(x)^{-1}. \tag{10}$$

Apply σ and use the relation (9).

$$R(x)^{-1}L(x)^{-1} = (L(x)\,R(y))^\sigma = (P(x^{-1}))^\sigma = (R(x)\,L(x))^{-1} = L(x^{-1})\,R(x^{-1}).$$

Consequently, $P(x)$, $R(x)$ and $L(x)$ commute pairwise. Thus the equation (1) does not depend on the particular choice of ρ and σ.

Now define $I = C_G(\sigma)$. Our aim is to define a binary composition which turns the cosets of I into a Moufang loop.

LEMMA 1. *If G is a group with triality and $I = C_G(\sigma)$, then for each coset Ig, there exists exactly one element x in S such that*

$$Ig \cap T_\lambda = \{L(x)\} \quad \textit{and} \quad Ig \cap T_\mu = \{R(x)\}.$$

Proof. Ig is the set of elements t such that $\sigma^t = P(x)\,\sigma$ for some element $x \in S$. But $\sigma^{L(x)} = P(x)\,\sigma = \sigma^{R(x)}$. The statement follows.

For $x \in S$ we denote the coset $IL(x) = IR(x)$, simply by Ix. This defines a permutation representation of G on S; if $(Ix)\,g = Iy$ for $x, y \in S$ and $g \in G$ let $xg = y$.

$$(P(x)\,\sigma)^{P(y)} = P(y^{-1})\,P(x)\,P(y^{-1})\,\sigma = P(y^{-1}.x^{-1})\,\sigma.$$

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

Therefore $$xP(y) = y^{-1}.x^{-1} = (y.x)^{-1}. \tag{11}$$

We may define a binary composition in S by using this permutation representation. If $IxR(y) = Iz$, define $xy = z$. Then right multiplications biject. We show

$$x^a x^b = x^{a+b} \tag{12}$$

and hence that powers may be interpreted unambiguously in the symmetric space or under this composition. It is enough to show

$$\sigma^{Ix^a R(x^b)} = P(x^{a+b})\,\sigma.$$

But
$$\begin{aligned}(P(x^a)\,\sigma)^{R(x^b)} &= R(x^{-b})\,P(x^a)\,L(x^{-b})\,\sigma \\ &= R(x^{-b})\,R(x^{-a})\,L(x^{-a})\,L(x^{-b})\,\sigma \\ &= R(x)^{-b}R(x)^{-a}L(x)^{-a}L(x)^{-b}\sigma \\ &= R(x^{-a-b})\,L(x^{-a-b})\,\sigma = P(x^{a+b})\,\sigma.\end{aligned}$$

If H is a subgroup of a group G, let

$$\mathrm{core}_G(H) = \bigcap_{g \in G} H^g.$$

If S is a Moufang loop and $\mathrm{Gr}(x)$ is its multiplication group, let $\mathscr{J}(S)$ represent the subgroup of elements which fix 1.

THEOREM 1. *Let G be a group with triality. Then the binary composition $(x, y) \mapsto xy$ defined above makes S into a Moufang loop and $G/\mathrm{core}_G(C(\sigma)) \cong \mathrm{Gr}(S)$. Furthermore, $C(\sigma)/\mathrm{core}_G(C(\sigma)) \cong \mathscr{J}(S)$.*

Proof. We have defined $xy = xR(y)$. We now aim to show

$$yL(x) = xy. \tag{13}$$

Conjugate by σ permutes the cosets of I. σ: $Ia \mapsto Ia^{-1}$ since $(L(a))^\sigma = R(a)^{-1}$.

$$Iyx = IL(y)\,R(x)$$

and so
$$I(yx)^{-1} = (Iyx)^\sigma = IR(y)^{-1}L(x)^{-1} = Iy^{-1}L(x)^{-1}.$$

Therefore $$(y^{-1}x^{-1})^{-1} = yL(x). \tag{14}$$

Now (10) and the commutativity of $L(x)$ and $R(x)$ imply

$$yL(x)\,R(x) = yR(x)\,L(x) = yP(x^{-1}),$$

hence by (14) and (11)

$$(y^{-1}x^{-1})^{-1}x = ((yx)^{-1}x^{-1})^{-1} = yP(x^{-1}) = (x^{-1}.y)^{-1} = x.y^{-1}. \tag{15}$$

But $R(x)\,R(y)\,R(x) = R(x.y^{-1})$ and so

$$(xy)\,x = x.y^{-1}.$$

Since right multiplication is 1–1, we conclude

$$(y^{-1}x^{-1})^{-1} = xy.$$

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

This equation, applied to (14) shows $yL(x) = xy$, and applied to (15) shows the flexible law $(xy)x = x(yx)$.

Since $R(x)R(y)R(x) = R(x.y^{-1})$ we have

$$((zx)y)x = z(x.y^{-1}) = z((xy)x) = z(x(yx)).$$

But in (4), it is demonstrated that the identity $((zx)y)x = z(x(yx))$ characterizes Moufang loops.

$G = [G, D]$, so G is generated by $T_\mu \cup T_\lambda$. Thus, (13) and (14) imply that $\mathrm{Gr}(S)$ is a homomorphic image of G. The kernel is the set of elements which induce the trivial permutation on S or equivalently on cosets of $I = C(\sigma)$. This kernel is $\mathrm{core}_G(C(\sigma))$.

Let $X \in G$, and 1 be the identity in S. Then $1X = 1$ if and only if $X \in C(\sigma)$. Thus, $C(\sigma)/\mathrm{core}\, C(\sigma) = \mathscr{J}(S)$.

COROLLARY 1. *Let G be a group with triality, associated with the Moufang loop S. If G_1 is a D-invariant normal subgroup, then G/G_1 is a group with triality. If G/G_1 is associated with the loop S_1, then S_1 is a homomorphic image of S. $S_1 \cong S$ if and only if $G_1 \subseteq C_G(GD)$. If $\bar{G} = G/C_G(GD)$ then $C_{\bar{G}}(\bar{G}D) = 1$.*

Proof. Certainly G/G_1 is a group with triality. For some $u \in G$, $L(x) = [u, \rho\sigma]$ and the map $L(x) = [u, \rho\sigma] \mapsto [u, \rho\sigma]G_1 = L(x)G_1$ may be used to induce a homomorphism from S to S_1. If $G_1 \subseteq C_G(GD) \subseteq \mathrm{core}_G(C(\sigma))$ then $L(x) \mapsto L(x)G_1$ induces an isomorphism from $\mathrm{Gr}(S)$ to $\mathrm{Gr}(S_1)$ so $S \cong S_1$.

Conversely, if $S \cong S_1$ then $G_1 \subseteq \mathrm{core}_G(C(\sigma))$ and since G_1 is D-invariant

$$G_1 \subseteq \mathrm{core}_G(C(\sigma) \cap C(\sigma\rho)) = \mathrm{core}_G(C(D)).$$

Since $G = [G, D]$, $G_1 \subseteq C_G(GD)$.

