Quasigroups and Related Systems **19** (2011), 69 – 108

Central automorphisms, Z*-theorems, and loop structure

Jonathan I. Hall

Abstract. We discuss central automorphisms of partial linear spaces, particularly those with three points per line. When these automorphisms have order two and their products are restricted to have odd order, we are in the situation of Glauberman's Z*-theorem. This sheds light on the structure of various coordinatizing loops, particularly Bol and Moufang loops.

1. Introduction

The topics to be considered here go back to Veblen and Young and even to Hilbert. They involve the interplay among geometry, group theory, and algebraic systems.

A partial linear space is a geometric incidence system, which may or may not come from some larger system with more structure, such as a vector space. Particular examples are 3-nets and Latin square designs. Central automorphisms are a particularly elegant sort of automorphism for the partial linear space; if there are many of them, then the space can often be coordinatized by a structured algebraic system. We encounter a fusion of geometry, group theory, and algebra. Various of these topics can then be used to shed light upon the others. That is our underlying theme.

In a paper [22] presented at an earlier conference in this series, the author discussed at great length the techniques associated with assigning coordinates and studying their properties. Less of that will be done here. Instead we will focus on the interaction of the areas. Some categorical scaffolding is erected for this. Certain algebraic and geometric questions require group theoretic Z*-theorems for their solution, but these theorems have much broader impact. Finally we discuss some consequences of the

2010 Mathematics Subject Classification: 20N05, 20B25, 20E25
Keywords: Moufang loop, Bol loop, group with triality, Latin square design, central automorphism, Z^*-theorem.

geometric, categorical, and group theoretic results for the structure of associated loops, particularly Bol and Moufang loops.

As this is a survey article, many results are left unproven or proofs are only suggested. This is a regrettable consequence of a lack of space and time. An exception is made for Fischer's Z*-Theorem 5.4, which we treat completely and in detail, providing it with a broader stage and a more accessible proof. Most of the missing proofs will appear elsewhere (especially in [23]). In any event, many of the results are not new. The primary message is that the varying points of view presented here can render topics more accessible.

Our general references for group theory are Aschbacher [1], Hall [26], and Kurzweil and Stellmacher [31]; for category theory, Jacobson [29]; for classical groups and geometry, Taylor [45]; for the octonions, Springer and Veldkamp [44]; and for general loop theory, Bruck [5] and Pflugfelder [40].

2. Quasigroups and loops

A *quasigroup* $(L, \cdot)$ is a nonempty set L equipped with a binary multiplication $\cdot\colon L \times L \longrightarrow L$ and such that, for each $a \in L$, the right and left translation maps $\mathrm{R}(a)\colon L \longrightarrow L$ and $\mathrm{L}(a)\colon L \longrightarrow L$ given by

$$q^{\mathrm{R}(a)} = q \cdot a \quad \text{and} \quad q^{\mathrm{L}(a)} = a \cdot q$$

are permutations of L. If there is a two-sided identity element $1_L = 1_{(L,\cdot)}$ then L is a *loop*. We typically write L in place of $(L, \cdot)$ when the multiplication is clear and also often denote multiplication by juxtaposition.

The requirement that $\mathrm{R}(a)$ and $\mathrm{L}(a)$ always be permuations is equivalent to the combinatorial statement that the multiplication table (Cayley table) of $(L, \cdot)$ is a *Latin square*: an $|L| \times |L|$ matrix in which each element of L is an entry exactly once in each row and exactly once in each column.

The *opposite* $(L, \star)$ of the quasigroup $(L, \cdot)$ is given by $a \star b = b \cdot a$. This corresponds to replacing the multiplication table by its transpose, clearly still a Latin square. There are four other *conjugate* quasigroups associated with $(L, \cdot)$ – the two quasigroups $(L, /)$ and $(L, \backslash)$ with multiplications given by

$$a/b = a\mathrm{R}(b)^{-1} \quad \text{and} \quad a\backslash b = b\mathrm{L}(a)^{-1}$$

and their opposites. At the level of Latin squares, the six conjugates correspond to the six possible permutations for the roles taken by rows, columns,

and entries. This is clearer in the context of Latin square designs, which will be introduced in Section 3.3.

A *homotopism* from the quasigroup $(L, \cdot)$ to the quasigroup $(R, \circ)$ is a triple (α, β, γ) of maps from L to R with the property that

$$x^\alpha \circ y^\beta = (x \cdot y)^\gamma$$

for all $x, y \in L$. A homotopism is an *isotopism* if each of its three maps is a bijection and an *autotopism* if $(R, \circ) = (L, \cdot)$. The autotopisms are thus triples (α, β, γ) of permutations of L with $x^\alpha y^\beta = (xy)^\gamma$ for all $x, y \in L$, and they form the group $\mathrm{Atp}(L)$ – the *autotopism group* of L.

A *homomorphism* from the loop $(L, \cdot)$ to the loop $(R, \circ)$ is a homotopism (α, β, γ) with $1_L^\alpha = 1_R$, $1_L^\beta = 1_R$, and $1_L^\gamma = 1_R$, from which it easily follows that $\alpha = \beta = \gamma$. The *kernel* of the homomorphism γ is then the subloop of elements x of L with $x^\gamma = 1_R$. A subloop of L is *normal* if it is the kernel of some homomorphism.

It is thus possible to talk about normal series for a loop and the factors in that series. In particular, a loop is *solvable* if it has a normal series of finite length in which all factors are abelian groups. There is also the stronger concept of nilpotency, which will be discussed below.

A nonidentity loop is *simple* if its only normal subloops are the identity and itself.

For L a quasigroup, we define within $\mathrm{Sym}(L)$ (the symmetric group on the set L) the *right multiplication group*

$$\mathrm{RMult}(L) = \langle\, \mathrm{R}(x) \mid x \in L \,\rangle\,,$$

the *left multiplication group*

$$\mathrm{LMult}(L) = \langle\, \mathrm{L}(x) \mid x \in L \,\rangle\,,$$

and the *multiplication group*

$$\mathrm{Mult}(L) = \langle\, \mathrm{R}(x), \mathrm{L}(x) \mid x \in L \,\rangle = \langle\, \mathrm{RMult}(L), \mathrm{LMult}(L) \rangle.$$

The *inner mapping group* is then the stabilizer of the identity in the multiplication group:

$$\mathrm{IMult}(L) = \{\, \alpha \in \mathrm{Mult}(L) \mid 1^\alpha = 1 \,\}\,.$$

The normal subloops of L are precisely those subloops fixed globally by $\mathrm{IMult}(L)$; see [5, p. 61] or [40, I.7.5].

In particular, the fixed points of $\mathrm{IMult}(L)$ form a normal subloop, the *center* of L. The loop L is then *nilpotent* if its ascending central series reaches L in a finite number of steps.

We shall particularly be interested in certain varieties of quasigroups and loops – subclasses that are defined through the satisfaction of particular identical relations. For instance, the category of groups arises as the variety of all loops that satisfy identically the associativity relation:

$$x(yz) = (xy)z.$$

A quasigroup is a *distributive quasigroup* if it satisfies the identical relations

$$(ax)(ay) = a(xy) \quad \text{and} \quad (xa)(ya) = (xy)a.$$

A loop is an *Moufang* loop if it satisfies the identical relation

$$(xa)(bx) = (x(ab))x.$$

With $a = 1$ in the Moufang identity, we get the *flexible* identity

$$x(bx) = (xb)x.$$

This implies that the opposite of a Moufang loop is again a Moufang loop.

A loop is an *(right) Bol* loop if it satisfies the identical relation

$$a(x(bx)) = (a(xb))x.$$

The opposite of a right Bol loop is a *left Bol* loop, given by the corresponding opposite identity. Our convention is to consider only right Bol loops, which we will refer to as Bol loops.

These last three identities are consequences of associativity. Therefore a group is a special type of Moufang loop and of Bol loop. It is also easy to see that a Moufang loop is a Bol loop. On the other hand, there are Bol loops that are not Moufang loops and Moufang loops that are not groups.

It turns out that Moufang loops are also *alternative*. That is, they satisfy the identities

$$a(xx) = (ax)x \quad \text{and} \quad (xx)a = x(xa).$$

In loops we must distinguish between right inverses and left inverses,

$$x({}^{-1}x) = 1 \quad \text{and} \quad (x^{-1})x = 1,$$

as they need not be the same. We say that inverses are *two-sided* if we have any one of the three equivalent identities

$$^{-1}x = x^{-1}, \quad (x^{-1})^{-1} = x\,, \quad \text{or} \quad ^{-1}(^{-1}x) = x.$$

A loop is a *right inverse property loop* if it satisfies the identity

$$(ax)(^{-1}x) = a$$

and a *left inverse property loop* if it satisfies the identity

$$x^{-1}(xa) = a.$$

The loop is an *inverse property loop* if it satisfies both of these identities. Moufang loops are inverse property loops, while in general right Bol loops have only the right inverse property (left Bol loops, the left inverse property).

In right inverse property loops and especially inverse property loops, inverses are always two sided. Indeed, if we set $a = {}^{-1}x$ in the right inverse property, we find $(^{-1}xx)(^{-1}x) = {}^{-1}x$. After cancelling ${}^{-1}x$ from the right, we are left with $^{-1}xx = 1$; inverses are two-sided.

3. Central automorphisms of partial linear spaces

A *partial linear space* $(\mathcal{P}, \mathcal{L})$ is a set of points $\mathcal{P}$ and a set of lines $\mathcal{L}$ together with an incidence relation $\sim$ satisfying:

> There do not exist distinct points a, b and distinct lines k, l with $a \sim k \sim b \sim l \sim a$.

The axiom is selfdual in the sense that $(\mathcal{P}, \mathcal{L})$ is a partial linear space if and only if $(\mathcal{L}, \mathcal{P})$ is. The partial linear space is a *linear space* when every pair of points is incident to a unique line.

The partial linear spaces of interest to us will typically have the further (selfdual) nondegeneracy axiom:

> Every point is incident to at least two lines, and every line is incident to at least two points.

Therefore we can identify each line with the subset of points incident to it. We do not require nondegeneracy, since we want to allow a set of points all incident to a unique line as a partial linear space, albeit a half degenerate

one. Even in that case, we can identify the line with the set of points incident to it.

For the partial linear space $(\mathcal{P}, \mathcal{L})$, consider a subset $\mathcal{P}_0$ of $\mathcal{P}$ with the property:

$$\text{if } \ell \in \mathcal{L} \text{ with } |\mathcal{P}_0 \cap \ell| \geqslant 2, \text{ then } \ell \subset \mathcal{P}_0.$$

Then $(\mathcal{P}_0, \mathcal{L}_0)$ is a *subspace* of $(\mathcal{P}, \mathcal{L})$, where $\mathcal{L}_0$ is the subset of lines of $\mathcal{L}$ meeting $\mathcal{P}_0$ in more than one point.

The *automorphism group* $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$ is the set of all permutations σ of $\mathcal{P}$ that take lines to lines:

$$\ell \in \mathcal{L} \iff \ell^\sigma \in \mathcal{L}\,.$$

The basic concept here is that of a *central automorphism* of $(\mathcal{P}, \mathcal{L})$. This is nonidentity automorphism σ for which there is a point $p \in P$ with the property that

$$p^\sigma = p \quad \text{and} \quad \ell^\sigma = \ell \text{ whenever } p \in \ell \in \mathcal{L}.$$

The point p is the *center* of σ. The dual of a center is an *axis* – a line that is fixed pointwise by σ. We say that the central automorphism σ with center p is *p-axis-free* if it has no axis incident to p.

3.1. Desarguesian planes

A *projective plane* is a linear space in which every pair of lines intersect in a unique point. (That is, a projective plane is a linear space whose dual is also a linear space.) To avoid degeneracies, we also require that there are four points with no three on a line. This assumption implies its dual and also that each line is incident to at least three points and dually. (For the material here on projective planes, see [26, Chap. 20] and [41].)

The canonical examples of projective planes are the *Desarguesian* planes: for D a division ring, the point set consists of all 1-spaces from the Cartesian cube D^3 and line set consists of all the 2-spaces of D^3; incidence is given by containment.

It is well-known [26, Theorem 20.4.1] that a central automorphism of a projective plane also acts as a central automorphism on the dual plane. Thus in the plane not only is there a point that is fixed linewise, there is also a line that is fixed pointwise, an axis; both center and axis are unique. The central automorphism is an *elation* if the center and axis are incident.

Let $(\mathcal{P}, \mathcal{L})$ be a projective plane. If a, b are two points of a line through p with neither on the line ℓ, then there is at most one central automorphism with center p and axis ℓ that takes a to b. A classical theorem characterizes the case where such an automorphism exists for all possible choices of a, b, p, ℓ.

Theorem 3.1. *A projective plane is Desarguesian if and only if it admits all possible central automorphisms.* □

That is, a plane that admits all possible central automorphisms can be coordinatized by a division ring.

We can consider more general coordinatizing rings.

