Quasigroups and Related Systems **10** (2003), xx – yy

Octonions, simple Moufang loops and triality

Gábor P. Nagy and Petr Vojtěchovský

Abstract

Nonassociative finite simple Moufang loops are exactly the loops constructed by Paige from Zorn vector matrix algebras. We prove this result anew, using geometric loop theory. In order to make the paper accessible to a broader audience, we carefully discuss the connections between composition algebras, simple Moufang loops, simple Moufang 3-nets, S-simple groups and groups with triality. Related results on multiplication groups, automorphisms groups and generators of Paige loops are provided.

Contents

2000 Mathematics Subject Classification: 20N05, 20D05
Keywords: simple Moufang loop, Paige loop, octonion, composition algebra, classical group, group with triality, net
The first author was supported by the FKFP grant 0063/2001 of the Hungarian Ministry for Education and the OTKA grants nos. F042959 and T043758. The second author partially supported by the Grant Agency of Charles University, grant number 269/2001/B-MAT/MFF.

1 Introduction

The goal of this paper is to present the classification of finite simple Moufang loops in an accessible and uniform way to a broad audience of researchers in nonassociative algebra. The results are not new but the arguments often are. Although not all proofs are included, our intention was to leave out only those proofs that are standard (that is those that can be found in many sources), those that are purely group-theoretical, and those that require only basic knowledge of loop theory. We have rewritten many proofs using geometric loop theory—a more suitable setting for this kind of reasoning. To emphasize the links to other areas of loop theory and algebra, we comment on definitions and results generously, although most of the remarks we make are not essential later in the text.

Here is a brief description of the content of this paper. After reviewing some basic properties of loops, nets and composition algebras, we construct a family of simple Moufang loops from the Zorn alternative algebras. These

loops are also known as Paige loops. We then briefly discuss the multiplication groups of Paige loops, because these are essential in the classification.

With every Moufang loop we associate a Moufang 3-net, and with this 3-net we associate a group with triality. An S-homomorphism is a homomorphism between two groups with triality that preserves the respective triality automorphisms. This leads us to the concept of S-simple groups with triality, which we classify. The group with triality G associated with a simple Moufang loop L must be S-simple. Moreover, when L is nonassociative G must be simple. This is the moment when we use results of Liebeck concerning the classification of finite simple groups with triality. His work is based on the classification of finite simple groups. The fact that there are no other nonassociative finite simple Moufang loops besides finite Paige loops then follows easily.

Building on the geometric understanding we have obtained so far, we determine the automorphism groups of all Paige loops constructed over perfect fields. We conclude the paper with several results concerning the generators of finite Paige loops and integral Cayley numbers. All these results are mentioned because they point once again towards classical groups. Several problems and conjectures are pondered in the last section.

A few words concerning the notation: As is the habit among many loop theorists, we write maps to the right of their arguments, and therefore compose maps from left to right. The only exception to this rule are some traditional maps, such as the determinant det. A subloop generated by S will be denoted by $\langle S \rangle$. The symmetric group on n points is denoted by S_n.

2 Loops and nets

We now give a brief overview of definitions and results concerning loops and nets. Nets (also called webs in the literature) form the foundations of the geometric loop theory. All material covered in 2.1–2.3 can be found in [4] and [25], with proofs. We refer the reader to [25, Ch. II] and [8, Ch. VIII, X] for further study of nets.

2.1 Quasigroups and loops

Let $Q = (Q, \cdot)$ be a groupoid. Then Q is a *quasigroup* if the equation $x \cdot y = z$ has a unique solution in Q whenever two of the three elements x, y, $z \in Q$ are specified. Quasigroups are interesting in their own right, but also appear in combinatorics under the name *latin squares* (more precisely, multiplication tables of finite quasigroups are exactly latin squares),

and in universal algebra, where subvarieties of quasigroups are often used to provide an instance of some universal algebraic notion that cannot be demonstrated in groups or other rigid objects. We ought to point out that in order to define the variety of quasigroups equationally, one must introduce additional operations $\backslash$ and $/$ for left and right division, respectively.

A quasigroup Q that possesses an element e satisfying $e \cdot x = x \cdot e = x$ for every $x \in Q$ is called a *loop* with *neutral element* e. The vastness of the variety of loops dictates to focus on some subvariety, usually defined by an identity approximating the associative law. (Associative loops are exactly groups.) In this paper, we will be concerned with *Moufang loops*, which are loops satisfying any one of the three equivalent *Moufang identities*

$$((xy)x)z = x(y(xz)), \quad ((xy)z)y = x(y(zy)), \quad (xy)(zx) = (x(yz))x, \quad (1)$$

and in particular with simple Moufang loops (see below). Every element x of a Moufang loop is accompanied by its *two-sided inverse* x^{-1} satisfying $xx^{-1} = x^{-1}x = e$. Any two elements of a Moufang loop generate a subgroup, and thus $(xy)^{-1} = y^{-1}x^{-1}$.

Each element x of a loop Q gives rise to two permutations on Q, the *left translation* $L_x : y \mapsto xy$ and the *right translation* $R_x : y \mapsto yx$. The group $\operatorname{Mlt} Q$ generated by all left and right translations is known as the *multiplication group* of Q. The subloop $\operatorname{Inn} Q$ of $\operatorname{Mlt} Q$ generated by all maps $L_xL_yL_{yx}^{-1}$, $R_xR_yR_{xy}^{-1}$ and $R_xL_x^{-1}$, for x, $y \in Q$, is called the *inner mapping group* of Q. It consists of all $\varphi \in \operatorname{Mlt} Q$ such that $e\varphi = e$.

A subloop S of Q is *normal* in Q if $S\varphi = S$ for every $\varphi \in \operatorname{Inn} Q$. The loop Q is said to be *simple* if the only normal subloops of Q are Q and $\{e\}$.

In any loop Q, the *commutator* of x, $y \in Q$ is the unique element $[x, y] \in Q$ satisfying $xy = (yx)[x, y]$, and the *associator* of x, y, $z \in Q$ is the unique element $[x, y, z] \in Q$ satisfying $(xy)z = (x(yz))[x, y, z]$. We prefer to call the subloop $C(Q)$ of Q consisting of all elements x such that $[x, y] = [y, x] = e$ for every $y \in Q$ the *commutant* of Q. (Some authors use the name *centrum* or *Moufang center*.) The subloop $N(Q)$ consisting of all $x \in Q$ such that $[x, y, z] = [y, x, z] = [y, z, x] = e$ holds for every y, $z \in Q$ is known as the *nucleus* of Q. Then $Z(Q) = C(Q) \cap N(Q)$ is the *center* of Q, which is always a normal subloop of Q.

2.2 Isotopisms versus isomorphisms

Quasigroups and loops can be classified up to isomorphism or up to isotopism. When Q_1, Q_2 are quasigroups, then the triple (α, β, γ) of bijections from Q_1 onto Q_2 is an *isotopism* of Q_1 onto Q_2 if $x\alpha \cdot y\beta = (x \cdot y)\gamma$ holds

for every x, $y \in Q_1$. An isotopism with $Q_1 = Q_2$ is called an *autotopism*. Every isomorphism α gives rise to an isotopism (α, α, α). The notion of isotopism is superfluous in group theory, as any two groups that are isotopic are already isomorphic.

In terms of multiplication tables, Q_1 and Q_2 are isotopic if the multiplication table of Q_2 can be obtained from the multiplication table of Q_1 by permuting the rows (by α), the columns (by β), and by renaming the elements (by γ). Isotopisms are therefore appropriate morphisms for the study of quasigroups and loops. On the other hand, every quasigroup is isotopic to a loop, which shows that the algebraic properties of isotopic quasigroups can differ substantially. Fortunately, the classification of finite simple Moufang loops is the same no matter which kind of equivalence (isotopism or isomorphism) we use. This is because (as we shall see) there is at most one nonassociative finite simple Moufang loop of a given order, up to isomorphism.

A loop L is a *G-loop* if every loop isotopic to L is isomorphic to L. So, finite simple Moufang loops are G-loops.

2.3 Loops and 3-nets

Let $k > 2$ be an integer, $\mathcal{P}$ a set, and $\mathcal{L}_1, \ldots, \mathcal{L}_k$ disjoint sets of subsets of $\mathcal{P}$. Put $\mathcal{L} = \bigcup \mathcal{L}_i$. We call the elements of $\mathcal{P}$ and $\mathcal{L}$ *points* and *lines*, respectively, and use the common geometric terminology, such as "all lines through the point P", etc. For $\ell \in \mathcal{L}_i$, we also speak of a *line of type* i or an *i-line*. Lines of the same type are called *parallel*.

The pair $(\mathcal{P}, \mathcal{L})$ is a *k-net* if the following axioms hold:

1) Distinct lines of the same type are disjoint.

2) Two lines of different types have precisely one point in common.

3) Through any point, there is precisely one line of each type.

Upon interchanging the roles of points and lines, we obtain *dual k-nets*. In that case, the points can be partitioned into k classes so that:

1′) Distinct points of the same type are not connected by a line.

2′) Two points of different types are connected by a unique line.

3′) Every line consists of k points of pairwise different types.

There is a natural relation between loops and 3-nets. Let us first start from a loop L and put $\mathcal{P} = L \times L$. Define the line classes

$$\begin{aligned} \mathcal{L}_1 &= \{\{(x,c) \mid x \in L\} \mid c \in L\}, \\ \mathcal{L}_2 &= \{\{(c,y) \mid y \in L\} \mid c \in L\}, \\ \mathcal{L}_3 &= \{\{(x,y) \mid x,y \in L,\, xy = c\} \mid c \in L\}. \end{aligned}$$

Then, $(\mathcal{P}, \mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3)$ is a 3-net. The lines of these classes are also called *horizontal, vertical* and *transversal lines,* respectively. The point $O = (e,e)$ is the *origin* of the net.