If $C_{\bar{G}}(\bar{G}D) \neq 1$, then let G_1 be the inverse image of $C_{\bar{G}}(\bar{G}D)$ in G. Let S, $\bar{S}$ and S_1 be the loops associated with G, $\bar{G}$ and G/G_1 respectively. Then $S \cong \bar{S} \cong S_1$, contradicting the fact that $G_1 \nsubseteq C_G(GD)$.

COROLLARY 2. *If G is a group with triality, then with notation as before,*

$$\left.\begin{aligned} P(y^{-1}x) &= L(y)P(x)R(y), \\ L(y^{-1}x) &= R(y)L(x)P(y), \\ R(y^{-1}x) &= P(y)R(x)L(y), \end{aligned}\right\} \tag{16}$$

$$\left.\begin{aligned} P(xy^{-1}) &= R(y)P(x)L(y), \\ L(xy^{-1}) &= P(y)L(x)R(y), \\ R(xy^{-1}) &= L(y)R(x)P(y). \end{aligned}\right\} \tag{17}$$

Proof. Let us first note that it is sufficient to prove one of these equations, since they are all conjugate under D. Consider the conjugate of $\sigma\rho$,

$$\begin{aligned} (R(x)\sigma\rho)^{P(y^{-1})} &= P(y)R(x)\sigma\rho P(y)^{-1} \\ &= P(y)R(x)L(y)\sigma\rho. \end{aligned}$$

This expression implies that $P(y)R(x)L(y) = R(u)$ for some u. On the other hand,

$$P(y)R(x)L(y) \equiv R(y^{-1}x) \bmod (\mathrm{core}(C(\sigma)))$$

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

because $y((y^{-1}zy^{-1})x) = z(y^{-1}x)$ in S, the loop associated with G. Thus

$$R(u) \equiv R(y^{-1}x) \bmod (\mathrm{core}(C(\sigma))) \quad \text{so} \quad u = y^{-1}x.$$

Given a group with triality G, associated with the loop S we define subgroups $\mathscr{L}$, $\mathscr{R}$ and $\mathscr{P}$ of G. $\mathscr{L} = \langle L(x): x \in S\rangle$, $\mathscr{R} = \langle R(x): x \in S\rangle$ and $\mathscr{P} = \langle P(x): x \in S\rangle$. Each of $\mathscr{L}$, $\mathscr{R}$, $\mathscr{P}$ is normal in G. It suffices to show $\mathscr{R}$ normalizes $\mathscr{P}$ because of the action of D.

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

We require an identity. By (16), $P(yx) = L(y^{-1})\,P(x)\,R(y^{-1})$. Therefore,

$$1 = L(yx)\,L(y^{-1})\,L(x^{-1})\,R(x^{-1})\,R(y^{-1})\,R(yx)$$

or

$$R(x)^{-1}R(y)^{-1}R(yx) = L(x)\,L(y)\,L(x^{-1}y^{-1}). \tag{18}$$

Define $T(x) = L(x)^{-1}R(x)$, $L(x,y) = L(x)\,L(y)\,L(yx)^{-1}$, $R(x,y) = R(x)\,R(y)\,R(xy)^{-1}$. By (18), σ centralizes $L(x,y)$ and $R(x,y)$. σ clearly centralizes $T(x)$.

COROLLARY 3. *If G is a group with triality then $I = C_G(\sigma)$ is generated by*

$$\{T(x), L(x,y), R(x,y): x, y \in S\}.$$

Proof. Let $I_1 = \langle R(x,y), L(x,y), T(x): x, y \in S\rangle$ $I_1 \subseteq I$. Let

$$K = \{k \in G: k \in I_1\,R(1k)\}.$$

$k \in K$ if and only if $k \in I_1\,L(1k)$ because $R(1k)^{-1}L(1k) \in I_1$. Let $k \in K$, $x \in S$ and $1k = t$, so $k = i_1\,R(t) = i_2\,L(t)$ where $i_1, i_2 \in I_1$. Then $1kR(x) = tx$. $kR(x) = i_1\,R(t,x)\,R(tx)$ and therefore $kR(x) \in K$. Similarly, $kL(x) \in K$. Thus $KG \subseteq K$ so $K = G$. Thus, if $1g = 1$, $g \in I_1$. Therefore $I_1 = I$.

COROLLARY 4. *If G is a group with triality, $G = \mathscr{P}$ and not every element of S has order 3, then all the automorphisms in D are outer.*

Proof. Since $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ and $\sigma\rho\sigma\rho^{-1} = \rho$, it is enough to show ρ is an outer automorphism. If not, ρ is conjugation by some $r \in \mathscr{P}$ so $r = P(x_1)\ldots P(x_n)$ for some $x_i \in S$. Since $\rho^{-1} = \rho\sigma$,

$$r^{-1} = P(x_n)^{-1}\ldots P(x_1)^{-1} = P(x_1)^{-1}\ldots P(x_n)^{-1},$$

$$r^{-2} = P(x_1)^{-1}\ldots P(x_n)^{-1}P(x_n)^{-1}\ldots P(x_1)^{-1}.$$

The formula (11) implies $\quad P(a)\,P(b)\,P(a) = P(aba).$

Thus, $r^{-2} = P(u)$, where $u = x_1^{-1}(\ldots(x_n^{-1}x_n^{-1})\ldots)x_1^{-1}$. Since r^{-2} induces the same automorphism as r, we may as well assume $r = P(u)$ for some u. Then

$$r = \rho^{-1}r\rho = L(u),$$

$$r = \rho r\rho^{-1} = R(u)$$

and $L(u) = R(u) = P(u) = L(u)^{-1}R(u)^{-1}$. Thus $u^3 = 1$. For all $x, y \in S$

$$\begin{aligned}(xy)\,u = (x((yu)\,u^{-1}))\,u &= (yu)\,\rho L(x)\,\rho^{-1}\\ &= (yu)\,\rho(x)\\ &= x^{-1}(yu)\,x^{-1}.\end{aligned}$$

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

If $x = y$, this implies $x^2u = ux^{-1}$. The same argument, applied to $r^{-1} = P(u^{-1})$ rather than to r, implies $x^{-1}u = ux^2$. Thus $x^3 = 1$. But for some x this is assumed not to hold.

Groups with triality actually constitute a category $\mathscr{T}$. Fix a subgroup D as before, and let an object in $\mathscr{T}$ be a group G together with an action of D on G which makes G a group with triality. A morphism $f: G \to H$ in the category $\mathscr{T}$ is a D-invariant map; that is, a group homomorphism $f: G \to H$ such that for all $\tau \in D$, and $g \in G$, $f(g^\tau) = (f(g))^\tau$.