Theorem 3.2. *A projective plane can be coordinatized by an alternative division algebra if and only if it admits all possible elations.* □

The first theorem is essentially due to Veblen and Young [48]. In fact a version only covering planes over fields was found by Hilbert. The second theorem was largely proven by Moufang [33] although a complete proof was first given by Hall [25].

Both theorems were classically phrased in terms of the closure of certain configurations of points and lines in the plane: the Desargues configuration for the first theorem, the Little Desargues configuration (a special case) for the second theorem. Hilbert's result replaced the Desargues configuration with the Pappus configuration. (See [41] for extensive discussion.)

Octonion division algebras are the prime examples of alternative division algebras, and they satisfy the Moufang identity. This led Moufang to the study of loops satisfying this and other related properties [34].

The equivalence of algebraic identities like those of Moufang and Bol with the existence of various geometric automorphisms, in turn equivalent to the closure of certain geometric figures (as discussed above) was an active topic of study in the first half of the last century. Reidermeister [42], Thomsen [46], Bol [3], and their collaborators worked on 3-nets (3-webs) of parallel classes of lines in the Euclidean plane. See also Bruck [5] and Pickert [41]. The geometric study has been revived more recently, particularly in the paper of Funk and P. Nagy [16] which describes in detail the relationships between Bol reflections on a 3-net (the dual of certain central automorphisms of the Latin square designs to be introduced in Section) and coordinatizing Bol loops. See also [24, 38].

3.2. Partial linear spaces with three points per line

We are particularly interested in partial linear spaces with exactly three points per line. In this case, the fixed point set of any automorphism is the point set of a subspace. A linear space with three points on each line is usually called a *Steiner triple system*. We call a partial linear space with exactly three points per line a *triple system*.

In the literature a point of a partial linear space is sometimes called *deep* if there is a proper subspace containing all of the lines on that point. We call $(\mathcal{P}, \mathcal{L})$ *shallow* if it has no deep points; that is, if the only subspace containing the lines through any given point is $(\mathcal{P}, \mathcal{L})$ itself. In particular all Steiner triple systems are shallow.

Proposition 3.3. *Let $(\mathcal{P}, \mathcal{L})$ be a shallow triple system. In $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$ there is at most one a-axis-free central automorphism τ_a with center a for each $a \in \mathcal{P}$. If τ_a exists then it has order 2 and is central in the stabilizer of a in $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$, and $\tau_a^g = \tau_{a^g}$ for all $g \in \mathrm{Aut}(\mathcal{P}, \mathcal{L})$.*

If τ_a and τ_b exist in $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$ with a and b collinear, then $\tau_a\tau_b$ has order 3 and $\langle \tau_a, \tau_b \rangle$ is isomorphic to $\mathrm{Sym}(3)$, the symmetric group of degree 3. The set of all points a for which τ_a exists is the point set of a subspace of $(\mathcal{P}, \mathcal{L})$.

Proof. If t_1 and t_2 are two a-axis-free central automorphisms of $(\mathcal{P}, \mathcal{L})$ with center a, then the automorphism $t = t_1 t_2$ of $(\mathcal{P}, \mathcal{L})$ is trivial on the points collinear with a. The fixed points of t form a subspace containing all these points, and as the space is shallow this subspace is the whole space. Therefore $t = 1$. We conclude that if there is an a-axis-free central automorphism with center a, then it is unique and has order 2.

For $g \in \mathrm{Aut}(\mathcal{P}, \mathcal{L})$, the conjugate τ_a^g is clearly an axis-free central automorphism of $(\mathcal{P}, \mathcal{L})$ with center a^g. Therefore by uniqueness $\tau_a^g = \tau_{a^g}$ and, especially, τ_a is in the center of the stabilizer of a in $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$.

In particular if $\{a, b, c\} \in \mathcal{L}$ and τ_a and τ_b are automorphisms, then

$$\tau_b\tau_a\tau_b = \tau_a^{\tau_b} = \tau_c = \tau_b^{\tau_a} = \tau_a\tau_b\tau_a$$

and therefore

$$(\tau_a\tau_b)^3 = (\tau_a\tau_b\tau_a)(\tau_b\tau_a\tau_b) = \tau_c^2 = 1.$$

Therefore $\langle \tau_a, \tau_b \rangle \simeq \mathrm{Sym}(3)$, and especially τ_c exists. □

The group Sym(3) is equally well the dihedral group of order 6, as the calculations above reveal. Dihedral groups and their generation properties form the backbone of Section 4.3 below and are discussed at length there.

Central automorphisms of triple systems first arose in the work of Hall [27]. There he showed that the Steiner triple systems admitting axis-free central automorphisms at each point are exactly the Steiner triple systems in which every set of three points lies in a subsytem (subspace) with exactly nine points – a copy of the affine plane over $\mathbb{F}_3$. Such Steiner triple systems are called *Hall triple systems*. Affine spaces of arbitrary dimension over $\mathbb{F}_3$ are examples, but he showed that others exist.

Central automorphisms of the affine plane over $\mathbb{F}_3$ must be axis-free, and so this holds for all Hall triple systems. By Proposition 3.3, the central automorphisms of Hall triple systems form a conjugacy class of elements of order 2 in the automorphism group with the property that any two have product of order 3. Groups of this type will be discussed at length in Section 4.3 below.

Hall found a Hall triple systems generated by four of its points that had 81 points, as opposed to the 27 points found in an affine space over $\mathbb{F}_3$ generated by four of its points. He did this by examining a presentation for a group generated by four elements of order 2, the putative central automorphisms, subject to relations forced by Proposition 3.3. Lemma 4.2 of [27] is equivalent to:

Lemma 3.4. *Let G be the group with presentation:*

Generators:
a, b, c, d;

Relations:
$a^2 = b^2 = c^2 = d^2 = 1$;
$(ab)^3 = (ac)^3 = (ad)^3 = (bc)^3 = (bd)^3 = (cd)^3 = 1$;
$(abac)^3 = (abad)^3 = (acad)^3 = (bcbd)^3 = 1$;
$(abacdc)^3 = (acabdb)^3 = (adabcb)^3 = 1$.

Then G has order $3^{10} \times 2$, and $a^G = \{a, b, c, d\}^G$ contains 81 elements of order two, the product of any two of these having order three. □

The center of the presented group G is elementary abelian of order 3^3, and $G/\mathrm{Z}(G)$ is a copy of the three generator Burnside group of exponent 3 and order 3^7, extended by an automorphism of order 2 inverting each generator. (See [26, Theorem 18.2.1].)

Soon after this, Bruck noticed [28] that Hall triple systems are equivalent to commutative Moufang loops of exponent 3. The 81 points of Hall's

example – the 81 elements of order two in the group of the proposition – naturally support the smallest such nonassociative loop.

At roughly the same time, Fischer [10] was studying the multiplication groups of distributive quasigroups and encountered exactly the same group theoretic problem that Hall did. (Again see Section 4.3.) Every distributive quasigroup is isotopic to a commutative Moufang loop [40, V.2.10].

Of course the elements of order 2 in Sym(3) are transpositions (2-cycles). Fischer began a program initially designed to characterize arbitrary symmetric groups by properties of their transposition class [11, 12]. This culminated in Fischer's definition and classification of 3-transposition groups.

A conjugacy class D of elements of order 2 in the group G is a class of 3-*transpositions* provided that, for $d, e \in D$, the order $|de|$ is always one of 1, 2, or 3. The case in which 2 never occurs is the one considered by Hall. The more general groups of Fischer still come from axis-free central automorphisms of certain triple systems. Buekenhout [6] called these *Fischer spaces*, and they are characterized by the axiom:

> every pair of intersecting lines sits in a subspace that is either an affine plane over $\mathbb{F}_3$ or a dual affine plane over $\mathbb{F}_2$.

Fischer spaces are always partial linear spaces but in general not linear spaces, since the dual affine plane over $\mathbb{F}_2$ consists of six points, each on two of its four lines. The Fischer spaces that are linear spaces are those in which only affine planes over $\mathbb{F}_3$ occur – these are precisely the Hall triple systems.

Fischer [13] characterized the finite groups that are generated by a conjugacy class of 3-transpositions and additionally have no nontrivial normal solvable subgroup. The groups studied by Hall do not occur, as they all have nontrivial normal 3-subgroups. Again the transpositions of the symmetric group (of degree at least 5) are the motivating examples, but there are others. In particular, the symmetry classes of orthogonal groups over $\mathbb{F}_2$ and $\mathbb{F}_3$ give two further infinite families of examples. In Fischer's theorem the groups of the conclusion fall into five infinite families (the three already mentioned, symplectic groups over $\mathbb{F}_2$, and unitary groups over $\mathbb{F}_4$) and five isolated examples. A particular special case of his result is

Theorem 3.5. *Let G be a finite group generated by the conjugacy class D of 3-transpositions. Assume that G has no nontrivial normal solvable subgroups and additionally that G' is* not *simple. Then G is isomorphic to either* $\mathrm{P}\Omega_8^+(2) \rtimes \mathrm{Sym}(3)$ *or* $\mathrm{P}\Omega_8^+(3) \rtimes \mathrm{Sym}(3)$. □

The author has studied groups generated by 3-transpositions extensively, particularly in work with Cuypers [8]. His interest was drawn to the conclusions of the previous theorem. These two groups are special cases of Cartan's triality groups [7] which come about as subgroups of automorphism groups of the Lie-type groups of type D_4 (that is, hyperbolic orthogonal groups in dimension 8).

Their study leads to the following definition, in the spirit of Fischer, of certain group generated by a conjugacy class of elements of order 2 for which the order of many (but not all) of the pair products is specified, indeed required to be 3.

Definition 3.6. Let D be a conjugacy class of elements of order two in the group $G = \langle D \rangle$, and let $\pi\colon G \longrightarrow \mathrm{Sym}(3)$ be a surjective group homomorphism. Further assume that

$$(*) \quad \text{for all } d, e \in D, \text{ if } \pi(d) \neq \pi(e), \text{ then } |de| = 3.$$

Then we say that (G, D, π) is a *group with triality* or *triality group*.

The primary examples here are Cartan's triality groups $\mathrm{P}\Omega_8^+(F) \rtimes \mathrm{Sym}(3)$, now defined over arbitrary fields F, not just those of order 2 and 3. But there are many other examples as well. For instance, the transposition class of every wreath product $H \wr \mathrm{Sym}(3)$ gives rise to a group with triality, as noted by Doro [9] and Zara [49].

Cartan observed a connection between his triality groups and the octonions. We shall learn that general groups with triality are related to Moufang loops. The wreath product example of the previous paragraph corresponds to the group H, groups being special examples of Moufang loops.

The original definition of abstract triality for groups, which is somewhat different from the one used here, was given by Doro [9] who had been motiviated by Glauberman's work on Moufang loops [17]. Tits [47] also considered an abstract version of Cartan's triality.

We shall see in the next section that, as is the case with 3-transposition groups, groups with triality arise as groups generated by central automorphism of certain triple systems.

3.3. Latin square designs

A *Latin square design* is a triple system (partial linear space with three points on each line) $(\mathcal{P}, \mathcal{L})$ with the property that "noncollinearity" is an

equivalence relation having exactly three equivalence classes, the *fibers* of the design. That is, $\mathcal{P} = O_R \uplus O_C \uplus O_E$ (disjoint union), and every line of $\mathcal{L}$ contains exactly one point from each fiber O_X for $X \in \{R, C, E\}$. Furthermore, for every pair of points x, y from different fibers, there is a unique line $\ell = \{x, y, z\} \in \mathcal{L}$.

By considering the lines through a fixed point we see that the three fibers have the same cardinality, the *order* of the Latin square design. Therefore for a set O of the appropriate cardinality, we can view the fibers as three subscripted copies of O. A Latin square design is degenerate precisely when it has order $|O| = 1$.

Again considering the lines through a fixed point, we see that a subspace (subdesign) containing all lines on a given point first contains the complement of that point's fiber and then contains that fiber as well. Therefore Latin square designs are always shallow. In particular, Proposition 3.3 on central automorphisms holds for every Latin square design.

As the fibers are the equivalence classes under noncollinearity, every automorphism must permute the set of fibers. A central automorphism τ_a of the Latin square design $(\mathcal{P}, \mathcal{L})$ switches the two fibers that complement the fiber O_X containing a. In particular, τ_a must be a-axis-free. Since every line of $\mathcal{L}$ contains two points of the complement to O_X, the permutation induced on the line set $\mathcal{L}$ by τ_a is uniquely determined. The existence question is then whether or not the action of τ_a can be defined on the remaining points of the fiber O_X to be consistent with this action on the lines.

A Latin square design is a *central Latin square design* if it admits a central automorphism at each of its points.

A basic observation is that quasigroups (and in particular Moufang loops) and groups with triality both lead naturally to Latin square designs.

