Groups with triality

J.I. Hall[1]
Department of Mathematics
Michigan State University

1 Combinatorics

An $n \times n$ Latin square is a square array of n^2 cells containing the numbers $1, \ldots, n$ in such a way that no number appears twice in the same row and no number appears twice in the same column:

1	2	3	4
4	1	2	3
2	3	4	1
3	4	1	2

1	2
2	1

We can index the rows and columns using the set $I = \{1, \ldots, n\}$ as well:

	1	2	3	4
1	1	2	3	4
2	4	1	2	3
3	2	3	4	1
4	3	4	1	2

	1	2
1	1	2
2	2	1

Having done this, we define the associated *Latin square design* $\mathbb{D} = (\mathcal{P}, \mathcal{L})$, an incidence system with point set $\mathcal{P}$ and line set $\mathcal{L}$. Here $\mathcal{P}$ is the disjoint union of its *fibers* $I_R \cup I_C \cup I_E$ and $\mathcal{L}$ consists of n^2 lines, one for each cell of the Latin square. The line $\{a_R, b_C, c_E\}$ encodes the fact that the cell located in row a and column b has entry c. So for instance, our 2×2 Latin square gives the four lines

$$\{1_R, 1_C, 1_E\},\ \{2_R, 1_C, 2_E\},\ \{2_R, 2_C, 1_E\},\ \{1_R, 2_C, 2_E\}$$

Among the 16 lines coming from the 4×4 example are $\{3_R, 2_C, 3_E\}$ and $\{4_R, 3_C, 1_E\}$.

[1]Partial support provided by the National Science Foundation, USA

2 Algebra

The Latin square with labeled rows can be viewed as the Cayley (or multiplication) table of a quasigroup $(I, \cdot)$. In our 4×4 example we have, for instance,

$$3 \cdot 2 = 3 \qquad \text{and} \qquad 4 \cdot 3 = 1$$

In the 2×2 example, the element 1 is a multiplicative identity element. Indeed if we reindex the rows and columns by the entries in the first row and column (respectively) then any Latin square becomes the Cayley table of a loop (a quasigroup with identity element and inverses):

	1	2	3	4
1	1	2	3	4
4	4	1	2	3
2	2	3	4	1
3	3	4	1	2

With appropriate definitions there are category equivalences among categories of Latin squares, Latin square designs, quasigroups, and loops.

One can ask how combinatorial properties of the Latin squares and Latin square designs are reflected in algebraic properties of the associated loops and quasigroups. For instance, a quasigroup is a "not necessarily associative group." There is a famous result of Reidermeister [17] stating that the rows and columns of a Latin square can be indexed to give the Cayley table of a group if and only if the Latin square has the "quadrangle condition."

Without giving that condition itself we suggest how it holds in our 4×4 example. For instance, for any entry 4 in the square, find the entry 2 in its row and 3 in its column. Then the cell that completes these three to a quadrangle will always have the same entry, in this case 1:

1	2	3	4
4	1	**2**	3
2	3	4	1
3	4	1	2

and

1	**2**	3	**4**
4	1	2	**3**
2	3	4	1
3	4	1	2

3 Groups

If the Latin square is symmetric, then the corresponding loop is commutative. This can also be stated in terms of automorphisms of the associated Latin

square design. For instance our 2×2 example is commutative, and the switching of the roles of rows and columns corresponds to the permutation $(1_R, 1_C)(2_R, 2_C)(1_E)(2_E)$ being an automorphism of the Latin square design.

We now come to a fundamental concept. Let p be a point of the Latin square design $\mathbb{D}$; that is, $p = a_R$, a_C, or a_E for some $a \in I$. A *central automorphism* τ_p of $\mathbb{D}$ with *center* $p \in \mathcal{P}$ is an nontrivial automorphism of $\mathbb{D}$ that fixes the point p and all lines through it. (In the dual world of 3-nets, this is a *Bol reflection* [1, 4].)

If τ_p exists then, for all $\{p, q, r\} \in \mathcal{L}$, we have

$$p^{\tau_p} = p, \quad q^{\tau_p} = r, \quad r^{\tau_p} = q\,.$$

In particular τ_p switches the two fibers that complement the fiber containing p. For instance, the permutation of the first paragraph is τ_{1_E}.

The following is elementary. (For this and other results discussed here, see [4, 10, 11].)

(3.1) PROPOSITION. *In* $\mathrm{Aut}(\mathbb{D})$ *there is at most one central automorphism* τ_p *with center* p *for each* $p \in \mathcal{P}$. *If* τ_p *exists in* $\mathrm{Aut}(\mathbb{D})$, *then it has order* 2. *If* τ_p *and* τ_q *exist in* $\mathrm{Aut}(\mathbb{D})$ *with* p *and* q *in different fibers, then* $\tau_p\tau_q$ *has order* 3 *and* $\langle \tau_p, \tau_q \rangle$ *is isomorphic to* $Sym(3)$. *If this is the case, then there is a unique conjugacy class* T *of central automorphisms in* $\mathrm{Aut}(\mathbb{D})$.