Let us now consider a 3-net $(\mathcal{P}, \mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3)$. Let $O \in \mathcal{P}$ be an arbitrary point, and let ℓ, k be the unique horizontal and vertical lines through O, respectively. Then the construction of Figure 1 defines a loop operation on ℓ with neutral element O.

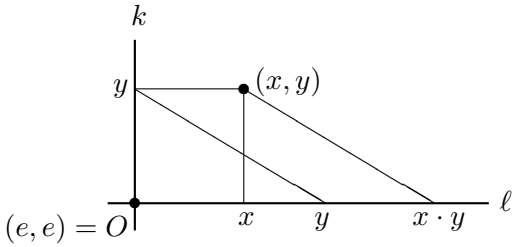

Figure 1: The geometric definition of the coordinate loop.

Since the parallel projections are bijections between lines of different type, we can index the points of k by points of ℓ, thus obtaining a bijection between $\mathcal{P}$ and $\ell \times \ell$. The three line classes are determined by the equations $X = c$, $Y = c$, $XY = c$, respectively, where c is a constant. We say that (ℓ, O) is a *coordinate loop* of the 3-net $(\mathcal{P}, \mathcal{L})$.

2.4 Collineations and autotopisms

Let $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ be a 3-net. *Collineations* are line preserving bijective maps $\mathcal{P} \to \mathcal{P}$. The group of collineations of $\mathcal{N}$ is denoted by $\mathrm{Coll}\mathcal{N}$. A collineation induces a permutation of the line classes. There is therefore a group homomorphism from $\mathrm{Coll}\mathcal{N}$ to the symmetric group S_3. The kernel of this homomorphism consists of the *direction preserving collineations.*

Let L be the coordinate loop of $\mathcal{N} = (\mathcal{P}, \mathcal{L})$ with respect to some origin $O \in \mathcal{P}$. Let $\varphi : \mathcal{P} \to \mathcal{P}$ be a bijection. Then φ preserves the line classes 1 and 2 if and only if it has the form $(x,y) \mapsto (x\alpha, y\beta)$ for some bijections $\alpha, \beta : L \to L$. Moreover, if φ preserves the line classes 1 and 2 then φ also preserves the third class if and only if there is a bijection $\gamma : L \to L$ such

that the triple (α, β, γ) is an autotopism of L. Automorphisms of L can be characterized in a similar way (see Lemma 7.2).

2.5 Bol reflections

Let $\mathcal{N}$ be a 3-net and $\ell_i \in \mathcal{L}_i$, for some i. We define a certain permutation σ_{ℓ_i} on the point set $\mathcal{P}$ (cf. Figure 2). For $P \in \mathcal{P}$, let a_j and a_k be the lines through P such that $a_j \in \mathcal{L}_j$, $a_k \in \mathcal{L}_k$, and $\{i, j, k\} = \{1, 2, 3\}$. Then there are unique intersection points $Q_j = a_j \cap \ell_i$, $Q_k = a_k \cap \ell_i$. We define $P\sigma_{\ell_i} = b_j \cap b_k$, where b_j is the unique j-line through Q_k, and b_k the unique k-line through Q_j. The permutation σ_{ℓ_i} is clearly an involution satisfying $\mathcal{L}_j\sigma_{\ell_i} = \mathcal{L}_k$, $\mathcal{L}_k\sigma_{\ell_i} = \mathcal{L}_j$. If it happens to be the case that σ_{ℓ_i} is a collineation, we call it the *Bol reflection with axis* ℓ_i.

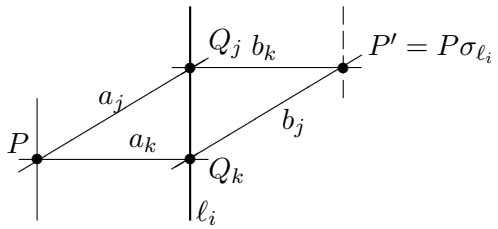

Figure 2: The Bol reflection with axis ℓ_i.

Obviously, every Bol reflection fixes a line pointwise (namely its axis) and interchanges the other two line classes. In fact, it is easy to see that any collineation with this property is a Bol reflection. Then for any $\gamma \in \mathrm{Coll}\mathcal{N}$ and $\ell \in \mathcal{L}$ we must have $\gamma^{-1}\sigma_\ell\gamma = \sigma_{\ell\gamma}$, as $\gamma^{-1}\sigma_\ell\gamma$ is a collineation fixing the line $\ell\gamma$ pointwise. In words, the set of Bol reflections of $\mathcal{N}$ is invariant under conjugations by elements of the collineation group of $\mathcal{N}$.

Let $\ell_i \in \mathcal{L}_i$, $i = 1, 2, 3$, be the lines through some point P of $\mathcal{N}$. As we have just seen, $\sigma_{\ell_1}\sigma_{\ell_2}\sigma_{\ell_1} = \sigma_{\ell_3}$, since $\ell_3\sigma_{\ell_1} = \ell_2$. Therefore $(\sigma_{\ell_1}\sigma_{\ell_2})^3 = \mathrm{id}$ and $\langle \sigma_{\ell_1}, \sigma_{\ell_2}, \sigma_{\ell_3} \rangle$ is isomorphic to S_3. This fact will be of importance later.

A 3-net $\mathcal{N}$ is called a *Moufang 3-net* if σ_ℓ is a Bol reflection for every line ℓ. The terminology is justified by Bol, who proved that $\mathcal{N}$ is a Moufang 3-net if and only if all coordinate loops of $\mathcal{N}$ are Moufang [4, p. 120].

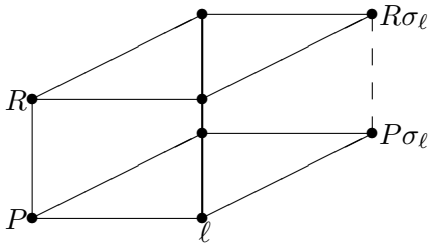

Figure 3: The 2-Bol configuration.

The configuration in Figure 3 is called the 2-*Bol configuration*. Using the other two directions of axes, we obtain 1- and 3-Bol configurations. With these configurations at hand, we see that the net $\mathcal{N}$ is Moufang if and only if all its Bol configurations close (i.e., $R\sigma_\ell$ and $P\sigma_\ell$ are collinear). See [25, Sec. II.3] for more on closures of net configurations.

3 Composition algebras

The most famous nonassociative Moufang loop is the multiplicative loop of real octonions. Recall that octonions are built up from quaternions in a way analogous to the construction of quaternions from complex numbers, or complex numbers from real numbers. Following Springer and Veldkamp [22], we will imitate this procedure over any field. We then construct a countable family of finite simple Moufang loops, one for every finite field $GF(q)$.

Let F be a field and V a vector space over F. A map $N : V \to F$ is a *quadratic form* if $\langle\ ,\ \rangle : V \times V \to F$ defined by $\langle u, v\rangle = (u+v)N - uN - vN$ is a bilinear form, and if $(\lambda u)N = \lambda^2(uN)$ holds for every $u \in V$ and $\lambda \in F$.

When $f : V \times V \to F$ is a bilinear form, then u, $v \in V$ are *orthogonal* (with respect to f) if $(u, v)f = 0$. We write $u \perp v$. The *orthogonal complement* $W^\perp$ of a subspace $W \leq V$ is the subspace $\{v \in V;\ v \perp w$ for every $w \in W\}$. The bilinear form f is said to be *non-degenerate* if $V^\perp = 0$. A quadratic form N is *non-degenerate* if the bilinear form $\langle\ ,\ \rangle$ associated with N is non-degenerate. When N is non-degenerate, the vector space V is said to be *nonsingular*. A subspace W of (V, N) is *totally isotropic* if $uN = 0$ for every $u \in W$. All maximal totally isotropic subspaces of (V, N) have the same dimension, called the *Witt index*. If N is non-degenerate and $\dim V \leq \infty$ then the Witt index cannot exceed $\dim V/2$.

In this paper, an *algebra* over F is a vector space over F with bilinear multiplication. Specifically, we do not assume that multiplication in an algebra is associative.

A *composition algebra* $C = (C, N)$ over F is an algebra with a multiplicative neutral element e such that the quadratic form $N : C \to F$ is non-degenerate and

$$(uv)N = uNvN \tag{2}$$

holds for every $u, v \in C$. In this context, the quadratic form N is called a *norm*.

When $\langle\ ,\ \rangle$ is the bilinear form associated with the norm N, the *conjugate* of $x \in C$ is the element $\overline{x} = \langle x, e\rangle e - x$. Every element $x \in C$ satisfies

$$x^2 - \langle x, e\rangle x + (xN)e = 0$$

(cf. [22, Prop. 1.2.3]), and thus also $x\overline{x} = \overline{x}x = (xN)e$. In particular, the multiplicative inverse of x is $x^{-1} = (xN)^{-1}\overline{x}$, as long as $xN \neq 0$. Furthermore, $0 \neq x \in C$ is a zero divisor if and only if $xN = 0$.

