Turk J Math
31 (2007) , 1 – 17.

Locally finite simple Moufang loops

J.I. Hall[*]

Abstract

A Moufang loop is a binary system that satisfies a particular weak form of the associative law. Doro and Glauberman observed that there is a direct connection between simple Moufang loops and simple groups with triality. Using this correspondence, Liebeck proved that nonassociative finite simple Moufang loops arise from split octonion algebras over finite fields. We extend Liebeck's theorem to the case of locally finite simple Moufang loops.

Key Words: Moufang loop, group with triality, locally finite group

1. Introduction

A *loop* $(L, \circ)$ is a set L equipped with a binary multiplication "$\circ$" having a two-sided identity element and with left and right multiplication always a permutation of L. That is, a loop is a "not necessarily associative group." We will usually write ax in place of $a \circ x$ and so forth.

A *Moufang loop* (after Ruth Moufang [21]) is a loop that satifies the *Moufang property*:

$$(ax)(ya) = a((xy)a) \quad \text{for all } a, x, y \in L\,.$$

This is a weak associativity law, so the class of associative Moufang loops is exactly the class of groups. A simple loop is one for which every surjective loop homomorphism is either trivial or an isomorphism.

Our starting point is the following theorem due to Martin Liebeck [19].

2000 *AMS Mathematics Subject Classification:* 20N05, 20D06.
[*]Partial support provided by the National Science Foundation (USA)

Theorem 1.1 *A finite simple Moufang loop is either associative (and so a finite simple group) or is isomorphic to a Paige loop* $\mathrm{PSOct}(\mathbb{F})$ *for* $\mathbb{F}$ *a finite field.*

Here $\mathrm{Oct}(\mathbb{F})$ is the algebra of split octonions over the field $\mathbb{F}$. The units of $\mathrm{Oct}(\mathbb{F})$ form a Moufang loop, and $\mathrm{SOct}(\mathbb{F})$ is the subloop consisting of those octonions of norm 1. The loop $\mathrm{PSOct}(\mathbb{F})$ then results from factoring out the normal subloop $\{\pm 1\}$ of $\mathrm{SOct}(\mathbb{F})$ and is a simple Moufang loop, as first noted by Paige [24].

An algebraic system is *locally finite* if the subsystem generated by any finite subset is itself finite. The main result of this paper is the direct extension of Liebeck's theorem to include locally finite simple Moufang loops.

Theorem 1.2 *A locally finite simple Moufang loop is either associative (and so a locally finite simple group) or is isomorphic to a Paige loop* $\mathrm{PSOct}(\mathbb{F})$ *for* $\mathbb{F}$ *a locally finite field.*

A locally finite field is isomorphic to a subfield of the algebraic closure $\overline{\mathbb{F}}_p$, for some prime p, and so is countable. The octonions $\mathrm{Oct}(\mathbb{F})$ are an eight dimensional algebra over $\mathbb{F}$, so the theorem gives us immediately a surprising corollary.

Corollary 1.3 *An uncountable locally finite simple Moufang loop is associative and so is a locally finite simple group.*

Our general references for group theory are Aschbacher [1] and Robinson [27]; for loop theory Bruck [5] and Pflugfelder [26]; and for the octonions Springer and Veldkamp [28].

2. Moufang loops

Over the field $\mathbb{F}$ a nondegenerate 8-dimensional split composition algebra [28, Chap.1] is uniquely determined up to isomorphism as the $\mathbb{F}$-algebra of split octonions $\mathrm{Oct}(\mathbb{F})$. These can be conveniently written as Zorn's vector matrices

$$m = \begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix}$$

with $a, d \in \mathbb{F}$ and $\vec{b}, \vec{c} \in \mathbb{F}^3$. Multiplication is given by

$$\begin{bmatrix} a & \vec{b} \\ \vec{c} & d \end{bmatrix} \begin{bmatrix} x & \vec{y} \\ \vec{z} & w \end{bmatrix} = \begin{bmatrix} ax + \vec{b} \cdot \vec{z} & a\vec{y} + w\vec{b} - \vec{c} \times \vec{z} \\ x\vec{c} + d\vec{z} + \vec{b} \times \vec{y} & \vec{c} \cdot \vec{y} + dw \end{bmatrix}$$

using the standard dot and cross products of 3-vectors. The associated quadratic form, which admits composition, is the norm (or determinant) $\delta(m) = ad - \vec{b} \cdot \vec{c}$.

In $\mathrm{Oct}(\mathbb{F})$ an element m is invertible if and only if $\delta(m) \neq 0$, and the loop of units $\mathrm{GOct}(\mathbb{F})$ is a Moufang loop. This possesses a normal subloop $\mathrm{SOct}(\mathbb{F})$ consisting of all units with norm 1. The scalars $\{\pm 1\}$ of $\mathrm{SOct}(\mathbb{F})$ form a normal subloop $\{\pm I\}$, and the *Paige loop* is the quotient $\mathrm{PSOct}(\mathbb{F}) = \mathrm{SOct}(\mathbb{F})/\{\pm I\}$.

The two loops $(L, \circ)$ and $(O, \diamond)$ are *isotopic* provided there are bijections α, β, and γ from L to O with

$$x \circ y = z \iff x^{\alpha} \diamond y^{\beta} = z^{\gamma} \, .$$

They are isomorphic if it is additionally possible to choose $\alpha = \beta = \gamma$ taking 1_L to 1_O. It is well-known that isotopic groups are isomorphic ([5, (i), p.57], [26, Corollary III.2.3]), but this is not in general true for loops and even Moufang loops. Nevertheless

Proposition 2.1 $\mathrm{PSOct}(F)$ *is a simple Moufang loop and is isomorphic to all its loop isotopes.*

Proof. Paige [24, Theorem 4.1] proved simplicity. Every Paige loop contains elements of order 2, for instance that represented by

$$\begin{bmatrix} 0 & (1,0,0) \\ (-1,0,0) & 0 \end{bmatrix} .$$

Therefore $\mathrm{PSOct}(F)$ is isomorphic to all its loop isotopes by [26, IV.4.8]. $\square$

