Quasigroups and Related Systems **15** (2007), 1 – 18

Advances in loop rings and their loops

Edgar G. Goodaire

Dedicated to the Memory of D. A. Robinson

Abstract

We describe some of the advances in the theory of loops whose loop rings satisfy "interesting" identities that have taken place in the past ten years.

1. Introduction

Let L be a loop and R a commutative associative ring with 1. The loop ring RL is constructed in precisely the same way the group ring would be constructed if L were associative. Of special significance is the fact that each $\alpha \in RL$ can be represented uniquely in the form $\alpha = \sum_{\ell \in L} \alpha_\ell \ell$, with the $\alpha_\ell \in R$ almost all 0.

While historically, loop rings made an occasional appearance in the literature, notably with a semisimplicity result of Bruck [2] (a nonassociative version of the theorem of Maschke for group rings), and a proof by Paige that in most characteristics, a commutative power associative loop algebra is a group algebra [31], nonassociative loop rings[1] appear to have been little more than a curiosity until the 1980s when the author found a class of nonassociative Moufang loops whose loop rings satisfy the alternative laws.

In 1998, at the fifteenth Brazilian "Escola de Álgebra" held that summer in Canela, I gave a talk on the history of loop rings, such as the subject was at that time [13]. "Loops '07" presents a natural forum for an update, which is the subject of this paper. Much of the work described here is joint with Orin Chein or César Polcino Milies.

2000 Mathematics Subject Classification: Primary: 20N05; Secondary: 17D05
Keywords: Loop, Moufang, Bol, Jordan, loop ring

[1] In this paper, "nonassociative" always means "not associative."

2. Alternative loop rings

Alternative rings are those satisfying

the right alternative law $(yx)x = yx^2$

and

the left alternative law $x(xy) = x^2y$

and can be thought of as the ring-theoretic analogues of Moufang loops. For instance, the subring of an alternative ring generated by any two elements is associative (this property is called *diassociativity*). Moreover, alternative rings satisfy the familiar

right Moufang identity $(xy \cdot z)y = x(y \cdot zy)$

and

left Moufang identity $(xy \cdot x)z = x(y \cdot xz)$.

Thus, if RL is an alternative ring, then L is a Moufang loop. The converse is certainly not true, in general. It is not hard to see that the repeated variable in a Moufang identity makes it unlikely to linearize to the ring RL. On the other hand, some Moufang loops do have alternative loop rings. Those that have alternative loop rings in any characteristic are called *RA loops*. Such loops are well understood.

Let G be any nonabelian group with an involution $g \mapsto g^*$ satisfying $gg^* \in \mathcal{Z}(G)$, the centre of G, for all $g \in G$. Let u be an indeterminate and let L be the set $G \cup Gu$. Extend the multiplication from G to L via the rules

$$g(hu) = (hg)u$$

$$(gu)h = (gh^*)u$$

$$(gu)(hu) = g_0h^*g$$

for $g, h \in G$, where $u^2 = g_0$ is central in G and $g_0^* = g_0$.

If L is RA, then L has form $M(G, *, g_0)$. Moreover,

- G has a unique nonidentity commutator, always denoted s, which is a unique nonidentity commutator and associator in L,

- both G and L have what is known as

  the LC property: $ab = ba$ if and only if a or b or ab is central

  and

- the involution on G takes the form

$$g^* = \begin{cases} g & \text{if } g \in \mathcal{Z}(G) \\ sg & \text{otherwise.} \end{cases} \tag{1}$$

These properties were first found by Orin Chein and the author [7] and are fully described in a monograph written with Eric Jespers and César Polcino Milies [15].

With a hint at what was to come in other varieties, it soon became clear that by restricting the coefficient ring to characteristic 2, many more loops have alternative loop rings. Calling such loops *RA2*, those with the structure $M(G, *, g_0)$ have been classified [13, 11], although there are indeed RA2 loops not of this form. The smallest is the one Chein denotes $M_{32}(B, 5)$.

Suggestion 1. (Reasonable) Find more classes of RA2 loops.

Suggestion 2. (Optimistic) Classify RA2 loops.

3. Strongly right alternative loop rings

A *right alternative* ring is a ring which satisfies the right alternative law. In characteristic different from 2, it is not hard to show that a right alternative ring satisfies

$$\text{the right Bol identity} \qquad (xy \cdot z)y = x(yz \cdot y).$$

It has long been known that a finite dimensional simple right alternative algebra with 1 is alternative [1]. This fact, together with Bruck's version of Maschke's theorem referenced earlier, allowed Chein and the author to conclude that in characteristic different from 2, when the loop is finite, a right alternative loop algebra must be alternative [8]. Later, Kenneth Kunen removed the restriction on finiteness and placed whatever theory might develop for right alternative loop rings squarely within the context of characteristic 2 [27], a rather idiosyncratic characteristic since it is the

only characteristic in which the right Bol identity is not a consequence of the right alternative law. In fact, Kunen has even found a right alternative loop ring which does not satisfy the right Bol identity. Since such rings are bizarre (and probably to be avoided), we say that a loop ring RL is *strongly right alternative* and the loop L is $SRAR$ (for *strongly right alternative ring*) if RL satisfies the right Bol identity, but not the left, $(x \cdot yx)z = x(y \cdot xz)$. [A ring satisfying both Bol identities is alternative.]

We emphasize that strongly right alternative loop rings that are not alternative can exist only in characteristic 2. In the 1990s, D. A. Robinson and the author showed that RL is strongly right alternative if and only if L is a (right) Bol loop (that is, a loop satisfying the right Bol identity,[2]) and, for every $x, y, z, w \in L$, at least one of the following conditions holds:

$$\begin{aligned} &D(x,y,z,w)\colon [(xy)z]w = x[(yz)w] \text{ and } [(xw)z]y = x[(wz)y] \\ &E(x,y,z,w)\colon [(xy)z]w = x[(wz)y] \text{ and } [(xw)z]y = x[(yz)w] \\ &F(x,y,z,w)\colon [(xy)z]w = [(xw)z]y \text{ and } x[(yz)w] = x[(wz)y]. \end{aligned} \tag{2}$$

It was observed that any Bol loop with a unique nonidentity commutator/associator is SRAR [24, 25] and, for a long time, such loops provided the only examples of SRAR loops. Indeed, there are families of Bol loops such as those Chein and the author have denoted $L(B, m, n, r, s, t, z, w)$ which are SRAR only if the subloop L' generated by all commutators and associatiors has order 2 [10].

Research with Orin Chein, currently still at the preprint stage, has shown that the conjecture that $|L'| = 2$ characterizes SRAR loops is false. Some of this work we now describe.

Let L be a Bol loop with an index 2 left nucleus N. Fix $u \in L \setminus N$. Then L is the union $N \cup Nu$ and multiplication in L can be defined entirely in terms of multiplication in N and two bijections $\theta\colon N \to N$ and $\phi\colon N \to N$, these being defined by

$$un = (n\theta)u \quad \text{and} \quad n\phi = u(nu).$$

Specifically, for $n_1, n_2 \in N$, we have

$$\begin{aligned} n_1(n_2u) &= (n_1n_2)u, \\ (n_1u)n_2 &= n_1(un_2) = [n_1(n_2\theta)]u \end{aligned} \tag{3}$$

[2] In this paper, all Bol loops are assumed to satisfy the right Bol identity.

and

$$(n_1u)(n_2u) = n_1[u(n_2u)] = n_1(n_2\phi).$$

Furthermore, if L is not Moufang, then in either of the cases $\theta = I$, the identity map on N, or $\phi = R(u^2)$, right multiplication by $u^2 \in N$, L is SRAR [6]. Using this fact, one can exhibit families of examples of SRAR loops many of which have more than a single nonidentity commutator/associator. We present two such families.

Let N be an elementary abelian 2-group of order at least 8, let $\theta = I$ and let ϕ be any nonidentity bijection on N such that $\phi^2 = I$ and ϕ is not a right multiplication map. Let $L = N \cup Nu$, u an indeterminate, and extend the binary operation on N to L by means of the equations (3). Then L is an SRAR loop with left nucleus N and, in many cases, $|L'| > 2$.

Alternatively, let N be an abelian group of exponent 4, let u^2 be any element of order 2 in N, let $\phi = R(u^2)$, let $n\theta = n^{-1}$ for $n \in N$ and construct a loop L as before. Again, L is SRAR and often $|L'| > 2$. In passing, we mention that this family of loops is one discussed by P. Vojtěchovský in [36], specifically the class labelled $G(\theta_{xy}, \theta_{xy}, \theta_{x^{-1}y}, \theta_{xy})$. (The reader should, however, be aware of the fact that Vojtěchovský's loops are left Bol.)