If $(I, \cdot)$ is a loop then we let $\mathbb{D}(I, \cdot) = \mathbb{D}$ be the Latin square design with point set $\mathcal{P} = I_R \cup I_C \cup I_E$ and line set $\mathcal{L}$ given by the Cayley table of $(I, \cdot)$:

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

A basic question is: how is the existence of central automorphisms of $\mathbb{D}(I, \cdot)$ reflected in the algebraic properties of the loop $(I, \cdot)$? Bol [1] proved:

(3.2) THEOREM. *Let* $(I, \cdot)$ *be a loop. Then we have* τ_p *in* $\mathrm{Aut}(\mathbb{D}(I, \cdot))$ *for every point* p *of* $\mathbb{D}(I, \cdot)$ *if and only if*

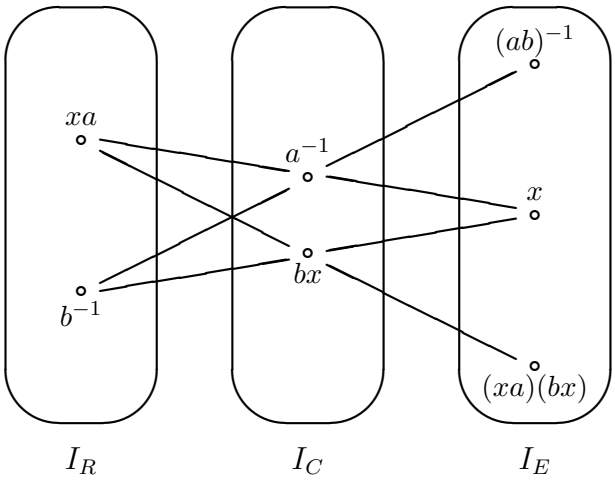
$$(xa)(bx) = (x(ab))x$$

for all x, a, b *in* I.

Indeed, the existence of τ_p for $p \in \{1_R, 1_C, 1_E\}$ is equivalent to

$$(xa)a^{-1} = x, \quad b^{-1}(bx) = x, \quad b^{-1}a^{-1} = (ab)^{-1}$$

for all $x, a, b \in I$. This gives us the picture



Suppose $\tau = \tau_{x_E}$ is an automorphism of $\mathbb{D}(I,\cdot)$. Setting $b = 1$ we see that $(a_E^{-1})^\tau = (xa)x_E$ for all $a \in I$.

As $\{b_R^{-1}, a_C^{-1}, (ab)_E^{-1}\}$ is certainly a generic line of $\mathbb{D}(I,\cdot)$, we see that τ (extended to I_E as in the previous paragraph) is an automorphism of $\mathbb{D}(I,\cdot)$ if and only if $(xa)(bx)_E$ is equal to $((ab)_E^{-1})^\tau$ for all a, b. That is, if and only if for all a, b we have $(xa)(bx) = (x(ab))x$, as claimed in the theorem.

Loops that satisfy the identity of Theorem 3.2 are called *Moufang loops* after Ruth Moufang [14] who first studied them. Since the Moufang Identity is a weak associative law, all groups are Moufang loops; but there are other examples. Moufang was interested in alternative algebras and proved that the loop of units in any alternative algebra satisfies the Moufang Identity. (Actually she studied an equivalent identity.)

Therefore to every Moufang loop there is associated a group of automorphisms generated by a conjugacy class of elements of order 2 enjoying the properties of Proposition 3.1. There is a converse:

(3.3) THEOREM. *Let T be a conjugacy class of elements of order 2 in the group $G = \langle T\rangle$; and let $\pi\colon G \longrightarrow Sym(3)$ be a surjective homomorphism. Further assume that we have*

$$(*) \quad \textit{for all } t, r \in T, \textit{ if } \pi(t) \neq \pi(r), \textit{ then } |\pi(t)\pi(r)| = 3\,.$$

Then there is a Moufang loop $(I,\cdot)$ with

$$G/Z(G) \simeq \mathrm{Aut}(\mathbb{D}(I,\cdot))^0\,,$$

where the class T maps bijectively to the class of central automorphisms of $\mathrm{Aut}(\mathbb{D}(L))^0$*, the subgroup of* $\mathrm{Aut}(\mathbb{D}(L))$ *generated by all central automorphisms.*

The groups $G = \langle T \rangle$ satisfying the hypothesis $(*)$ of Theorem 3.3 have been studied extensively, starting with Glauberman [7] and Doro [3], under the name of *groups with triality*.

If the Moufang loop is in fact a group H, then the associated group with triality is (essentially) the wreath product $H \wr Sym(3)$. Since any octonion algebra is alternating, the units of norm 1 in the split octonians (over any field) form a Moufang loop. The associated group with triality is Cartan's triality group $\mathrm{P}\Omega_8^+(\mathbb{F})$:$Sym(3)$ (motivating the terminology).

The category equivalence between loops and Latin square designs mentioned above restricts to a category equivalence between Moufang loops and Latin square designs admitting all possible central automorphisms. These are in turn equivalent to an appropriate category of groups with triality.