3. Groups with triality

Let D be a conjugacy class of involutions (that is, elements of order 2) in the group $G = \langle D \rangle$; and let $\pi \colon G \longrightarrow \mathrm{Sym}(3)$, the symmetric group on $\{1, 2, 3\}$, be a homomorphism in which $\pi(D)$ is the transposition (that is, 2-cycle) class of $\mathrm{Sym}(3)$. Further assume that, for all $t, r \in D$, if $\pi(t) \neq \pi(r)$, then $|tr| = 3$. Then we say that (G, D, π) is a *group with triality* or *triality group*. (We may abuse this by calling G itself a triality group when D and π are evident.) A subgroup $T = \langle T \cap D \rangle \simeq \mathrm{Sym}(3)$ with $\pi(T) = \mathrm{Sym}(3)$ is a *complementing subgroup* in G. A G-conjugate of a complementing subgroup is also complementing. If T is a complementing subgroup, then D is the G-class containing the transpositions of T and π factors through the isomorphism of T with $\mathrm{Sym}(3)$.

The motivating example (and the source of the name) is Cartan's triality group $G = \mathrm{P}\Omega_8^+(\mathbb{F})\colon \mathrm{Sym}(3)$ with D the class of G containing the symmetries of $\mathrm{PO}_8^+(\mathbb{F})$ and π the map $G \longrightarrow G/G'' \simeq \mathrm{Sym}(3)$. A more elementary example is $G = \mathrm{Sym}(4)$ with D the class of transpositions and $\ker\pi = \langle(1,2)(3,4),(1,3)(2,4)\rangle$.

The study of abstract groups with triality was initiated by Doro [7] following Glauberman [9]. Doro's formulation was different but essentially equivalent to that given here, which follows [12, 13, 14]. In particular, if (G, D, π) is a group with triality in the present sense, then Doro's corresponding "group with triality" would be a pair $(\ker\pi, T)$ where T is some complementing subgroup in G.

For a general group with triality (G, D, π), each of G, D, and π need not determine the other two uniquely. Of particular interest here will be a certain strong type of uniqueness. Let T be a complementing subgroup in G, whence G is the split extension $\ker\pi \rtimes T$. Suppose that $\ker\pi$ admits an action of $T_0 \simeq \mathrm{Sym}(3)$ for which T_0 is a complementing subgroup in the group with triality $G_0 = \ker\pi \rtimes T_0$. We say that the conjugacy class of complementing subgroups is uniquely determined by $\ker\pi$ if, in this case, there is always an isomorphism of G with G_0 that takes $\ker\pi$ to itself and T to T_0.

The group with triality (G, D, π) is *triality-simple* if $\ker\pi$ is nontrivial and a minimal normal subgroup of G. That is, if $\ker\pi$ is T-simple for any complementing subgroup T of G.

Lemma 3.1 *Let S be a nonabelian simple group. Then $S \wr \mathrm{Sym}(3)$ is a group with triality with $\ker\pi$ the base group $S_1 \times S_2 \times S_3$ and D the class containing the tranpositions of $\mathrm{Sym}(3)$. For distinct $a, b \in \{1,2,3\}$*

$$(a,b)^{\ker\pi} = \{\, h_a h_b^{-1}(a,b) \mid h \in S \,\}$$

hence

$$[\ker\pi, (a,b)] = S_a \times S_b\,.$$

$S \wr \mathrm{Sym}(3)$ is triality-simple, and its class of complementing subgroups $\mathrm{Sym}(3)$ is uniquely determined by $\ker\pi = S_1 \times S_2 \times S_3$.

Proof. For nonabelian simple S the wreath product

$$S \wr \mathrm{Sym}(3) = (S_1 \times S_2 \times S_3) \rtimes \mathrm{Sym}(3)$$

has base group $S_1 \times S_2 \times S_3$ with automorphism group

$$\mathrm{Aut}(S) \wr \mathrm{Sym}(3) = (\mathrm{Aut}(S_1) \times \mathrm{Aut}(S_2) \times \mathrm{Aut}(S_3)) \rtimes \mathrm{Sym}(3)\,.$$

In any wreath product $H \wr \mathrm{Sym}(3) = (H_1 \times H_2 \times H_3) \rtimes \mathrm{Sym}(3)$ the involutions of the coset $(H_1 \times H_2 \times H_3)(a,b)$ are exactly the elements $h_a h_b^{-1} k_c(a,b)$ with h arbitrary in H and $k \in H$ arbitrary subject to $k^2 = 1$.

Let $r = h_1 h_2^{-1} k_3(1,2)$ and $t = m_1 n_2 n_3^{-1}(2,3)$ be involutions of $\mathrm{Aut}(S) \wr \mathrm{Sym}(3)$. The element rt has order 3 if and only if $rtr = trt$ if and only if $k = m$ and $[k, nh] = 1$ in $\mathrm{Aut}(S)$. Suppose that $\langle r,t\rangle \simeq \mathrm{Sym}(3)$ is a complementing subgroup within the group with triality $(S_1 \times S_2 \times S_3) \rtimes \langle r,t\rangle$. The calculation of $|rt^{s_1}| = 3$ then reveals that $k = m^s$ for every $s \in S$. This is true precisely when $k = m = 1$ (in which case $[k,nh] = 1$ is immediate). But now $\langle r,t\rangle$ is conjugate to $\langle (1,2),(2,3)\rangle$ by $h_1^{-1} n_3^{-1} \in \mathrm{Aut}(S_1) \times \mathrm{Aut}(S_2) \times \mathrm{Aut}(S_3) \leq \mathrm{Aut}(\ker \pi)$. □