If G is a group with triality, let $M(G)$ be the Moufang loop associated with G. M is actually a functor from the category $\mathscr{T}$ to the category of Moufang loops. Suppose $f: G \to H$ is a morphism of $\mathscr{T}$. Then $f([g, \sigma]) = [f(g), \sigma]$. Define a function

$$M(f): M(G) \to M(H) \quad \text{by setting} \quad f(P(s)) = P(M(f)s).$$

Then $f(L(s)) = L(M(f)s)$ and $f(R(s)) = R(M(f)s)$. Clearly, $M(f)1 = 1$. Also,

$$M(f)(y^{-1}x) = M(f)y^{-1}M(f)x,$$

because

$$P(M(f)(y^{-1}x)) = f(P(y^{-1}x)) = f(L(y)P(x)R(y)) = f(L(y))f(P(x))f(R(y)) = P(M(f)y^{-1}M(f)x).$$

Therefore, $M(f)$ is a Moufang loop homomorphism.

The groups $G(S)$. In this section we show that for any Moufang loop S, there is a group with triality $G(S) = G$ such that $M(G) = S$. This group $G(S)$ will have a universal property among all groups H with $M(H) = S$, namely there is a unique homomorphism $G(S) \to H$ determined by $L_G(x) \mapsto L_H(x)$, $R_G(x) \mapsto R_H(x)$, where we distinguish $L(x) \in G$ from $L(x) \in H$ by the appropriate subscripts.

The association of $G(S)$ to S is also a functor. Consequently, there is a one-to-one correspondence between simple Moufang loops and D-simple groups with triality. Finite loops correspond to finite groups. This may be used to obtain results about finite Moufang loops.

Let S be a Moufang loop and let $G(S)$ be the group with three sets of generators, indexed by elements of S, $\{P_x, L_x, R_x : x \in S\}$ and the relations

$$\left.\begin{gathered} P_1 = L_1 = R_1 = 1, \\ P_x L_x R_x = 1, \quad L_x L_y L_x = L_{xyx}, \quad R_x R_y R_x = R_{xyx}, \\ P_x P_y P_x = P_{xyx}, \quad P_{y^{-1}x} = L_y P_x R_y, \quad L_{y^{-1}x} = R_y L_x P_y, \quad R_{y^{-1}x} = P_y R_x L_y, \\ P_{xy^{-1}} = R_y P_x L_y, \quad L_{xy^{-1}} = P_y L_x R_y, \quad R_{xy^{-1}} = L_y R_x P_y. \end{gathered}\right\} \tag{19}$$

Then if Q is one of P, R, L we have $Q_{x^a} = (Q_x)^a$ for any integer a, and P_x, R_x and L_x commute. Therefore, $G(S)$ admits automorphisms ρ, σ given by

$$\left.\begin{aligned} P_x^\rho &= L_x, \quad & L_x^\rho &= R_x, \quad & R_x^\rho &= P_x, \\ P_x^\sigma &= P_x^{-1}, \quad & L_x^\sigma &= R_x^{-1}, \quad & R_x^\sigma &= L_x^{-1}, \end{aligned}\right\} \tag{20}$$

ρ and σ generate a group D which is dihedral of order 6.

THEOREM 2. *The group $G(S)$ is a group with triality and $M(G(S)) = S$. $G(S)$ has the universal property described above and the correspondence of $G(S)$ to S is a functor.*

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

Proof. Let $G = G(S)$. We work inside the semidirect product GD. Let Q be one of the letters P, L, R. If $x, y \in S$, there exists $z \in S$ with $(P_x\sigma)^{Q_y} = P_z\sigma$.

$$\left.\begin{aligned}(P_x\sigma)^{P_y} &= P_y^{-1}P_xP_y^{-1}\sigma = P_{y^{-1}xy^{-1}}\sigma,\\ (P_x\sigma)^{L_y} &= L_y^{-1}P_xR_y^{-1}\sigma = P_{yx}\sigma,\\ (P_x\sigma)^{R_y} &= R_y^{-1}P_xL_y^{-1} = P_{xy}\sigma.\end{aligned}\right\} \tag{21}$$

If x is an arbitrary element of G, x may be represented as $x = Q^1_{a_1}\dots Q^n_{a_n}$ where each Q^i is one of P, L, R and $a_k \in S$. Then $\sigma^x = P_z\sigma$ for some $z \in S$. Hence,

$$T_\pi = \{[x,\sigma]: x \in G\} = \{P_z: z \in S\}.$$

Furthermore, $P_a \neq P_b$ unless $a = b$ because the multiplication group $\mathrm{Gr}(S)$ is a homomorphic image of $G(S)$, since the identities we have imposed in (19) correspond to identities in $\mathrm{Gr}(S)$. In the same way, $T_\lambda = \{[x,\sigma\rho]: x \in G\} = \{R_z: z \in S\}$. G is a group with triality because $[x,\sigma][x,\sigma]^\rho[x,\sigma]^{\rho^2} = P_zP_z^\rho P_z^{\rho^2} = P_zL_zR_z = 1$, and $G = [G, D]$ since G is generated by T_π, T_λ and T_μ. If we proceed to construct $M(G)$ as in Theorem 1, (21) implies $aL_b = ba$, $aR_b = ab$ so that $M(G) = S$ and we may revert to our former notation, $L_a = L(a)$, $R_a = R(a)$, $P_a = P(a)$.

Now if H is another group with triality and $M(H) = S$, then (10), (16) and (17) imply that the generators $L_H(x)$, $R_H(x)$, $P_H(x)$ of H satisfy the identities (19). Thus

$$L_x \mapsto L_H(x)$$

induces a unique homomorphism from G to H.

Now suppose S_1 is another Moufang loop. Let $G_1 = G(S_1)$ and suppose $\phi: S \to S_1$ is a homomorphism. The map $L_x \mapsto L_{\phi(x)}$, $R_x \mapsto R_{\phi(x)}$ and $P_x \mapsto P_{\phi(x)}$ can be extended to a homomorphism, provided that the image of an identity (19) in G is an identity in G_1, and this is readily verified.

Let $G_0(S) = G(S)/C_{G(S)}(DG(S))$. By the Corollary 1 to Theorem 1, $G_0(S)$ is also a group with triality with $M(G_0(S)) = S$. $G_0(S)$ is the minimal such group: any other such group has $G_0(S)$ as a homomorphic image.

COROLLARY 1. *Let G_1 and G_2 be groups with triality such that $S = M(G_1) = M(G_2)$. Then $G_1/C_{G_1}(G_1D) \cong G_2/C_{G_2}(G_2D) \cong G_0(S)$.*

Proof. By Theorem 2, G_1 and G_2 are homomorphic images of $G(S)$. Suppose $G_1 = G(S)/K_1$ and $G_2 = G(S)/K_2$ for D-invariant normal subgroups K_1 and K_2. By Corollary 1 to Theorem 1, K_1 and K_2 are contained in $C_{G(S)}(DG(S))$. The corollary follows.