We conclude this section with some suggestions for further investigations. It may be important to note that this is certainly not the first time that loops with large nuclei have appeared in the literature. Indeed, some years ago, D. A. Robinson and the author showed that any loop with an index 2 nucleus is *conjugacy closed* and hence a *G-loop*, that is, isomorphic to all its loop isotopes [23]. This is certainly not the case for a Bol loop with left nucleus of index 2. Still, such loops may have other elements of interest.

Suggestion 3. What can be said about a Bol loop with index 2 left nucleus?

Suggestion 4. While it is probably unrealistic to try to characterize SRAR loops at this time, it would be useful to find more families of SRAR loops.

4. Jordan loops

Much of the work described in this section is joint with a student, Rebecca Keeping.

The theorem of Lowell Paige cited earlier, asserting that in most characteristics a commutative power associative loop ring is associative, may

explain why the possible existence of Jordan loop rings has been overlooked. A ring is *Jordan* if it is commutative and satisfies

$$\text{the Jordan identity} \qquad (x^2y)x = x^2(yx).$$

Paige's work (with a small correction by Marshall Osborn [30]) shows that a Jordan loop ring is associative in characteristic prime to 6, so nonassociative Jordan loop rings can exist only in characteristics divisible by 2 or by 3. As we shall see, they certainly exist in characteristic 2.

Theorem 1. [16] *Let R be a commutative, associative ring with 1 and of characteristic 2 and let L be a loop. The loop ring RL is nonassociative Jordan if and only if L is a nonassociative commutative loop satisfying the Jordan identity and either*

1. *R is a Boolean ring, that is, $r^2 = r$ for all $r \in R$, and, given any elements $x, y, z \in L$, either*

   $J1: \ (x^2y)z = x^2(yz) \ \ and \ \ x(yz^2) = (xy)z^2, \ \ or$
   $J2: \ (x^2y)z = (xy)z^2 \ \ and \ \ x(yz^2) = x^2(yz), \ \ or$
   $J3: \ (x^2y)z = x(yz^2) \ \ and \ \ x^2(yz) = (xy)z^2$

   or else

2. *$J1$ holds for all $x, y, z \in L$.*

Each of the properties RA, RA2 and SRAR is equivalent to conditions just on the loop. Those which characterize SRAR loops were given in (2), for instance. Theorem 1 highlights the first instance of a situation where the possibility of a loop ring satisfying an "interesting" identity may depend also on the coefficient ring. (No examples of this phenomenon are known as yet.)

Question 5. *Does there exist a nonassociative loop whose loop ring is Jordan over one coefficient ring of characteristic 2 but not over some other ring of characteristic 2?*

Until this question has been answered, we use the term $RJ2$ to describe a loop which has a nonassociative Jordan loop ring over **some** coefficient ring of characteristic 2.

There are other instances in the literature where the existence of an identity in an algebra may depend on the field of coefficients. L. Kokoris, for example, has shown that a Jordan algebra over a field of characteristic 2 is power associative provided that field contains at least four elements [26]. It follows from this that any loop which is $RJ2$ because it satisfies J1 identically must be power associative. We do not know if this must always be the case.

Question 6. Is an $RJ2$ loop power associative?

One can also ask an apparently stronger question.

Question 7. Is a Jordan loop ring power associative?

The second question might follow from the first, of course.

Question 8. *Is the loop ring of a power associative $RJ2$ loop power associative?*

Call a loop *Jordan* if it is commutative and satisfies the Jordan identity. Clearly any $RJ2$ loop is Jordan though the converse is certainly false. Jordan loops exist in abundance as we demonstrate with an observation and some constructions. Any commutative loop of exponent 2 is Jordan and even $RJ2$ because it clearly satisfies J1 identically. Here is a way to construct some such loops.

Let n be an odd positive integer, let $A = \{1, 2, 3, \ldots, n\}$, and define $f\colon A \times A \to \{0, 1, 2, \ldots, n-1\}$ by the rule

$$f(i,j) = \frac{1}{2}(n+1)(j-1) - \frac{1}{2}(n-1)(i-1) \pmod{n}.$$

It is easily checked that for each fixed i, $f(i,\cdot)\colon A \to \{0, 1, 2, \ldots, n-1\}$ is a bijection and for each fixed j, $f(\cdot, j)\colon A \to \{0, 1, 2, \ldots, n-1\}$ is a bijection. One can also verify that $f(i,j) = f(j,i)$ for all i, j and $f(i,i) = i - 1 \pmod{n}$ for each i. As a consequence, the $n \times n$ array whose (i,j) entry is $f(i,j) + 2$ is a symmetric Latin square on the integers $\{2, 3, 4, \ldots, n+1\}$ with (i,i) entry $i+1$. Now form the $(n+1) \times (n+1)$ table that has this square in the lower right corner with all diagonal entries changed to 1, and which has the integers $1, 2, 3, \ldots, n+1$ in their natural order in row one and in column one. The unique nonassociative commutative loop of order 6 arises from this construction with $n = 5$ and is defined by Table 1. For reasons noted, the loop ring of this loop is Jordan in characteristic 2.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	5	3	6	4
3	3	5	1	6	4	2
4	4	3	6	1	2	5
5	5	6	4	2	1	3
6	6	4	2	5	3	1

Table 1: The unique (nonassociative) Jordan loop of order 6.

The literature contains many examples of nonassociative loops constructed by "doubling" groups [35, 36, 4, 5],[15, §II.5]. Suggested by the notation $M(G, 2)$ which Orin Chein introduced for a certain family of Moufang loops, we label $J(G, \alpha)$ a Jordan loop constructed by the following theorem.

Theorem 2. [16] *Let G be an abelian group, let u be an indeterminate, let $L = G \cup Gu$ and let $\alpha\colon G \times G \to G$ be any symmetric map, that is, a map satisfying $\alpha(g, h) = \alpha(h, g)$ for all $g, h \in G$. Extend the multiplication in G to L by setting*

$$g(hu) = (hu)g = (gh)u$$

and

$$(gu)(hu) = \alpha(g, h)$$

for $g, h \in G$. The pair $(L, \cdot)$ is a loop if and only if for each $g \in G$, the function $\alpha_g\colon G \to G$ defined by $\alpha_g(x) = \alpha(g, x)$ is a bijection and, when this is the case,

1. *Jordan if and only if $\alpha(\alpha(g, g)h, g) = \alpha(g, g)\alpha(g, h)$ for all $g, h \in G$, and*
2. *associative if and only if there exists $a \in G$ such that $\alpha(g, h) = agh$ for all $g, h \in G$.*

Remark 3. *Notice that maps α which define loops correspond to $|G| \times |G|$ Latin squares with $\alpha(g, h)$ in position (g, h).*

As an example of how this theorem can be used, start with $G = \mathsf{Z}_n$, the group of integers under addition (mod n). We require a symmetric map $\alpha\colon \mathsf{Z}_n \times \mathsf{Z}_n \to \mathsf{Z}_n$ with the property that

$$\alpha(i, \alpha(i, i) + j) = \alpha(i, i) + \alpha(i, j)$$

for all $i, j \in G$. Equivalently, writing $\alpha_i(\cdot) = \alpha(i, \cdot)$ and setting $\lambda_i = \alpha_i(i)$, for each $i \in \{0, 1, 2, \ldots, n\}$, we need a bijection α_i of $\{0, 1, 2, \ldots, n-1\}$ (which becomes row i of a Latin square) satisfying

$$\alpha_i(\lambda_i + j) = \lambda_i + \alpha_i(j) \tag{4}$$

for all i, j. To avoid associativity, we must also ensure that $\alpha_i(j) - i - j$ is not constant.

One obvious solution to (4) can be obtained by setting $\lambda_i = 0$ for all i, in which case any (symmetric) Latin square with 0s on the diagonal defines a suitable α. The table

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array} \tag{5}$$

shows a smallest such square and yields the loop $J(\mathsf{Z}_4, \alpha)$ described by Table 2. While this loop is not of exponent 2, it is $RJ2$ by virtue of Theorem 4 that follows.

0	1	2	3	4	5	6	7
1	2	3	0	5	6	7	4
2	3	0	1	6	7	4	5
3	0	1	2	7	4	5	6
4	5	6	7	0	1	2	3
5	6	7	4	1	0	3	2
6	7	4	5	2	3	0	1
7	4	5	6	3	2	1	0

Table 2: The loop $J(\mathsf{Z}_4, \alpha)$ has a Jordan loop ring.