Remark 3.2 (1) *For p prime, the transpositions of $Z_p \wr \mathrm{Sym}(3)$ generate a subgroup $Z_p^2 \rtimes \mathrm{Sym}(3)$ of index p that is a group with triality (as the calculations of the previous proof reveal). This group is triality-simple except when $p = 3$ where there is a central subgroup of order 3. Also for $p \neq 3$ there is a unique class of subgroups complementing the base Z_p^2 in $Z_p^2 \rtimes \mathrm{Sym}(3)$ (by Sylow's Theorem), while for $p = 3$ there are three such classes, all conjugate within the normalizer of the base subgroup in $\mathrm{Aut}(Z_3^2 \rtimes \mathrm{Sym}(3))$. (The base subgroup Z_3^2 is not characteristic in $Z_3^2 \rtimes \mathrm{Sym}(3)$.)*

(2) *If the triality-simple group (G, D, π) is solvable, then the T-simple subgroup $\ker \pi$ must be an elementary abelian p-group, for some prime p. It is an easy exercise to prove that when $p \neq 3$ we have the above subgroup $(Z_p \times Z_p) \rtimes \mathrm{Sym}(3)$ of $Z_p \wr \mathrm{Sym}(3)$. When $p = 3$ we have its central quotient $Z_3 \rtimes \mathrm{Sym}(3) = Z_3^2 \rtimes Z_2$, an element of order 2 inverting an elementary abelian group of order 9.*

Lemma 3.3 (Doro [7], Nagy and Valsecchi [22]) *Let (G, D, π) be a nonsolvable triality-simple group. Then one of:*

(a) $G \simeq S \wr \mathrm{Sym}(3)$ for a nonabelian simple group S;

(b) $\ker \pi$ is a nonabelian simple group. □

Doro assumed G to be finite, but he used this assumption only in showing that $\ker \pi$ cannot be a direct product of two isomorphic nonabelian simple groups. Nagy and

Valsecchi showed that finiteness was not necessary to rule out this possibility. All these arguments were elementary. In contrast, Liebeck used the classification of finite simple groups to prove:

Theorem 3.4 (Liebeck [19]) *Let (G, D, π) be finite triality-simple group with $\ker\pi$ nonabelian and simple. Then $G \simeq \mathrm{P}\Omega_8^+(\mathbb{F})\colon \mathrm{Sym}(3)$ for a finite field $\mathbb{F}$. The class of complementing subgroups is uniquely determined by $\ker\pi \simeq \mathrm{P}\Omega_8^+(\mathbb{F})$.*

Proof. This first part is [19, Proposition] while uniqueness is [19, Theorem 4.1]. □

4. Moufang loops and groups with triality

Doro [7], motivated by work of Glauberman [9], showed that Moufang loops and groups with triality are essentially the same thing.

Definition 4.1 *For a loop L, the group $\mathrm{U}(L)$ has the following presentation:*

Generators:
$\langle\!\langle k\,;\,a\,,b\rangle\!\rangle$ *for arbitrary $k \in L$ and distinct $a, b \in \{1,2,3\}$;*

Relations:
for arbitrary $k, h \in L$ and distinct $a, b, c \in \{1,2,3\}$:
(1) $\langle\!\langle k\,;\,a\,,b\rangle\!\rangle^2 = 1$;
(2) $\langle\!\langle k\,;\,a\,,b\rangle\!\rangle = \langle\!\langle k^{-1}\,;\,b\,,a\rangle\!\rangle$;
(3) $\langle\!\langle k\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle h\,;\,b\,,c\rangle\!\rangle} = \langle\!\langle kh\,;\,a\,,c\rangle\!\rangle$.

Lemma 4.2 *In $\mathrm{U}(L)$ we have always $\langle\!\langle k\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle h\,;\,a\,,b\rangle\!\rangle} = \langle\!\langle h(k^{-1}h)\,;\,a\,,b\rangle\!\rangle$.*

Proof.

$$\begin{aligned}
\langle\!\langle k\,;\,a\,,b\rangle\!\rangle^{\langle\!\langle h\,;\,a\,,b\rangle\!\rangle} &= \langle\!\langle k^{-1}\,;\,b\,,a\rangle\!\rangle^{\langle\!\langle h\,;\,a\,,b\rangle\!\rangle} \\
&= \left(\langle\!\langle k^{-1}\,;\,c\,,a\rangle\!\rangle\langle\!\langle 1\,;\,b\,,c\rangle\!\rangle\langle\!\langle k^{-1}\,;\,c\,,a\rangle\!\rangle\right)^{\langle\!\langle h\,;\,a\,,b\rangle\!\rangle} \\
&= \langle\!\langle k^{-1}\,;\,c\,,a\rangle\!\rangle^{\langle\!\langle h;\,a\,,b\rangle\!\rangle}\langle\!\langle 1\,;\,c\,,b\rangle\!\rangle^{\langle\!\langle h^{-1}\,;\,b\,,a\rangle\!\rangle}\langle\!\langle k^{-1}\,;\,c\,,a\rangle\!\rangle^{\langle\!\langle h;\,a,b\rangle\!\rangle} \\
&= \langle\!\langle k^{-1}h\,;\,c\,,b\rangle\!\rangle\langle\!\langle h^{-1}\,;\,c\,,a\rangle\!\rangle\langle\!\langle k^{-1}h\,;\,c\,,b\rangle\!\rangle \\
&= \langle\!\langle k^{-1}h\,;\,c\,,b\rangle\!\rangle\langle\!\langle h\,;\,a\,,c\rangle\!\rangle\langle\!\langle k^{-1}h\,;\,c\,,b\rangle\!\rangle \\
&= \langle\!\langle h(k^{-1}h)\,;\,a\,,b\rangle\!\rangle\,.
\end{aligned}$$

□

We say that $\mathrm{U}(L)$ is *faithful* on L if

$$k \mapsto \langle\!\langle k\,;\,a\,,b \rangle\!\rangle$$

is a bijection of L with $\{\,\langle\!\langle k\,;\,a\,,b \rangle\!\rangle \mid k \in L\,\}$ for each fixed 2-subset $\{a,b\}$ of $\{1,2,3\}$.