COROLLARY 2. *$G_0(M)$ is D-simple if and only if M is a simple Moufang loop.*

Proof. By Corollary 1 to Theorem 1, $C_{G_0(M)}(DG_0(M)) = 1$. Thus, if $G_0(M) \supset K \supset 1$, where K is D-invariant and normal, then $G_0(M)/K$ is a group with triality whose associated loop is a proper homomorphic image of M. Conversely, if $M \supset N \supset 1$, where $N \lhd M$, then the homomorphism $G(M) \to G(M/N)$ induces a homomorphism $G_0(M) \to G_0(M/N)$ with D-invariant kernel so that G_0 is not D-simple.

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

If G is a group with triality and $G \supseteq G_1 \supseteq \ldots \supseteq G_n = 1$ is a series of D-invariant subgroups such that $G_k \lhd G_{k-1}$, then there is a corresponding normal series for

$$M = M(G), \quad M \supseteq M_1 \supseteq \ldots \supseteq M_n = 1, \quad \text{where} \quad M_k = M(G_k).$$

The factor groups correspond to factor loops; however, the corresponding loop may be trivial. If D centralizes G_{k-1}/G_k, the corresponding loop is 1.

COROLLARY 3. *If M is a finite Moufang loop, $G(M)$ is a finite group, whose order is bounded by a function of $|M|$.*

Proof. We shall show the semidirect product $DG(M)$ is finite. Note that

$$\mathrm{ccl}_{DG(M)}\sigma = \{P(x)\sigma, L(x)\rho\sigma, R(x)\sigma\rho : x \in M\}$$

is a finite conjugacy class which generates $DG(M)$. Therefore, $DG(M)$ is finite. For suppose $|\mathrm{ccl}_{DG(M)}\sigma| = n$. x in G may be written as a word $x = w_1 \ldots w_k$, where the letters $w_1, \ldots, w_k$ are members of $\mathrm{ccl}_{DG(M)}\sigma$. These letters are all distinct if k is minimal, otherwise a series of conjugations would reduce the length.

Let M be an associative Moufang loop (a group) and consider the wreath product $M \wr S_3$. This contains a normal subgroup $M_1 = M \times M \times M$ and M_1 satisfies (1), if S_3 is identified with the group D of automorphisms. We always represent $M \times M \times M$ as a set of ordered triples. Let $M_0 = [M_1, D] = [[M_1, D], D]$. M_0 is generated by elements $(a, a^{-1}, 1)$ and $(b, 1, b^{-1})$; hence, it contains $(a^{-1}b^{-1}ab, 1, 1)$. Thus $M_0 \supseteq M' \times M' \times M'$ and $M_0/M_0' = \{(a, b, c) : abc \equiv 1 \bmod M'\}$. M_0 is a group with triality. Suppose

$$(a, b, c)^\rho = (c, a, b) \quad \text{and} \quad (a, b, c)^\sigma = (c, b, a).$$

Define $$L(g) = (1, g, g^{-1}) \quad \text{and} \quad R(g) = (g, g^{-1}, 1).$$

Note that $$L(g^{-1})\,R(g) = (g, g^{-2}, g) \in I = C_{M_0}(\sigma).$$

Then $$(Ig)\,R(h) = I(g, g^{-1}, 1)\,(h, h^{-1}, 1) = I(1, [g, h], 1)\,(gh, h^{-1}g^{-1}, 1) = I(gh)$$

for g, h in G so that $M(M_0) = M$.

More generally, suppose $K \subseteq C_{M_0}(DM_0)$. An element of K is a triple (x, x, x) and $S = \{x : (x, x, x) \in K\}$ is a subgroup of $\mathbb{Z}(M)$. M_0/K is a group with triality and

$$M(M_0/K) \cong M/S.$$

We shall call a group with triality of the form M_0/K, for some group M, a wreathlike group and may still represent its elements by ordered triples, though not uniquely.

COROLLARY 4. *Let G be a finite group with triality such that $M(G)$ is a group M. Then $C_G(DG) \subseteq G'$ and if $G = G_0(M)$ or if $M = M'$, then G is wreathlike.*

Proof. The group M_0 constructed above is a group with triality such that $M(M_0) = M$. Therefore, $G_0(M)$ is a homomorphic image of M_0, so $G_0(M)$ is wreathlike.

G/G' is an abelian group with triality and $M(G/G') = M/M'$. If $M = M'$,

$$M(G/G') = 1, \quad \text{so} \quad [G/G', D] = 1.$$

Thus $G = G'$. To show G is wreathlike, it is enough to show $G(M)$ is wreathlike so assume $G = G(M)$. There is a homomorphism $G \to M \times M \times M$ with image M_0 and

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

kernel $K \subseteq G'$. If M^* is the extension by M of its Schur multiplier, then the extension by $M \times M \times M$ of the Schur multiplier of $M \times M \times M$ is $M^* \times M^* \times M^*$. G is a covering group of $M \times M \times M$. Therefore, G is a homomorphic image of $M^* \times M^* \times M^*$, hence G is wreathlike.

If $M \neq M'$, then $G(M)$ is not necessarily wreathlike. For there are cases in which M has non-isomorphic extensions by its Schur multiplier, say M^* and M^{**}. Construct $M^* \wr S_3$ and $M^{**} \wr S_3$ and define M_0^* and M_0^{**} as before. It can happen that $M_0^* \ncong M_0^{**}$, for instance, with $M = Z_2 \times Z_2$. Then $G(M)$ has both M_0^* and M_0^{**} as homomorphic images, so $G(M)$ is not wreathlike.

COROLLARY 5. *Let S be a Moufang loop with* $\mathrm{Nuc}(S) = 1$. *Then* $G_0(S) \cong \mathrm{Gr}(S)$.

Proof. $G_0(S)$ is characterized as the group with triality G such that $M(G) = S$ and $C_G(DG) = 1$. Let inv be the permutation of S, $\mathrm{inv}: x \mapsto x^{-1}$. Conjugation by inv yields an automorphism σ of $\mathrm{Gr}(S)$. As in (6), II, theorem 6, for any $g \in \mathrm{Gr}(S)$, there is a unique element g^ρ such that $(g, g^\rho, g^{\sigma\rho})$ is an automorphism. $\langle \rho, \sigma \rangle$ is a dihedral group of automorphisms of $\mathrm{Gr}(S)$ and the equations (7)–(10) hold. In particular,

$$[L(x), \sigma\rho] = R(x) \quad \text{and} \quad [R(x), \rho\sigma] = L(x),$$

so $\mathrm{Gr}(S)$ is a group with triality and $M(\mathrm{Gr}(S)) = S$. If $g \in C_{\mathrm{Gr}(S)}(D\,\mathrm{Gr}(S))$, then g is an automorphism of S; so for any x in S, $xg = 1\,R(x)\,g = 1\,gR(x) = x$, whence $g = 1$. Thus $\mathrm{Gr}(S) \cong G_0(S)$.