3.1 The Cayley-Dickson process

Let $C = (C, N)$ be a composition algebra over F and $\lambda \in F^* = F \setminus \{0\}$. Define a new product on $D = C \times C$ by

$$(x,\, y)(u,\, v) = (xu + \lambda\overline{v}y,\, vx + y\overline{u}),$$

where x, y, u, v are elements of C. Also define the norm M on D by

$$(x,\, y)M = xN - \lambda(yN),$$

where x, $y \in C$. By [22, Prop. 1.5.3], if C is associative then $D = (D, M)$ is a composition algebra. Moreover, D is associative if and only if C is commutative and associative. The above procedure is known as the *Cayley-Dickson process*.

We would now like to construct all composition algebras by iterating the Cayley-Dickson process starting with F. However, there is a twist when F is of characteristic 2. Namely, when $\operatorname{char} F = 2$ then F is not a composition algebra since $\langle x, x\rangle = (x + x)N - xN - xN = 0$ for every $x \in F$, thus $\langle x, y\rangle = \langle x, \lambda x\rangle = \lambda\langle x, x\rangle = 0$ for every x, $y \in F$, and N is therefore degenerate. The situation looks as follows:

Theorem 3.1 (Thm. 1.6.2. [22]). *Every composition algebra over F is obtained by iterating the Cayley-Dickson process, starting from F if* $\operatorname{char} F$ *is not equal to* 2*, and from a* 2*-dimensional composition algebra when* $\operatorname{char} F$ *is equal to* 2*. The possible dimensions of a composition algebra are* 1, 2,

4 *and* 8. *Composition algebras of dimension* 1 *or* 2 *are commutative and associative, those of dimension* 4 *are associative but not commutative, and those of dimension* 8 *are neither commutative nor associative.*

A composition algebra of dimension 2 *over* F *is either a quadratic field extension of* F *or is isomorphic to* $F \oplus F$.

For a generalization of composition algebras into dimension 16 we refer the reader to [26].

3.2 Split octonion algebras

Composition algebras of dimension 8 are known as *octonion algebras*. Since there is a parameter λ in the Cayley-Dickson process, it is conceivable (and sometimes true) that there exist two octonion algebras over F that are not isomorphic.

A composition algebra (C, N) is called *split* if there is $0 \neq x \in C$ such that $xN = 0$. By [22, Thm. 1.8.1], over any field F there is exactly one split composition algebra in dimension 2, 4 and 8, up to isomorphism. As we have already noticed, split composition algebras are precisely composition algebras with zero divisors. The unique split octonion algebra over F will be denoted by $\mathbb{O}(F)$. (It is worth mentioning that when F is finite then every octonion algebra over F is isomorphic to $\mathbb{O}(F)$, cf. [22, p. 22].)

All split octonion algebras $\mathbb{O}(F)$ were known already to Zorn, who constructed them using the *vector matrices*

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}, \tag{3}$$

where a, $b \in F$ and α, β are vectors in F^3. The norm N is given as the "determinant" $\det x = ab - \alpha \cdot \beta$, where $\alpha \cdot \beta$ is the usual dot product

$$(\alpha_1, \alpha_2, \alpha_3) \cdot (\beta_1, \beta_2, \beta_3) = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3.$$

The conjugate of x is

$$\overline{x} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}, \tag{4}$$

and two vector matrices are multiplied according to

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix}, \tag{5}$$

where $\beta \times \delta$ is the usual vector product

$$(\beta_1, \beta_2, \beta_3) \times (\delta_1, \delta_2, \delta_3) = (\beta_2\delta_3 - \beta_3\delta_2,\ \beta_3\delta_1 - \beta_1\delta_3,\ \beta_1\delta_2 - \beta_2\delta_1).$$

The reader can think of this *Zorn vector algebra* anytime we speak of $\mathbb{O}(F)$.

It turns out that every composition algebra satisfies the *alternative laws*

$$(xy)x = x(yx), \quad x(xy) = x^2y, \quad (xy)y = xy^2.$$

This is an easy corollary of the (not so easy) fact that composition algebras satisfy the Moufang identities (1), cf. [22, Prop. 1.4.1].

4 A class of classical simple Moufang loops

4.1 Paige loops

Although the octonion algebra $\mathbb{O}(F)$ satisfies the Moufang identities, it is not a Moufang loop yet, since it is not even a quasigroup ($0 \cdot x = 0$ for every $x \in \mathbb{O}(F)$). Denote by $M(F)$ the subset of $\mathbb{O}(F)$ consisting of all elements of norm (determinant) 1. We have $\det x \det y = \det xy$ since $\mathbb{O}(F)$ is a composition algebra, which means that $M(F)$ is closed under multiplication. The neutral element of $M(F)$ is

$$e = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 1 \end{pmatrix},$$

and the two-sided inverse of $x \in M(F)$ is $x^{-1} = \overline{x}$, where x is as in (3) and $\overline{x}$ is as in (4).

Let Z be the center of the Moufang loop $M(F)$. We have $Z = \{e\}$ when $\operatorname{char} F = 2$, and $Z = \{e, -e\}$ when $\operatorname{char} F \neq 2$. Denote by $M^*(F)$ the Moufang loop $M(F)/Z$.

Theorem 4.1 (Paige [23]). *Let F be a field and $M^*(F)$ the loop of Zorn vector matrices of norm one modulo the center, multiplied according to* (5)*. Then $M^*(F)$ is a nonassociative simple Moufang loop. When $F = GF(q)$ is finite, the order of $M^*(F)$ is $\frac{1}{d}q^3(q^4-1)$, where $d = (2, q-1)$.*

The noncommutative loops $M^*(F)$ of Theorem 4.1 are sometimes called *Paige loops*.

In the remaining part of this section, we investigate the multiplication groups of loops $M(F)$ and $M^*(F)$ constructed over an arbitrary field F.

4.2 Orthogonal groups

Let V be a vector space over F with a non-degenerate quadratic form $N : V \to F$. A linear transformation $f : V \to V$ is *orthogonal with respect to* N if it preserves N, i.e., if $(xf)N = xN$ for all $x \in V$. Then f preserves the associated bilinear form $\langle\ ,\ \rangle$ as well:

$$\begin{aligned}\langle xf, yf\rangle &= (xf+yf)N - (xf)N - (yf)N \\ &= (x+y)N - (x)N - (y)N \\ &= \langle x, y\rangle.\end{aligned}$$

The group consisting of all orthogonal transformations of (V, N) is known as the *orthogonal group* $O(V) = O(V, N)$. The determinant of an orthogonal transformation is ± 1. Orthogonal transformations with determinant 1 form the *special orthogonal group* $SO(V)$. The elements of $SO(V)$ are called *rotations*. One usually denotes by $\Omega(V)$ the commutator subgroup $O'(V)$ of $O(V)$. By definition, every element of $\Omega(V)$ is a rotation, and we would like to see which rotations belong to $\Omega(V)$.

Take an element $g \in SO(V)$ and consider the map $1 - g : x \mapsto x - xg$. Define the bilinear form χ_g on $V(1-g)$ by $(u, v)\chi_g = \langle u, w\rangle$, where w is an arbitrary vector from V satisfying $w(1-g) = v$. Then χ_g is well-defined and non-degenerate, by [27, Thm. 11.32]. Recall that the *discriminant* $\mathrm{discr}(f)$ of a bilinear form f with respect to some basis is the determinant of its matrix. Whether or not the discriminant of χ_g is a square in F does not depend on the choice of the basis in $V(1-g)$. This property characterizes elements of $\Omega(V)$.

Lemma 4.2 (11.50 Thm. [27]). *The rotation $g \in SO(V)$ belongs to $\Omega(V)$ if and only if* $\mathrm{discr}(\chi_g) \in F^2$.

Pick any element $\sigma \in O(V)$ with $\sigma^2 = \mathrm{id}$. The two subspaces

$$\begin{aligned}U &= V(\sigma - 1) = \{x\sigma - x \mid x \in V\}, \\ W &= V(\sigma + 1) = \{x\sigma + x \mid x \in V\}\end{aligned}$$

are orthogonal to each other. Indeed,

$$\langle x\sigma - x, y\sigma + y\rangle = \langle x\sigma, y\rangle - \langle x, y\sigma\rangle = \langle x\sigma, y\rangle - \langle x\sigma, y\sigma^2\rangle = 0.$$

The subspace W consists of vectors invariant under σ. If W is a non-singular hyperplane (that is, a subspace of dimension $\dim V - 1$) then σ is called a *symmetry with respect to* W. (If $\mathrm{char}(F) = 2$ then σ is usually called a *transvection*.) If σ is a symmetry with respect to W and $g \in O(V)$, the conjugate $\sigma^g = g^{-1}\sigma g$ is a symmetry with respect to Wg.

4.3 Multiplication groups of Paige loops

Let now $V = \mathbb{O}(F)$ be the split octonion algebra over F. We identify the vector matrix

$$x = \begin{pmatrix} x_0 & (x_1, x_2, x_3) \\ (x_4, x_5, x_6) & x_7 \end{pmatrix}$$

with the column vector $(x_0, \ldots, x_7)^t$, and we use the canonical basis of F^8 as the basis of V. Since $\langle x, y\rangle = \det(x+y) - \det x - \det y = x_7y_0 - x_4y_1 - x_5y_2 - x_6y_3 - x_1y_4 - x_2y_5 - x_3y_6 + x_0y_7$, the bilinear from $\langle x, y\rangle$ can be expressed as x^tJy, where

$$J = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{6}$$

Recall that $M(F)$ consists of all elements of $\mathbb{O}(F)$ that are of norm 1.