Theorem 4.3 (1) *The group* $\mathrm{U}(L)$ *is a group with triality with respect to the conjugacy class* $\mathrm{D}(L) = \{\,\langle\!\langle k\,;\,a\,,b \rangle\!\rangle \mid k \in L,\, a,b \in \{1,2,3\}\,\}$ *and the homomorphism* π_L *determined by* $\pi_L(\langle\!\langle k\,;\,a\,,b \rangle\!\rangle) = (a,b) \in \mathrm{Sym}(3)$. *It is faithful on* L *if and only if* L *has the Moufang property.*

(2) *Let* (G,D,π) *be a group with triality. Then there is a Moufang loop* $L = \mathrm{L}(G,D,\pi)$ *(unique up to isotopy) and a central subgroup* Z *of* $\mathrm{U}(L)$ *with* $G \simeq \mathrm{U}(L)/Z$. *Here the class* D *is the bijective image of the class* $\mathrm{D}(L)$ *and the map* π_L *factors through* π.

Proof. See [12, Theorem 4.1] and [13, Theorem 4.5]. □

As a direct consequence of this:

Corollary 4.4 *If* $(G,D,\pi) \longrightarrow (G^0,D^0,\pi^0)$ *is a homomorphism of groups with triality (in that the image of* D *is within* D^0 *and* π *factors through* π^0*), then there is a corresponding natural loop homomorphism* $\mathrm{L}(G,D,\pi) \longrightarrow \mathrm{L}(G^0,D^0,\pi^0)$.

Conversely if $L \longrightarrow K$ *is a loop homomorphism, then there is a canonically induced homomorphism of groups with triality* $(\mathrm{U}(L),\mathrm{D}(L),\pi_L) \longrightarrow (\mathrm{U}(K),\mathrm{D}(K),\pi_K)$. □

In particular

Corollary 4.5 *The Moufang loop* L *is simple if and only if the group* $\mathrm{U}(L)/Z(\mathrm{U}(L))$ *is triality-simple.* □

Doro also, starting from a Moufang loop L, defined via presentation a universal group with triality $\mathrm{G}(L)$ and noted its "functoriality" as in Corollary 4.4. It is easy to see that his $\mathrm{G}(L)$ is our $\ker \pi_L$, with the presentation for $\mathrm{U}(L)$ leading naturally to the Doro presentation for its subgroup $\ker \pi_L$ via the usual Reidermeister-Schreier methodology [27, 6.1.8]. Therefore the previous corollary is a restatement of Doro's [7, Cor.2.2].

Similarly, Doro's [7, Proposition 1] essentially contains

Proposition 4.6 (1) *For S a nonabelian simple group,* $\mathrm{U}(S)/Z(\mathrm{U}(S)) \simeq S \wr \mathrm{Sym}(3)$*.*

(2) *For p prime, the group* $\mathrm{U}(Z_p)/Z(\mathrm{U}(Z_p))$ *is* $Z_p^2 \rtimes \mathrm{Sym}(3)$ *when $p \neq 3$ and* $Z_3 \rtimes \mathrm{Sym}(3)$ *when $p = 3$.*

Proof. By Lemma 3.1 the map $\langle\!\langle h\,;\,a\,,b\rangle\!\rangle \mapsto h_a h_b^{-1}(a,b)$ is a bijection from $\mathrm{D}(S)$ that extends to a homomorphism $\eta\colon\ \mathrm{U}(S) \longrightarrow S \wr \mathrm{Sym}(3)$ with central kernel as in Theorem 4.3 and Corollary 4.4.

If S is nonabelian, then S^3 is is generated by the image of $\mathrm{D}(S)$; so η is surjective and its kernel is exactly $Z(\mathrm{U}(S))$.

If $S \simeq Z_p$ then the image of η is the transposition generated subgroup $Z_p^2 \rtimes \mathrm{Sym}(3)$ of the wreath product $Z_p \wr \mathrm{Sym}(3)$, as discussed in Remark 3.2. This has trivial center except for $p = 3$ where its center has order 3. $\square$

Theorem 4.7 *Let L be a simple Moufang loop for which* $\mathrm{U}(L)/Z(\mathrm{U}(L))$ *is either solvable or isomorphic to* $S \wr \mathrm{Sym}(3)$ *for a nonabelian simple group S. Then L is associative and isomorphic to the simple group S, where in the solvable case S is Z_p for some prime p.*

Proof. If $\mathrm{U}(L)$ is solvable, then by Remark 3.2 and Proposition 4.6 the group $\mathrm{U}(L)/Z(\mathrm{U}(L))$ is isomorphic to $\mathrm{U}(S)/Z(\mathrm{U}(S))$, where $S = Z_p$ for some prime p, via an isomorphism that respects complementing subgroup classes.

If $\mathrm{U}(L)/Z(\mathrm{U}(L)) \simeq S \wr \mathrm{Sym}(3)$ for a nonabelian simple group S, then by Proposition 4.6 we have $\mathrm{U}(L)/Z(\mathrm{U}(L)) \simeq \mathrm{U}(S)/Z(\mathrm{U}(S))$; and the isomorphism respects the classes of complementing subgroups by Lemma 3.1.

In both cases by Theorem 4.3 the loop L is isotopic to the group S. Therefore by [5, (i), p.57] or [26, Corollary III.2.3], the loop L is in fact isomorphic to the group S and, in particular, is associative. $\square$

Proposition 4.8 $\mathrm{U}(\mathrm{PSOct}(\mathbb{F}))/Z(\mathrm{U}(\mathrm{PSOct}(\mathbb{F}))) \simeq \mathrm{P}\Omega_8^+(\mathbb{F})\colon \mathrm{Sym}(3)$.

Proof. Versions of this are well-known; see [23, 30]. We sketch a proof. By Lemma 3.3, Corollary 4.5, and Theorem 4.7 the group $K = \ker \pi_{\mathrm{PSOct}(\mathbb{F})}/Z(\mathrm{U}(\mathrm{PSOct}(\mathbb{F})))$ is simple. In particular K is faithful in its permutation action on $\{\, \langle\!\langle m\,;\,a\,,b\rangle\!\rangle \mid m \in \mathrm{PSOct}(\mathbb{F}) \,\}$ for fixed a, b. We must identify K as $\mathrm{P}\Omega_8^+(\mathbb{F})$.