PROPOSITION 1. *Let S be a finite, simple Moufang loop. If $S = \mathbb{Z}_p$, where p is a prime and $p \neq 3$, then $G_0(S) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and ρ and σ are represented by the matrices over $GF(p)$,*

$$\rho = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

If $S = \mathbb{Z}_3$, $G_0(S) \cong \mathbb{Z}_3$ and ρ acts trivially while σ inverts $G_0(S)$. If S is associative but not commutative, $G_0(S) \cong S \times S \times S$, If S is non-associative, $G_0(S)$ is a finite, simple group.

Proof. In the cases where S is associative, the proposition is readily checked. Suppose then, that S is simple and non-associative, so that $G_0(S)$ is D-simple. $G_0(S)$ is at least characteristically simple. If $G_0(S)$ is elementary abelian, $L(x)$ and $R(y)$ commute so S is associative. Thus $G_0(S)$ is the direct sum of 1, 2, 3 or 6 isomorphic simple groups, which D permutes transitively.

If $G_0(S) = A_1 \times A_\rho \times A_{\rho^2} \times A_\sigma \times A_{\sigma\rho} \times A_{\rho\sigma}$, where the components are permuted according to $(A_\phi)^\tau = A_{\phi\tau}$, for $\phi, \tau \in D$, one can verify that for $x = (a, 1, 1, 1, 1, 1)$, equation (1) does not hold. If $G_0(S) = A \times A \times A$, where ρ acts transitively, then we may assume

$$(a, b, c)^\rho = (c, a, b),$$
$$(a, b, c)^\sigma = (b^{\sigma_2}, a^{\sigma_1}, c^{\sigma_3}) \quad \text{where} \quad \sigma_1, \sigma_2, \sigma_3 \in \mathrm{Aut}\,A.$$

$\sigma_1\sigma_2 = id$, $\sigma_3^2 = id$. Then (1) implies $a^{-1}b^{\sigma_2}b^{-1}a^{\sigma_1}c^{-1}c^{\sigma_3} = 1$ for all $a, b, c \in A$. Letting two of a, b, c equal 1, we conclude $\sigma_1 = \sigma_2 = \sigma_3 = id$ and $DG_0(S)$ is the wreath product $A \wr S_3$. Thus $A \cong S$ is associative.

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

If $G_0(S) = A_1 \times A_2$, where $A_1 \cong A_2 \cong A$ is a simple group, then we may assume

$$(a, b)^\sigma = (b, a), \quad (a, b)^\rho = (a^\phi, b^\psi), \quad \phi, \psi \in \mathrm{Aut}\, A.$$

$\phi^3 = id$ and since $\sigma\rho\sigma = \rho^{-1}, \psi = \phi^{-1}$.

Now by (10), cor. 3, since A is non-solvable, A contains a subgroup generated by two elements a and b which is non-solvable. $(a, a^{-1}) = P(u)$, $(b, b^{-1}) = P(v)$, for some $u, v \in S$, and $\langle L(u), L(v), R(u), R(v)\rangle = H$ is a group with triality such that $M(H) = \langle u, v\rangle$. Thus $M(H)$ is associative, so that $H/C_H(DH)$ is a wreathlike group. $M(H)$ is non-solvable, so that there exists D-invariant subgroups J and K of H with $K \lhd J$, such that $H \supseteq J \supset K \supseteq 1$ and $J/K = B_1 \times B_2 \times B_3$, where $B_k \cong B$ for $k = 1, 2, 3$ and B is a non-abelian simple group. Let H_k be the subgroup of J containing K such that $H_k/K = B_k$.

We claim H_k is contained in precisely one of $A_1 K, A_2 K$. Otherwise, there exists T such that $H_k \subseteq T \subseteq A_1 \times A_2$ and $T/K \cong T_1 \times T_2$, where $T_1 K \subseteq A_1 K$ and $T_2 K \subseteq A_2 K$ and $T_1/K \cong B \cong T_2/K$. Therefore, $[T, D]/K$ is the direct product of six simple groups which D permutes transitively. This situation has been shown to be impossible.

Without loss of generality then, H_1 and H_2 are contained in $A_1 K$. But since D acts like S_3 on $\{B_1, B_2, B_3\}$, one of $\{\sigma, \sigma\rho, \rho\sigma\}$ interchanges H_1 and H_2, and hence fixes A_1. This contradicts the assumptions on the action of σ and ρ.

Therefore, if S is non-associative, $G_0(S)$ is a non-abelian simple group.

COROLLARY. *Let A be a finite group with an automorphism ϕ such that for all $x \in G$, $xx^\phi x^{\phi^2} = 1$. Then A is solvable.*

Proof. Otherwise, let $G = A_1 \times A_2$ where $A_1 \cong A_2 = A$ and define ρ and σ by

$$(a, b)^\rho = (a^\phi, b^{\phi^2}), \quad (a, b)^\sigma = (b, a).$$

The proof of Proposition 1 shows that such a G is solvable.

Proposition 1 shows that a classification of finite simple Moufang loops could be deduced from a classification of finite simple groups and the determination of their automorphism groups. Let us illustrate this. Let G be a group with triality and $S = M(G)$. Consider $\sigma^G = \{P(x)\,\sigma : x \in S\}$. $|P(x)| = |(P(x)\,\sigma)\,\sigma|$. If $|S|$ is odd, then the product of two involutions in σ^G has odd order. By Glauberman's Z^*-theorem, G has odd order and hence by the Feit–Thompson theorem G is solvable. This implies S is solvable. We conclude that a simple Moufang loop must contain an involution.

If S is a simple Moufang loop, then by Corollary 4 of Theorem 1, the automorphisms D of Gr (S) are outer.

More generally, define a Moufang loop of odd type to be a finite Moufang loop such that every element either has odd order or is an involution.

PROPOSITION 2. *The simple Moufang loops of odd type are $M(q)$ where q is either 3, 5 or a power of 2, the groups $L_2(q)$ where q is a power of 2 and the cyclic groups of prime order.*

Proof. $\sigma^{G_0(M)}$ is a class of odd transpositions. Therefore, the classification of (2) may be applied. An examination of the automorphisms of the groups classified there, yields the conclusion.

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

Let us call an orbit of $\mathscr{J}(M)$ on M a conjugacy class.

PROPOSITION 3. *If M has just three conjugacy classes, including 1, and M is a simple Moufang loop, then $M = M(2)$ or $M(3)$.*

Proof. The order of an element is invariant under the action of $\mathscr{J}(M)$, which acts on M by symmetric space automorphisms which fix the base point 1. By Glauberman's results in (6) and (7), there exists an involution and a non-identity odd order element. Thus there are just these three classes. Now Proposition 2 may be applied.