Given the group with triality (G, D, π), we form a partial linear space $(\mathcal{P}, \mathcal{L}) = (G, D, \pi)\mathbf{C}$ with point set $\mathcal{P} = D$ and whose lines are the various triples of elements of D in a subgroup $S \simeq \mathrm{Sym}(3)$ generated by members of D and having $\pi(S) = \mathrm{Sym}(3)$. Then $(\mathcal{P}, \mathcal{L}) = (G, D, \pi)\mathbf{C}$ is a Latin square design whose fibers are the three sets

$$D \cap \pi^{-1}((2,3)), \quad D \cap \pi^{-1}((1,3)), \quad D \cap \pi^{-1}((1,2)).$$

G acts naturally by conjugation on $(\mathcal{P}, \mathcal{L})$, the kernel of the action being $Z(G)$, the center of G. The design $(\mathcal{P}, \mathcal{L}) = (G, D, \pi)\mathbf{C}$ is in fact a central Latin square design, since each element $d \in D$ acts canonically on $(\mathcal{P}, \mathcal{L})$ as the central automorphism τ_d with center d.

On the other hand, let $(\mathcal{P}, \mathcal{L})$ be a central Latin square design with $\mathcal{P} = O_R \uplus O_C \uplus O_E$. Set $D = \{ \tau_x \mid x \in \mathcal{P} \}$ and $G = \langle D \rangle$, a normal subgroup of $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$. Further define the homomorphism $\pi = \pi_{(\mathcal{P},\mathcal{L})} \colon G \longrightarrow \mathrm{Sym}(3)$ to extend the map

$$\tau_x \mapsto \begin{cases} (2,3) & \text{for } x \in O_R \\ (1,3) & \text{for } x \in O_C \\ (1,2) & \text{for } x \in O_E \end{cases}$$

Then $(G, D, \pi) = (\mathcal{P}, \mathcal{L})\mathbf{A}$ is a group with triality by Proposition 3.3.

It is reasonably clear that $(\mathcal{P}, \mathcal{L})\mathbf{AC}$ and $(\mathcal{P}, \mathcal{L})$ are isomorphic Latin square designs.

For the loop $L = (L, \cdot)$ we let $(\mathcal{P}, \mathcal{L}) = L\mathbf{T}$ be the Latin square design with point set $\mathcal{P} = L_R \uplus L_C \uplus L_E$ and line set $\mathcal{L}$ given by the Cayley table of L:

$$\{a_R, b_C, c_E\} \in \mathcal{L} \iff a \cdot b = c\,.$$

The autotopism group of L can be identified with the normal subgroup of automorphisms of $L\mathbf{T}$ that acts trivially on the set of fibers.

Unlike the situation above, every Latin square design is isomorphic to one constructed in this manner. Indeed there is a natural inverse map $\mathbf{S}$ to $\mathbf{T}$. Let $(\mathcal{P}, \mathcal{L})$ be a Latin square design with I a line of $\mathcal{L}$. We identify $(\mathcal{P}, \mathcal{L})$ with an isomorphic Latin square design by renaming the members of it point set $\mathcal{P} = O_R \uplus O_C \uplus O_E$. First relabel the elements of O_E as $L_E = \{ x_{\mathrm{E}} \mid x \in L \}$ for a set L (in bijection with O) with $1 \in L$ so that $1_E = I \cap L_E$. Next we let $I = \{1_R, 1_C, 1_E\}$ and, more generally, for each $x \in L$, rename the points $x_R \in L_R$ and $x_C \in L_C$ according to

$$\{x_R, 1_C, x_E\},\ \{1_R, x_C, x_E\} \in \mathcal{L}\,.$$

We can now define on L the structure $(L, \circ)$ whose binary operation is given by

$$\{x_R, y_C, (x \circ y)_E\} \in \mathcal{L}\,.$$

As $(\mathcal{P}, \mathcal{L})$ is a Latin square design, $(L, \circ)$ is in fact a loop with identity element 1. We set $(L, \circ) = (\mathcal{P}, \mathcal{L})\mathbf{S}$.

It is reasonably clear that $(\mathcal{P}, \mathcal{L})\mathbf{ST}$ and $(\mathcal{P}, \mathcal{L})$ are isomorphic Latin square designs, while $(L, \cdot)\mathbf{TS}$ and $(L, \cdot)$ are isotopic loops. In particular isomorphic Latin square designs correspond to isotopic loops.

We see here how Latin square designs get their name. If we use the same set L to label the rows and columns and to serve as entries in a Latin

square, then the triple $\{x_R, y_C, z_E\}$ in the corresponding Latin square design indicates that the entry in the row x, column y position of the square is z. Every Latin square design can be thought of as coming from a Latin square in this fashion.

The dual of a Latin square design is a 3-*net* (sometimes 3-*web*). This was the preferred realm for Bol [3] and others. In this context, the members of $\mathcal{L}$ can be thought of as the points of a configuration within a 3-space L^3 "coordinatized" by L. The line set of the 3-net is naturally partitioned into three parallel classes of lines given by the fibers. In this dual world of 3-nets, a central automorphism is usually called a *Bol reflection* [16]. The action of a putative Bol reflection on the points of the 3-net (that is, the lines of $\mathcal{L}$) is evident, and the question is whether or not this induces a permutation of the lines of the 3-net (the points of $\mathcal{P}$).

Every Latin square design can be realized as $(L, \cdot)\mathbf{T}$ for some loop. Following the theorems of Section 3.1, we can consider how the existence of central automorphisms/Bol reflections is related to algebraic properties of the coordinatizing loop.

3.4. Central automorphisms of Latin square designs

Much of the material of the present section was discussed at length in the earlier paper [22]. The treatment here is therefore abbreviated, with many of the results and proofs taken from [22] (sometimes in a slightly modified form).

To simplify notation, for each $a \in L$ we will write ρ_a in place of τ_{a_R}; κ_a in place of τ_{a_C}; and ϵ_a in place of τ_{a_E}. (This notation indicates that the central automorphism has center corresponding to, respectively, a row, column, or entry of the associated Latin square.)

Lemma 3.7.

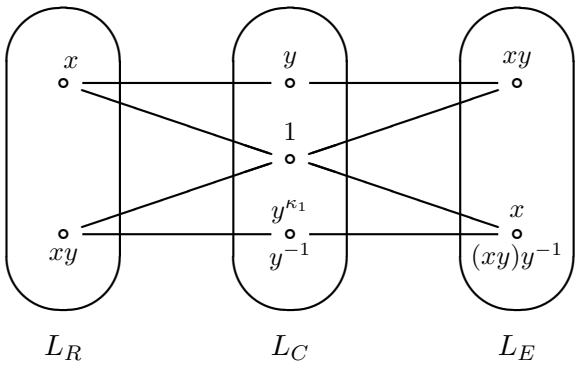
(*a*) $\kappa_1 \in \mathrm{Aut}(L\mathbf{T})$ *if and only if* L *has the right inverse property* $(xy)({}^{-1}y) = x$ *for all* $x, y \in L$. *In this case inverses are two-sided and* $x_C^{\kappa_1} = x_C^{-1}$.

(*b*) $\rho_1 \in \mathrm{Aut}(L\mathbf{T})$ *if and only if* L *has the left inverse property* $x^{-1}(xy) = y$ *for all* $x, y \in L$. *In this case inverses are two-sided and* $x_R^{\rho_1} = x_R^{-1}$.

(*c*) $\epsilon_1 \in \mathrm{Aut}(L\mathbf{T})$ *if and only if* L *has the anti-automorphic inverse property* $(xy)^{-1} = y^{-1}x^{-1}$ *for all* $x, y \in L$. *In this case inverses are two-sided and* $x_E^{\epsilon_1} = x_E^{-1}$.

Proof. We prove (a); the other parts are equivalent to (a) in suitable conjugates of the loop L.

Assume that κ_1 is an automorphism of $L\mathbf{T}$, and let $x, y \in L$. The two lines $\{x_R, 1_C, x_E\}$ and $\{xy_R, 1_C, xy_E\}$ are mapped to themselves by κ_1.



The image of the line $\{x_R, y_C, xy_E\}$ under κ_1 is then the line

$$\{x_R^{\kappa_1}, y_C^{\kappa_1}, xy_E^{\kappa_1}\} = \{x_E, y_C^{\kappa_1}, xy_R\} = \{xy_R, y_C^{\kappa_1}, x_E\}\,.$$

In the special case $x = 1$, this line is $\{y_R, y_C^{\kappa_1}, 1_E\}$. As $\{y_R, ({}^{-1}y)_C, 1_E\}$ is always a line, we must have $y_C^{\kappa_1} = ({}^{-1}y)_C$. Repeating this twice we find $y_C = y_C^{\kappa_1\kappa_1} = ({}^{-1}({}^{-1}y))_C$. In particular $y = {}^{-1}({}^{-1}y)$, so inverses are two-sided.

Therefore in the general case the image line becomes $\{xy_R, y_C^{-1}, x_E\}$. But $\{xy_R, y_C^{-1}, (xy)y_E^{-1}\}$ is certainly a line of $\mathcal{L}$. We conclude that $x = (xy)y^{-1}$, the right inverse property.

Now assume that L has the right inverse property. In particular, inverses are two-sided (as seen in Section 2). The line $\{x_R, y_C, xy_E\}$ is generic in $\mathcal{L}$, and the picture above shows that its image under κ_1 is also a line (with the image of y_C under κ_1 defined to be y_C^{-1}). Therefore this κ_1 is a central automorphism of $L\mathbf{T}$. □

In particular, if ρ_1 and κ_1 are automorphisms, then so is $\epsilon_1 \in \langle \rho_1, \kappa_1 \rangle \simeq \mathrm{Sym}(3)$ (by Proposition 3.3 or direct calculation). Since Sym(3) is generated by any two of its elements of order 2, any two of the properties discussed in the lemma guarantee the third. Especially the loop is an inverse property loop.

A calculation (see [22, Prop. 3.3]) similar to that of the previous lemma gives

Proposition 3.8. *Let L be a loop with $\kappa_1 \in \mathrm{Aut}(L\mathbf{T})$. Then, for the element x of L, we have $\kappa_x \in \mathrm{Aut}(L\mathbf{T})$ if and only if we have*

$$a((xb)x) = ((ax)b)x$$

for all a, b in L. In this case $y_C^{\kappa_x} = (xy^{-1})x_C$ for all y in L. □

Therefore we immediately have

Theorem 3.9. *The loop L is a Bol loop if and only if $\kappa_x \in \mathrm{Aut}(L\mathbf{T})$ for all x of L.* □

Recall our convention that Bol loops are right Bol loops.

Isotopic loops correspond to isomorphic Latin square designs, hence we also have the following well-known result (see [40, IV.6.15]).

Theorem 3.10. *All loop isotopes of a Bol loop are Bol loops.* □

For x in the loop L, define powers of x recursively by

$$x^0 = 1, \quad x^n = (x^{n-1})x, \text{ and } x^{-n} = (x^{-1})^n \text{ for } n \in \mathbb{Z}^+ .$$

The *order* of x, written $|x|$, is the smallest positive integer n (if any) with $x^n = 1$. Otherwise x has infinite order.

The following lemma will be important later, so we repeat its proof from [22, Lemma 3.9].

Lemma 3.11. *Let L be a loop with $\kappa_1, \kappa_x \in \mathrm{Aut}(L\mathbf{T})$ for some x of L.*

(*a*) *For arbitrary $a \in L$ and integers i, j, we have $(ax^i)(x^j) = ax^{i+j}$. In particular $x^{i+j} = x^i x^j$ and $(x^i)^{-1} = (x^{-1})^i$.*

(*b*) *$\kappa_{x^n} \in \mathrm{Aut}(L\mathbf{T})$ and $(\kappa_x\kappa_1)^n = \kappa_{x^n}\kappa_1$. In particular $|x| = |\kappa_x\kappa_1|$.*

Proof. By Lemma 3.7 inverses are two-sided.
(*a*) We show that (*a*) follows from (*b*) (indeed from (*b*) with $n \in \{i, j, i+j\}$). For arbitrary z with $\kappa_z \in \mathrm{Aut}(L\mathbf{T})$ and arbitrary $a \in L$, we have

$$(a_R)^{\kappa_z\kappa_1} = (az_E)^{\kappa_1} = az_R .$$

Therefore

$$(ax^{i+j})_R = a_R^{\kappa_{x^{i+j}}\kappa_1} = a_R^{(\kappa_x\kappa_1)^{i+j}} = a_R^{(\kappa_x\kappa_1)^i(\kappa_x\kappa_1)^j} = a_R^{(\kappa_{x^i}\kappa_1)(\kappa_{x^j}\kappa_1)} = ((ax^i)x^j)_R ,$$

as claimed.
(*b*) For $\kappa_z \in \mathrm{Aut}(L\mathbf{T})$ and arbitrary $y \in L$ we have $y_C^{\kappa_z} = (zy^{-1})z_C$ by Proposition 3.8. Therefore if $\kappa_y \in \mathrm{Aut}(L\mathbf{T})$ then by Proposition 3.3 $\kappa_z\kappa_y\kappa_z = \kappa_{(zy^{-1})z}$. In particular $\kappa_1\kappa_y\kappa_1 = \kappa_{y^{-1}}$ and $(\kappa_y\kappa_1)^{-1} = \kappa_1\kappa_y = \kappa_{y^{-1}}\kappa_1$, so (*b*) for negative n follows from (*b*) for positive $-n$.