Consider the Moufang loop $\mathrm{PGOct}(\mathbb{F})$ of units in the octonions $\mathrm{Oct}(\mathbb{F})$ modulo scalars. As a consequence of Lemma 4.2, the involution $\langle\!\langle k\,;\,a\,,b\rangle\!\rangle$ has the same action on $X = \{ \langle\!\langle m\,;\, a\,, b \rangle\!\rangle \mid m \in \mathrm{PGOct}(\mathbb{F}) \}$ as the orthogonal symmetry with center k has on PGOct($\mathbb{F}$). By the Cartan-Dieudonné Theorem [6, I.5.1] $\mathrm{PO}_8^+(\mathbb{F})$ is generated by these symmetries; so $\langle X \rangle$ acts as $\mathrm{PO}_8^+(\mathbb{F})$ on X. As in Theorem 4.3 and Corollary 4.4, the embedding of PSOct($\mathbb{F}$) as a normal subloop of PGOct($\mathbb{F}$) here gives us a nontrivial homomorphism of K into $\mathrm{PO}_8^+(\mathbb{F})$ with normal image. As $\mathrm{PO}_8^+(\mathbb{F})$ has the unique minimal normal subgroup $\mathrm{P\Omega}_8^+(\mathbb{F})$, we find $K \simeq \mathrm{P\Omega}_8^+(\mathbb{F})$ as desired. □

5. Locally finite Moufang loops and groups

An algebraic object is *locally finite* if each subobject generated by a finite subset is itself finite. For example the algebraic closure $\overline{\mathbb{F}}_p$ of any finite field $\mathbb{F}_p$ is a locally finite field since any finite subset of $\overline{\mathbb{F}}_p$ lies in a extension that has finite degree over $\mathbb{F}_p$ and so is itself finite. Indeed a field is locally finite precisely when it is isomorphic to a subfield of $\overline{\mathbb{F}}_p$ for some prime p.

Proposition 5.1 *The Moufang loop L is locally finite if and only if the associated universal triality group* $\mathrm{U}(L)$ *is locally finite.*

Proof. First let L be a locally finite Moufang loop and E a finite subset of the associated group $\mathrm{U}(L)$. The group $\mathrm{U}(L)$ is generated by the various $\langle\!\langle h\,;\, a\,, b \rangle\!\rangle$ for $h \in L$ and distinct $a, b \in \{1, 2, 3\}$. Therefore there is a finite subset E_0 of L with $E \subseteq \langle\, \langle\!\langle h\,;\, a\,, b \rangle\!\rangle \mid h \in E_0,\ a, b \in \{1, 2, 3\} \,\rangle$. Let K be the finite subloop of L generated by E_0, so $E \subseteq H = \langle\, \langle\!\langle h\,;\, a\,, b \rangle\!\rangle \mid h \in K,\ a, b \in \{1, 2, 3\} \,\rangle$. By Theorem 4.3 and Corollary 4.4 the subgroup H of $\mathrm{U}(L)$ is a central quotient of $\mathrm{U}(K)$. The group $\mathrm{U}(K)/Z(\mathrm{U}(K))$ is a faithful permutation group of the conjugacy class $\mathrm{D}(K)$ of finite size $3|K|$ and so is finite. As $Z(\mathrm{U}(K)) \le \ker \pi_K \le \mathrm{U}(K)'$, this implies [27, 10.1.4] that $\mathrm{U}(K)$ and its image H are finite, as desired.

Next suppose that $\mathrm{U}(L)$ is locally finite and E a finite subset of L. Then the subgroup

$$H = \langle\, \langle\!\langle h\,;\, a\,, b \rangle\!\rangle \mid h \in E \cup \{1\},\ a, b \in \{1, 2, 3\} \,\rangle$$

of $\mathrm{U}(L)$ is finitely generated and so finite. But then it is easy to see [8, Proposition 2.6] that $K = \{ h \in L \mid \langle\!\langle h\,;\, a\,, b \rangle\!\rangle \in H \}$ is a subloop of L that contains E. The subloop K is finite as H is. □

Let T be a finite group of automorphisms of the locally finite group H. A *T-sectional cover* $\mathcal{T} = \{\,(H_i, N_i) \mid i \in I\,\}$ of H is a set of T-invariant finite subgroup pairs (H_i, N_i) with N_i normal in H_i and such that:

for each finite subgroup E of H there is an $i \in I$ with $E \leq H_i$ and $E \cap N_i = 1$.

The indexing set I then becomes a directed set $(I, \prec)$ under the partial order given by

$$i \prec j \iff H_i < H_j \text{ with } H_i \cap N_j = 1\,.$$

If I_0 is a subset of I with the property that $\mathcal{T}_0 = \{\,(H_i, N_i) \mid i \in I_0\,\}$ is itself a T-sectional cover of H, then we call $\mathcal{T}_0$ a *subcover* of $\mathcal{T}$.

Proposition 5.2 *If H is locally finite and T-simple, for finite T, then H has a T-sectional cover $\{\,(H_i, N_i) \mid i \in I\,\}$ with H_i/N_i a T-simple group for each $i \in I$.*

Proof. For $T = 1$ this is a well-known and important observation of Kegel [17]. The various proofs of Kegel's result all extend easily to the case of finite T; see [10, 17, 18, 20, 25]. □

6. Locally finite triality-simple groups

This section is devoted to a proof of:

Theorem 6.1 *Let (G, D, π) be a nonsolvable and locally finite triality-simple group. Then we have one of:*

(*a*) $G \simeq S \wr \mathrm{Sym}(3)$ *for a nonabelian locally finite simple group S;*

(*b*) $G \simeq \mathrm{P}\Omega_8^+(\mathbb{F})\colon \mathrm{Sym}(3)$ *for a locally finite field $\mathbb{F}$.*

Furthermore, in each case the class of complementing subgroups is determined uniquely by $\ker \pi$.

Throughout this section, let (G, D, π) be a nonsolvable and locally finite triality-simple group. Set $H = \ker \pi$. If G is finite, then the theorem is true by Lemmas 3.1 and 3.3 and Theorem 3.4; so we may assume that G and H are infinite.