Theorem 4. *Let $L = J(G, \alpha)$ be a loop constructed as in Theorem 2. Suppose*

i. $\alpha(g^2 h, k) = g^2 \alpha(h, k)$ *and*

ii. $\alpha(\alpha(g, g)h, k) = \alpha(g, g)\alpha(h, k)$

for all $g, h, k \in G$. If $\alpha(g, h)g^{-1}h^{-1}$ is not constant, then L is $RJ2$.

Is there a future for Jordan loops? They have little structure. We have noted that they need not be power associative. They don't satisfy the inverse property, $(xy)y^{-1} = x$ (which is the same as the cross inverse property in a commutative loop), nor the weak inverse property, $y(xy)^{-1} = x^{-1}$. Also, even in a finite power associative Jordan loop where there is a well-defined notion of "order of an element," the order of an element need not divide the order of the loop nor must conjugate elements have the same order.

As to existence, we recall that any commutative loop of order less than 6 is associative and we have shown how to construct nonassociative Jordan loops of every even order $n \geqslant 6$. There are two Jordan loops of order 7 (neither of which is $RJ2$) so, by taking direct products, we have a nonassociative Jordan loop of order $7k$ for any positive integer k. A referee has reported a construction that produces Jordan loops of order $2^n - 1$ and perhaps of some other odd orders as well. All this work addresses a natural question.

Question 9. *For what positive integers n does there exist a nonassociative Jordan loop of order n?*

5. The unit loop of an alternative loop ring

Just as with associative rings, the set of invertible elements or *units* of an alternative ring is closed under multiplication and hence forms a (Moufang) loop. The loops of units in alternative loop rings present a class of Moufang loops which have been and continue to be studied from a number of points of view.

5.1 Properties shared by L and $\mathcal{U}(\mathbf{RL})$. An RA loop L is a subloop of the unit loop $\mathcal{U}(RL)$ and so one can ask what these loops might have in common. Here, the coefficient ring R is critical since, for example, over the integers, if L is finite and $\mathcal{U}(\mathbb{Z}L)$ contains nontrivial units ($\mathcal{U}(\mathbb{Z}L) \neq \pm L$), then it contains a free group [15, §VIII.5], so it is rare that $\mathcal{U}(\mathbb{Z}L)$ is nilpotent or solvable or torsion over its centre, these being known properties of L. These properties do prove interesting, however, for infinite loops and over fields. It turns out that the *torsion subloop* of L, this being the set of all elements of finite order in L (which is a subloop of an RA loop), often plays an important role. Here is a typical result.

Theorem 5. [20] *Let L be an RA loop with torsion subloop T and let K be a field of characteristic 0. Assume $\mathcal{U} = \mathcal{U}(KL)$ contains an element of infinite order. Then the following statements are equivalent:*

1. *$\mathcal{U}$ is torsion over its centre;*
2. *T is central;*
3. *$u^2 \in \mathcal{Z}(\mathcal{U})$ for all $u \in \mathcal{U}$;*
4. *$\mathcal{U}$ is torsion of bounded exponent over its centre.*

5.2 Involutions of RA Loops. An RA loop L has a canonical involution $\ell \mapsto \ell^*$, defined by lifting the involution in (1), whose fixed point set is precisely $\mathcal{Z}(L)$, the centre of L. Any involution of L extends linearly to an involution of the loop ring and, when canonical, the fixed point set of this extended involution is $\mathcal{Z}(RL)$, the centre of RL. Interestingly, this is the only involution of an RA loop with this property.

Theorem 6. *[22] Let θ be an involution of an RA loop and let $(RL)^+ = \{\alpha \in RL \mid \alpha^\theta = \alpha\}$ denote the fixed points of RL. Assuming* $\operatorname{char} R \neq 2$*, the following statements are equivalent:*

1. *$(RL)^+$ is closed under multiplication;*
2. *the elements of $(RL)^+$ commute;*
3. *$(RL)^+ = \mathcal{Z}(RL)$;*
4. *$\theta = *$ is the canonical involution on L.*

Incidentally, Polcino Milies and the author have also considered the possibility that the set $(RL)^- = \{\alpha \in RL \mid \alpha^\theta = -\alpha\}$ of skew-symmetric elements of an involution θ commute. This happens only in characteristic 2 or 4 and in characteristic 2, often with severe restrictions on L [22].

Theorem 7. [21] *Let L be a finite RA 2-loop, F a field of characteristic 2 and θ the involution of RL which is the linear extension of $\ell \mapsto \ell^{-1}$ for $\ell \in L$. If $(RL)^-$ is a commutative set, then $L = L_0 \times A$ is the direct product of an abelian group A and a loop L_0 which is either the Cayley loop or the loop $M(16\Gamma_2 c_2, 16\Gamma_2 c_2, 16\Gamma_2 c_2^\sharp, 16\Gamma_2 c_2^\sharp)$ (in the notation of Chein* [5]).

5.3 The units of a right alternative loop ring. The units of a strongly right alternative loop ring form a loop in the presence of a certain condition on the *augmentation ideal*, this being the kernel $\Delta(L)$ of the *augmentation map* $\epsilon\colon RL \to R$ which is defined by $\epsilon(\sum \alpha_\ell \ell) = \sum \alpha_\ell$. Thus

$$\Delta(L) = \{\textstyle\sum \alpha_\ell \ell \in L \mid \sum \alpha_\ell = 0\}.$$

If $\delta \in \Delta(L)$ is *nil*, that is, $\delta^n = 0$ for some $n \geqslant 1$, then it is easily checked that $1+\delta$ is a unit with inverse $1+\delta+\delta^2+\cdots+\delta^{n-1}$. (We now necessarily assume characteristic 2.) Conversely, if $u \in RL$ is a unit, then $uv = 1$ for some v yields $\epsilon(u) = 1$, because ϵ is a homomorphism, so $\delta = 1+u \in \Delta(L)$ and $u = 1+\delta$. These observations show that if $\Delta(L)$ is nil, then

$$\mathcal{U}(RL) = \{u \in RL \mid \epsilon(u) = 1\},$$

a set which is clearly closed under multiplication and hence a Bol loop.

If L is a finite 2-group or RA2 2-loop and F is a field of characteristic 2, then the augmentation ideal of FL is actually *nilpotent*: there exists a fixed n so that any product of n elements is always 0 [28, 12]. Gábor Nagy has shown the same thing for Bol 2-loops with a unique nonidentity commutator/associator [29] but the unrestricted case appears to be open.

Question 10. *If L is any SRAR 2-loop, is $\Delta(L)$ nilpotent?*

A positive answer would imply that the unit loop of RL is Bol for any SRAR loop L, a fact currently known just for SRAR loops with a unique nonidentity commutator/associator [14].

5.4 Normal Complements. As we have noted, if L is a group, then $\mathcal{U}(RL)$ is a group and if L is RA, then $\mathcal{U}(RL)$ is a loop. It is often (perhaps always) the case that if L is SRAR, then $\mathcal{U}(RL)$ is loop. Whenever this happens, it is of interest to know how L sits within $\mathcal{U}(RL)$. It is rare that L is normal. A torsion RA loop L is normal in $\mathcal{U}(\mathbb{Z}L)$, for instance, only in the trivial case that $\mathcal{U}(\mathbb{Z}L) = \pm L$ [17] and, if finite, never normal in $\mathcal{U}(FL)$ when F is a field [19].

Question 11. *Can an infinite RA loop L ever be normal in $\mathcal{U}(FL)$, F a field?*

Assuming L is not normal, it is natural then to ask just what the normalizer of L in $\mathcal{U}(RL)$ might be. Certainly L normalizes itself, as

does the centre of $\mathcal{U}(RL)$. The "normalizer conjecture," which asserts $\mathcal{N}_{\mathcal{U}}(L) = \mathcal{Z}[\mathcal{U}(RL)] \cdot L$, says that these are essentially the only normalizing sets. The conjecture is true for torsion RA loops in their integral loop rings [17].

Perhaps the most famous problem in the theory of loop rings has always been the *isomorphism problem*: When does $RL_1 \cong RL_2$ imply $L_1 \cong L_2$? Of special interest because of its connection to the isomorphism problem is the possibility that L might have a *normal complement* in $\mathcal{U} = \mathcal{U}(RL)$, a subloop N that is normal in $\mathcal{U}$ and satisfies $L \cap N = \{1\}$ and $\mathcal{U} = LN$. It is known, for example, that if L is a finite RA loop, then L has a normal complement in $\mathcal{U}(\mathsf{Z}L)$ which is also *torsion-free*: $u^n = 1$ with $n > 1$ implies $u = 1$. So the isomorphism problem has a positive solution over Z and the proof is not hard.