We prove $\kappa_{x^n} \in \mathrm{Aut}(L\mathbf{T})$ and $(\kappa_x\kappa_1)^n = \kappa_{x^n}\kappa_1$ for nonnegative n by induction, the result being clear for $n = 0, 1$. Let $n \geqslant 1$ and assume the result for $0 \leqslant k \leqslant n$. Using the previous paragraph, induction, and (*a*) with $\{i, j\} = \{1, n-1\}$, we find

$$\begin{aligned}
\kappa_{x^{n+1}}\kappa_1 &= \kappa_{x^n x}\kappa_1 \\
&= \kappa_{(xx^{n-1})x}\kappa_1 \\
&= \kappa_x\kappa_{(x^{n-1})^{-1}}\kappa_x\kappa_1 \\
&= \kappa_x\kappa_1\kappa_{x^{n-1}}\kappa_1\kappa_x\kappa_1 \\
&= \kappa_x\kappa_1(\kappa_x\kappa_1)^{n-1}\kappa_x\kappa_1 \\
&= (\kappa_x\kappa_1)^{n+1},
\end{aligned}$$

as desired. As κ_x and κ_1 are in $\mathrm{Aut}(L\mathbf{T})$, so is $\kappa_{x^{n+1}} = (\kappa_x\kappa_1)^{n+1}\kappa_1$. □

We have two well-known results (see [40, IV.6.6] and [15, Prop. 6.1]).

Corollary 3.12. *Bol loops are power associative.* □

Corollary 3.13. *In a Bol loop of finite order, the order of every element divides the order of the loop.*

Proof. In a power associative loop, the powers of the element x form a cyclic subgroup X of order $|x|$. By the first part of the lemma, the cosets aX all have size $|x|$ and partition the loop. □

Another calculation (see now [22, Prop. 3.11]) similar to that of Lemma 3.7 leads to

Proposition 3.14. *Let L be an inverse property loop. Then, for the element x of L, we have $\epsilon_x \in \mathrm{Aut}(L\mathbf{T})$ if and only if we have*

$$(xa)(bx) = x((ab)x)$$

for all a, b in L. In this case $(xy)x = x(yx)$ and $y_E^{\epsilon_x} = x(y^{-1}x)_E$, for all y in L. □

Moufang loops are inverse property loops ([40, IV.1.4]). Therefore we get a fundamental characterization of Moufang loops (see [22, Theorem 3.13]).

Theorem 3.15. *The loop L is a Moufang loop if and only if the Latin square design $L\mathbf{T}$ admits a central automorphism with center p, for each of its points p.* □

Central automorphisms lead to elements of the autotopism group of the associated loop. In proving Lemma 3.11 we observed

$$a_R^{\kappa_z\kappa_1} = (az)_R = a_R^{\mathrm{R}(z)}\,.$$

That is, $\kappa_z\kappa_1$ acts as $\mathrm{R}(z)$ on L_R. Similar calculations lead to part (a) of the next proposition. Part (b) then follows by applying (a) in the opposite loop.

Proposition 3.16. *Let L be a loop.*

(a) *If $\kappa_1, \kappa_z \in \mathrm{Aut}(L\mathbf{T})$ for some z of L, then*

$$\kappa_1\kappa_z = (\,\mathrm{R}(z^{-1}),\, \mathrm{L}(z)\mathrm{R}(z),\, \mathrm{R}(z)) \in \mathrm{Sym}(L_R) \times \mathrm{Sym}(L_C) \times \mathrm{Sym}(L_E)\,.$$

(b) *If $\rho_1, \rho_z \in \mathrm{Aut}(L\mathbf{T})$ for some z of L, then*

$$\rho_1\rho_z = (\,\mathrm{R}(z)\mathrm{L}(z),\, \mathrm{L}(z^{-1}),\, \mathrm{L}(z)) \in \mathrm{Sym}(L_R)\times\mathrm{Sym}(L_C)\times\mathrm{Sym}(L_E).$$ □

We thus have

Theorem 3.17.

(a) *If L is a Bol loop, then the $L\mathbf{T}$-automorphism group*

$$\langle\, \kappa_1\kappa_z \mid z \in L \,\rangle = \langle\, \kappa_x\kappa_y \mid x, y \in L \,\rangle$$

is an autotopism group that induces $\mathrm{RMult}(L)$ *on the fibers L_R and L_E.*

(b) *If L is a Moufang loop, then the $L\mathbf{T}$-automorphism group*

$$\langle\, \rho_x\rho_y,\, \kappa_x\kappa_y \mid x, y \in L \,\rangle = \langle\, \rho_x\rho_y,\, \kappa_x\kappa_y,\, \epsilon_x\epsilon_y \mid x, y \in L \,\rangle$$

is an autotopism group of that induces $\mathrm{Mult}(L)$ *on each of the fibers L_R, L_C, and L_E.* □

This theorem (phrased in the dual language of 3-nets and their Bol reflections) was one of the main results of Funk and Nagy [16]. They went on to explore many of its consequences, particularly for Bol loops.

4. Some categories and category equivalence

A detailed treatment of the material presented in this section will appear in [23]. The categorical basics can be found in [29].

4.1. Some categories

4.1.1. Loops

We let Loop be the category whose object class consists of all loops, the set $\mathrm{Hom}_{\mathsf{Loop}}(A, B)$ being that of all homotopisms from the loop A to the loop B. The category Mouf is the full subcategory of Loop that consists of all Moufang loops.

4.1.2. Latin square designs

We define the category LSD whose object class consists of all Latin square designs. If $(\mathcal{P}, \mathcal{L})$ and $(\mathcal{P}', \mathcal{L}')$ are Latin square designs ($\mathcal{P} = O_R \uplus O_C \uplus O_E$ and $\mathcal{P}' = O'_R \uplus O'_C \uplus O'_E$), then $f = (\alpha, \beta, \gamma) \in \mathrm{Hom}_{\mathsf{LSD}}((\mathcal{P}, \mathcal{L}), (\mathcal{P}', \mathcal{L}'))$ is a triple of maps

$$\alpha\colon O_R \longrightarrow O'_R\,, \quad \beta\colon O_C \longrightarrow O'_C\,, \quad \gamma\colon O_E \longrightarrow O'_E$$

with the property:

if (x, y, z) is a line of $\mathcal{L}$, then $(x, y, z)^f = (x^\alpha, y^\beta, z^\gamma)$ is a line of $\mathcal{L}_0$.

In particular the set $(O_R)^\alpha \cup (O_C)^\beta \cup (O_E)^\gamma$ carries a Latin square subdesign of $(\mathcal{P}', \mathcal{L}')$. If any of α, β, or γ are injections then they all are; in this case we say that f is *injective*.

Let CLSD be the full subcategory of LSD consisting of the central Latin square designs, those Latin square designs that admit a central automorphism at every point.

In these categories the morphisms are required to respect the fiber names: "rows" are mapped to "rows" and so forth. In particular, central automorphisms of $(\mathcal{P}, \mathcal{L})$ are not in the category automorphism group $\mathrm{Aut}_{\mathsf{LSD}}(\mathcal{P}, \mathcal{L})$ as they interchange two fibers. Indeed for a central Latin square design, the automorphism group $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$ induces the full $\mathrm{Sym}(3)$ on the set of fibers, and we have $\mathrm{Aut}(\mathcal{P}, \mathcal{L}) = \mathrm{Aut}_{\mathsf{CLSD}}(\mathcal{P}, \mathcal{L}) \rtimes I$, where $I = \langle \tau_x, \tau_y \rangle \simeq \mathrm{Sym}(3)$, for any x and y from different fibers.

4.1.3. Groups with triality

If (G, D, π) and (G_0, D_0, π_0) are two groups with triality, then a *triality homomorphism* $f\colon (G, D, \pi) \longrightarrow (G_0, D_0, \pi_0)$ is a group homomorphism

$f\colon G \longrightarrow G_0$ that additionally has $D^f \subseteq D_0$ and $\pi = f\pi_0$. We then have the category TriGrp whose object class is all groups with triality and whose morphisms are the triality homomorphisms.

The kernel of the triality homomorphism f is a normal subgroup N of G that is contained in $\ker\pi$. Conversely, for any such normal subgroup N, the quotient $\bar{G} = G/N$ has a natural structure $(\bar{G}, \bar{D}, \bar{\pi})$ as group with triality.

4.1.4. Terminal objects and pointed categories

A *terminal object* in the category C is an object I for which $\mathrm{Hom}_{\mathsf{C}}(A, I)$ has cardinality 1 for every object A. A *initial object* has the same requirement with the roles of A and I reversed, and a *zero object* is one that is both terminal and initial. In all three cases, if such an object exists then it is unique up to isomorphism in C.

Each of our categories Loop, Mouf, LSD, CLSD, and TriGrp has terminal objects. In the first four cases, these are just the objects of order 1. In TriGrp the group with triality $(\mathrm{Sym}(3), \{(2,3),(1,3),(1,2)\}, \mathrm{Id}_{\mathrm{Sym}(3)})$ is a terminal object.

There is a uniform technique for promoting a terminal object in a category to zero object status in a new category: replace C with the *pointed category* $\mathsf{C}^\star$, whose objects are all pairs (A, a) for A an object of C and a a C-morphism from the terminal object I to A. Morphisms in $\mathsf{C}^\star$ are then defined in terms of appropriate commutative diagrams from C.

For $\mathsf{LSD}^\star$ and $\mathsf{CLSD}^\star$ this amounts to choosing particular lines of the designs and then requiring morphisms to respect these special lines. For $\mathsf{TriGrp}^\star$ we similarly choose and respect special subgroups $I \simeq \mathrm{Sym}(3)$. In a sense made specific in [23], Doro's approach to abstract triality [9] is focused on the category $\mathsf{TriGrp}^\star$ rather than our focal point TriGrp.

Something similar happens for the two loop categories, but it is better (and equivalent) to think of the two pointed categories $\mathsf{Loop}^\star$ and $\mathsf{Mouf}^\star$ as having the same object classes as Loop and Mouf but allowing as morphisms only loop homomorphisms.

4.2. Category equivalence

The maps **T** and **S** that were introduced in Section above are in fact functors between the appropriate categories, once their natural action on morphisms has been noted. By Theorem 3.15 these functors, which connect the two categories Loop and LSD, restrict to functors between Mouf and CLSD. The discussion of Section 3.3 can be formalized to produce

Theorem 4.1. *The pair* $(\mathbf{T}, \mathbf{S})$ *gives a category equivalence of* Loop *and* LSD *that restricts to a category equivalence of* Mouf *and* CLSD. □

That is, in a precise way, loops and Latin square designs are the same thing, an observation we have already made loosely. Similarly Moufang loops and central Latin square designs are the same thing – this is the essential content of Theorem 3.15.

The two other maps defined in Section 3.3 connect central Latin square designs and groups with triality, as indicated:

$$\mathsf{Mouf} \underset{\mathbf{S}}{\overset{\mathbf{T}}{\rightleftarrows}} \mathsf{CLSD} \underset{\mathbf{C}}{\overset{\mathbf{A}}{\rightleftarrows}} \mathsf{TriGrp}$$

Unfortunately the pair $(\mathbf{A}, \mathbf{C})$ does not give a category equivalence, despite the fact that $\mathbf{AC}$ takes central Latin square designs to isomorphic designs, as was observed.

The difficulty is two-fold – the category TriGrp is too large and the map $\mathbf{A}$ is not a functor – but both difficulties have the same source: proper treatment of the centers of groups with triality.

As a group with triality is defined in terms of its action by conjugation on one of its conjugacy classes, the center of the group is relatively hidden. The groups $(\mathcal{P}, \mathcal{L})\mathbf{A}$ have trivial center, since any automorphism that commutes with the central automorphism τ_p must fix the center p. All groups with triality in the image of $\mathbf{A}$ have trivial center, whereas to guarantee that morphisms behave properly, when moved from CLSD to TriGrp, we must admit triality groups with nontrivial center.

The answer is to restrict to triality groups with centers as large as possible and to replace the map $\mathbf{A}$ with a functor $\mathbf{B}$ whose object images are in the corresponding subclass of groups with triality. Two similar group presentations accomplish this.

Presentation 4.2. *For a group with triality* (G, D, π)*, the group* G^{U} *has the following presentation:*

Generators:
$\tilde{d}$*, for arbitrary* $d \in D$*;*

Relations:
for arbitrary $d, e \in D$ *with* $d^\pi \neq e^\pi$*:*
(1) $\tilde{d}^2 = 1$*;*
(2) $\tilde{d}\tilde{e}\tilde{d} = \widetilde{ded}$.