Choose a complementing subgroup $T = \langle T \cap D \rangle \simeq \mathrm{Sym}(3)$ with $\pi(T) = \mathrm{Sym}(3)$. In particular H is T-simple, so by Proposition 5.2 there is a T-sectional cover $\mathcal{T} = \{\,(H_i, N_i) \mid i \in I\,\}$ in which every section H_i/N_i is T-simple.

Lemma 6.2 *We may assume that H_i/N_i is nonabelian for all $i \in I$.*

Proof. As G is nonsolvable, H is not abelian. Select $x, y \in H$ with $[x, y] \neq 1$. Let I_0 be the set of those $i \in I$ with $\langle x, y\rangle \leq H_i$ and $\langle x, y\rangle \cap N_i = 1$. Then $\mathcal{T}_0 = \{\, (H_i/N_i) \mid i \in I_0 \,\}$ is itself a T-sectional cover of H with nonabelian T-simple sections. We now may replace $\mathcal{T}$ with the subcover $\mathcal{T}_0$. $\square$

Lemma 6.3 *For $i \in I$ we have one of:*

(a) *$H_i/N_i \simeq S_i^3$ for a finite nonabelian simple group S_i;*

(b) *$H_i/N_i \simeq \mathrm{P}\Omega_8^+(F_i)$ for F_i a finite field of order q_i.*

Proof. As H_i and N_i are T-invariant with H_i/N_i being T-simple, the group $(H_i/N_i) \rtimes T$ is finite and triality-simple. By Lemma 3.3 and Theorem 3.4 we must have either (a) or (b). $\square$

Let $I = I_A \cup I_B$ where I_A is the set of indices with H_i/N_i as in (a) of the lemma and I_B is the set of indices with H_i/N_i as in (b) of the lemma. Then set $\mathcal{T}_A = \{\, (H_i, N_i) \mid i \in I_A \,\}$ and $\mathcal{T}_B = \{\, (H_i, N_i) \mid i \in I_B \,\}$.

Lemma 6.4 *Either $\mathcal{T}_A$ or $\mathcal{T}_B$ is a T-sectional cover of H.*

Proof. Otherwise there is a finite subgroup E_A of H not covered by any of the sections of $\mathcal{T}_A$ and a finite subgroup E_B of H not covered by any of the sections of $\mathcal{T}_B$. Then the finite subgroup $E = \langle E_A, E_B\rangle$ is not covered by any of the sections of $\mathcal{T}$, a contradiction. $\square$

Proposition 6.5 *If $\mathcal{T}_B$ is a T-sectional cover of H, then there is a locally finite field $\mathbb{F}$ with $H \simeq \mathrm{P}\Omega_8^+(\mathbb{F})$. Furthermore the class of complementing subgroups is uniquely determined by H.*

Proof. By Mal'cev's Representation Theorem [10, Theorem C.4], H has a faithful representation as a linear group. The proposition then largely comes from the **BBHST** Theorem [10, Theorem 1.2] of Belyaev [2, 3], Borovik [4], Hartley and Shute [16], and Thomas [29].

As these authors showed, under the hypothesis of the proposition there is a linearly ordered subset $(J, \prec)$ of $(I_B, \prec)$ such that

- the subcover $\mathcal{T}_J = \{ (H_j, N_j) \mid j \in J \}$ of $\mathcal{T}_B$ has $N_j = 1$, for all $j \in J$, and
- q_j divides q_k, for all $j \prec k$ of J, with $H_j \simeq \mathrm{P}\Omega_8^+(\mathbb{F}_{q_j})$ naturally embedded in $H_k \simeq \mathrm{P}\Omega_8^+(\mathbb{F}_{q_k})$.

The group H is then the ascending union $\bigcup_j H_j$ and is naturally isomorphic to $\mathrm{P}\Omega_8^+(\mathbb{F})$ for $\mathbb{F}$ the ascending union of the fields $\mathbb{F}_{q_j}$.

Let $T^{[0]}$ and $T^{[1]}$ be two subgroups Sym(3) of Aut(H) such that both groups $G^{[i]} = H \rtimes T^{[i]}$ are groups with triality with $\ker \pi^{[i]} = H$. Our work up to this point shows that each $T^{[i]}$ leaves invariant natural subgroups $\mathrm{P}\Omega_8^+(\mathbb{F}_{p^*})$ of H, where p is the characteristic of $\mathbb{F}$. By Liebeck's Theorem 3.4 both leave invariant natural subgroups $\mathrm{P}\Omega_8^+(\mathbb{F}_p)$. Since all such subgroups are conjugate in Aut(H), we may assume that the $T^{[i]}$ leave invariant the same subgroup $O \simeq \mathrm{P}\Omega_8^+(\mathbb{F}_p)$. Now Liebeck's theorem applied again shows that the $T^{[i]}$ are conjugate in $\mathrm{Aut}(O) \le \mathrm{Aut}(H)$. □

In view of the proposition, we may now assume that $\mathcal{T}_A = \{ (H_i, N_i) \mid i \in I_A \}$ is a subcover of $\mathcal{T}$.

For $i \in I_A$ and $t \in T \cap D$ with $\pi(t) = (a, b) \in \mathrm{Sym}(3)$ we define $H_i^{\{a,b\}} = [H, t]$ and then set $H_i^{\{a\}} = H_i^{\{a,b\}} \cap H_i^{\{a,c\}}$.

Lemma 6.6 (1) *For $i \prec j$ in I_A and $a \in \{1, 2, 3\}$ we have $1 \neq H_i^{\{a\}} \le H_j^{\{a\}} \trianglelefteq H_j$.*

(2) *For all $i \in I_A$ we have*

$$\langle H_i^{\{1\}}, H_i^{\{2\}}, H_i^{\{3\}} \rangle \simeq H_i^{\{1\}} \times H_i^{\{2\}} \times H_i^{\{3\}} .$$

Proof. (1) As $H_i \le H_j$, we have $H_i^{\{a,b\}} = [H_i, t] \le [H_j, t] = H_j^{\{a,b\}} \trianglelefteq H_j$. It remains to prove $1 \neq H_i^{\{a\}}$.