Lemma 4.3. *For every $a \in M(F)$, we have $L_a, R_a \in \Omega(V)$.*

Proof. We only deal with the case L_a. Since $aN = 1$, we have $L_a \in O(V)$, by (2). Let $a = (a_0, \ldots, a_7)^t$ and write matrix maps to the left of their arguments. Then L_a can be identified with

$$\begin{pmatrix} a_0 & 0 & 0 & 0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & 0 & 0 & 0 & a_6 & -a_5 & a_1 \\ 0 & 0 & a_0 & 0 & -a_6 & 0 & a_4 & a_2 \\ 0 & 0 & 0 & a_0 & a_5 & -a_4 & 0 & a_3 \\ a_4 & 0 & -a_3 & a_2 & a_7 & 0 & 0 & 0 \\ a_5 & a_3 & 0 & -a_1 & 0 & a_7 & 0 & 0 \\ a_6 & -a_2 & a_1 & 0 & 0 & 0 & a_7 & 0 \\ 0 & a_4 & a_5 & a_6 & 0 & 0 & 0 & a_7 \end{pmatrix}.$$

Routine calculation yields $\det(L_a) = (aN)^4$, and $L_a \in SO(V)$ follows. By Lemma 4.2, it suffices to show $\mathrm{discr}(\chi_{L_a}) \in F^2$.

Assume first that $(e-a)N \neq 0$. Then $V(1-L_a) = V(e-a) = V$, and $((e-a)^{-1}v)(1-L_a) = v$ for every $v \in V$. Thus $(u,v)\chi_{La} = \langle u, vL_{e-a}^{-1}\rangle$, and

the matrix of χ_{L_a} is JL_{e-a}^{-1}, where J is as in (6). Therefore $\operatorname{discr}(\chi_{L_a}) = \det(J)\det(L_{e-a})^{-1} = ((e-a)N)^{-4} \in F^2$.

Suppose now $(e-a)N = 0$ and exclude the trivial case $e-a \in F$. Define the elements

$$e_0 = \begin{pmatrix} 1 & (0,0,0) \\ (0,0,0) & 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 & (1,0,0) \\ (0,0,0) & 0 \end{pmatrix},$$
$$e_2 = \begin{pmatrix} 0 & (0,1,0) \\ (0,0,0) & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 & (0,0,1) \\ (0,0,0) & 0 \end{pmatrix}$$

and

$$f_0 = (e-a)e_0 = \begin{pmatrix} 1-a_0 & (0,0,0) \\ (-a_4,-a_5,-a_6) & 0 \end{pmatrix},$$
$$f_1 = (e-a)e_1 = \begin{pmatrix} 0 & (1-a_0,0,0) \\ (0,-a_3,a_2) & -a_4 \end{pmatrix},$$
$$f_2 = (e-a)e_2 = \begin{pmatrix} 0 & (0,1-a_0,0) \\ (a_3,0,-a_1) & -a_5 \end{pmatrix},$$
$$f_3 = (e-a)e_3 = \begin{pmatrix} 0 & (0,0,1-a_0) \\ (-a_2,a_1,0) & -a_6 \end{pmatrix}.$$

The vectors e_i span a totally isotropic subspace of V and $f_i \in (e-a)V$. Since $\langle (e-a)x, (e-a)y\rangle = (e-a)N\langle x,y\rangle = 0$, $(e-a)V$ is totally isotropic as well. In particular, $\dim((e-a)V) \leq 4$.

Assume $a_0 \neq 1$. Then, the vectors f_i are linearly independent and hence form a basis of $(e-a)V$. The matrix $M = (m_{ij})$ of χ_{L_a} with respect to the basis $\{f_0, f_1, f_2, f_3\}$ satisfies $m_{ij} = (f_i, f_j)\chi_{L_a} = \langle f_i, e_j\rangle$, which yields

$$M = \begin{pmatrix} 0 & a_4 & a_5 & a_6 \\ -a_4 & 0 & a_3 & -a_2 \\ -a_5 & -a_3 & 0 & a_1 \\ -a_6 & a_2 & -a_1 & 0 \end{pmatrix},$$

by calculation. Then $\operatorname{discr}(\chi_{L_a}) = \det M = (a_1a_4 + a_2a_5 + a_3a_6)^2 \in F^2$.

The special case $a_0 = 1$ can be calculated similarly. □

For the rest of this section, let ι denote the conjugation map $x \mapsto \overline{x}$. Note that $\iota \in O(V)$ and $e\iota = e$.

Lemma 4.4. *Any element $g \in O(V)$ with $eg = e$ commutes with ι.*

Proof. We have $\overline{x}g = (\langle x,e\rangle e - x)g = \langle x,e\rangle eg - xg = \langle xg, eg\rangle eg - xg = \langle xg, e\rangle e - xg = \overline{xg}$. □

Lemma 4.5. *For an arbitrary element $g \in O(V)$, we define $\iota^g = g^{-1}\iota g$. Put $a = eg$. Then $aN = 1$ and $x\iota^g = a\overline{x}a$ holds for all $x \in V$.*

Proof. On the one hand, $aN = (eg)N = eN = 1$, therefore $a\overline{a} = e$ and $a^{-1} = \overline{a}$. On the other hand, $g = hL_a$ for some h with $eh = e$. By the previous lemma, $\iota^g = L_a^{-1}\iota L_a$ and $x\iota^g = ((xL_a^{-1})\iota)L_a = a(\overline{a^{-1}x}) = a\overline{x}a$. □

The map $-\iota : x \mapsto -\bar{x}$ is a symmetry with respect to the 7-dimensional nonsingular hyperplane

$$H = \left\{ \begin{pmatrix} x_0 & (x_1, x_2, x_3) \\ (x_4, x_5, x_6) & -x_0 \end{pmatrix} \;\middle|\; x_i \in F \right\}.$$

The conjugate $-\iota^g$ is a symmetry with respect to Hg. This means that

$$\mathcal{C} = \{-\iota^g \mid g \in O(V)\} = \{-L_a^{-1}\iota L_a \mid a \in M(F)\}$$

is a complete conjugacy class consisting of symmetries.

Theorem 4.6. *The multiplication group of $M(F)$ is $\Omega(\mathbb{O}(F), N)$.*

Proof. By Lemma 4.3, $\mathrm{Mlt}(M(F)) \leq \Omega(V)$. We have $(ax)\iota = x\iota\,\bar{a}$, which implies

$$\iota\iota^g = \iota L_a^{-1}\iota L_a = R_a L_a$$

and

$$\iota^g\iota^h = (\iota\iota^g)^{-1}(\iota\iota^h) = (R_a L_a)^{-1}(R_b L_b) \in \mathrm{Mlt}(M(F))$$

for $g, h \in O(V)$. Let us denote by $\mathcal{D}$ the set consisting of $\iota^g\iota^h$, $g, h \in O(V)$. $\mathcal{D}$ is clearly an invariant subset of $O(V)$. By [1, Thm. 5.27], $\mathcal{D}$ generates $\Omega(V)$, which proves $\mathrm{Mlt}(M(F)) = \Omega(\mathbb{O}(F), N)$. □

Finally, we determine the multiplication groups of Paige loops.

Corollary 4.7. *The multiplication group of the Paige loop $M^*(F)$ is the simple group $P\Omega(\mathbb{O}(F), N) = P\Omega_8^+(F)$.*

Proof. The surjective homomorphism $\varphi : M(F) \to M^*(F)$, $x \mapsto \pm x$ induces a surjective homomorphism $\Phi : \mathrm{Mlt}(M(F)) \to \mathrm{Mlt}(M^*(F))$. On the one hand, the kernel of Φ contains $\pm\mathrm{id}$. On the other hand $P\Omega(V) = \Omega(V)/\{\pm\mathrm{id}\}$ is a simple group, cf. [1, Thm. 5.27]. Since $\mathrm{Mlt}(M^*(F))$ is not trivial, we must have $\mathrm{Mlt}(M^*(F)) = P\Omega(V)$. Finally, the norm N has maximal Witt index 4, therefore the notation $P\Omega_8^+(F)$ is justified. □

Remark 4.8. The result of Theorem 4.6 is *folklore,* that is, most of the authors (Freudenthal, Doro, Liebeck, etc.) use it as a *well-known* fact without making a reference. The authors of the present paper are not aware of any reference, however, especially one that would handle all fields at once.

5 Groups with triality

5.1 Triality

Let G be a group. We use the usual notation $x^y = y^{-1}xy$ and $[x,y] = x^{-1}y^{-1}xy = x^{-1}x^y$ for x, $y \in G$. Let α be an automorphism of G, then $x\alpha$ will be denoted by x^α as well, and $[x,\alpha]$ will stand for $x^{-1}x^\alpha$. The element $\alpha^y \in \operatorname{Aut} G$ maps x to $x^{y^{-1}\alpha y} = ((x^{y^{-1}})^\alpha)^y$.

Let S_n be the symmetric group on $\{1,\dots,n\}$. $G \times H$ and $G \rtimes H$ will stand for the direct and semidirect product of G and H, respectively. In the latter case, H acts on G.

We have the following definition due to Doro [10].

Definition 5.1. The pair (G,S) is called a *group with triality*, if G is a group, $S \le \operatorname{Aut} G$, $S = \langle \sigma,\rho |\ \sigma^2 = \rho^3 = (\sigma\rho)^2 = 1\rangle \cong S_3$, and for all $g \in G$ the *triality identity*

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

holds.