In this situation we set $D^{\mathrm{U}} = \{\, \tilde{d} \mid d \in D \,\}$ and $\pi^{\mathrm{U}}(\tilde{d}) = \pi(d)$.

Theorem 4.3.

(a) *For a group with triality* (G, D, π) *the triple* $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ *is also a group with triality.*

(b) *There is a surjective triality homomorphism* ζ *from* $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ *to* (G, D, π) *whose kernel is central in* G^{U}. *If* φ *is a surjective triality homomorphism from* (G_0, D_0, π_0) *to* (G, D, π) *with* $\ker\varphi$ *central in* G_0, *then* ζ *factors through* φ; *that is, there is a unique triality homomorphism* η *from* $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ *to* (G_0, D_0, π_0) *with* $\zeta = \eta\varphi$. □

This is not a surprise: in the presentation, the various $\tilde{d}$ are legislated to form a generating class of elements of order 2, subject only to those relations (all conjugations) that reveal (G, D, π) as a group with triality.

Part (*b*) of the theorem says that the group with triality $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ is a universal central extension of (G, D, π) in the category of groups with triality. (The concepts "surjective" and "central kernel" are not categorical but can be made so in this context [23].) This is particularly satisfying since, in the category of groups, only perfect groups H possess universal central extensions [1, (33.4)]. Existence for the perfect group H is proven via a presentation that encodes the full Cayley table of H. Here we only need to encode the transform table for the conjugacy class D of (G, D, π), so the presentation is simpler and the construction works in all cases.

Accordingly, we call $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}})$ a *universal* group with triality, and we let $\mathsf{UTriGrp}$ be the full subcategory of TriGrp consisting of all universal groups. Set $(G^{\mathrm{U}}, D^{\mathrm{U}}, \pi^{\mathrm{U}}) = (G, D, \pi)\mathbf{U}$. Then the map $\mathbf{U}$ is a functor from TriGrp to its universal subcategory $\mathsf{UTriGrp}$.

Presentation 4.4. *For the Latin square design* $(\mathcal{P}, \mathcal{L})$ *in* CLSD, *the group* $\mathrm{G}_{(\mathcal{P},\mathcal{L})}$ *has the following presentation:*

Generators:
$\tilde{p}$, *for arbitrary* $p \in \mathcal{P}$;
Relations:
for arbitrary $p \in \mathcal{P}$ *and* $\{p, q, r\} \in \mathcal{L}$:
(1) $\tilde{p}^2 = 1$;
(2) $\tilde{p}\tilde{q}\tilde{p} = \tilde{r}$.

In this situation we set $\tilde{\mathcal{P}} = \{\, \tilde{p} \mid p \in \mathcal{P} \,\}$ and $\pi_{(\mathcal{P},\mathcal{L})}(\tilde{p}) = \pi_{(\mathcal{P},\mathcal{L})}(p)$.

The triple $(\mathrm{G}_{(\mathcal{P},\mathcal{L})}, \tilde{\mathcal{P}}, \pi_{(\mathcal{P},\mathcal{L})})$ is another group with triality that is universal. Indeed it is reasonably clear that $\mathbf{U} = \mathbf{CB}$ for the functor $\mathbf{B}$ given by $(\mathcal{P}, \mathcal{L})\mathbf{B} = (\mathrm{G}_{(\mathcal{P},\mathcal{L})}, \tilde{\mathcal{P}}, \pi_{(\mathcal{P},\mathcal{L})})$.

Now

$$\mathsf{Mouf} \underset{\mathbf{S}}{\overset{\mathbf{T}}{\rightleftarrows}} \mathsf{CLSD} \underset{\mathbf{C}}{\overset{\mathbf{B}}{\rightleftarrows}} \mathsf{UTriGrp}$$

gives the equivalences needed for a proof of:

Theorem 4.5. *The categories* Mouf, CLSD, *and* UTriGrp *are equivalent.* □

This in turn leads to the equivalence of the corresponding pointed categories Mouf*, CLSD*, and UTriGrp*.

The distinction between the categories TriGrp and UTriGrp is important. These two categories are not equivalent [23], so the category TriGrp is not equivalent to either Mouf or CLSD.

4.3. Monics and simplicity

The morphism $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ is called *monic* if it is right cancellable:

$$\text{for all } Z \text{ and } g_1, g_2 \in \mathrm{Hom}_{\mathsf{C}}(Z, A),\ g_1 f = g_2 f \implies g_1 = g_2\,.$$

Category equivalences take monic morphisms to monic morphisms.

Monic maps are the categorical counterparts of injective maps. In several of our categories, monic maps behave as expected.

Lemma 4.6. *In* Mouf, Mouf*, CLSD, *and* CLSD* *a morphism is monic if and only if it is injective on the appropriate underlying set.* □

In the triality categories things are slightly more subtle.

Lemma 4.7. *In* TriGrp *and* TriGrp* *a triality homomorphism from G is monic if and only if its kernel is central in G.* □

There seems to be no accepted definition for simplicity of an object in a general category. In a category with terminal objects we say that a morphism is *trivial* if it factors through a terminal object. Then we say that a nonterminal object is *simple* if every morphism from it is either monic or trivial. Category equivalences take simple objects to simple objects.

Recall from Section 2 that the subloop M of the loop L is normal if there is a loop homomorphism with kernel M, and the nonidentity loop L is simple if its only normal subloops are the identity and itself.

Proposition 4.8. *Let L be a Moufang loop. The following are equivalent:*

(1) *L is simple in* Mouf.

(2) *L is simple in* Mouf*.

(3) *L is simple.* □

The group with triality (G, D, π) with $G \not\cong \mathrm{Sym}(3)$ is *triality quasisimple* provided the only normal subgroups of G properly contained in $\ker\pi$ are the subgroups of $\mathrm{Z}(G)$. Similarly (G, D, π) is *triality simple* provided it is triality quasisimple with $\mathrm{Z}(G) = 1$.

Proposition 4.9. *Let (G, D, π) be a group with triality in* UTriGrp. *Let $(\bar{G}, \bar{D}, \bar{\pi})$ be the associated group with triality for $\bar{G} = G/\mathrm{Z}(G)$. The following are equivalent:*

(1) *(G, D, π) is simple in* UTriGrp.

(2) *(G, D, π) is simple in* TriGrp.

(3) *(G, D, π) is triality quasisimple.*

(4) *$(\bar{G}, \bar{D}, \bar{\pi})$ is triality simple.* □

5. Z*-theorems

In the group G the largest normal subgroup of odd order is denoted $\mathrm{O}(G)$, and then $\mathrm{Z}^*(G)$ is the preimage in G of $\mathrm{Z}(G/\mathrm{O}(G))$. If p is a prime, then $\mathrm{O}_p(G)$ is the largest normal p-group in G, and $\mathrm{Z}_p^*(G)$ is the preimage in G of $\mathrm{Z}(G/\mathrm{O}_p(G))$.

We present three related results, all stating that a given element of order 2 is in $\mathrm{Z}^*(G)$.

5.1. Dihedral groups

In a group an *involution* is an element of order 2.

We start with one of the most important results in finite group theory:

Lemma 5.1. *Two involutions s, t generate a dihedral group $T = \langle s, t\rangle$ with normal cyclic subgroup $N = \langle st\rangle$ of index 2.* □

We will need more detailed structure.

Lemma 5.2. *Continue as in Lemma* 5.1.

(a) $s^T = s^N$ *and* $t^T = t^N$; $T \setminus N = s^T \cup t^T$ *is composed of involutions, each of which inverts* N; *that is, for* $a \in T \setminus N$ *and* $x \in N$, $a^{-1}xa = axa = x^{-1}$.

(b) *If* $|N| = n$ *is odd, then* $T \setminus N = s^T = t^T$. *In particular,* s *and* t *are conjugate in* T.

(c) *If* $|N|$ *is not odd, then* $T \setminus N = s^T \uplus t^T$ *is the disjoint union of* s^T *and* t^T, *and* T *contains exactly two dihedral subgroups of index* 2, *namely* $\langle (st)^2 \rangle \cup s^T$ *and* $\langle (st)^2 \rangle \cup t^T$.

(d) *If* $|N| = 2m$ *with* m *odd, then for each* $x \in t^T$, $C_T(x) = \{1, x, a, ax\} \simeq \mathrm{Z}_2 \times \mathrm{Z}_2$ *with* $a \in s^T$ *and* $\mathrm{Z}(T) = \langle ax \rangle \simeq \mathrm{Z}_2$.

Note that in Lemma 5.2(c) we allow the possibility that N is an infinite cyclic subgroup.

5.2. The Z*-theorems

Consider the following hypotheses:

(G) D is a conjugacy class of involutions in the finite group G such that $|de|$ is odd, for all $d, e \in D$.

(F_p) D is a conjugacy class of involutions in the finite group G such that $|de|$ is a power of the odd prime p, for all $d, e \in D$.

We then have:

Theorem 5.3. (Glauberman's Z*-theorem, 1966)
Under (G) *we have* $D \subset \mathrm{O}(G)\langle d \rangle \leqslant \mathrm{Z}^*(G)$ *for any* $d \in D$. □

Theorem 5.4. (Fischer's Z*-theorem, 1964)
Under (F_p) *we have* $D \subset \mathrm{O}_p(G)\langle d \rangle \leqslant \mathrm{Z}_p^*(G)$ *for any* $d \in D$. □

Theorem 5.5. (Bruck-Hall Z*-theorem, 1960/1965)
Under (F_3) *we have* $D \subset \mathrm{O}_3(G)\langle d \rangle \leqslant \mathrm{Z}_3^*(G)$ *for any* $d \in D$. □

Glauberman's Z*-theorem [18] originated with his work on the solvability of Moufang loops of odd order and later became a crucial tool in the classification of finite simple groups.

Fischer's Z*-theorem [10], particularly in the case $p = 3$, was an important step in his proof that the multiplication group of a distributive quasigroup is solvable. This led to his work on 3-transposition groups [13], which was also a critical part of the classification of finite simple groups.

The Bruck-Hall Z*-theorem [28] was motivated by Hall's work on Steiner triple systems admitting axis-free central automorphisms at each point [27]. Bruck pointed out that the problem was equivalent to that of commutative Moufang loops of exponent 3 and as such was a consequence of his (and Slaby's) work in [5].

Clearly the Bruck-Hall theorem is contained in Fischer's. Also Fischer's theorem is an easy consequence of Glauberman's. (See Remark 5.14 below.) We separate them in this way not just for historical reasons but also because the level of difficulty varies. Glauberman's theorem, the newest of the three, is the hardest to prove, while the Bruck-Hall theorem, in some sense the oldest, is the easiest to prove.

Glauberman's original proof of the Z*-theorem is still the only known proof and makes elegant use of the modular representation theory of finite groups. The Hall-Bruck theorem admits a totally elementary proof, needing only Hall's Lemma 3.4 above and the group theoretic "Baer's Lemma" [31, 6.76]. (See [20] for the details of this argument.)

Fischer's theorem is nearly elementary. The only nonelementary result he requires is also needed by Glauberman.

Theorem 5.6. (Brauer-Suzuki Theorem, 1959 [4, 19])
A finite group G with generalized quaternion Sylow 2-subgroups has a unique conjugacy class of involutions D. For this class the hypothesis (G) *is valid and Theorem* 5.3 *holds.* □

Brauer and Suzuki's proof (as augmented by Glauberman) was the seminal example of the method of exceptional characters in ordinary representation theory.

5.3. Fischer's Z*-theorem

We present a complete (modulo the Brauer-Suzuki Theorem 5.6) and somewhat streamlined version of Fischer's original proof of Theorem 5.4. In certain parts of the argument, only the weaker hypothesis (G) of Glauberman is used.

Various of the intermediate results are true for infinite groups as well, but the ultimate result requires counting and so there is little insight into the infinite case.

Theorem 5.7. *Let D be the unique class of involutions in the group G. Under* (G) *Theorem* 5.3 *holds. Under* (F_p)*, additionally $|D|$ is a power of the prime p.*

Proof. Let S be a Sylow 2-subgroup of G. Under (G), $D \cap S$ contains exactly one element. As D is the only class of involutions in G, the 2-group S contains a unique involution. It well known (see, for instance, [31, 5.3.7]) that such a finite 2-group is either cyclic or generalized quaternion.

In any finite group with cyclic Sylow 2-subgroup $S = \langle s \rangle$, the element s acts as an odd permutation in the permutation representation of G on the cosets of S. Therefore G has a normal subgroup of index 2, and by induction $G = \mathrm{O}(G)S$. In particular $D \subset \mathrm{O}(G)\langle d \rangle$, as required for Theorem 5.3.

If S is generalized quaternion, then $D \subset \mathrm{O}(G)\langle d \rangle$ by the Brauer-Suzuki Theorem 5.6.