On ρ^{-G}. Throughout this section, G is a finite group with triality, $I = C(\sigma)$, $S = C(\rho)$ and $M = M(G)$. The purpose of this section is to describe an approach to the problem of classifying finite simple groups with triality. No classifications are obtained because the requisite results in group theory are not known at present; nevertheless, it is interesting to note that the complete classification of finite non-associative Moufang loops may be reduced to certain problems in finite group theory which are analogous to known results. More precisely, when $a, b \in \mathrm{ccl}_G(\rho)$, $\langle a, b\rangle$ is contained in a semidirect product $\langle a\rangle H$, where H is a group with triality such that $M(H)$ is associative. Thus, the situation is similar to that discussed in (2), (3), where two members of a certain conjugacy class generate a certain restricted type of group. If we assume $(|M|, 3) = 1$, then $3 \nmid |H|$. Therefore, 3′-Moufang loops could be classified if the analogue of the Glauberman Z^* theorem for the prime 3 were known.

Suppose M contains a subloop N. Define $G_M(N) = \langle L(x), R(x) : x \in N\rangle$, a subgroup of G. $G_M(N)$ is a group with triality whose corresponding loop is N. Thus, there is a homomorphism $G_M(N) \to G_0(N)$. The kernel of this map, $C_{G_M(N)}(DG_M(N))$, need not be trivial. For example, if $G = \mathrm{Gr}(M(q))$ for an odd q, $M(q)$ contains subloops N isomorphic to $PSL_2(q)$ for which the corresponding group $G_M(N)$ is $SL_2(q) \curlyvee SL_2(q) \curlyvee SL_2(q)$ with centres identified.

Define a 3′-Moufang loop to be one which contains no elements of order 3.

Define the Moufang centre of M by $C(M) = \{x \in M : yL(x) = yR(x) \text{ for all } y \in M\}$. $C(M)$ is a characteristic subloop, but this does not necessarily imply $C(M)$ is normal. It is unknown whether there exist simple Moufang loops with $C(M) \neq 1$.

Conjecture 1. If $\mathrm{Nuc}(M) = 1$, then $C(M)$ is normal in M.

LEMMA 2.

(*a*) *If ρ acts trivially, M is a commutative Moufang loop of exponent* 3.

(*b*) *If M is simple, I is a maximal subgroup.*

(*c*) *If $C(M)$ is* 1 *or if M is a* 3′ *loop, $S = I \cap I^\rho = I \cap I^\rho \cap I^{\rho^2}$.*

(*d*) *If $\mathrm{Nuc}(M) = 1$, $C(M)$ is commutative, of exponent* 3.

Proof. If ρ acts trivially, $L(x) = R(x) = P(x)$ and (*a*) follows. Suppose $I \subset H \subset G$. Cosets of I in H define a subset T of M. T is a set of imprimitivity for the permutation representation of G on M. Hence if $x \in T$, $L(x) : 1 \mapsto x$, $R(x) : 1 \mapsto x$, so $L(x)$ and $R(x)$ preserve T so that T is a subloop. I preserves T so T is normal, by (1). If $C(M) = 1$ or M is 3′, then $S \subseteq I$. Otherwise, S is a group with triality, since σ normalizes ρ. If $x \in S - C(\sigma)$, $[x, \sigma] = P(z)$ for some $z \neq 1$ and $L(z) = R(z) = P(z)$ so $C(M) \neq 1$. $C(M)$

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

contains an element of order 3. Therefore, $I \cap I^\rho \subseteq S \subseteq I \cap I^\rho \cap I^{\rho^2}$ so equality prevails. Finally, if $\mathrm{Nuc}(M) = 1$, G may be taken as $\mathrm{Gr}(M)$, so the equation $L(z) = R(z)$ in $\mathrm{Gr}(M)$ implies $L(z) = R(z) = P(z)$ and $z^3 = 1$.

Part (*d*) is the same as Remark 3 of (6), II.

LEMMA 3. *If $C(M) = 1$ or if M is a 3′ loop, S induces automorphisms on M.*

Proof. The equations

$$\left.\begin{aligned}(aL(b))\,(cR(b)) &= (ac)\,P(b^{-1}),\\ (aR(b))\,(cP(b)) &= (ac)\,R(b^{-1}),\\ (aP(b))\,(cL(b)) &= (ac)\,L(b^{-1})\end{aligned}\right\} \tag{22}$$

imply $(aX)\,(cX^\rho) = acX^{\sigma\rho}$ for any $X \in G$ acting on $a, c \in M$. Thus if $X \in S$ and $C(M) = 1$ or if M is a 3′ loop then $X \in C(D)$ and X induces an automorphism of M.

We now repeat the basic construction of this paper, for the three involutions σ, $\sigma\rho$ and $\rho\sigma$. Take the direct sum of three copies of M, $M_\pi \times M_\mu \times M_\lambda$. We define a map k: $G \to M_\pi \times M_\mu \times M_\lambda$ by defining it for each component. $[g, \sigma] = P(t)$ for some $t \in M$; define $g_\pi = t$. Similarly, define g_μ by $R(g_\mu) = [g, \sigma\rho]$ and g_λ by $L(g_\lambda) = [g, \rho\sigma]$. Define $k(g) = (g_\pi, g_\mu, g_\lambda) \in M_\pi \times M_\mu \times M_\lambda$. The elements of $k(G)$ will be called special triples. Ig is the set of elements which conjugate σ to $P(g_\pi)\,\sigma$ so Ig contains $L(g_\pi)$ and $R(g_\pi)$. By (16) and (17), $\sigma^{IgL(t)} = L(t^{-1})\,P(g_\pi)\,R(t^{-1})\,\sigma = P(tg_\pi)\,\sigma$ and similarly for $R(t)$. Now define an action of G on M_π by

$$(g_\pi)\,x = (gx)_\pi \quad \text{or} \quad [g, \sigma] \mapsto [gx, \sigma].$$

Then $g_\pi L(t) = tg_\pi$, $g_\pi R(t) = g_\pi t$ and $g_\pi P(t) = t^{-1} g_\pi t^{-1}$. We shall call this the standard action of G on M.

Similarly, define an action of G on M_λ by $(x_\lambda)\,g = (xg)_\lambda$. Making elements of M correspond with G-conjugates of $\rho\sigma$ associates x_λ with $L(x_\lambda)\,\rho\sigma$ and $x_\lambda g$ corresponds to $(L(x_\lambda)\,\rho\sigma)^g$. Thus we get $x_\lambda R(t) = tx_\lambda$, $x_\lambda P(t) = x_\lambda t$ and $x_\lambda L(t) = t^{-1} x_\lambda t^{-1}$.

Similarly if $x_\mu g = (xg)_\mu$ then $x_\mu R(t) = t^{-1} x_\mu t^{-1}$, $x_\mu L(t) = x_\mu(t)$, $x_\mu P(t) = tx_\mu$. Consequently, $(a, b, c)\,g = (ag, bg^\rho, cg^{\rho^2})$, where here we use the standard action of G on M. G acts as symmetric space automorphisms of $M \times M \times M$ with kernel $C_G(DG)$ so $M \times M \times M$ affords a faithful permutation representation for $G_0(M)$. If we define further automorphisms of $M \times M \times M$ by r: $(a, b, c) \mapsto (b, c, a)$ and

$$s\colon (a, b, c) \mapsto (a^{-1}, c^{-1}, b^{-1})$$

then one can verify that conjugation by r induces ρ on $G/C_G(DG)$ and conjugation by s induces σ.