The principle of triality was introduced by Cartan [6] in 1938 as a property of orthogonal groups in dimension 8, and his examples motivated Tits [28]. Doro was the first one to define the concept of an abstract group with triality, away from any context of a given geometric or algebraic object.

Definition 5.2. Let $(G_i, \langle \sigma_i, \rho_i\rangle)$, $i = 1,2$ be groups with triality. The homomorphism $\varphi : G_1 \to G_2$ is an *S-homomorphism* if $g\sigma_1\varphi = g\varphi\sigma_2$ and $g\rho_1\varphi = g\varphi\rho_2$ hold for all $g \in G_1$. The kernel of an S-homomorphism is an S-invariant normal subgroup. The group with triality G is said to be *S-simple* if it has no proper S-invariant normal subgroups.

The following examples of groups with triality are of fundamental importance. They are adopted from Doro [10].

Example 5.3. Let A be a group, $G = A^3$, and let σ, $\rho \in \operatorname{Aut} G$ be defined by $\sigma : (a_1,a_2,a_3) \mapsto (a_2,a_1,a_3)$ and $\rho : (a_1,a_2,a_3) \mapsto (a_2,a_3,a_1)$. Then G is a group with triality with respect to $S = \langle \sigma,\rho\rangle$.

Example 5.4. Let A be a group with $\varphi \in \operatorname{Aut} A$, $\varphi \neq \mathrm{id}_A$, satisfying $x\,x^\varphi\,x^{\varphi^2} = 1$ for all $x \in A$. Put $G = A \times A$, $\sigma : (a_1,a_2) \mapsto (a_2,a_1)$ and $\rho : (a_1,a_2) \mapsto (a_1^\varphi, a_2^{\varphi^{-1}})$. Then G is a group with triality with respect to $S = \langle \sigma,\rho\rangle$.

If A is of exponent 3 and $\varphi = \mathrm{id}_A$ then G is a group with triality in a wider sense, meaning that the triality identity is satisfied but S is not isomorphic to S_3.

Example 5.5. Let V be a two-dimensional vector space over a field of characteristic different from 3. Let S be the linear group generated by the matrices

$$\rho = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then the additive group of V and S form a group with triality.

Remark 5.6. If A is a simple group then the constructions in Examples 5.3 and 5.4 yield S-simple groups with triality. Obviously, if (G, S) is a group with triality and G is simple (as a group) then (G, S) is S-simple. Below, we are concerned with the converse of this statement.

5.2 Triality of Moufang nets

In the following, (G, S) stands for a group G with automorphism group S isomorphic to S_3. Let σ, $\rho \in S$ be such that $\sigma^2 = \rho^3 = \mathrm{id}$. Let the three involutions of S be $\sigma_1 = \sigma$, $\sigma_2 = \sigma\rho$ and $\sigma_3 = \rho\sigma = \sigma\rho^2$. Finally, the conjugacy class σ_i^G will be denoted by $\mathcal{C}_i$.

The following lemma gives a more conceptual reformulation of Doro's triality. (It is similar to Lemma 3.2 of [17], attributed by Liebeck to Richard Parker.)

Lemma 5.7. *The pair (G, S) is a group with triality if and only if $(\tau_i\tau_j)^3 = \mathrm{id}$ for every $\tau_i \in \mathcal{C}_i$, $\tau_j \in \mathcal{C}_j$, where i, $j \in \{1, 2, 3\}$ and $i \neq j$. In this case, $(G, \langle \tau_i, \tau_j \rangle)$ is a group with triality as well.*

Proof. The condition of the first statement claims something about the conjugacy classes $\mathcal{C}_i$, which do not change if we replace S by $\langle \tau_i, \tau_j \rangle$. This means that the first statement implies the second one.

For the first statement, it suffices to investigate the case $i = 1$, $j = 3$, $\tau_1 = \sigma^g$ and $\tau_3 = \sigma\rho^2$, with arbitrary $g \in G$. Then the following equations are equivalent for every $g \in G$:

$$\begin{aligned} 1 &= (\sigma^g(\sigma\rho^2))^3, \\ 1 &= \sigma^g(\sigma\rho^2) \cdot \sigma^g(\sigma\rho^2) \cdot \sigma^g(\sigma\rho^2), \\ 1 &= [g,\sigma]\rho^2 \cdot [g,\sigma]\rho^2 \cdot [g,\sigma]\rho^2, \\ 1 &= [g,\sigma] \cdot \rho^{-1}[g,\sigma]\rho \cdot \rho[g,\sigma]\rho^2, \\ 1 &= [g,\sigma]\,[g,\sigma]^{\rho}\,[g,\sigma]^{\rho^2}. \end{aligned}$$

This finishes the proof. □

The next lemma already foreshadows the relation between Moufang 3-nets and groups with triality.

Lemma 5.8. *Let P be a point of the Moufang 3-net $\mathcal{N}$. Denote by ℓ_1, ℓ_2 and ℓ_3 the three lines through P with corresponding Bol reflections σ_1, σ_2, σ_3. Then the collineation group $S = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \cong S_3$ acts faithfully on the set $\{\ell_1, \ell_2, \ell_3\}$. This action is equivalent to the induced action of S on the parallel classes of $\mathcal{N}$.*

Proof. As we have demonstrated in Section 2, the conjugate of a Bol reflection is a Bol reflection. Thus $\sigma_1\sigma_2\sigma_1 = \sigma_3 = \sigma_2\sigma_1\sigma_2$, which proves the first statement. The rest is trivial. □

Using these lemmas, we can prove two key propositions.

Proposition 5.9. *Let $\mathcal{N}$ be a Moufang 3-net and let M be the group of collineations generated by all Bol reflections of $\mathcal{N}$. Let $M_0 \leq M$ be the direction preserving subgroup of M. Let us fix an arbitrary point P of $\mathcal{N}$ and denote by S the group generated by the Bol reflections with axes through P. Then $M_0 \triangleleft M$, $M = M_0S$, and the pair (M_0, S) is a group with triality.*

Proof. $M_0 \triangleleft M = M_0S$ is obvious. Thus S is a group of automorphism of M_0 by conjugation. By Lemma 5.7, it is sufficient to show $\langle \sigma_i^g, \sigma_j^h \rangle \cong S_3$ for all g, $h \in M_0$, where σ_i and σ_j are the reflections on two different lines through P. Since g, h preserve directions, the axes of σ_i^g and σ_j^h intersect in some point P'. Hence $\langle \sigma_1^g, \sigma_2^h \rangle \cong S_3$, by Lemma 5.8. □

The converse of the proposition is true as well.

Proposition 5.10. *Let (G, S) be a group with triality. The following construction determines a Moufang 3-net $\mathcal{N}(G, S)$. Let the three line classes be the conjugacy classes $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$. By definition, three mutually non-parallel lines $\tau_i \in \mathcal{C}_i$ $(i = 1, 2, 3)$ intersect in a common point if and only if*

$$\langle \tau_1, \tau_2, \tau_3 \rangle \cong S_3.$$

Moreover, if $G_1 = [G, S]S = \langle \mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \rangle$, then the group $M(\mathcal{N})$ generated by the Bol reflections of $\mathcal{N}$ is isomorphic to $G_1/Z(G_1)$.

Proof. By definition, parallel lines do not intersect. When formulating the triality identity as in Lemma 5.7, we see that two non-parallel lines have a point in common such that there is precisely one line from the third parallel class incident with this point. This shows that $\mathcal{N}(G,S)$ is a 3-net indeed.

The Moufang property follows from the construction immediately, since one can naturally associate an involutorial collineation to any line $\tau_i \in \mathcal{C}_i$, namely the one induced by τ_i on G. This induced map $\bar{\tau}_i$ interchanges the two other parallel classes $\mathcal{C}_j$, $\mathcal{C}_k$ and fixes the points on its axis, that is, it normalizes the S_3 subgroups containing τ_i.

Finally, since a Bol reflection acts on the line set in the same way that the associated $\mathcal{C}_i$-element acts on the set $\cup\mathcal{C}_j$ by conjugation, we have the isomorphism $M(\mathcal{N}) \cong G_1/Z(G_1)$. □

Remark 5.11. From the point of view of dual 3-nets, the point set is the union of the three classes $\mathcal{C}_i$, and lines consist of the intersections of an S_3 subgroup with each of the three classes.

Remark 5.12. One finds another construction of groups with triality using the geometry of the associated 3-net in P. O. Mikheev's paper [18]. A different approach to groups with triality is given in J. D. Phillips' paper [24].

5.3 Triality collineations in coordinates

At this point, we find it useful to write down the above maps in the coordinate system of the 3-net. If we denote by $\sigma_m^{(v)}, \sigma_m^{(h)}, \sigma_m^{(t)}$ the Bol reflections with axes $X = m$, $Y = m$, $XY = m$, respectively, then we have

$$\begin{aligned}
\sigma_m^{(v)} &: (x,y) \mapsto (m(x^{-1}m), m^{-1}(xy)),\\
\sigma_m^{(h)} &: (x,y) \mapsto ((xy)m^{-1}, (my^{-1})m),\\
\sigma_m^{(t)} &: (x,y) \mapsto (my^{-1}, x^{-1}m).
\end{aligned}$$

This yields

$$\begin{aligned}
\sigma_m^{(v)}\sigma_1^{(v)} &: (x,y) \mapsto (m^{-1}(xm^{-1}), my),\\
\sigma_m^{(h)}\sigma_1^{(h)} &: (x,y) \mapsto (xm, (m^{-1}y)m^{-1}),\\
\sigma_{m^{-1}}^{(t)}\sigma_1^{(t)} &: (x,y) \mapsto (mx, ym).
\end{aligned}$$

These are direction preserving collineations generating G.