Now assume that $D \subset \mathrm{O}(G)\langle d \rangle = H$ and that (F_p) holds. Let R be a Sylow r-subgroup of $\mathrm{O}(G)$ and H, for some odd $r \neq p$. Then by Sylow's Theorem $|H\colon \mathrm{N}_H(R)| = |\mathrm{O}(G)\colon \mathrm{N}_{\mathrm{O}(G)}(R)|$ is the number of Sylow r-subgroups in H and $\mathrm{O}(G)$. As H is twice as big as $\mathrm{O}(G)$, also $\mathrm{N}_H(R)$ is twice as big as $\mathrm{N}_{\mathrm{O}(G)}(R)$; that is, it has even order and so contains a conjugate d^g of d (again by Sylow's Theorem). Replacing R by $R^{g^{-1}}$, we have a Sylow r-subgroup R that is invariant under d. For $x \in R$, $x^{-1}x^d = d^x d$ is in R and is a product of two elements of D. By (F_p), we must have $d^x d = 1$. That is, $d^x = d$ and x commutes with d. We conclude that R commutes with d.

We now know that $|\mathrm{C}_H(d)|$ is divisible by the p'-part of $|\mathrm{O}(G)|$. That is, $|D| = |H\colon \mathrm{C}_H(d)|$ is a power of p. □

Theorem 5.8. *Under* (G)*, for x an involution of G we have*

$$D = \biguplus_{a \in \mathrm{C}_D(x)} \mathrm{C}_D(ax)\,.$$

That is, D is the disjoint union of the subsets of D commuting with the various involutions ax, as a runs through the set of all elements of D that commute with x.

Proof. If $x \in D$, then $\mathrm{C}_D(x) = \{x\}$ (by (G)) and $\mathrm{C}_D(xx) = \mathrm{C}_D(1) = D$. Therefore we may assume that $x \notin D$.

For each $d \in D$, the subgroup $T = \langle d, x \rangle$ is dihedral. By Lemma 5.2(b) the element dx has even order $2m$ as d and x are not conjugate. On the other hand, $(dx)^2 = dxdx = dd^x$ is a product of two conjugates of d and so has odd order m.

Lemma 5.2(d) gives $\mathrm{C}_T(x) = \{1, x, a, ax\}$ for involutions $a \in D$ and $ax \in \mathrm{Z}(T)$. In particular $d \in \mathrm{C}_D(ax)$ with $a \in \mathrm{C}_D(x)$, so at least D is the union of the appropriate subsets.

To prove the union to be disjoint, consider an arbitrary $b \in \mathrm{C}_D(x)$ with $d \in \mathrm{C}_D(bx)$. Then $d^{bx} = d$, so $d^b = d^x$ and

$$T^b = \langle d, x\rangle^b = \langle d^b, x^b\rangle = \langle d^x, x\rangle = T\,.$$

As $D \cap T = d^T$ has odd cardinality m (by Lemma 5.2(c)), the normalizing element b must centralize some element of $D \cap T$. But $\{b\} = \mathrm{C}_D(b)$, so $b \in \mathrm{C}_T(x) \cap D = \{a\}$. That is, $b = a$ and the various subsets of the union are indeed pairwise disjoint. □

The rest of this section is devoted to our proof of Theorem 5.4. *Accordingly we let G have* (F_p) *throughout.* The proof is by induction on $|G|$, the case $|G| = 2$ being trivial.

Lemma 5.9. *Let H be a subgroup of G with $E = D \cap H$ nonempty, and let N be a normal subgroup of H not containing E. If $(H, N) \neq (G, 1)$, then in $\bar{H} = H/N$ the set $\bar{E}$ is a conjugacy class contained in $\mathrm{O}_p(\bar{H})\langle\bar{e}\rangle$, for all $e \in E$.*

Proof. By Lemmas 5.1 and 5.2(b) the two elements d, e of E are conjugate in the dihedral group they generate. Therefore E is a conjugacy class in H as is $\bar{E}$ in $\bar{H}$. It inherits (F_p) from D, so by induction $E \subset \mathrm{O}_p(\bar{H})\langle\bar{e}\rangle$ for all $e \in E$. □

Lemma 5.10. *We may assume that* $\mathrm{Z}(G) = 1$.

Proof. Suppose that $\mathrm{Z}(G) \neq 1$. Then by induction, in $\bar{G} = G/\mathrm{Z}(G)$ the class $\bar{D}$ generates a subgroup $\bar{P}\langle\bar{d}\rangle$ with $d \in D$ and $\bar{P}$ a normal p-subgroup of $\bar{G}$.

Let P be a Sylow p-subgroup of the preimage P_0 of $\bar{P}$ in G, so $P_0 = \mathrm{Z}(G)P$. Especially P is the unique Sylow p-subgroup of the normal subgroup P_0, and hence P itself is normal in G.

In $\widetilde{G} = G/P$ the image of P_0 is the normal abelian group $\widetilde{\mathrm{Z}(G)\langle d\rangle}$. But then $\langle\widetilde{D}\rangle = \langle\tilde{d}\rangle$. Therefore back in G we have $\langle D\rangle = P\langle d\rangle$. In particular $D \subset \mathrm{O}_p(G)\langle d\rangle$ and Theorem 5.4 holds. □

Lemma 5.11. *$|D|$ is a power of the prime p.*

Proof. By Theorem 5.7 we already know this if D is the only class of involutions in G. Therefore we can assume that x is an involution of G that is not in D.

By the previous lemma $Z(G) = 1$, so $H = \langle \mathrm{C}_D(x) \rangle$ is a proper subgroup of G. By induction, $\mathrm{C}_D(x)$ is a conjugacy class of H with cardinality p^i for some integer i.

Furthermore $H \leqslant C_G(x)$ permutes the various sets $\mathrm{C}_D(ax)$, for a from the class $\mathrm{C}_D(x)$, transitively by conjugation. In particular they all have the same cardinality.

For a fixed but arbitrary $a \in \mathrm{C}_D(x)$, we have $1 \neq ax \notin Z(G)$ as $x \notin D$. Therefore by induction in $\langle \mathrm{C}_D(ax) \rangle$ the conjugacy class $\mathrm{C}_D(ax)$ has cardinality p^j, for some j that is independent of a by the previous paragraph.

By Theorem 5.8

$$|D| = |\mathrm{C}_D(x)|\,|\mathrm{C}_D(ax)| = p^i \cdot p^j = p^{i+j}\,,$$

as desired.

Lemma 5.12. *For each Sylow p-subgroup P and $d \in D$ we have $D = d^P$.*

Proof. We have

$$|\mathrm{C}_G(d)P| = |\mathrm{C}_G(d)|\,|P|/|\mathrm{C}_G(d) \cap P| \geqslant |\mathrm{C}_G(d)|\,|P|/|Q| = |\mathrm{C}_G(d)|_{p'}\,|P|\,,$$

where Q is a Sylow p-subgroup of $\mathrm{C}_G(d)$ containing $\mathrm{C}_P(d)$ and $|\mathrm{C}_G(d)|_{p'}$ is the p'-part of the order of $\mathrm{C}_G(d)$. As $|D| = |G\colon \mathrm{C}_G(d)|$, Lemma 5.11 gives $|\mathrm{C}_G(d)|_{p'}\,|P| = |G|$. Therefore $\mathrm{C}_G(d)P = G$ and $D = d^G = d^{\mathrm{C}_G(d)P} = d^P$. □

Lemma 5.13. *For $d \in D$ there is a d-invariant Sylow p-subgroup P. Therefore $D \subset \mathrm{O}_p(G)\langle d \rangle$, and Theorem 5.4 holds.*

Proof. As $\mathrm{Z}(G) = 1$ we have $D \neq \{d\}$. Let $e \in D \setminus \{d\}$, so that $\langle de \rangle$ is a nontrivial d-invariant p-subgroup of G. Now let P be a maximal d-invariant p-subgroup with $de \in P$. We claim that P is a Sylow p-subgroup of G.

Set $N = \mathrm{N}_G(P)$. By induction, in $\bar{N} = N/P$ the normal subgroup $\langle \overline{D \cap N} \rangle$ is a normal p-subgroup $\bar{R}$ extended by $\langle \bar{d} \rangle$. The preimage R of $\bar{R}$ in N is a normal d-invariant p-subgroup containing P, so $R = P$ by maximality. That is, $\langle \overline{D \cap N} \rangle = \langle \bar{d} \rangle$ is a normal subgroup of order 2 in $\bar{N}$ and so is in $\mathrm{Z}(\bar{N})$.

Therefore for $\bar{Q}$ a Sylow p-subgroup of $\bar{N}$, its preimage Q in $N = \mathrm{N}_G(P)$ is a Sylow p-subgroup that is again d-invariant. By maximality $Q = P$ is a Sylow p-subgroup of its own normalizer. But then (see [31, 5.1.3]) nilpotent P must be a Sylow p-subgroup of G, as claimed.

The normal subgroup $\langle D\rangle$ is $\langle d^P\rangle$ by Lemma 5.12 and is in $P\langle d\rangle$ by the previous paragraph. Therefore $\langle D\rangle = S\langle d\rangle$ for some p-subgroup S of P that is normal in G. In particular, $D \subset S\langle d\rangle \leqslant \mathrm{O}_p(G)\langle d\rangle$, as desired. □

The lemma completes our proof of Theorem 5.4.

Remark 5.14. To deduce Fischer's Z*-Theorem 5.4 from Glauberman's Z*-Theorem 5.3, argue as in the second half of the proof of Theorem 5.7 to show that $\mathrm{O}(G)\langle d\rangle$ contains a d-invariant Sylow p-subgroup P and $|D|$ is a power of p. Then the arguments of Lemma 5.12 and the end of Lemma 5.13 prove that $\langle D\rangle \leqslant P\langle d\rangle$ hence $D \subset \mathrm{O}_p(G)\langle d\rangle$.

This argument can be taken further to note, as Glauberman [17] does, that if, for the involution class D, all the products $|de|$ (for $d, e \in D$) have order a π-number, for some set π of odd primes, then $\langle D\rangle$ is the extension of a normal π-subgroup P by $\langle d\rangle$.

6. Applications to loop structure

The results of the previous sections can illuminate the structure of coordinatizing loops. Various of the results in this section are known, although some appear to be new. Even for the known results the proofs here are elementary (sometimes modulo one of the Z*-theorems) and reasonably transparent.

6.1. Spectra of Bol loops

We start with three results that illustrate the gulf between Bol loops of odd order and Bol loops of even order.

Theorem 6.1. (Kinyon, Wanless [30])
If a Bol loop has exponent three, then all its isotopes also have exponent three. □

Theorem 6.2. (Robinson [43])
If all isotopes of a Bol loop have exponent two, then the loop is an elementary abelian 2-group. □

Theorem 6.3. (Nagy [35], Baumeister and Stein [2])
There is a simple Bol loop of exponent two and order 96. □

We give proofs of the first two theorems. The third theorem is more difficult, involving a delicate and lengthy construction. It will not be touched here.

The actual result [43, Cor. 3.2.1] proven by Robinson is more general than the one given above as Theorem 6.2. The author thanks Michael Kinyon for providing this reference and for suggesting the context of Theorem 6.5 and its first corollary.

The *spectrum* of the loop L is the set of orders of the elements of L (as defined in Section 3.4):

$$\mathrm{Spec(L)} = \{\, |\mathrm{x}| \mid \mathrm{x} \in \mathrm{L} \,\}\,.$$

The spectrum is particularly useful if L is power associative, as is the case with Bol loops by Corollary 3.12. For instance, power associative loops have two-sided inverses, so Cayley's trick of pairing an element with its inverse shows that a finite power associative loop has odd order if all its elements have odd order.

From Lemma 3.11 we have immediately

Proposition 6.4. *For the Bol loop L,* $\mathrm{Spec(L)} = \{\, |\kappa_{\mathrm{x}}\kappa_1| \mid \mathrm{x} \in \mathrm{L} \,\}\,.$ □

A loop is said to be 2-*divisible* if every element is a square. This is certainly true if every element generates a cyclic subgroup of odd order, but there are other places where this can happen as well (for instance, in the additive group of the rationals, where division by 2 is always possible – hence the name). Thus in a power associative context, the class of 2-divisible loops is an extension of the class of finite loops of odd order.

Theorem 6.5. *Let L be a 2-divisible Bol loop. Then all the central automorphisms κ_x are conjugate by elements of* $\mathrm{Aut}_{\mathsf{LSD}}(L\mathbf{T})$.

Proof. It is enough to show that each κ_x is conjugate to κ_1 by elements of $\mathrm{Aut}_{\mathsf{LSD}}(L\mathbf{T})$.

First suppose that $|\kappa_x\kappa_1| = |x|$ is odd. Then by Lemma 5.2(a,b), the involutions κ_x and κ_1 are conjugate in the dihedral subgroup $\langle \kappa_1, \kappa_x\kappa_1 \rangle$ they generate, that conjugation achieved by some element of $\langle \kappa_x\kappa_1 \rangle \leqslant \mathrm{Aut}_{\mathsf{LSD}}(L\mathbf{T})$.