Theorem 8. [19, 18] *Let L and L_1 be finite RA loops and suppose that $\mathsf{Z}L_1 \cong \mathsf{Z}L$. Then $L_1 \cong L$.*

Proof. We observe that L and L_1 have the same order since each is the rank of the same free Z-module. Suppose $\varphi\colon \mathsf{Z}L_1 \to \mathsf{Z}L$ is the given isomorphism and let N be a torsion-free normal complement for L_1 in $\mathcal{U}(\mathsf{Z}L_1)$. Then $\varphi(N)$ is torsion-free in $\mathcal{U}(\mathsf{Z}L)$, so $L \cap \varphi(N) = \{1\}$ and $L\varphi(N)/\varphi(N) \cong L/(L \cap \varphi(N)) \cong L$.

Since $[\mathcal{U}(\mathsf{Z}L)\colon \varphi(N)] = |L_1| = |L| = [L\varphi(N)\colon \varphi(N)]$, we have $\mathcal{U}(\mathsf{Z}L) = L\varphi(N)$. Thus

$$L_1 \cong \mathcal{U}(\mathsf{Z}L_1)/N \cong \mathcal{U}(\mathsf{Z}L)/\varphi(N) \cong L\varphi(N)/\varphi(N) \cong L. \qquad \square$$

Another setting in which the isomorphism problem has been investigated for group rings is that where the group is a finite p-group and the coefficient ring is the field of p elements, the so-called *modular case*.

Suppose $G = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_d\rangle$ is an abelian p-group written as the direct product of cyclic groups generated by elements a_i of order $|a_i|$, $i = 1, \ldots, d$. For each d-tuple $\delta = (\delta_1, \delta_2, \ldots, \delta_d)$ of integers δ_i, $0 \leqslant \delta_i < |a_i|$ not all divisible by p, let $P(\delta) = (a_1 - 1)^{\delta_1}(a_2 - 1)^{\delta_2} \cdots (a_d - 1)^{\delta_d}$. Robert Sandling has shown that the elements $1 + P(\delta)$ generate the cyclic components of $\mathcal{U}(FG)$, F the field of p elements [33].

It is helpful to look at an example. Suppose $p = 2$ and $G = \langle a\rangle \times \langle b\rangle$ is the direct product of cyclic groups of orders 2 and 4, respectively. The

elements $P(\delta)$ are

$$\begin{aligned} x_1 &= a+1 \\ x_2 &= (a+1)(b+1) \\ x_3 &= (a+1)(b+1)^2 \\ x_4 &= (a+1)(b+1)^3 \\ x_5 &= b+1 \\ x_6 &= (b+1)^3, \end{aligned}$$

so $\mathcal{U}(FG) = \prod\langle 1+x_i\rangle$. Notice that $1+x_1 = a$ and $1+x_5 = b$, so that G is actually a direct factor of the unit group.

Now suppose G is a finite nonabelian p-group. Write

$$G/G' = \langle \bar{a}_1\rangle \times \langle \bar{a}_2\rangle \times \cdots \times \langle \bar{a}_d\rangle,$$

with $\bar{a} = G'a$ and this time, for each d-tuple $\delta = (\delta_1, \delta_2, \ldots, \delta_d)$ of integers δ_i, $0 \leqslant \delta_i < |\bar{a}_i|$ not all divisible by p, let

$$P(\delta) = (a_1 - 1)^{\delta_1}(a_2 - 1)^{\delta_2} \cdots (a_d - 1)^{\delta_d}.$$

Let $J = \Delta(G)\Delta(G') + \Delta(G')\Delta(G)$ and let $w(G)$ be the ideal generated by $1 + J$ and the set of all $1 + P(\delta)$. Under certain conditions, which include the case $|G'| = 2$ of interest to us, Sandling proves that $w(G)$ is a normal complement to G in $\mathcal{U}(FG)$ [34] and then, with just a little more work, establishes a positive solution to the isomorphism problem. Here's an example.

Writing $D_4 = \langle a, b \mid a^4 = b^2 = 1, ba = a^{-1}b\rangle$ and $C_2 = \langle c\rangle$, let $G = D_4 \times C_2$. We have $G' = \{1, s\}$ with $s = a^2$ and $G/G' = \langle \bar{a}\rangle \times \langle \bar{b}\rangle \times \langle \bar{c}\rangle \cong C_2 \times C_2 \times C_2$, so the elements $P(\delta)$ here are precisely the elements

$$\begin{aligned} x_1 &= a+1 \\ x_2 &= (a+1)(b+1) \\ x_3 &= (a+1)(c+1) \\ x_4 &= b+1 \\ x_5 &= (b+1)(c+1) \\ x_6 &= c+1 \\ x_7 &= (a+1)(b+1)(c+1). \end{aligned}$$

Since $\Delta(G') = \{0, 1+s\}$, the ideal $J = \Delta(G)(1+s) = (1+s)X$, with $X = \{1, a, b, c, ab, ac, bc, abc\}$, and the subgroup $w(G)$ generated by $1+J$ and the $1+P(\delta)$ is a normal complement to G in $\mathcal{U}(FG)$. It is delightful that the normal complements described are so concrete.

While attempts have been made to adapt Sandling's arguments to the case of RA loops, these cannot meet with success, as we now show.

Let a, b, x be three elements which do not associate in an RA 2-loop L. The LC property says $(a,x) = (b,x) = (ab,x) = s$. (Noteworthy is the fact that such elements do not exist in the associative case.) With F the field of two elements, we compute

$$\begin{aligned} x^{-1}[(a+1)(b+1)]x &= x^{-1}(ab+a+b+1)x \\ &= sab + sa + sb + 1 \\ &= 1 + s[1 + (a+1)(b+1)] \end{aligned}$$

and obtain

$$x^{-1}[1 + (a+1)(b+1)]x = s[1 + (a+1)(b+1)]. \tag{6}$$

Now think of a and b as amongst the generators of L/L' so that $1 + (a+1)(b+1) = 1 + P(\delta)$ for a certain δ. If $w(L)$ is normal, it contains the element (6), which is $s(1+P(\delta))$, so it contains s. We conclude that if $w(L)$ is normal, it is not a complement for L in $\mathcal{U}(FL)$.

This observation, of course, begs the question as to whether or not L might have some other normal complement. In this connection, we can report that Eric Moorhouse has verified computationally that none of the Moufang loops of order 16 (these are all RA2) has a normal complement in $\mathcal{U}(FL)$, F the field of two elements. Moreover, again via computation, it has been shown that three of the six nonMoufang Bol loops of order 8 (which are all SRAR) have normal complements in the units of FL (these are $B_8(\Pi_2)$, $B_8(\Pi_5)$,$B_8(\Pi_6)$ in the notation of R. P. Burn [3]), and three do not.

Question 12. *If L is an RA (even an RA2) 2-loop, can L ever have a normal complement in $\mathcal{U}(FL)$, F the field of two elements?*

Suggestion 13. *Find conditions under which L has a normal complement in $\mathcal{U}(FL)$ in the case that L is an SRAR 2-loop, F the field of two elements, assuming the units of FL form a loop.*

Tribute

This paper has been written with a heavy heart within a month of the passing of a dear friend and research partner. I met Dan Robinson at Oberwolfach in the spring of 1976. During a sabbatical year at the Georgia Institute of Technology in 1979-80, Dan told me about loops and introduced me to some basic theory. It was during that year that my first paper on alternative loop rings was written. Daniel Robinson was a wonderful friend and mathematician whom I miss every day.

References

[1] **A. A. Albert**: *On right alternative algebras*, Anal. Math. **50** (1949), 318 – 328.

[2] **R. H. Bruck**: *Some results in the theory of linear nonassociative algebras*, Trans. Amer. Math. Soc. **56** (1944), 141 – 199.

[3] **R. P. Burn**: *Finite Bol loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), 377 – 385.

[4] **O. Chein**: *Moufang loops of small order I*, Trans. Amer. Math. Soc. **188** (1974), 31 – 51.

[5] **O. Chein**: *Moufang loops of small order*, Mem. Amer. Math. Soc. **13** (1978), no. 197, 1 – 131.

[6] **O. Chein and E. G. Goodaire**: *Bol loops with more than two commutators*, preprint.

[7] **O. Chein and E. G. Goodaire**: *Loops whose loop rings are alternative*, Comm. Algebra **14** (1986), 293 – 310.