They can be written in the form $\sigma_m^{(v)}\sigma_1^{(v)} = (L_m^{-1}R_m^{-1}, L_m)$, $\sigma_m^{(h)}\sigma_1^{(h)} = (R_m, L_m^{-1}R_m^{-1})$ and $\sigma_m^{(t)}\sigma_1^{(t)} = (L_m, R_m)$ as well. The associated autotopisms are

$$(L_m^{-1}R_m^{-1}, L_m, L_m^{-1}), \quad (R_m, L_m^{-1}R_m^{-1}, R_m^{-1}), \quad (L_m, R_m, L_mR_m),$$

respectively. By the way, the fact that these triples are autotopisms is equivalent with the Moufang identities (1).

6 The classification of nonassociative finite simple Moufang loops

6.1 Simple 3-nets

The classification of finite simple Moufang loops is based on the classification of finite simple groups with triality. Using the results of the previous section, the classification can be done in the following steps.

Proposition 6.1. *Let $\varphi : \mathcal{N}_1 \to \mathcal{N}_2$ be a map between two 3-nets that preserves incidence and directions.*

(i) *Suppose that $\varphi(P_1) = P_2$ holds for the points $P_1 \in \mathcal{N}_1$, $P_2 \in \mathcal{N}_2$. Then φ defines a homomorphism $\bar{\varphi} : L_1 \to L_2$ in a natural way, where L_i is the coordinate loop of the 3-net $\mathcal{N}_i$ with origin P_i. Conversely, the loop homomorphism $\bar{\varphi} : L_1 \to L_2$ uniquely determines a collineation $\mathcal{N}_1 \to \mathcal{N}_2$, namely φ.*

(ii) *Suppose that the 3-nets $\mathcal{N}_i$ $(i = 1, 2)$ are Moufang and φ is a collineation onto. Let us denote by (M_i, S) the group with triality that corresponds to the 3-net $\mathcal{N}_i$. Then the maps $\sigma_\ell \mapsto \sigma_{\ell\varphi}$ induce a surjective S-homomorphism $\tilde{\varphi} : M_1 \to M_2$, where σ_ℓ is the Bol reflection in $\mathcal{N}_1$ with axis ℓ. Conversely, an S-homomorphism $M_1 \to M_2$ defines a direction preserving collineation between the 3-nets $\mathcal{N}(M_1, S)$ and $\mathcal{N}(M_2, S)$.*

Proof. The first part of statement (i) follows from the geometric definition of the loop operation in a coordinate loop; the second part is trivial. For the (ii) statement, it is sufficient to see that a relation of the reflections σ_ℓ corresponds to a point-line configuration of the 3-net, and that the φ-image of the configuration induces the same relation on the reflections $\sigma_{\varphi(\ell)}$. The converse follows from Proposition 5.10. □

In the sense of the proposition above, we can speak of *simple* 3*-nets*, that is, of 3-nets having only trivial homomorphisms. The next proposition follows immediately.

Proposition 6.2. *If L is a simple Moufang loop, then the associated* 3*-net $\mathcal{N}$ is simple as well. That is, the group (M_0, S) with triality determined by $\mathcal{N}$ is S-simple.*

6.2 S-simple groups with triality

The structure of S-simple groups with triality is rather transparent. It is clear that G is S-simple if and only if it has no S-invariant proper nontrivial normal subgroups.

Let G be such a group and let $N \triangleleft G$ be an arbitrary proper normal subgroup of G. Let us denote by N_i the images of N under the elements of S, $i = 1, \ldots, 6$.

Since the union and the intersection of the groups N_i is an S-invariant normal subgroup of G, we have $G = N_1 \cdots N_6$ and $\{1\} = N_1 \cap \ldots \cap N_6$. If $N_i \cap N_j$ is a proper subgroup of N_i for some i, $j = 1, \ldots, 6$, then we replace N_i by $N_i \cap N_j$. We can therefore assume that the groups N_i intersect pairwise trivially. Since S acts transitively on the groups N_i, one of the following cases must occur:

Case A. G is a simple group. In this case, there is no proper normal subgroup N.

Case B. The number of distinct groups N_i is 2. Then $N = N^\rho$, $M = N^\sigma$, $G = NM$, $N \cap M = \{1\}$ and elements of N and M commute. Every element $g \in G$ can be written as $g = ab^\sigma$. ρ induces an automorphism φ on N. Then, $g^\sigma = a^\sigma b = ba^\sigma$ and $g^\rho = a^\rho b^{\sigma\rho} = a^\rho b^{\rho^{-1}\sigma} = a^\varphi b^{\varphi^{-1}\sigma}$.

Moreover, applying the triality identity on $a \in N$, we obtain

$$(a^{\varphi^2} a^\varphi a)^{-1} (a a^\varphi a^{\varphi^2})^\sigma = 1,$$

which is equivalent with the identity $a a^\varphi a^{\varphi^2} = 1$. This means that the map $N \times N \to G$, $(a, b) \mapsto ab^\sigma$ defines an S-isomorphism between G and the construction in Example 5.4.

However, a result of Khukhro claims that the existence of the automorphism φ of N implies that N is nilpotent of class at most 3 (see [16, p. 223], [20, Thm. 3.3]). Therefore, no S-simple group with triality can be constructed in this case.

Case C. The number of distinct groups N_i is 3: $N = N_1$, $N^\rho = N_2$, $N^{\rho^2} = N_3$. We can assume $N_1^\sigma = N_1$ and $N_2^\sigma = N_3$.

Case C/1. Assume that $M = N_1 \cap (N_2N_3)$ is a proper subgroup of N_1. Then $M^\rho \in N_1^\rho = N_2 \subseteq N_2N_3$, similarly $M^{\rho^2} \in N_2N_3$. Moreover, $M^\sigma = N_1^\sigma \cap (N_2^\sigma N_2^\sigma) = M$. Hence, $MM^\rho M^{\rho^2}$ is a proper S-invariant normal subgroup of G, a contradiction.
Case C/2. Assume $N_1 \cap (N_2N_3) = \{1\}$. Then $G = N_1 \times N_2 \times N_3 \cong N^3$. By the triality identity, we have $a^{-1}a^\sigma \in N_1 \cap (N_2N_3)$ for any $a \in N_1$, thus, $a^\sigma = a$. Consider the map $\Phi : N^3 \to G$, $\Phi(a,b,c) = ab^\rho c^{\rho^2}$. By

$$(ab^\rho c^{\rho^2})^\sigma = ac^\rho b^{\rho^2} \qquad \text{and} \qquad (ab^\rho c^{\rho^2})^\rho = ca^\rho b^{\rho^2},$$

Φ defines an S-isomorphism between G and the group with triality in Example 5.3.
Case C/3. Assume $N_1 \subseteq N_2N_3$, G noncommutative. We have $G = N_1 \times N_2 \cong N^2$. Since G is S-simple, we must have $Z(G) = \{1\}$ and $Z(N) = \{1\}$. Let us assume that $a^\rho = a_1a_2$ with $1 \neq a_1 \in N_1$, $a_2 \in N_2$ for some element $a \in N_1 = N$. Take $b \in N$ with $a_1b \neq ba_1$. Every element of N_1 commutes with every element of N_2. This implies

$$1 \neq [a_1a_2, b] = [a^\rho, b] \in N \cap N^\rho,$$

a contradiction.
Case C/4. If G is commutative and S-simple, then we are in the situation of Example 5.5. The proof is left to the reader.

We summarize these results in the following proposition. In the finite case the result was proved by S. Doro [10]. In the infinite case, it is due to G. P. Nagy and M. Valsecchi [20].

Proposition 6.3. *Let G be a noncommutative S-simple group with triality. Then either G is simple or $G = A \times A \times A$, where A is a simple group and the triality automorphisms satisfy $(a,b,c)^\rho = (c,a,b)$, $(a,b,c)^\sigma = (a,c,b)$.*

6.3 The classification

Lemma 6.4. *Let $G = A \times A \times A$ be an S-simple group with triality. Then the associated loop is isomorphic to the group A.*

Proof. We leave to the reader to check that an associative simple Moufang loop A has $G = A \times A \times A$ as a group with triality. Since the group with triality determines the 3-net uniquely, and since groups are G-loops, that is, the coordinate loop does not depend on the choice of the origin, we are done. □

Also the following result is due to Doro, but the way of proving is based on the geometric approach, hence new.

Lemma 6.5 (Doro). *Assume that G is a group with triality such that ρ is an inner automorphism. Then the associated Moufang loop has exponent 3.*

Proof. Let ρ be an inner automorphism of G. We assume G to be a group of direction preserving collineations of the 3-net $\mathcal{N}$ associated with L. We consider ρ as a collineation of $\mathcal{N}$ permuting the directions cyclicly. We denote by Γ^+ the collineation group of $\mathcal{N}$ generated by G and ρ. Γ^+ consists of collineations which induce an even permutation on the set of directions.

Let $\alpha \in G$ be a direction preserving collineation which induces ρ on G and put $r = \alpha^{-1}\rho$. Obviously, $\Gamma^+ = \langle G, r\rangle$, hence $r \in Z(\Gamma^+)$. Moreover, since Γ^+ is invariant under σ, we have $r^\sigma \in Z(\Gamma^+)$.