Next suppose that $|\kappa_x\kappa_1| = |x|$ is not odd. Then by assumption, there is a y with $y^2 = x$. Consider the dihedral group $T = \langle \kappa_y, \kappa_1 \rangle$. Certainly $|y| = |\kappa_y\kappa_1|$ is also not odd, so by Lemma 5.2(c) T has exactly two dihedral subgroups containing $(\kappa_y\kappa_1)^2 = \kappa_{y^2}\kappa_1 = \kappa_x\kappa_1$. (See Lemma 3.11 for the first equality.) One of these is $\langle \kappa_x\kappa_1, \kappa_1 \rangle = \langle \kappa_x, \kappa_1 \rangle$. Again by Lemma 5.2(a,c), the involutions κ_x and κ_1 of this subgroup are conjugate by some element of $\langle \kappa_y\kappa_1 \rangle \leqslant \mathrm{Aut}_{\mathsf{LSD}}(L\mathbf{T})$. □

Corollary 6.6. *Let L be a 2-divisible Bol loop. Then* Spec(L) *is an isotopy invariant.*

Proof. Let $(L,\cdot)$ and $(R,\circ)$ be isotopic. Then the Latin square designs $(L,\cdot)\mathbf{T}$ and $(R,\circ)\mathbf{T}$ are isomorphic. Furthermore, the induced isomorphism φ of $\mathrm{Aut}((L,\cdot)\mathbf{T})$ and $\mathrm{Aut}((R,\circ)\mathbf{T})$ takes central automorphisms κ_x $(x \in L)$ to central automorphisms κ_y $(y \in R)$. Since all the central automorphisms κ_x are conjugate by elements of $\mathrm{Aut}_{\mathsf{LSD}}((L,\cdot)\mathbf{T})$, we can assume that $\kappa_{1_L}^{\varphi} = \kappa_{1_R}$. But then

$$\begin{aligned}\mathrm{Spec(L},\cdot) &= \{\,|\kappa_x\kappa_{1_L}|\mid x \in L\,\} = \{\,|(\kappa_x\kappa_{1_L})^{\varphi}|\mid x \in L\,\}\\ &= \{\,|\kappa_x^{\varphi}\kappa_{1_L}^{\varphi}|\mid x \in L\,\} = \{\,|\kappa_y\kappa_{1_R}|\mid y \in R\,\}\\ &= \mathrm{Spec(R},\circ)\,,\end{aligned}$$

as desired. □

As the exponent of a loop is the least common multiple of its spectrum, we have immediately

Corollary 6.7. *Let L be a Bol loop of odd exponent. Then the exponent is an isotopy invariant.* □

The case of exponent three is Theorem 6.1 due to Kinyon and Wanless.

At the other end of the spectrum, we have

Lemma 6.8. *Let L be a Bol loop. Then L has exponent two if and only if κ_1 commutes with all the central automorphisms κ_x of* $\mathrm{Aut}(L\mathbf{T})$.

Proof. In a group, distinct elements of order 2 commute if and only if they have product of order 2. □

Thus in the situation of Theorem 6.2, the central automorphisms generate an elementary abelian 2-group. By Theorem 3.17 the group $\mathrm{RMult}(L)$ is a homomorphic image and so is also an elementary abelian 2-group. Transitive abelian groups are regular, so Theorem 6.2 follows directly.

We return to finite Bol loops with odd spectrum, which by Corollary 3.13 is equivalent to having odd order. The various Z*-theorems of Section 5 become relevant.

Theorem 6.9. *Let L be a finite Bol loop with exponent a power of some odd prime p. Then* $\mathrm{RMult}(L)$ *is a p-group. In particular $|L|$ is a power of p.*

Proof. The group $\langle \kappa_x \mid x \in L \rangle$ satisfies the hypotheses of Fischer's Z*-Theorem 5.4 and so the conclusions. Thus $\langle \kappa_x\kappa_1 \mid x \in L \rangle$ is a p-group that has RMult(L) as an image by Theorem 3.17. The p-group RMult(L) is transitive on L, so $|L|$ divides its order. □

In particular the finite Bol loops of exponent three studied by Kinyon and Wanless [30] all have order a power of three.

The theorem is known; see Foguel, Kinyon, and Phillips [15, Theorem 6.7], where the authors extract from Glauberman [17] the correponding result with p replaced by a set π of odd primes. The proof makes use of the argument under Remark 5.14 in place of Fischer's Z*-theorem.

Similarly Glauberman's Z*-Theorem 5.3 gives Corollary 6.8 of [15]:

Proposition 6.10. *If L is a finite Bol loop of odd order, then* RMult(L) *is of odd order, hence (by the Feit-Thompson Theorem) solvable.* □

The Bol loops of Theorem 6.9 have nilpotent RMult(L) but need not themselves be solvable, as an example of Foguel and Kinyon [14] demonstrates. Equally well, Bol loops of odd order have solvable RMult(L) (as just seen) but need not be solvable, as a simple Bol loop of order 1053 due to Nagy [36] shows.

When we have access to the full multiplication group, such stronger results are possible. We have a result of Glauberman [17] (with what amounts to his proof).

Theorem 6.11. *A finite Moufang loop with order a power of the odd prime p is nilpotent.*

Proof. By Corollary 3.13 all elements have order a power of the odd prime p. By Theorem 3.15 and Fischer's Z*-Theorem 5.4 each of the groups $\langle \rho_x\rho_1 \mid x \in L \rangle$, $\langle \kappa_x\kappa_1 \mid x \in L \rangle$, and $\langle \epsilon_x\epsilon_1 \mid x \in L \rangle$ is a finite p-group, and they normalize each other. Thus by Theorem 3.17 the group Mult(L) is a quotient of the p-group

$$\langle \rho_x\rho_1, \kappa_x\kappa_1, \epsilon_x\epsilon_1 \mid x \in L \rangle$$

and so is itself a p-group. In any nontrivial transitive permutation representation of a finite p-group, the stabilizer of a point must fix more than one point. Therefore the center of L is nontrivial, and induction takes over. □

Finally we have the result that inspired most of this later work.

Theorem 6.12. (Glauberman [17])
If L is a Moufang loop of odd order, then $\mathrm{Mult}(L)$ *has odd order.*

Proof. By Glauberman's Z*-Theorem 5.3 each of the groups $\langle\, \rho_x\rho_1 \mid x \in L \,\rangle$, $\langle\, \kappa_x\kappa_1 \mid x \in L \,\rangle$, and $\langle\, \epsilon_x\epsilon_1 \mid x \in L \,\rangle$ has odd order, so the quotient $\mathrm{Mult}(L)$ of the group they generate does as well. □

By the Feit-Thompson Theorem the group $\mathrm{Mult}(L)$ of odd order is solvable, and Glauberman was led to the solvability of Moufang loops of odd order.

6.2. Simple Moufang loops

In Section 4.3 we saw that every simple Moufang loop M is related to a triality simple group, namely $M\mathbf{TB}$ modulo its center, that is, $M\mathbf{TA}$. There are only a few possibilities for such a group.

Theorem 6.13. (Doro [9], Nagy and Valsecchi [37])
Let (G, D, π) be triality simple, and let M be the associated Moufang loop $(G, D, \pi)\mathbf{CS}$. Then exactly one of:

(1) $G \simeq (\mathrm{Z}_3 \times \mathrm{Z}_3) \rtimes \mathrm{Z}_2$, *and M is a cyclic group of order* 3.
(2) $G \simeq \mathrm{Z}_p^2 \rtimes \mathrm{Sym}(3)$, *and M is a cyclic group of order p, a prime not equal to* 3.
(3) *G is isomorphic to the wreath product $M \wr \mathrm{Sym}(3)$, and M is a nonabelian simple group.*
(4) $H = \ker\pi$ *is a nonabelian simple group, and M is nonabelian, nonassociative, and simple.* □

In particular nonassociative simple Moufang loops M are associated with a group with triality $H \rtimes \mathrm{Sym}(3)$ for a nonabelian simple group H. By Theorem 3.17 this simple group H is also the multiplication group of M.

All known examples of nonassociative simple Moufang loops come from octonions. An octonion algebra O over the field F is an 8-dimensional nonassociative but alternative F-algebra with identity on which there is a nondegenerate quadratic form $\delta\colon O \longrightarrow F$, the *norm*, that admits composition:

$$\delta(a)\delta(b) = \delta(ab)\,,$$

for all $a, b \in O$. See [44].

As Moufang observed, all octonion algebras satisfy the Moufang identity. Therefore the loop of units (invertible elements) of an octonion algebra is a

Moufang loop. As $\delta(1) = 1$, in order for the element a of O to be invertible, $\delta(a)$ must be nonzero; it turns out that this is also sufficient.

There are two basics types of octonion algebras. First are the division algebras. These featured in Moufang's work on coordinatizing projective planes, and their loop of units consists of all nonzero elements. In the division algebra case, the quadratic form δ is anisotropic.

If, on the other hand, there are nonzero elements a with $\delta(a) = 0$, then in fact δ is a hyperbolic form. This is the split case, and O is uniquely determined up to isomorphism by the field F. The split octonions over F will be denoted $\mathrm{Oct}^+(F)$.

If in $\mathrm{Oct}^+(F)$ we take the Moufang loop $\mathrm{SOct}^+(F)$ of norm 1 elements and factor out the center $\{\pm 1\}$, then we have a simple loop $\mathrm{PSOct}^+(F)$, called a *Paige loop* after Paige who first observed and proved simplicity [39].

We emphasize that, because of category equivalence and Propositions 4.8 and 4.9, simplicity of the loop and triality simplicity of a corresponding group with triality are equivalent; it is not necessary to check both, as Paige effectively did.

Let O be an octonion algebra, $\mathrm{GOct}(O)$ its loop of units, $\mathrm{SOct}(O)$ the normal subloop of norm 1 elements, and $\mathrm{PSOct}(O)$ the quotient of that by its center $\{\pm 1\}$. It has been conjectured that every nonassociative simple Moufang loop is isomorphic to $\mathrm{PSOct}(O)$ for some octonion algebra O. Liebeck [32], using the classification of finite simple groups, confirmed this for finite Moufang loops, as did the current author for locally finite Moufang loops [21].

Theorem 6.14. (Liebeck [32])
A finite simple Moufang loop is either associative (*and so a finite simple group*) *or is isomorphic to a Paige loop* $\mathrm{PSOct}^+(F)$ *over a finite field* F. □

Liebeck searched the list of nonabelian finite simple groups H, looking for triality simple groups $H \rtimes \mathrm{Sym}(3)$. He proved that the only examples are $\mathrm{P}\Omega_8^+(F) \rtimes \mathrm{Sym}(3)$ over finite fields F. The associated loops are then the Paige loops $\mathrm{PSOct}^+(F)$.

This last remark is equivalent to the statement that the multiplication group of the Paige loop $\mathrm{PSOct}^+(F)$ is the simple group $\mathrm{P}\Omega_8^+(F)$. (For simplicity, see [45, 11.48].) At an earlier workshop in this series, Nagy and Vojtěchovský [38] noted that this observation is "folklore" and is rarely (if ever, before [38]) provided with a complete proof. Nagy and Vojtěchovský gave calculations that are complete.

The material discussed here can be used to extend the proof from [38].

Consider the octonion algebra O as orthogonal space of dimension 8 over F admitting the nondegenerate quadratic form δ. The *general orthogonal group* $\mathrm{GO}(O)$ consists of the *similarities*, those invertible F-linear transformations t of O with

$$\delta(at) = \mu(t)\delta(a)\,,$$

for all $a \in O$, where $\mu(t) \in E = F \setminus \{0\}$ is a multiplier that depends only on t. The map μ taking t to $\mu(t)$ is a homomorphism from $\mathrm{GO}(O)$ to the multiplicative group E of F. The kernel of μ is the full *orthogonal group* $\mathrm{O}(O)$ – the similarities with multiplier $\mu(t) = 1$. The center of $\mathrm{GO}(O)$ consists of all nonzero scalar matrices, while the center of $\mathrm{O}(O)$ is $\{\pm 1\}$.

Let $(\cdot,\cdot)$ be the symmetric bilinear form associated with the quadratic form δ:

$$(a,b) = \delta(a+b) - \delta(a) - \delta(b)\,.$$

For x in O with $\delta(x) \neq 0$, we have the orthogonal *symmetry*

$$\mathrm{s}_x \colon a \longrightarrow a - (a,x)\delta(x)^{-1}x\,.$$

Replacing x by a nonzero scalar multiple does not change the symmetry. By the Cartan-Dieudonné Theorem [45, 11.42], the orthogonal group $\mathrm{O}(O)$ is generated by the symmetries. The rotation group $\mathrm{RO}(O)$ is the subgroup of index two consisting of products of an even number of symmetries. The group $\mathrm{RGO}(O)$ is the corresponding subgroup of index 2 in $\mathrm{GO}(O)$.