Now recall the commutator identities:

$$\left.\begin{aligned}[xy, z] &= [x, z]^y\,[y, z],\\ [x, yz] &= [x, z]\,[x, y]^z,\\ [x, yzw] &= [x, w]\,[x, z]^w\,[x, y]^{zw}.\end{aligned}\right\} \tag{23}$$

Applying these,

$$[x, \rho\sigma] = [x, \sigma(\sigma\rho)\,\sigma] = [x, \sigma]\,[x, \sigma\rho]^\sigma\,[x, \sigma]^{\sigma\rho\sigma}.$$

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

So $L(x_\lambda) = P(x_\pi)\,L(x_\mu)^{-1}R(x_\pi)$

$$[x, \rho\sigma] = [x, \sigma\rho(\sigma)\,\sigma\rho] = [x, \sigma\rho]\,[x, \sigma]^{\sigma\rho}\,[x, \sigma\rho]^{\sigma(\sigma\rho)},$$

$$L(x_\lambda) = R(x_\mu)\,L(x_\pi)^{-1}P(x_\mu).$$

Applying this equation to $1 \in M$, $x_\lambda = x_\mu^{-1}(x_\pi^{-1}x_\mu)\,x_\mu^{-1}$. This implies x_π, x_λ and x_μ associate and so

$$x_\pi x_\mu x_\lambda = 1. \tag{24}$$

Call a triple (a, b, c) such that $abc = 1$ an equation of M. By (22) G permutes the set of equations. If we identify ρ with r and σ with s, then DG permutes the set of equations.

In this context, we mention a Cauchy theorem for Moufang loops at the prime 3:

LEMMA 4. *If the order of a finite Moufang loop M is divisible by 3 then M has an element of order 3.*

Proof. ρ permutes the set of equations and a fixed point corresponds to an element (a, a, a) such that $a^3 = 1$. Therefore $|M|^2 \equiv |\{a : a^3 = 1\}| \equiv 0 \bmod 3$, whence

$$|\{a \neq 1 : a^3 = 1\}| \neq 0.$$

Define $O^3(M) = \langle x : (|x|, 3) = 1\rangle$. This agrees with established notation if M is associative. Also define $LO^3(M) = \{x \in M$: there exists an associative $H \subseteq M$ with $x \in O^3(H)\}$. Of course, from its definition it is not clear that $LO^3(M)$ is a loop; if $LO^3(M)$ is a loop then it coincides with $O^3(M)$.

Conjecture 2. $LO^3(M) = O^3(M)$, for any finite Moufang loop M.

We intend to show that if $M = LO^3(M)$ then the notions of equation and special triple coincide. If $a, b \in M \times M \times M$ write $a \sim b$ if there exists $g \in G$ with $ag = b$. Then our goal is to show transitivity of G on the set of equations. Since G is transitive on M_π, it is enough to show that every element $(1, a, a^{-1})$ is a special triple. This is equivalent to the transitivity of I^ρ acting on M via the standard actions.

LEMMA 5. *Suppose $M(G)$ is associative. Then $(1, 1, 1) \sim (1, b, b^{-1})$ if and only if $bO^3(M) \in \mathfrak{V}^1(M/O^3(M))$. In particular, if $M = O^3(M)$, G is transitive on equations.*

Proof. Since the result depends only on the permutation representation on $M \times M \times M$, one may assume $G = G_0(M)$. Then $G = M_0 \subseteq M \times M \times M$. If $x = (t, u, v) \in G$,

$$P(x_\pi) = (1, u^{-1}v, v^{-1}u),\quad L(x_\lambda) = (t^{-1}u, u^{-1}t, 1),\quad R(x_\mu) = (t^{-1}v, 1, v^{-1}t).$$

If $(1, 1, 1) \in M_\pi \times M_\mu \times M_\lambda$, then $(1, 1, 1)x = (u^{-1}v, v^{-1}t, t^{-1}u)$. To show transitivity, it is required that for an arbitrary $(a, b, c) \in M_\pi \times M_\mu \times M_\lambda$, with $(a, b, c) = 1$, we must solve the equations $a = u^{-1}v, b = v^{-1}t, c = t^{-1}u$, for t, u and v. This is always possible in $M \times M \times M$. The condition that $x \in M_0$ means that $tuv \equiv 1 \bmod M'$. Suppose $a = 1$ so $b^{-1} = c$. Then $u = v$ so that $b = v^{-1}t \equiv v^{-3} \bmod M'$. This equation is solvable precisely when $bO^3(M) \in \mathfrak{V}^1(M/O^3(M))$.

PROPOSITION 4. *Let G be a group with triality, M the corresponding loop and suppose $LO^3(M) = M$. Then G is transitive on equations.*

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

Proof. For any $x \in M$, there exists an associative $H \subseteq M$ with $x \in O^3(H)$. Then $G_M(H) \subseteq G$ and $(1, 1, 1) \sim (1, x, x^{-1})$ via an element of $G_M(H)$. Thus G is transitive.

COROLLARY 1. *If* $M = LO^3(M)$ *and* $C(M) = 1$, *then* $|G:S| = |M|^2$.

Proof. G acts on M_π as on cosets of $C(\sigma)$ and G acts on M_μ as on cosets of $C(\sigma\rho)$; hence G acts on the set of equations as on cosets of $C(\rho) = C(\sigma) \cap C(\sigma\rho)$. There are $|M|^2$ equations.

This corollary may be illustrated by the example of $M(q)$, the loops discussed in (8). Let $G = D_4(q)$, $S = G_2(q)$, $|G| = (\frac{1}{4})^\epsilon q^{12}(q^2-1)(q^4-1)(q^6-1)(q^4-1)$,

$$|G_2(q)| = q^6(q^6-1)(q^2-1).$$

Therefore $|G:S| = ((\frac{1}{2})^\epsilon q^3(q^4-1))^2$ where $\epsilon = 0$ if q is even and $\epsilon = 1$ if q is odd.

PROPOSITION 5. *Let* $\rho_1 \in \mathrm{ccl}_G(\rho^{-1})$. *Then* $\langle \rho^{-1}, \rho_1 \rangle$ *is contained in a semidirect product* $\langle \rho \rangle H$, *where* H *is a* D*-invariant group with triality and* $N = M(H)$ *is associative.*

Proof. Let $\rho_1 = (\rho^{-1})^x = [x, \rho]\rho^{-1}, x \in G$. By (23),

$$[x, \rho] = [x, (\sigma\rho)(\rho\sigma)] = [x, \rho\sigma][x, \sigma\rho]^{\rho\sigma} = L(x_\lambda)R(x_\mu)^{\rho\sigma} = L(x_\lambda)P(x_\mu)^{-1}.$$

Similarly, computing $[x, \sigma]$ as $[x, \sigma(\sigma\rho)]$ and as $[x, (\rho\sigma)\sigma]$ we find

$$[x, \rho] = L(x_\lambda)P(x_\mu)^{-1} = R(x_\mu)L(x_\pi)^{-1} = P(x_\pi)R(x_\lambda)^{-1}. \tag{25}$$

Therefore if $H = G_M(\langle x_\pi, x_\mu \rangle)$, then the proposition holds.