[8] **O. Chein and E. G. Goodaire**: *Is a right alternative loop ring alternative?*, Algebras Groups Geom. **5** (1988), 297 – 304.

[9] **O. Chein and E. G. Goodaire**: *Code loops are RA2 loops*, J. Algebra **130** (1990), 385 – –387.

[10] **O. Chein and E. G. Goodaire**: *When is an $L(B, m, n, r, s, t, z, w)$ loop SRAR?*, Abh. Math. Sem. Univ. Hamburg **75** (2005), 245 – 255.

[11] **E. G. Goodaire**: *Groups embeddable in alternative loop rings*, Contributions to General Algebra **7** (1991), 169 – 176.

[12] **E. G. Goodaire**: *The radical of a modular alternative loop algebra*, Proc. Amer. Math. Soc. **123** (1995), 3289 – 3299.

[13] **E. G. Goodaire**: *A brief history of loop rings*, Mat. Contemp. **16** (1999), 93 – 109.

[14] **E. G. Goodaire**: *Units in right alternative loop rings*, Publ. Math. Debrecen **59** (2001), 353 – 362.

[15] **E. G. Goodaire, E. Jespers and C. P. Milies**: *Alternative loop rings*, North-Holland Math. Studies, vol. 184, Elsevier, Amsterdam, 1996.

[16] **E. G. Goodaire and R. G. Keeping**: *Jordan loops and loop rings*, to appear, Publ. Mat. Debebrecen, post 2006.

[17] **E. G. Goodaire and Yuanlin Li**: *The normalizer conjecture in the alternative case*, Algebra Colloq. **8** (2001), 455 – 462.

[18] **E. G. Goodaire and C. P. Milies**: *Isomorphisms of integral alternative loop rings*, Rend. Circ. Mat. Palermo **37** (1988), 126 – 135.

[19] **E. G. Goodaire and C. P. Milies**: *Normal subloops in the integral loop ring of an RA loop*, Canad. Math. Bull. **44** (2001), 27 – 35.

[20] **E. G. Goodaire and C. P. Milies**: *Moufang unit loops torsion over their centres*, Quaestiones Math. **25** (2002), 1 – 12.

[21] **E. G. Goodaire and C. P. Milies**: *Symmetric units in alternative loop rings*, Algebra Colloq. **13** (2006), 361 – 370.

[22] **E. G. Goodaire and C. P. Milies**: *Involutions of RA loops*, to appear, Canad. Math. Bull., post 2006.

[23] **E. G. Goodaire and D. A. Robinson**: *A class of loops which are isomorphic to all loop isotopes*, Canad. J. Math. **34** (1982), 662 – 672.

[24] **E. G. Goodaire and D. A. Robinson**: *A class of loops with right alternative loop rings*, Comm. Algebra **22** (1995), 5623 – 5634.

[25] **E. G. Goodaire and D. A. Robinson**: *A construction of loops which admit right alternative loop rings*, Resultate Math. **59** (1996), 56 – 62.

[26] **L. A. Kokoris**: *Power-associative rings of characteristic two*, Proc. Amer. Math. Soc. **6** (1955), 705 – 710.

[27] **K. Kunen**: *Alternative loop rings*, Comm. Algebra **26** (1998), 557−564.

[28] **C. P. Milies and S. K. Sehgal**: *An introduction to group rings*, Algebras and Applications, Kluwer Academic Publishers, Dortrecht, 2002.

[29] **G. P. Nagy**: *On nilpotent loop rings and a problem of Goodaire*, Publ. Math. Debrecen **61** (2002), 549 – 554.

[30] **J. M. Osborn**: *Lie-admissible noncommutative Jordan loop rings*, Algebras Groups Geom. **1** (1984), 453 – 489.

[31] **L. J. Paige**: *A theorem on commutative power associative loop algebras*, Proc. Amer. Math. Soc. **6** (1955), 279 – 280.

[32] **D. A. Robinson**: *A Bol loop isomorphic to all loop isotopes*, Proc. Amer. Math. Soc. **19** (1968), 671 – 672.

[33] **R. Sandling**: *Units in the modular group algebra of a finite abelian p-group*, J. Pure Appl. Algebra **33** (1984), 337 – 346.

[34] **R. Sandling**: *The modular group algebra of a central-elementary-by-abelian p-group*, Arch. Math. (Basel) **52** (1989), 22 – 27.

[35] **P. Vojtěchovský**: *On the uniqueness of loops $M(G, 2)$*, Comment. Math. Univ. Carolin. **44** (2003), 629 – 635.

[36] **P. Vojtěchovský**: *A class of Bol loops with a subgroup of index two*, Comment. Math. Univ. Carolin. **45** (2004), 371 – 381.

Received May 8, 2007

Department of Mathematics and Statistics
Memorial University
St. John's, Newfoundland
Canada A1C 5S7
E-mail: edgar@math.mun.ca

Quasigroups and Related Systems **15** (2007), 19 – 46

Central automorphisms of Latin square designs and loops

Jonathan I. Hall

Abstract

We discuss special automorphisms of Latin square designs or equivalently the 3-nets that are dual to them. We focus on the relationships between these automorphisms and the algebraic properties of the associated loops, especially Moufang loops.

1. Introduction

Let O be a set and consider a relation $\mathcal{R} \subset O^3$ with the property that projection onto any pair of coordinates gives a copy of O^2. That is, for every pair a and b of (not necessarily distinct) members of O there are unique triples $(a, b, *)$, $(a, *, b)$, and $(*, a, b)$ in $\mathcal{R}$.

Such relations $\mathcal{R}$ are equivalent to Latin squares, to quasigroups, to 3-nets, and to Latin square designs. Let R, C, E be a fixed permutation of the index set $\{1, 2, 3\}$. We construct a Latin square L from $\mathcal{R}$ by, for each triple $t = (t_1, t_2, t_3) \in \mathcal{R}$, letting t_E be the entry in row t_R and column t_C. The associated quasigroup $Q = (O, \circ)$ then has L as its Cayley (multiplication) table: if $a = t_R$, $b = t_C$, and $c = t_E$, then $a \circ b = c$. Each Latin square and quasigroup occurs naturally as one of six different conjugates, coming from a fixed $\mathcal{R}$ and one of the six permutations of R, C, E.

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 $a \sim k \sim b \sim l \sim a$.

2000 Mathematics Subject Classification: 20N05.
Keywords:Latin square design, 3-net, Bol loop, Moufang loop, inverse property.
Partial support provided by the National Science Foundation, USA

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. In almost all examples of interest to us we will 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.

In this case, we may identify each line with the subset of points incident to it.

The *Latin square design* associated with the relation $\mathcal{R}$ is the partial linear space with point set $\mathcal{P} = O_1 \cup O_2 \cup O_3$ (of size $3|O|$) and line set $\mathcal{L}$ (of size $|O|^2$) given by

$$\{a_1, b_2, c_3\} \in \mathcal{L} \iff (a, b, c) \in \mathcal{R}\,.$$

Every line contains exactly three points, and x_i is collinear with y_j if and only if $i \neq j$. The noncollinearity relation on $\mathcal{P}$ is an equivalence relation whose classes O_i are the *fibers* of the Latin square design. The cardinality $|O|$ of each fiber is the *order* of the Latin square design (and Latin square and quasigroup). A Latin square design is degenerate precisely when it has order $|O| = 1$, and even in that case we may identify the unique line with its set of three incident points.

The dual of a Latin square design is a 3-*net* (sometimes 3-*web*). The line set of the 3-net is naturally partitioned into the three parallel classes of lines O_i.

In this survey we are particularly interested in automorphisms of Latin square designs (or equivalently the 3-nets dual to them) and the relationships between certain geometrically defined automorphisms and the algebraic properties of the associated quasigroups and loops.

Much of what we present here is not new. Indeed such relationships have been studied for nearly one hundred years. The equivalence of algebraic identities to the existence of various geometric automorphisms and closure of configurations goes back to Veblen and Young [33] (who considered automorphisms of projective planes and their relationship to Desargues' configurations) and to Reidermeister [29], Thomsen [31], Bol [2], and their collaborators who, in a remarkable series of papers entitled "Topologische Fragen der Differentialgeometrie," worked on 3-nets (3-webs) of parallel classes of lines in the projective plane. Tits [32] studied automorphisms of nets and their connection to groups with triality specifically in the context of the octonions and Cartan's triality groups. Glauberman [12] and Doro

[8] later defined and studied abstract groups with triality and the loops that can be used to coordinatize them. The geometric study has been revived more recently, particularly in the paper of Funk and P. Nagy [9], which describes in detail the relationships between Bol reflections on a 3-net and coordinatizing Bol loops. The approach we take here is closer to that of Hall and G.P. Nagy [16] and G.P. Nagy and Vojtěchovský [24], which discusses the case of simple Moufang loops extensively.