As the quadratic form δ admits composition, the subset

$$N_\delta = \{\, q(x) \mid x \in \mathrm{GOct}(O) \,\}$$

of E is actually a subgroup of E. We let $\mathrm{RNO}(O)$ be the subgroup of $\mathrm{RGO}(O)$ consisting of rotational similarities with multiplier from the subgroup N_δ.

The *spinor norm* is the homomorphism taking $\mathrm{RO}(O)$ to E/E^2 and given by

$$\prod_i \mathrm{s}_{x_i} \mapsto \prod_i \delta(x_i)E^2\,.$$

The group $\Omega(O)$ is the kernel of the spinor norm. Its normal subgroup $\Omega^1(O)$ is generated by all products $\mathrm{s}_1\,\mathrm{s}_x$ for $\delta(x) = 1$ (equivalently $\delta(x) \in E^2$).

Theorem 6.15. *Let O be an octonion algebra. The multiplication group of $\mathrm{GOct}(O)$ is $\mathrm{RNO}(O)$, and the multiplication group of $\mathrm{SOct}(O)$ is a normal subgroup of $\Omega(O)$ containing $\Omega^1(O)$.*

We briefly discuss the proof of this theorem.

As O is a composition algebra, for each $x \in \mathrm{GOct}(O)$

$$\delta(a\mathrm{L}(x)) = \delta(xa) = \delta(x)\delta(a) = \delta(a)\delta(x)$$

and

$$\delta(a\mathrm{R}(x)) = \delta(ax) = \delta(a)\delta(x).$$

Therefore $\mathrm{L}(x)$ and $\mathrm{R}(x)$ are similarities with multiplier $\delta(x)$. These generate $G = \mathrm{Mult}(\mathrm{GOct}(O))$, which is thus a subgroup of $\mathrm{RNO}(O)$ with $\mu(G) = N_\delta$. We must now determine $G \cap \mathrm{O}(O)$.

An easy calculation in O gives

$$y\,\mathrm{s}_x = -\delta(yx^{-1})\,xy^{-1}x\,,$$

for all $y \in \mathrm{GOct}(O)$ (recall that O is diassociative), and hence

$$y\,\mathrm{s}_1\,\mathrm{s}_x = \delta(x)^{-1}\,xyx.$$

That is, the element $\mathrm{L}(x)\mathrm{R}(x)\mathrm{L}(\delta(x))^{-1}$ of G induces the rotation $\mathrm{s}_1\,\mathrm{s}_x$ on $\mathrm{GOct}(O)$. The full rotation group $\mathrm{RO}(O)$ is generated by such rotations, so $\mathrm{RO}(O) \leqslant G \cap \mathrm{O}(O)$.

If $\mathrm{RO}(O) < G \cap \mathrm{O}(O)$, then the index is 2 and $\mathrm{s}_1 \in G$. By Proposition 3.14 the element ϵ_1 of $\mathrm{Aut}(\mathrm{GOct}(O)\mathbf{C})$ acts on the fiber $\mathrm{GOct}(O)_E$ via $y_E^{\epsilon_1} = (y^{-1})_E$. Then by the above calculation and Theorem 3.17 there would be a nontrivial automorphism of $\mathrm{GOct}(O)\mathbf{C}$ acting on the fiber $\mathrm{GOct}(O)_E$ according to $y_E \mapsto -\delta(y)y_E$. This leads to a contradiction. We conclude that $\mathrm{RO}(O) = G \cap \mathrm{O}(O)$ and $G = \mathrm{RNO}(O)$, as claimed in the first part of theorem.

We have a natural injection of $\mathrm{SOct}(O)$ into $\mathrm{GOct}(O)$, but this does not guarantee an injection of its multiplication group into G. The injection is, however, a monic map in the category Mouf by Lemma 4.6. Therefore the category equivalence takes it to a monic map in the category UTriGrp. By Lemma 4.7 this is a triality homomorphism whose kernel is central. Therefore the subgroup S of G generated by the various $\mathrm{L}(x)$ and $\mathrm{R}(x)$ with $\delta(x) = 1$ is at worst a central extension of $\mathrm{Mult}(\mathrm{SOct}(O))$. For such an x, the earlier calculations yield

$$y\,\mathrm{s}_1\,\mathrm{s}_x = xyx = y\mathrm{L}(x)\mathrm{R}(x)\,,$$

for all $y \in \mathrm{GOct}(O)$. Therefore S includes at least the normal subgroup $\Omega^1(O)$. This group is already irreducible on O, so all the center that S can have is in $\{\pm 1\}$. Especially $S \simeq \mathrm{Mult}(\mathrm{SOct}(O))$. It remains to prove that each $\mathrm{L}(x)$ for $\delta(x) = 1$ is within the spinor kernel $\Omega(O)$. This can be done by direct calculation (as Nagy and Vojtěchovský [38] do in the split case), or by using Proposition 3.16 to show that the subgroup $\langle \rho_1, \kappa_1, \epsilon_1 \rangle \simeq \mathrm{Sym}(3)$

of $\mathrm{Aut}(\mathrm{GOct}(O)\mathbf{C})$ leaves the subdesign $\mathrm{SOct}(O)\mathbf{C}$ invariant and induces an embedding of $\langle\, \mathrm{L}(x) \mid \delta(x) = 1 \,\rangle$ in $\Omega(O)$. This completes the theorem.

The center of the Moufang loop $\mathrm{SOct}(O)$ is $\{\pm 1\}$ of order at most 2. Thus the influence of the passage to $\mathrm{PSOct}(O)$ on the multiplication group is easy to understand directly or through another appeal to category equivalence. The normal structure of many of the groups $\Omega(O)$ and their projective quotients $\mathrm{P}\Omega(O) = \Omega(O)/\{\pm 1\}$ is well known [45]. For instance in the split case $\Omega(O)$ is quasisimple, so $\Omega(O) = \Omega^1(O)$ and $\mathrm{P}\Omega(O) = \mathrm{P}\Omega^1(O) = \mathrm{P}\Omega_8^+(F)$ is simple.

This returns us to the verification due to Nagy and Vojtěchovský [38].

Corollary 6.16. $\mathrm{Mult}(\mathrm{PSOct}^+(F)) = \mathrm{P}\Omega_8^+(F)$. *In particular Paige loops are always simple, as* $\mathrm{P}\Omega_8^+(F)$ *is.* □

We also have two of Paige's original observations [39].

Corollary 6.17.

(a) *Let O be the real compact octonions (the original Graves-Cayley octonions). Then* $\mathrm{Mult}(\mathrm{PSOct}(O)) = \mathrm{P}\Omega(O)$*, and in particular* $\mathrm{PSOct}(O)$ *is simple, as* $\mathrm{P}\Omega(O)$ *is.*

(b) *Let O_1 be the real compact octonions tensored up to the field $\mathbb{R}((t))$ of Laurent polynomials. Then* $\mathrm{Mult}(\mathrm{PSOct}(O_1)) = \mathrm{P}\Omega(O_1)$*, and in particular* $\mathrm{PSOct}(O_1)$ *is not simple, as* $\mathrm{P}\Omega(O_1)$ *is not.* □

References

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

[2] **B. Baumeister and A. Stein**, *Self-invariant 1-factorizations of complete graphs and finite Bol loops of exponent 2*, Beiträge Algebra Geom. **51** (2010), 117 – 135.

[3] **G. Bol**, *Gewebe und Gruppen (Topologische Fragen der Differentialgeometrie 65.)*, Math. Ann. **114** (1937), 414 – 431.

[4] **R.D. Brauer and M. Suzuki**, *On finite groups of even order whose 2-Sylow group is a quaternion group*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 1757 – 1759.

[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] **F. Buekenhout**, *La géometrié des groupes de Fischer*, unpublished notes, Université Libre de Bruxelles (1974).

[7] **E. Cartan**, *Le principe de dualité et la théorie des groupes simples et semi-simple*, Bull. Sc. Math. **49** (1925), 367 – 374.

[8] **H. Cuypers and J.I. Hall**, *The* 3*-transposition groups with trivial center*, J. Algebra **178** (1995), 149 – 193.

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

[10] **B. Fischer**, *Distributive Quasigruppen endlicher Ordnung*, Math. Z. **83** (1964), 267 – 303.

[11] **B. Fischer**, *A characterization of the symmetric groups on* 4 *and* 5 *letters*, J. Algebra **3** (1966), 88 – 98.

[12] **B. Fischer**, *Eine Kennzeichnung der symmetrischen Gruppen vom Grade* 6 *und* 7, Math. Z. **95** (1967), 288 – 298.

[13] **B. Fischer**, *Finite groups generated by* 3*-transpositions. I*, Invent. Math. **13** (1971), 232 – 246.

[14] **T. Foguel and M. Kinyon**, *Uniquely* 2*-divisible Bol loops*, J. Algebra Appl. **9** (2010), 591 – 601.

[15] **T. Foguel, M.K. Kinyon and J.D. Phillips**, *On twisted subgroups and Bol loops of odd order*, Rocky Mountain J. Math. **36** (2006), 183 – 212.

[16] **M. Funk and P.T. Nagy**, *On collineation groups generated by Bol reflections*, J. Geom. **48** (1993), 63 – 78.

[17] **G. Glauberman**, *On loops of odd order, I*, J. Algebra **1** (1964), 374 – 396, *II*, J. Algebra **8** (1968), 393 – 414.

[18] **G. Glauberman**, *Central elements in core-free groups*, J. Algebra **4** (1966), 403 – 420.

[19] **G. Glauberman**, *On groups with a quaternion Sylow* 2*-subgroup*, Illinois J. Math. **18** (1974), 60 – 65.

[20] **J.I. Hall**, *On the order of Hall triple systems*, J. Combin. Theory Ser. A **29** (1980), 261 – 262.

[21] **J.I. Hall**, *Locally finite simple Moufang loops*, Turkish J. Math. **31** (2007), 45 – 61.

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

[23] **J.I. Hall**, *Moufang loops and groups with triality are essentially the same thing*, Memoirs Amer. Math. Soc. (in preparation).

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

[25] **M. Hall, Jr.**, *Projective planes*, Trans. Amer. Math. Soc. **54** (1943), 229–277 (Correction: Trans. Amer. Math. Soc. **65** (1949), 473).

[26] **M. Hall, Jr.**, *The theory of groups*, Macmillan, New York, 1959.

[27] **M. Hall, Jr.**, *Automorphisms of Steiner triple systems*, IBM J. Res. Develop **4** (1960), 460 – 472.

[28] **M. Hall, Jr.**, *Group theory and block designs*, Proc. Internat. Conf. Theory of Groups (Canberra, 1965), eds. L.G. Kovács, B.H. Neumann, Gordon and Breach, 1967, 115 – 144.

[29] **N. Jacobson**, *Basic algebra II*, Second edition, W. H. Freeman and Company, New York, 1989.

[30] **M. Kinyon and I. Wanless**, *Loops with exponent three in all isotopes*, arXiv preprint 1103.0054.

[31] **H. Kurzweil and B. Stellmacher**, *The theory of finite groups*, Springer Universitext, 2004.

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

[33] **R. Moufang**, *Alternativkörpern und der Satz vom vollständigen Vierseit*, Abh. Math. Sem. Hamburg **9** (1933), 207 – 222.

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

[35] **G.P. Nagy**, *A class of finite simple Bol loops of exponent* 2, Trans. Amer. Math. Soc. **361** (2009), 5331 – 5343.

[36] **G.P. Nagy**, `www.math.u-szeged.hu/~nagyg/pub/simple_bol_loops.html`

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

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

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

[40] **H.O. Pflugfelder**, *Quasigroups and loops: Introduction*, Sigma Series in Pure Math. **7**, Heldermann Verlag, Berlin, 1990.

[41] **G. Pickert**, *Projektive Ebenen*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Bercksichtigung der Anwendungsgebiete, **80**, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.

[42] **K. Reidermeister**, *Topologische Fragen der Differentialgeometrie. V. Gewebe und Gruppen*, Math. Z. **29** (1929), 427 – 435.

[43] **D.A. Robinson**, *Bol loops*, Trans. Amer. Math. Soc. **123** (1966), 341 – 354.

[44] **T.A. Springer and F.D. Veldkamp**, *Octonions, Jordan Algebras and Exceptional Groups*, Springer Monographs in Math., Berlin, 2000.

[45] **D.E. Taylor**, *The geometry of the classical groups*, Sigma Series in Pure Math. **9**, Heldermann Verlag, Berlin, 1992.

[46] **G. Thomsen**, *Topologische Fragen der Differentialgeometrie XII, Schnittpunktssätze in ebenen Geweben*, Abh. Math. Semin. Univ. Hambg. **7** (1929), 99 – 106.

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

[48] **O. Veblen and J.W. Young**, *Projective geometry*, Vol. 1, Ginn and Co., Boston, 1916.

[49] **F. Zara**, *Classification des couples fischeriens*, Thése, Amiens, 1985.

Department of Mathematics, Michigan State University, East Lansing, Michigan 48824, U.S.A.
E-mail: jhall@math.msu.edu