One can give a good description of ρ^{-G} in the case where $C(M) = 1$ and $LO^3(M) = M$.

PROPOSITION 6. *If* $M = LO^3(M)$ *and* $C(M) = 1$, *then the map*: $(\rho^{-1})^x \mapsto (x_\pi, x_\mu, x_\lambda)$ *is a one-to-one correspondence of* ρ^{-G} *with the collection of equations. The permutation representation of* G *on equations corresponds to the action of* G *by conjugation on* ρ^{-G} *and conjugation by* ρ *corresponds to the action of* $r \in \mathrm{Aut}(M \times M \times M)$.

Proof. As in the proof of Corollary 1 to Proposition 4, the permutation representation of G on equations is equivalent to the representation of G on conjugates of ρ^{-1}. Making $(\rho^{-1})^x$ correspond with $(x_\pi, x_\mu, x_\lambda)$ make $(\rho^{-1})^{xg}$ correspond with $(x_\pi, x_\mu, x_\lambda)$. Furthermore, $(\rho^{-1})^{x\rho} = (\rho^{-1})^{\rho^{-1}x\rho}$ and so $P(x_\pi^\rho) = [x^\rho, \sigma] = [x, \sigma\rho]^\rho = P(x_\mu)$.

$$R(x_\mu^\rho) = R(x_\lambda) \quad \text{and} \quad L(x_\lambda^\rho) = L(x_\pi).$$

Therefore, $(x_\pi, x_\mu, x_\lambda)\rho = (x_\mu, x_\lambda, x_\pi)$. But every equation (a, b, c) has the form

$$(x_\pi, x_\mu, x_\lambda)$$

for some x, thus ρ may be identified with r.

As in (9), if x is an element of G of order 3 and P is a Sylow 3-subgroup of G containing x, we shall say x satisfies the unique conjugacy condition if x is not G-conjugate to any other element of P. In this context, there is an old question of Glauberman which we state as a conjecture. Let $O_{3'}(G)$ be the unique maximal normal 3′-subgroup of G.

Conjecture 3. If x satisfies the unique conjugacy condition then $x \in Z(G/O_{3'}(G))$.

Shult's paper (9) gives some special cases in which this is known to hold.

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press

Now, one would like to show that there are no 3′ non-associative, simple Moufang loops. If the conjecture above could be shown even if only in our special case, then the next theorem would show that $\mathrm{Gr}(M)$ would be a simple 3′-group, hence a Suzuki group. But Suzuki groups do not admit the requisite automorphism, so there would be no 3′ non-associative, simple Moufang loops.

THEOREM 3. *Let M be a finite, simple, non-associative Moufang loop with $(|M|,3) = 1$, and let $G = \mathrm{Gr}(M)$. Then ρ^{-G} is in one-to-one correspondence with triples $(a, b, c) \in M \times M \times M$ such that $abc = 1$. If $\rho_1 \in \rho^{-G}$, $\langle \rho_1, \rho \rangle$ is contained in a semidirect product $\langle \rho \rangle H$, where $(|H|, 3) = 1$. H is a group with triality under the action of D and $M(H) = N$ is a group. ρ satisfies the unique conjugacy condition in $\langle \rho \rangle^G$.*

Proof. By Lemma 4, M has no elements of order 3, so by Lemma 2, $C(M) = 1$. Clearly, $LO^3(M) = M$. If $\rho_1 \in \rho^{-G}$ then $\langle \rho, \rho_1 \rangle \subseteq \langle \rho \rangle H$ where H is D-invariant. H is a group with triality and $N = M(H)$ is associative. Thus $H/C_H(DH)$ is a 3′-group. By Corollary 4 to Theorem 2, $C_H(DH) \subseteq H'$ so $3 \nmid |C_H(DH)|$, since the Schur multiplier of a finite group is divisible only by primes which divide the group order. H is a 3′-group so $\langle \rho \rangle$ is a Sylow 3-subgroup of $\langle \rho, \rho_1 \rangle$. Therefore, ρ does not centralize ρ_1 and $\langle \rho \rangle$ is conjugate to ρ_1 in $\langle \rho, \rho_1 \rangle$. In the language of (3), $\{\langle \rho \rangle^g : g \in G\}$ is a locally conjugate collection of subgroups.

Now let T be a Sylow 3-subgroup of $\langle \rho \rangle G$ and let $\mathscr{T} = T \cap \rho^{\langle \rho \rangle G}$. Suppose $\mathscr{T}$ is the union of n orbits $T_1, \ldots, T_n$ under T. Suppose $\rho \in T_1$. Then $\{\rho\} = T_1$, since otherwise ρ centralizes some other element in T_1 since $|T_1|$ is a power of 3. Since $\{\rho\} = T_1, \rho \in \mathbb{Z}(T)$ so $n = 1$ and ρ satisfies the unique conjugacy condition.

REFERENCES

(1) ALBERT, A. A. Quasigroups: I. *Trans. Amer. Math. Soc.* **54** (1943), 507–519. II. *Trans. Amer. Math. Soc.* **55** (1944), 401–419.

(2) ASCHBACHER, M. On finite groups generated by odd transpositions: I. *Math. Z.* **127** (1972), 45–56; II, III, IV. *J. Algebra* **26** (1973), 451–491.

(3) ASCHBACHER, M. and HALL, M., JR. Groups generated by a class of elements of order 3. *J. Algebra* **24** (1973), 591–612.

(4) BRUCK, R. H. *A survey of binary systems* (Berlin, Gottingen, Heidelberg: Springer-Verlag, 1958).

(5) DORO, S. Finite symmetric spaces. (To appear.)

(6) GLAUBERMAN, G. On loops of odd order: I. *J. Algebra* **1** (1964), 374–396; II. *J. Algebra* **8** (1968), 393–414.

(7) GLAUBERMAN, G. and WRIGHT, C. Nilpotence of finite Moufang 2-loops. *J. Algebra* **8** (1968), 415–417.

(8) PAIGE, L. J. A class of simple Moufang loops. *Proc. Amer. Math. Soc.* **7** (1956), 471–482.

(9) SHULT, E. Some analogues of the Z^*-theorem. *Proc. Amer. Math. Soc.* **17** (1966), 1186–1190.

(10) THOMPSON, J. G. Non-solvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968), 383–437.

https://doi.org/10.1017/S0305004100054669 Published online by Cambridge University Press