Let τ be a Bol reflection whose axis is parallel to the axis of σ. On the one hand, $\sigma\tau \in G$ and

$$\sigma\tau = r^{-1}\sigma\tau r = (\sigma^r\sigma)(\sigma\tau^r)$$

holds. On the other hand, $\sigma^r\sigma = r^{-1}r^\sigma \in Z(\Gamma^+)$ and $\sigma\tau^r \in \Gamma^+$. Therefore,

$$(\sigma\tau)^3 = (\sigma^r\sigma)^3\,(\sigma\tau^r)^3 = \mathrm{id}$$

by the modified triality property, cf. Lemma 5.7.

Assume now that the axis of the Bol reflections σ and τ are vertical with equation $X = e$ and $X = a$. As we have seen in Section 5.3, the coordinate forms of these maps are $(x, y)\sigma = (x^{-1}, xy)$ and $(x, y)\tau = (ax^{-1}a, a^{-1}(xy))$. This implies $(x, y)\sigma\tau = (axa, a^{-1}y)$ and $(x, y)(\sigma\tau)^3 = (a^3xa^3, a^{-3}y)$. By $(\sigma\tau)^3 = \mathrm{id}$, we have $a^3 = 1$. Since we chose τ arbitrarily, L must be of exponent 3. □

Corollary 6.6. *If G is a finite group with triality which determines a non-commutative simple Moufang loop then all triality automorphisms are outer.*

Proof. Assume that σ is an inner automorphism. Then so are σ^ρ and $\rho = \sigma^\rho\sigma$. We have the same implication if we suppose $\sigma\rho$ or $\rho\sigma$ to be inner. In any case, ρ will be inner and L will be a finite Moufang loop of exponent 3. By [13, Thm. 4], L is either not simple or commutative. □

Theorem 6.7 (Liebeck's Theorem [17]). *The only finite simple groups with triality are the simple groups $(P\Omega_8^+(q), S)$. The triality automorphisms are uniquely determined up to conjugation. (They are the so called graph automorphisms of $P\Omega_8^+(q)$.)*

Corollary 6.8 (Thm. [17]). *The only nonassociative finite simple Moufang loops are the Paige loops $M^*(q) = M^*(GF(q))$, where q is a prime power.*

7 Automorphism groups of Paige loops over perfect fields

Now that we have found all nonassociative finite simple Moufang loops, we will determine their automorphism groups. In fact, we will determine $\mathrm{Aut}\, M^*(F)$ whenever F is perfect. Recall that a field of characteristic p is *perfect* if the Frobenius map $x \mapsto x^p$ is an automorphism of F. The approach here is based on [21].

7.1 The automorphisms of the split octonion algebras

Let C be a composition algebra over F. A map $\alpha : C \to C$ is a *linear automorphism* (resp. *semilinear automorphism*) of C if it is a bijective F-linear (resp. F-semilinear) map preserving the multiplication, i.e., satisfying $(uv)\alpha = (u\alpha)(v\alpha)$ for every u, $v \in C$. It is well known that the group of linear automorphisms of $\mathbb{O}(F)$ is isomorphic to the Chevalley group $G_2(F)$, cf. [11, Sec. 3], [22, Ch. 2]. The group of semilinear automorphisms of $\mathbb{O}(F)$ is therefore isomorphic to $G_2(F) \rtimes \mathrm{Aut}\, F$.

Since every linear automorphism of a composition algebra is an isometry [22, Sec. 1.7], it induces an automorphism on the loops $M(F)$ and $M^*(F)$. The following result—that is interesting in its own right—shows that every element of $\mathbb{O}(F)$ is a sum of two elements of norm one. Consequently, $\mathrm{Aut}\, \mathbb{O}(F) \leq \mathrm{Aut}\, M^*(F)$.

Theorem 7.1 (Thm. 3.3 [29]). *Let F be any field and $\mathbb{O}(F)$ the split octonion algebra over F. Then every element of $\mathbb{O}(F)$ is a sum of two elements of norm one.*

Proof. As before, we identify $\mathbb{O}(F)$ with the Zorn vector matrix algebra over F, where the norm is given by the determinant. Let

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix}$$

be an element of $\mathbb{O}(F)$. First assume that $\beta \neq 0$. Note that for every $\lambda \in F$ there is $\gamma \in F^3$ such that $\gamma \cdot \beta = \lambda$. Pick $\gamma \in F^3$ so that $\gamma \cdot \beta = a + b - ab + \alpha \cdot \beta$. Then choose $\delta \in \gamma^\perp \cap \alpha^\perp \neq 0$. This choice guarantees

that $(a-1)(b-1)-(\alpha-\gamma)\cdot(\beta-\delta)=ab-a-b+1-\alpha\cdot\beta+\gamma\cdot\beta=1$. Thus

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} = \begin{pmatrix} 1 & \gamma \\ \delta & 1 \end{pmatrix} + \begin{pmatrix} a-1 & \alpha-\gamma \\ \beta-\delta & b-1 \end{pmatrix}$$

is the desired decomposition of x into a sum of two elements of norm 1. Note that the above procedure works for every α.

Now assume that $\beta=0$. If $\alpha\neq 0$, we use a symmetrical argument as before to decompose x. It remains to discuss the case when $\alpha=\beta=0$. Then the equality

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & (1,0,0) \\ (-1,0,0) & 0 \end{pmatrix} + \begin{pmatrix} 0 & (-1,0,0) \\ (1,0,0) & b \end{pmatrix}$$

does the job. □

An automorphism $f\in\operatorname{Aut}M^*(F)$ will be called *(semi)linear* if it is induced by a (semi)linear automorphism of $\mathbb{O}(F)$.

7.2 Geometric description of loop automorphisms

By considering extensions of automorphisms of $M^*(F)$, it was proved in [29] that $\operatorname{Aut}M^*(2)$ is isomorphic to $G_2(2)$. The aim of this section is to generalize this result (although using different techniques) and prove that every automorphism of $\operatorname{Aut}M^*(F)$ is semilinear, provided F is perfect. We reach this aim by identifying $\operatorname{Aut}M^*(F)$ with a certain subgroup of the automorphism group of the group with triality associated with $M^*(F)$.

To begin with, we recall the geometrical characterization of automorphisms of a loop, as promised in Subsection 2.4.

Lemma 7.2 (Thm. 10.2 [3]). *Let L be a loop and $\mathcal{N}$ its associated 3-net. Any direction preserving collineation which fixes the origin of $\mathcal{N}$ is of the form $(x,\,y)\mapsto(x\alpha,\,y\alpha)$ for some $\alpha\in\operatorname{Aut}L$. Conversely, the map $\alpha: L\to L$ is an automorphism of L if and only if $(x,\,y)\mapsto(x\alpha,\,y\alpha)$ is a direction preserving collineation of $\mathcal{N}$.*

We will denote the map $(x,\,y)\mapsto(x\alpha,\,y\alpha)$ by φ_α. Before reading any further, recall Propositions 5.9 and 5.10.

Proposition 7.3. *Let L be a Moufang loop and $\mathcal{N}$ its associated 3-net. Let M be the group of collineations generated by the Bol reflections of $\mathcal{N}$, M_0 the direction preserving part of M, and $S\cong S_3$ the group generated by the Bol reflections whose axis contains the origin of $\mathcal{N}$. Then $\operatorname{Aut}L\cong C_{\operatorname{Aut}M_0}(S)$.*

Proof. As the set of Bol reflections of $\mathcal{N}$ is invariant under conjugations by collineations, every element $\varphi \in \operatorname{Coll}\mathcal{N}$ normalizes the group M_0 and induces an automorphism $\widehat{\varphi}$ of M. It is not difficult to see that φ fixes the three lines through the origin of $\mathcal{N}$ if and only if $\widehat{\varphi}$ centralizes (the involutions of) S.

Pick $\alpha \in \operatorname{Aut} L$, and let $\widehat{\varphi_\alpha}$ be the automorphism of M_0 induced by the collineation φ_α. As φ_α fixes the three lines through the origin, $\widehat{\varphi_\alpha}$ belongs to $C_{\operatorname{Aut} M_0}(S)$, by the first paragraph.

Conversely, an element $\psi \in C_{\operatorname{Aut} M_0}(S)$ normalizes the conjugacy class of σ in M_0S and preserves the incidence structure defined by the embedding of $\mathcal{N}$. This means that $\psi = \widehat{\varphi}$ for some collineation $\varphi \in \operatorname{Coll}\mathcal{N}$. Now, ψ centralizes S, therefore φ fixes the three lines through the origin. Thus φ must be direction preserving, and there is $\alpha \in \operatorname{Aut} L$ such that $\varphi = \varphi_\alpha$, by Lemma 7.2. □

7.3 The automorphisms of Paige loops

Theorem 7.4. *Let F be a perfect field. Then the automorphism group of the nonassociative simple Moufang loop $M^*(F)$ constructed over F is isomorphic to the semidirect product $G_2(F) \rtimes \operatorname{Aut} F$. Every automorphism of $M^*(F)$ is induced by a semilinear automorphism of the split octonion algebra $\mathbb{O}(F)$.*

Proof. We fix a perfect field F, and assume that all simple Moufang loops and Lie groups mentioned below are constructed over F.

The group with triality associated with M^* is the multiplicative group $\operatorname{Mlt} M^* \cong D_4$, and the graph automorphisms of D_4 are exactly the triality automorphisms of M^* (cf. [11], [10]). To be more precise, Freudenthal proved this for the reals and Doro for finite fields, however they based their arguments only on the root system and parabolic subgroups, and that is why their result is valid over any field.