Since the early work in this area dealt with the study of line sets in Euclidean planes, it was naturally phrased in terms of 3-nets. We prefer the equivalent but dual world of Latin square designs and will largely stay there.

Our general reference for combinatorics is M. Hall, Jr. [17], for group theory Aschbacher [1], and for general loop theory Bruck [3] and Pflugfelder [26]. For the octonions, see [30].

2. Automorphisms of Latin square designs

Let $\mathbb{D} = (\mathcal{P}, \mathcal{L})$ be a Latin square design of order n with fibers O_R, O_C, and O_E. The group $\mathrm{Aut}(\mathbb{D})$ is the automorphism group of $\mathbb{D}$, the set of all permutations σ of $\mathcal{P} = O_R \cup O_C \cup O_E$ that take lines to lines:

$$\{a, b, c\} \in \mathcal{L} \iff \{a^\sigma, b^\sigma, c^\sigma\} \in \mathcal{L}\,.$$

Any automorphism of $\mathbb{D}$ must preserve the noncollinearity equivalence relation whose equivalence classes are O_R, O_C and O_E. The automorphism group of this equivalence relation is the wreath product $Sym(O) \wr Sym(3)$ consisting of the normal *base subgroup* $Sym(O_R) \times Sym(O_C) \times Sym(O_E)$ extended by the symmetric group of degree 3, $Sym(\{R, C, E\}) \simeq Sym(3)$. The *base subgroup* $\mathrm{BAut}(\mathbb{D})$ of $\mathrm{Aut}(\mathbb{D})$ is its intersection with the base subgroup of the wreath product. (See Section 4.1 below for further discussion of full wreath products.)

A *subdesign* $\mathbb{D}_0 = (\mathcal{P}_0, \mathcal{L}_0)$ is given by a subset $\mathcal{P}_0$ of $\mathcal{P}$ with the property that, for $l \in \mathcal{L}$, we have $l \in \mathcal{L}_0$ and $l \subseteq \mathcal{P}_0$ if and only if $|l \cap P_0| \geqslant 2$. A subdesign is a Latin square design in its own right, although we must allow for degenerate examples with one line or no lines (which happens when $\mathcal{P}_0$ is contained in a single fiber). The subset $\mathcal{P}_0$ determines $\mathbb{D}_0$ completely, so we often (with mild abuse) identify a subdesign with its set of points.

Lemma 2.1. *If A is a subset of* $\mathrm{Aut}(\mathbb{D})$*, then the set of common fixed points of A in $\mathbb{D}$ is a subdesign of $\mathbb{D}$. In particular, the subgroup of* $\mathrm{Aut}(\mathbb{D})$ *that*

fixes a fiber pointwise is semiregular on the remaining points. (*That is, only the identity fixes additional points.*)

Proof. If an automorphism fixes two points of a line, then it fixes the line and so the third point of the line. Therefore the fixed points of A form a subdesign. The smallest subdesign of $\mathbb{D}$ containing a fiber and at least one point not in that fiber is $\mathbb{D}$ itself. □

A *shear* of $\mathbb{D}$ is an automorphism that fixes one fiber pointwise and fixes the other fibers globally (that is, belongs to the base subgroup of $\mathrm{Aut}(\mathbb{D})$). By the lemma, the group of all shears with fixed fiber Q is semiregular on each of the other fibers. A basic result of the sort we are interested in here is the following, due to Praeger [28]. (See [7] for another proof.)

Theorem 2.2. *Let $\mathbb{D}$ be a Latin square design, and let Q be a fiber. Then the group S of all shears with fixed fiber Q is regular on some other fiber if and only if $\mathbb{D}$ is the Latin square design associated with the Cayley table of the group S.* □

We now come to one of the fundamental concepts of this paper. A *central automorphism* τ_a of the Latin square design $\mathbb{D}$ with *center* $a \in \mathcal{P}$ is a nontrivial automorphism of $\mathbb{D}$ that fixes the point a and all lines through it. Therefore, if τ_a exists then, for all $\{a, b, c\} \in \mathcal{L}$, we have

$$a^{\tau_a} = a, \quad b^{\tau_a} = c, \quad c^{\tau_a} = b\,.$$

In particular τ_a switches the two fibers that complement the fiber F containing a. Since every line of $\mathcal{L}$ contains two points of this complement, the permutation induced on the line set $\mathcal{L}$ by τ_a is uniquely determined. The question is whether or not the action of τ_a can be defined on the remaining points of the fiber F to be consistent with this action on the lines.

In the dual world of 3-nets, a central automorphism is usually called a *Bol reflection* [9]. There the action of a putative Bol reflection on the points of the 3-net (that is, the lines of $\mathbb{D}$) is evident, and the question is whether or not this induces a permutation of the lines of the 3-net (the points of $\mathbb{D}$).

Proposition 2.3. *In* $\mathrm{Aut}(\mathbb{D})$ *there is at most one central automorphism τ_a with center a for each $a \in \mathcal{P}$. If τ_a exists in* $\mathrm{Aut}(\mathbb{D})$*, then it has order* 2 *and is central in the stabilizer of a in* $\mathrm{Aut}(\mathbb{D})$*, and $\tau_a^g = \tau_{a^g}$ for all $g \in \mathrm{Aut}(\mathbb{D})$.*

If τ_a and τ_b exist in $\mathrm{Aut}(\mathbb{D})$ *with a and b in different fibers, then $\tau_a\tau_b$ has order* 3 *and $\langle \tau_a, \tau_b \rangle$ is isomorphic to $Sym(3)$. If this is the case, then*

there is a unique conjugacy class T of central automorphisms in $\mathrm{Aut}(\mathbb{D})$*, and the centers of the members of T form a subdesign of $\mathbb{D}$.*

Proof. If t_1 and t_2 are two central automorphisms of $\mathbb{D}$ with center a, then the automorphism t_1t_2 of $\mathbb{D}$ is trivial on both fibers off a and so is the identity by Lemma 2.1. Therefore if there is a central automorphism with center a, then it is unique and has order 2.

For $g \in \mathrm{Aut}(\mathbb{D})$, the conjugate τ_a^g is clearly a central automorphism of $\mathbb{D}$ 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 $\mathrm{Aut}(\mathbb{D})$.

In particular if $\{a, b, c\} \in \mathcal{L}$, 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

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

If τ_x and τ_y are two central automorphisms of $\mathbb{D}$, then either they are in different fibers and so conjugate in $\langle \tau_x, \tau_y\rangle \simeq Sym(3)$, or they are in the same fiber and so both conjugate to τ_z where $z \in \{a, b\}$ is not in the fiber of x and y.

If l is a line of $\mathcal{L}$ with $l \cap \{p \,|\, \tau_p \in T\} \supset \{x, y\}$, say, then $\tau_z = \tau_x^{\tau_y} \in T$, where $l = \{x, y, z\}$. □

The stength of the proposition can be seen in

Corollary 2.4. *Suppose that a, b, c are from different fibers of $\mathbb{D}$ and that $\tau_a, \tau_b, \tau_c \in \mathrm{Aut}(\mathbb{D})$. Then $\langle \tau_a, \tau_b, \tau_c\rangle$ is a quotient of $(\mathbb{Z} \times \mathbb{Z}) : Sym(3)$.*

Proof. $(\mathbb{Z} \times \mathbb{Z}) : Sym(3)$ is the Weyl group of affine type $\tilde{A}_2$ with presentation $\langle x, y, z \,|\, 1 = x^2 = y^2 = z^2 = (xy)^3 = (xz)^3 = (yz)^3\rangle$. (This has a direct proof. The subgroup $N = \langle xyzy, yxzx, zxyx\rangle = \langle xyzy, yxzx\rangle$ is easily seen to be normal and abelian, and the whole group is N extended by $\langle x, y\rangle$ which is isomorphic to $Sym(3)$.) □

The proposition shows that there is a unique maximal subdesign $\mathbb{D}_0$ of $\mathbb{D}$ with the property that every central automorphism of $\mathbb{D}_0$ exists and extends to a central automorphism of $\mathbb{D}$. It is also true that (in a sense which will be made precise at the end of Section 4.2 below) there is a unique maximal quotient design of $\mathbb{D}$ that admits all possible central automorphisms.