Set $\{a, b, c\} = \{1, 2, 3\}$. As $\langle (a, b), (b, c) \rangle = \mathrm{Sym}(3)$, we have

$$H_i^{\{a,c\}} \le [H_i, T] = H_i^{\{a,b\}} H_i^{\{b,c\}} .$$

Suppose that $1 = H_i^{\{a\}} = H_i^{\{a,b\}} \cap H_i^{\{a,c\}}$. Then by the action of T we also have

$$1 = H_i^{\{a,b\}} \cap H_i^{\{b,c\}} = H_i^{\{a,c\}} \cap H_i^{\{b,c\}} ,$$

and therefore

$$1 = [H_i^{\{a,b\}}, H_i^{\{a,c\}}] = [H_i^{\{a,b\}}, H_i^{\{b,c\}}] = [H_i^{\{a,c\}}, H_i^{\{b,c\}}]\,.$$

But then

$$H_i^{\{a,c\}} \leq [H_i, T] \cap C(H_i^{\{a,b\}} H_i^{\{b,c\}}) = Z([H_i, T])\,.$$

Similarly $H_i^{\{a,b\}} \leq Z([H_i, T])$, and so indeed $[H_i, T] = Z([H_i, T])$ is abelian. But this is not the case since by Lemma 3.1 the subgroup $[H_i, T]$ of H_i covers the nonsolvable quotient $H_i/N_i \simeq S_i^3$.

We conclude that $1 \neq H_i^{\{a,b\}} \cap H_i^{\{a,c\}} = H_i^{\{a\}}$.

(2) Choose $i \prec j$ and set

$$\bar{H}_j = H_j/N_j \simeq S_{j,1} \times S_{j,2} \times S_{j,3}$$

for S_j nonabelian simple since $j \in I_A$. As $\mathcal{T}_A$ is a sectional cover, the map $H_i \longrightarrow \bar{H}_j$ is an injection. By Lemma 3.1 we have $H_i^{\{a,b\}} = [H_i, t]$ mapped into $[\bar{H}_j, t] = S_{j,a} \times S_{j,b}$ hence $\bar{H}_i^{\{a\}} \leq S_{j,a}$. □

Lemma 6.7 *For each $a \in \{1, 2, 3\}$, set $H^{\{a\}} = \bigcup_{i \in I_A} H_i^{\{a\}}$. Then $1 \neq H^{\{a\}} \trianglelefteq H$ and $[H^{\{a\}}, H^{\{b\}}] = 1$ for $a \neq b$.*

Proof. By Lemma 6.6(1) $H^{\{a\}}$ is a nontrivial subgroup of H.

Let $g \in G$. For each $h \in H^{\{a\}}$ there is an $i \in I_A$ with $h \in H_i^{\{a\}}$. Choose $i \prec j$ with $g \in H_j$. Then by Lemma 6.6(1) we have

$$[h, g] \leq [H_i^{\{a\}}, g] \leq [H_j^{\{a\}}, g] \leq H_j^{\{a\}} \leq H^{\{a\}}\,.$$

Therefore g normalizes $H^{\{a\}}$, as desired.

For $g \in H^{\{a\}}$ and $h \in H^{\{b\}}$ (with $a \neq b$), choose $i, j \in I_A$ with $g \in H_i^{\{a\}}$ and $h \in H_j^{\{b\}}$. Next select $k \in I_A$ with $i \prec k$ and $j \prec k$. Then by Lemma 6.6

$$[g, h] \in [H_i^{\{a\}}, H_j^{\{b\}}] \leq [H_k^{\{a\}}, H_k^{\{b\}}] = 1\,.$$

We conclude that $[H^{\{a\}}, H^{\{b\}}] = 1$. □

Our proof of Theorem 6.1 is then completed by

Proposition 6.8 *If $\mathcal{T}_A$ is a T-sectional cover of H, then there is a nonabelian locally finite simple group S with $H \simeq S^3$ and $G \simeq S \wr \mathrm{Sym}(3)$. Furthermore the class of complementing subgroups T is uniquely determined by H.*

Proof. The T-simple group H is not simple by Lemma 6.7. Therefore by Lemma 3.3 we have $H \simeq S^3$ and $G \simeq S \wr \mathrm{Sym}(3)$ for a nonabelian simple group S, which must be locally finite as G and H are. By Lemma 3.1 the class of complementing subgroups such as T is uniquely determined by H. $\square$

Remark 6.9 *With only a small amount of additional effort we could have proven directly that $H = H^{\{1\}} \times H^{\{2\}} \times H^{\{3\}}$ with $H^{\{1\}} \simeq S$ locally finite and simple and that $G = H \rtimes T \simeq S \wr \mathrm{Sym}(3)$.*

7. Locally finite simple Moufang loops

We are now in a position to prove Theorem 1.2 and Corollary 1.3.

Let L be a locally finite simple Moufang loop. By Proposition 5.1 the group with triality $(\mathrm{U}(L), \mathrm{D}(L), \pi_L)$ is then locally finite, and $\mathrm{U}(L)/Z(\mathrm{U}(L))$ is triality-simple by Corollary 4.5.

Either $\mathrm{U}(L)$ is solvable or we are under Theorem 6.1(a) or (b). If either $\mathrm{U}(L)$ is solvable or, as in Theorem 6.1(a), $\mathrm{U}(L)/Z(\mathrm{U}(L)) \simeq S \wr \mathrm{Sym}(3)$ for a nonabelian locally finite simple group S, then L is associative by Theorem 4.7.