4 Finite

Moufang loops are very close to groups, so it is not surprising that many things can be proven using the connection between finite Moufang loops and finite groups with triality.

4.1 Glauberman's Z^*-theorem

There is a natural concept of homomorphism for loops, so there is a reasonable theory of composition series and so forth [2, Chap. IV]. Glauberman [7] proved that the Feit-Thompson Theorem can be extended to say that every Moufang loop of odd order is solvable. If $\mathbb{D}$ is the associated Latin square design, then the set of central automorphisms in $\mathrm{Aut}(\mathbb{D})$ is a conjugacy class of elements of order 2 with the property that any two of them have product of odd order. This led Glauberman to his Z^*-theorem [6] which then became a crucial tool in his proof of the odd order theorem for Moufang loops. Of course the Z^*-theorem has had many other important applications.

4.2 Finite simple Moufang loops

A nonidentity loop is *simple* if every surjective loop homomorphism is either bijective or has image the identity. For instance, if in the split octonians over a field $\mathbb{F}$ we take the Moufang loop of norm 1 elements and factor out the center $\{\pm 1\}$, then we have a simple loop $\mathrm{P}(\mathbb{F})$, called a *Paige loop* after L.J. Paige who first observed and proved simplicity [16].

A group G with $S \leq \mathrm{Aut}(G)$ is *S-simple* if the identity and G are the only S-invariant normal subgroups of G. The group G is *triality-simple* if it is S-simple for $S \simeq Sym(3)$ and additionally the group $G.S$ is a group with triality with respect to the conjugacy class containing the transpositions of S.

Doro [3] initiated the study of simple Moufang loops via the study of the associated triality-simple groups. Liebeck [12], using the classification of finite simple groups, proved

(4.1) Theorem. *If G is a nonabelian finite triality-simple group, then $G.S$ is one of:*

(a) *$N \wr Sym(3)$ for a nonabelian finite simple group N.*

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

Using Doro's results, Liebeck then easily derived

(4.2) Theorem. [12, Theorem] *A finite simple Moufang loop is either associative (and so a finite simple group) or is isomorphic to a Paige loop $\mathrm{P}(\mathbb{F})$ over a finite field $\mathbb{F}$.*

4.3 Lagrange's theorem

Lagrange's Theorem says that every subgroup of the finite group G has order that divides the order of G. It had long been conjectured that Lagrange's Theorem remains true for finite Moufang loops. A result of Bruck [2, Lemma V.2.1] shows that Lagrange's Theorem is true for all finite Moufang loops if and only if it is true for all finite simple Moufang loops. It is certainly true in the finite simple groups, so by Liebeck's Theorem 4.2 it remained to check whether or not Lagrange's Theorem holds in finite Paige loops. This was done by several groups of people independently, the first being Grishkov and Zavarnitsine [8]. Therefore we have

(4.3) THEOREM. [5, 8, 13] *Every subloop of the finite Moufang loop* $(I, \cdot)$ *has order that divides* $|I|$.

All of the proofs relate subloops of the octonians to subgroups of the associated group with triality $\mathrm{P}\Omega_8^+(\mathbb{F})$:$Sym(3)$ and then carefully study the subgroup structure of this group.

5 And

It is remarkable that at present every known nonassociative simple Moufang loop, finite or infinite, arises as the central quotient of the norm 1 units from some octonion algebra. Nagy, Vojtěchovský, Grishkov, Zavarnitsine and perhaps others have asked whether these are the only examples (although they may not be comfortable phrasing this as a conjecture).

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

It turns out [9] that Liebeck's theorems remain valid when extended by replacing every instance of "finite" by "locally finite."

(5.1) THEOREM. *If* G *is a nonabelian locally finite triality-simple group, then* $G.S$ *is one of:*

(a) $N \wr Sym(3)$ *for a nonabelian locally finite simple group* N.

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

(5.2) THEOREM. *A locally finite simple Moufang loop is either associative (and so a locally finite simple group) or is isomorphic to a Paige loop* $\mathrm{P}(\mathbb{F})$ *over a locally finite field* $\mathbb{F}$.

An initial observation in the proof is that the Moufang loop $(I, \cdot)$ is locally finite if and only if the associated group with triality $\mathrm{Aut}(\mathbb{D}(I, \cdot))^0$ is locally finite.

All locally finite fields are countable, and a finite dimensional matrix algebra over a countable field is countable. Therefore we have the remarkable

(5.3) COROLLARY. *An uncountable locally finite simple Moufang loop is associative and so is a locally finite simple group.*

References

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

[2] R.H. Bruck, "A Survey of Binary Systems," Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft **20**, Springer Verlag, Berlin-Göttingen-Heidelberg, 195

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

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

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

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

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

[8] A.N. Grishkov and A.V. Zavarnitsine, Lagrange's theorem for Moufang loops, Math. Proc. Cambridge Philos. Soc., **139** (2005), 41–57.

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

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

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

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

[13] G.E. Moorhouse, personal communication, Aug. 2004.

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

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

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

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