3. Central automorphisms and loops

Let $\mathbb{D} = (\mathcal{P}, \mathcal{L})$ be a Latin square design with fibers O_R, O_C, and O_E for the underlying set O. Any permutation (α, β, γ) from the base group $Sym(O_R) \times Sym(O_C) \times Sym(O_E)$ acts on $\mathcal{P} = O_R \cup O_C \cup O_E$, producing a Latin square design isomorphic to $\mathbb{D}$. At the level of Latin squares, this corresponds to passing to an *equivalent* Latin square by permuting rows, permuting columns, and permuting the entry labels. In the quasigroup context, we are speaking of an *isotopic* quasigroup $(O, \diamond)$ given by

$$x \circ y = z \iff x^\alpha \diamond y^\beta = z^\gamma; \quad \text{that is,} \quad p \diamond q = (p^{\alpha^{-1}} \circ q^{\beta^{-1}})^\gamma .$$

It is well-known and easy to see that every Latin square on the set $O = \{1, 2, \ldots, n\}$ is equivalent to one whose first row and first column are $1, 2, \ldots, n$ in order. That is, every quasigroup is isotopic to a *loop*, a quasigroup with a two-sided identity element 1. In particular, in the equation $xy = 1$, the element x determines its right inverse y uniquely and y determines its left inverse x uniquely. We write $x^{-1} = y$ and ${}^{-1}y = x$.

For the loop $L = (L, \cdot)$ (with mild abuse) we let $\mathbb{D}(L) = \mathbb{D}$ be the Latin square design with point set $\mathcal{P} = L_R \cup L_C \cup L_E$ 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 basic question we approach here is: how is the existence of central automorphisms of $\mathbb{D}(L)$ reflected in the algebraic properties of the loop L?

To simplify our 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.)

3.1. Inverse property loops

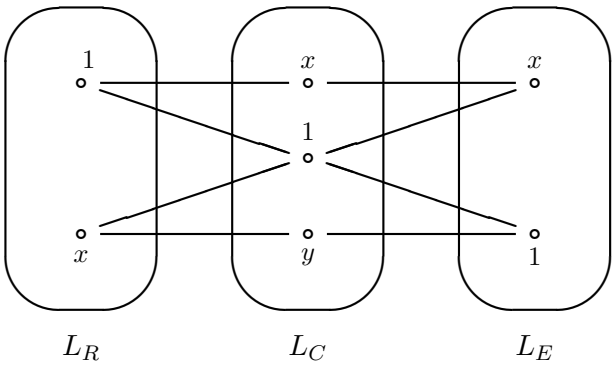
Lemma 3.1.

(a) $\kappa_1 \in \mathrm{Aut}(\mathbb{D}(L))$ *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 (that is,* ${}^{-1}x = x^{-1}$ *and* $(x^{-1})^{-1} = x$ *always) and* $x_C^{\kappa_1} = x_C^{-1}$.

(b) $\rho_1 \in \mathrm{Aut}(\mathbb{D}(L))$ *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) $\epsilon_1 \in \mathrm{Aut}(\mathbb{D}(L))$ *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 part (a) in detail, the other two parts being similar. (Indeed they are equivalent to (a) in conjugates of the loop L.) Pictures of the following type are helpful.



Suppose we have $xy = 1$ in L. We then have

$$1 \cdot x = x\,, \quad x \cdot 1 = x\,, \quad \text{and} \quad x \cdot y = 1\,,$$

giving in $\mathbb{D}(L)$ the three lines $\{1_R, x_C, x_E\}$, $\{x_R, 1_C, x_E\}$, and $\{x_R, y_C, 1_E\}$, which are drawn in the picture along with the line $\{1_R, 1_C, 1_E\}$.

Assume that κ_1 is an automorphism of $\mathbb{D}(L)$. Then $1_C^{\kappa_1} = 1_C$ and the lines $\{1_R, 1_C, 1_E\}$ and $\{x_R, 1_C, x_E\}$ through 1_C are mapped to themselves via

$$1_R^{\kappa_1} = 1_E\,, \quad 1_E^{\kappa_1} = 1_R\,, \quad x_R^{\kappa_1} = x_E\,, \quad x_E^{\kappa_1} = x_R\,.$$

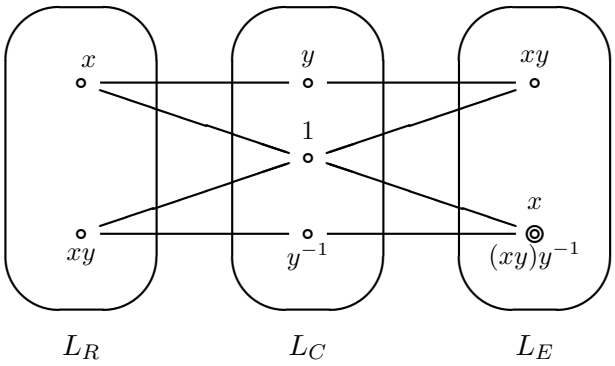
Therefore

$$\{1_R, x_C, x_E\}^{\kappa_1} = \{1_R^{\kappa_1}, x_C^{\kappa_1}, x_E^{\kappa_1}\} = \{1_E, x_C^{\kappa_1}, x_R\} = \{x_R, y_C, 1_E\}\,,$$

since a line of $\mathbb{D}$ is uniquely determined by any two of its points. In particular $x_C^{\kappa_1} = y_C$ and also $y_C^{\kappa_1} = x_C$ (as κ_1 has order 2). The first equality says that (in the fiber L_C) every element of L is moved by κ_1 to its right inverse, but the second equality says that every element is moved by κ_1 to its left inverse. Therefore right inverses are always equal to left inverses. That is,

each x has a two-sided inverse ${}^{-1}x = x^{-1}$, $(x^{-1})^{-1} = x$, and $x_C^{\kappa_1} = x_C^{-1}$, as claimed.

Next consider, for arbitrary $x, y \in \mathcal{P}$:



The lines here come from the equations

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

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

$$\{x_R^{\kappa_1}, y_C^{\kappa_1}, xy_E^{\kappa_1}\} = \{x_E, y_C^{-1}, xy_R\} = \{xy_R, y_C^{-1}, x_E\}\,.$$

As $\{xy_R, y_C^{-1}, (xy)y_E^{-1}\}$ is clearly a line of $\mathcal{L}$, we conclude that $x = (xy)y^{-1}$, proving the right inverse property.[1]

Now assume that L has the right inverse property. Thus $({}^{-1}yy)({}^{-1}y) = {}^{-1}y$, hence (by cancellation) inverses are two-sided. 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 $\mathbb{D}(L)$. □

If ρ_1, κ_1, and ϵ_1 are all automorphisms of $\mathbb{D}(L)$, then L is called an *inverse property loop*. Since the group $\langle \rho_1, \kappa_1, \epsilon_1 \rangle$ is a copy of $Sym(3)$ (by Proposition 2.3 or direct calculation) and so is generated by any two of the three central automorphisms in it, we have the immediate

[1] This argument illustrates how Reidermeister [29], Thomsen [31], Bol [2], and others were able to relate the closure of certain geometric configurations to identities satisfied by coordinatizing binary systems.

Corollary 3.2. *If the loop L has any two of the right inverse property, the left inverse property, and the anti-automorphic inverse property, then it is an inverse property loop and has all three properties.* □

3.2. Bol loops

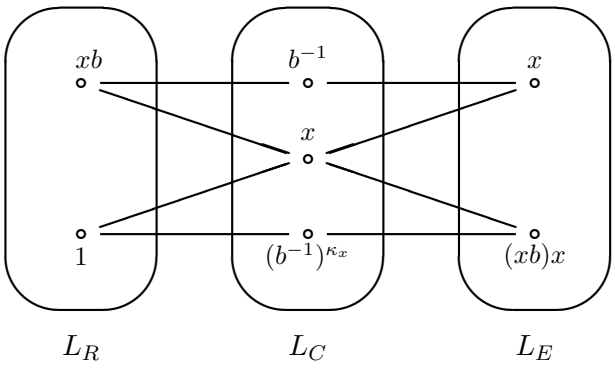
Proposition 3.3. *Let L be a loop with $\kappa_1 \in \mathrm{Aut}(\mathbb{D}(L))$. Then, for the element x of L, we have $\kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ if and only if we have*

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

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

Proof. As $\kappa_1 \in \mathrm{Aut}(\mathbb{D}(L))$ by hypothesis, L has the right inverse property by Lemma 3.1. In particular, inverses are two-sided.