Under Theorem 6.1(b) $\mathrm{U}(L)/Z(\mathrm{U}(L)) \simeq \mathrm{P}\Omega_8^+(\mathbb{F}) \colon \mathrm{Sym}(3)$ for a locally finite field $\mathbb{F}$, and furthermore the class of complementing subgroups is uniquely determined by the kernel $\mathrm{P}\Omega_8^+(\mathbb{F})$. By Proposition 4.8 we have

$$\mathrm{U}(L)/Z(\mathrm{U}(L)) \simeq \mathrm{U}(\mathrm{PSOct}(\mathbb{F}))/Z(\mathrm{U}(\mathrm{PSOct}(\mathbb{F})))$$

with the isomorphism respecting the classes of complementing subgroups. Therefore by Theorem 4.3 the loops L and $\mathrm{PSOct}(\mathbb{F})$ are isotopic, and so by Proposition 2.1 the loop L is in fact isomorphic to the Paige loop $\mathrm{PSOct}(\mathbb{F})$.

This completes the proof of Theorem 1.2.

All locally finite fields are countable as they are subfields of some algebraic closure $\overline{\mathbb{F}}_p$, a countable field; and a finite dimensional algebra over a countable field is countable. Therefore over the locally finite field $\mathbb{F}$ the octonions $\mathrm{Oct}(\mathbb{F})$ and the associated Paige loop $\mathrm{PSOct}(\mathbb{F})$ are countable. Corollary 1.3 is thus an immediate consequence of Theorem 1.2.

References

[1] M. Aschbacher, "Finite Group Theory," Second edition, Cambridge Studies in Advanced Mathematics, **10**, Cambridge University Press, Cambridge, 2000.

[2] V.V. Belyaev, Locally finite Chevalley groups, in: "Studies in Group Theory," Urals Scientific Centre of the Academy of Sciences of USSR, Sverdlovsk, 1984, 39–50 (in Russian).

[3] V.V. Belyaev, Semisimple periodic groups of finitary transformations, Algebra i Logika, **32** (1993), 17–33 (English translation 8–16).

[4] A.V. Borovik, Periodic linear groups of odd characteristic, Dokl. Akad. Nauk. SSSR, **266** (1982), 1289–1291.

[5] R.H. Bruck, "A Survey of Binary Systems," Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[6] C. Chevalley, "The Algebraic Theory of Spinors and Clifford Algebras, Collected Works, Volume 2," eds.: P. Cartier, C. Chevalley, Springer-Verlag, 1997.

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

[8] S.M. Gagola III and J.I. Hall, Lagrange's theorem for Moufang loops, Acta Sci. Math. (Szeged), **71** (2005), 45–64.

[9] G. Glauberman, On loops of odd order, II, J. Algebra, **8** (1968), 393–414.

[10] J.I. Hall, Locally finite simple groups of finitary linear transformations, in: "Finite and Locally Finite Groups (Istanbul, 1994)," eds.: B. Hartley, G.M. Seitz, A.V. Borovik, and R.M. Bryant, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., **471**, Kluwer Acad. Publ., Dordrecht, 1995, 147–188.

[11] J.I. Hall, Periodic simple groups of finitary linear transformations, Ann. of Math. (2), **163** (2006), 445–498.

[12] J.I. Hall, A characterization of the full wreath product, J. Algebra, **300** (2006), 529–554.

[13] J.I. Hall, Central automorphisms of Latin squares and loops, Quasigroups Related Systems, **15** (2007), 19–46.

[14] J.I. Hall and G.P. Nagy, On Moufang 3-nets and groups with triality, Acta Sci. Math. (Szeged), **67** (2001), 675–685.

[15] B. Hartley, Simple locally finite groups, in: "Finite and Locally Finite Groups (Istanbul, 1994)," eds. B. Hartley, G.M. Seitz, A.V. Borovik, R.M. Bryant, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., **471**, Kluwer Acad. Publ., Dordrecht, 1995, 1–44.

[16] B. Hartley and G. Shute, Monomorphisms and direct limits of finite groups of Lie type, Quart. J. Math. (Ser. 2), **35** (1984), 49–71.

[17] O.H. Kegel, Über einfache, lokal endliche Gruppen, Math. Z., **95** (1967), 169–195.

[18] O.H. Kegel and B.A.F. Wehrfritz, "Locally Finite Groups," North Holland, Amsterdam, 1973.

[19] M.W. Liebeck, The classification of finite simple Moufang loops, Math. Proc. Cambridge Philos. Soc., **102** (1987), 33–47.

[20] U. Meierfrankenfeld, Non-finitary simple locally finite groups, in: "Finite and Locally Finite Groups (Istanbul, 1994)," eds. B. Hartley, G.M. Seitz, A.V. Borovik, R.M. Bryant, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., **471**, Kluwer Acad. Publ., Dordrecht, 1995, 189–212.

[21] R. Moufang, Zur Struktur von Alternativkörpern, Math. Ann., **110** (1935), 416–430.

[22] G.P. Nagy and M. Valsecchi, Splitting automorphisms and Moufang loops, Glasg. Math. J., **46** (2004), 305–310.

[23] G.P. Nagy and P. Vojtěchovský, Octonions, simple Moufang loops and triality, Quasigroups Related Systems, **10** (2003), 65–94.

[24] L.J. Paige, A class of simple Moufang loops, Proc. Amer. Math. Soc., **7** (1956), 471–482.

[25] R.E. Phillips, On absolutely simple locally finite groups, Rend. Sem. Mat. Univ. Padova, **79** (1988), 213–220.

[26] H.O. Pflugfelder, "Quasigroups and Loops: Introduction," Sigma Series in Pure Mathematics, **7**, Heldermann Verlag, Berlin, 1990.

[27] D.J.S. Robinson, "A Course in the Theory of Groups," Graduate Texts in Mathematics, **80**, Springer-Verlag, New York-Berlin, 1982.

[28] T.A. Springer and F.D. Veldkamp, "Octonions, Jordan Algebras and Exceptional Groups," Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[29] S. Thomas, The classification of the simple periodic linear groups, Arch. Math., **41** (1983), 103–116.

[30] J. Tits, Sur la trialité et les algèbres d'octaves, Acad. Roy. Belg. Bull. Cl. Sci., **44** (1958), 332–350.

Jonathan I. HALL
Department of Mathematics
Michigan State University
East Lansing, MI 48824 USA
e-mail:jhall@math.msu.edu

Received 04.10.2007