By [11], $C_{D_4}(\sigma) = B_3$, and by [17, Lemmas 4.9, 4.10 and 4.3], $C_{D_4}(\rho) = G_2$. As $G_2 < B_3$, by [14, p. 28], we have $C_{D_4}(S_3) = G_2$.

Since F is perfect, $\operatorname{Aut} D_4$ is isomorphic to $\Delta \rtimes (\operatorname{Aut} F \times S_3)$, by a result of Steinberg (cf. [7, Chapter 12]). Here, Δ is the group of the inner and diagonal automorphisms of D_4, and S_3 is the group of graph automorphisms of D_4. When $\operatorname{char} F = 2$ then no diagonal automorphisms exist, and $\Delta = \operatorname{Inn} D_4$. When $\operatorname{char} F \neq 2$ then S_3 acts faithfully on $\Delta/\operatorname{Inn} D_4 \cong C_2 \times C_2$. Hence, in any case, $C_\Delta(S_3) = C_{D_4}(S_3)$. Moreover, for the field and graph automorphisms commute, we have $C_{\operatorname{Aut} D_4}(S_3) = C_{D_4}(S_3) \rtimes \operatorname{Aut} F$.

We have proved $\operatorname{Aut} M^* \cong G_2 \rtimes \operatorname{Aut} F$. The last statement follows from the fact that the group of linear automorphisms of the split octonion algebra is isomorphic to G_2. □

8 Related results, prospects and open problems

We conclude with a few results and open problems concerning simple Moufang loops.

8.1 Generators for finite Paige loops

It is well known that every finite simple group is generated by at most 2 elements. This result requires the classification of finite simple groups, and was finalized in [2]. Since any two elements of a Moufang loop generate a subgroup, no nonassociative Moufang loop can be 2-generated. The following theorem can be proved using some classical results on generators of groups $SL(2,q)$, cf. [31]:

Theorem 8.1. *Every Paige loop $M^*(q)$ is 3-generated. When $q > 2$, the generators can be chosen as*

$$\begin{pmatrix} 0 & e_1 \\ -e_1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} 0 & e_2 \\ -e_2 & \lambda \end{pmatrix}, \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix},$$

where λ is a primitive element of $GF(q)$, and e_i is the 3-vector whose only nonzero coordinate is in position i and is equal to 1. When $q = 2$, the generators can be chosen as

$$\begin{pmatrix} 1 & e_1 \\ e_1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & e_2 \\ e_2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & e_3 \\ e_3 & 1 \end{pmatrix}.$$

8.2 Generators for integral Cayley numbers of norm one

Let $C = (C, N)$ be a real composition algebra. The *set of integral elements* of C is the maximal subset of C containing 1, closed under multiplication and subtraction, and such that both aN and $a + \overline{a}$ are integers for each a in the set.

Let $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$ be the classical real composition algebras, i.e., those obtained from $\mathbb{R}$ by the Cayley-Dickson process with parameter $\lambda = -1$. The real octonions $\mathbb{O}$ are often called *Cayley numbers*. For $C \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$, there is a unique set of integral elements of C. (For instance, when $C = \mathbb{C}$

this set is known as the Gaussian integers.) When $C = \mathbb{O}$, there are seven such sets, all isomorphic, as Coxeter showed in [9].

We use the notation of [9] here. Let J be one of the sets of integral elements in $\mathbb{O}$, and let $J' = \{x \in J |\ xN = 1\}$. Then $|J'| = 240$, and $J'/\{1, -1\}$ is isomorphic to $M^*(2)$. (This may seem strange, however, $M^*(2)$ is a subloop of any $M^*(q)$, too.) Hence, by Theorem 8.1, $J'/\{1, -1\}$ must be 3-generated. Let i, j, k be the usual units in $\mathbb{H}$, and let e be the unit that is added to $\mathbb{H}$ when constructing $\mathbb{O}$. Following Dickson and Coxeter, let $h = (i + j + k + e)/2$. Then one can show that i, j and h generate $J'/\{1, -1\}$ (multiplicatively). Since $i^2 = -1$, it follows that every set of integral elements of unit norm in $\mathbb{O}$ is 3-generated, too. See [30] for details.

8.3 Problems and Conjectures

Problem 8.2. *Find a presentation for $M^*(q)$ in the variety of Moufang loops, possibly based on the generators of Theorem* 8.1.

Problem 8.3. *Find (necessarily infinite) nonassociative simple Moufang loops that are not Paige loops.*

Conjecture 8.4. *Let L be a nonassociative simple Moufang loop and let $H = \mathrm{Mlt}(L)_e$ be the stabilizer of the neutral element in the multiplication group of L. Then H is simple.*

Problem 8.5. *Find a function $f : \mathbb{N} \to \mathbb{N}$ such that the order of the multiplication group of a Moufang loop of order n is less that $f(n)$.*

For the finite Paige loop $M^*(q)$, we have

$$\begin{aligned} |M^*(q)| &= \frac{1}{d} q^3(q^4 - 1), \\ |P\Omega_8^+(q)| &= \frac{1}{d^2} q^{12}(q^2 - 1)(q^4 - 1)^2(q^6 - 1), \end{aligned}$$

where $d = (2, q - 1)$. Hence $|\mathrm{Mlt}(M^*(q))| < 4|M^*(q)|^4$ holds. This motivated us to state:

Conjecture 8.6. *The function $f(n) = 4n^4$ solves Problem* 8.5.

References

[1] **E. Artin:** *Geometric Algebra*, Interscience Publishers, New York, 1957.

[2] **M. Aschbacher, R. Guralnick:** *Some applications of the first cohomology group*, J. Algebra **90** (1984), 446 – 460.

[3] **A. Barlotti, K. Strambach:** *The geometry of binary systems*, Advances Math. **49** (1983), 1 – 105.

[4] **R. H. Bruck:** *A Survey of Binary Systems*, Springer-Verlag, Berlin-Heidelberg-New York, 1958.

[5] **R. H. Bruck:** *What is a loop?*, in Studies in Modern Algebra, A. A. Albert (ed.), MAA Studies in Mathematics, 1963, 59 – 99.

[6] **E. Cartan:** *Leçons sur la Théorie des Spineurs*, Hermann et Cie., Paris, 1938.

[7] **R. W. Carter:** *Simple groups of Lie type*, Wiley Interscience, 1972.

[8] **O. Chein, H. O. Pflugfelder, J. D. H. Smith:** *Quasigroups and Loops: Theory and Applications*, Sigma Series in Pure Mathematics **8**, Heldermann Verlag Berlin, 1990.

[9] **H. S. M. Coxeter:** *Integral Cayley numbers*, Duke Mathematical Journal **13**, No. **4**, December 1946. Reprinted in H. S. M. Coxeter, *Twelve Geometric Essays*, Southern Illinois University Press, 1968.

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

[11] **H. Freudenthal:** *Oktaven, Ausnahmegruppen und Oktavengeometrie*, Geometria Dedicata **19** (1985), 1 – 63.

[12] **M. Funk, P. T. Nagy:** *On collineation groups generated by Bol reflections*, J. Geom. **41** (1993), 63 – 78.

[13] **G. Glauberman:** *On loops of odd order II*, J. Algebra **8** (1968), 383 – 414.

[14] **D. Gorenstein, R. Lyons, R. Solomon:** *The classification of the finite simple groups*, No. 3. Part I, Mathematical Surveys and Monographs **40**(3) (Providence, R.I., AMS, 1998).

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

[16] **E. I. Khukhro:** *Nilpotent groups and their automorphisms*, De Gruyter Expositions in Mathematics, W. de Gruyter, Berlin, 1993.

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

[18] **P. O. Mikheev:** *Moufang loops and their enveloping groups*, Webs and quasigroups (1993), 33 – 43.

[19] **G. P. Nagy:** *Burnside problems for Moufang and Bol loops of small exponent*, Acta Sci. Szeged **67**(3-4) (2001), 687 – 696.

[20] **G. P. Nagy, M. Valsecchi:** *Splitting automorphisms and Moufang loops.* Manuscript, 2003.

[21] **G. P. Nagy, P. Vojtěchovský:** *Automorphism Groups of Simple Moufang Loops over Perfect Fields*, to appear in Math. Proc. Cambridge Philos. Soc.

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

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

[24] **J. D. Phillips:** *Moufang loop multiplication groups with triality*, Rocky Mountain J. of Math. **29/4** (1999), 1483 – 1490.

[25] **H. O. Pflugfelder:** *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.

[26] **J. D. H. Smith:** *A left loop on the* 15*-sphere*, J. Algebra **176** (1995), 128 – 138.

[27] **D. E. Taylor:**, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992.

[28] **J. Tits:** *Sur la trialité et les algèbres d'octaves*, Acad. Roy. Belg. Bull. Cl. Sci. **44**(5) (1958), 332 – 350.

[29] **P. Vojtěchovský:** *Finite simple Moufang loops.* PhD Thesis, Iowa State University, 2001.

[30] **P. Vojtěchovský:** *Generators of nonassociative simple Moufang loops over finite prime fields*, J. Algebra **241** (2001), 186 – 192.

[31] **P. Vojtěchovský:** *Generators for finite simple Moufang loops*, J. Group Theory **6** (2003), 169 – 174.

Received April 29, 2003

Gábor P. Nagy
Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
H-6720 Szeged
Hungary
e-mail: nagyg@math.u-szeged.hu

Petr Vojtěchovský
Department of Mathematics
University of Denver
2360 S Gaylord St
Denver, Colorado 80208
U.S.A.
e-mail: petr@math.du.edu