Assume κ_x is an automorphism and consider

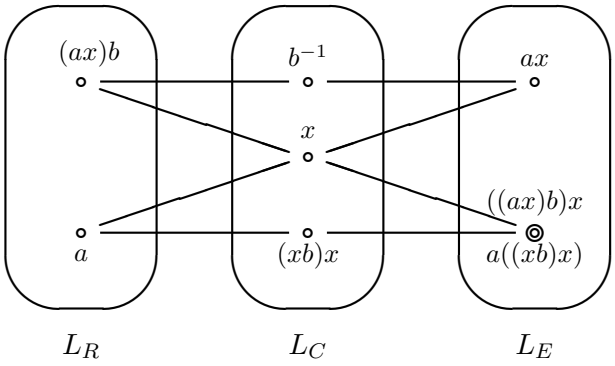


As L has the right inverse property, in picture the top line

$$\{xb_R, b_C^{-1}, (xb)b_E^{-1}\} = \{xb_R, b_C^{-1}, x_E\}$$

is indeed in $\mathcal{L}$. The image of this line under the automorphism κ_x is then the line $\{1_R, (b^{-1})_C^{\kappa_x}, (xb)x_E\}$. Therefore $(b^{-1})^{\kappa_x} = (xb)x$; and so $y^{\kappa_x} = (xy^{-1})x$, for all $y \in L$, as claimed.

The above picture is the $a = 1$ case of

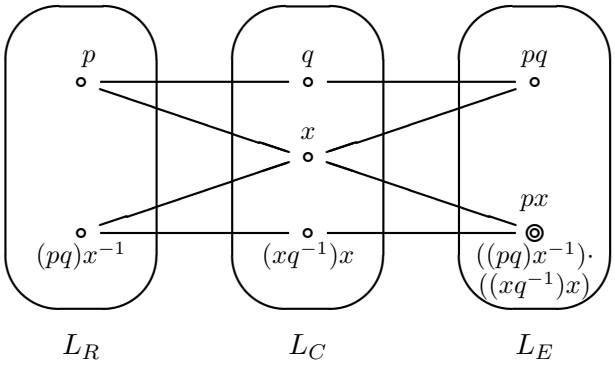


where again the top line is valid because of the right inverse property. We conclude that, for all $a, b \in L$,

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

as desired.

Conversely assume that in the right inverse property loop L we have $a((xb)x) = ((ax)b)x$, for a fixed x and all a, b. Let $\{p_R, q_C, pq_E\}$ be an arbitrary line of $\mathbb{D}(L)$. Consider



We use the given property and the right inverse property (twice) to calculate

$$((pq)x^{-1})((xq^{-1})x) = (((pq)x^{-1})x)q^{-1})x = ((pq)q^{-1})x = px\,.$$

This shows that, with the image of q_C under κ_x defined to be $(xq^{-1})x$, the image of $\{p_R, q_C, pq_E\}$ is indeed a line. Therefore κ_x is a central automorphism of $\mathbb{D}(L)$ with center x_C, as desired. □

The identity

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

is called the *right Bol identity*, and a loop in which this holds for all a, b, x is a *right Bol loop*.

Theorem 3.4. *Let L be a loop. Then L is a right Bol loop if and only if $\kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all x of L.*

Proof. Setting $b = {}^{-1}x$ in $a((xb)x) = ((ax)b)x$, we learn that a right Bol loop has the right inverse property. Therefore the theorem is an immediate consequence of Proposition 3.3. □

As already mentioned, trading L for an isotopic loop corresponds to replacing $\mathbb{D}(L)$ with an isomorphic Latin square design. Since this clearly does not affect the existence of central automorphisms, we have immediately the well-known

Theorem 3.5.

(*a*) *All loop isotopes of a right Bol loop are right Bol loops* [26, IV.6.15].

(*b*) *The loop L is a right Bol loop if and only if all its loop isotopes are right inverse property loops* [26, II.3.9]. □

Corresponding to the right Bol identity we have the *left Bol identity*

$$(x(ax))b = x(a(xb))\,.$$

A loop in which the left Bol identity holds for all a, b, x is a *left Bol loop*. The corresponding versions of the previous three results remain true (by passing to the opposite loop given by $x \diamond y = y \cdot x$).

Proposition 3.6. *Let L be a loop with $\rho_1 \in \mathrm{Aut}(\mathbb{D}(L))$. Then, for the element x of L, we have $\rho_x \in \mathrm{Aut}(\mathbb{D}(L))$ if and only if we have*

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

for all a, b in L. In this case $y^{\rho_x} = x(y^{-1}x)$ for all y in L. □

Theorem 3.7. *Let L be a loop. Then L is a left Bol loop if and only if $\rho_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all x of L.* □

Theorem 3.8.

(*a*) *All loop isotopes of a left Bol loop are left Bol loops.*

(*b*) *The loop L is a left Bol loop if and only if all its loop isotopes are left inverse property loops* [26, II.3.8]. □

Many of the properties of Bol loops can be easily derived in this context. 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.

Lemma 3.9. *Let L be a loop with $\kappa_1, \kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ 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*) *$\kappa_{x^n} \in \mathrm{Aut}(\mathbb{D}(L))$ and $(\kappa_x\kappa_1)^n = \kappa_{x^n}\kappa_1$. In particular $|x| = |\kappa_x\kappa_1|$.*

Proof. (*a*) We show that (*a*) follows from (*b*) (indeed from (*b*) with $n \in \{i, j, i+j\}$). For arbitrary z with $\kappa_z \in \mathrm{Aut}(\mathbb{D}(L))$ and arbitrary $a \in L$, we have

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

Therefore

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

as claimed.

(*b*) For $\kappa_z \in \mathrm{Aut}(\mathbb{D}(L))$ and arbitrary $y \in L$ we have $y_C^{\kappa_z} = (zy^{-1})z_C$ by Proposition 3.3. Therefore if $\kappa_y \in \mathrm{Aut}(\mathbb{D}(L))$ then by Proposition 2.3 $\kappa_z\kappa_y\kappa_z = \kappa_{(zy^{-1})z}$. 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 $\kappa_{x^n} \in \mathrm{Aut}(\mathbb{D}(L))$ 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 $\mathrm{Aut}(\mathbb{D}(L))$, so is $\kappa_{x^{n+1}} = (\kappa_x\kappa_1)^{n+1}\kappa_1$. □

Corollary 3.10. [26, IV.6.6] *Right Bol loops are power associative.* □

Of course, the same result is true for left Bol loops as well.

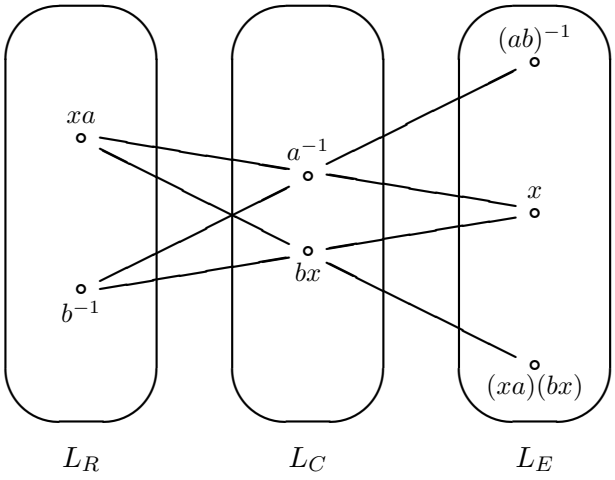
For loops admitting ϵ_1 and ϵ_x there does not seem to be a nice counterpart to the Bol identities. The following more specialized result is important in the next section.

Proposition 3.11. *Let L be an inverse property loop. Then, for the element x of L, we have $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ 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 $y^{\epsilon_x} = x(y^{-1}x)$, for all y in L.

Proof. Consider the picture



Here we have the line $\{xa_R, a_C^{-1}, x_E\}$ because of the right inverse property, line $\{b_R^{-1}, bx_C, x_E\}$ because of the left inverse property, and $\{b_R^{-1}, a_C^{-1}, (ab)_E^{-1}\}$ because of the anti-automorphic inverse property.

Suppose ϵ_x is an automorphism of $\mathbb{D}(L)$. Setting $b = 1$ we find $(a_E^{-1})^{\epsilon_x} = (xa)x_E$, and setting $a = 1$ we find $(b_E^{-1})^{\epsilon_x} = x(bx)_E$. Therefore ϵ_x can only be an automorphism if $y_E^{\epsilon_x} = x(y^{-1}x)_E$ and $(xy)x = x(yx)$ for all y in L.

As $\{b_R^{-1}, a_C^{-1}, (ab)_E^{-1}\}$ is certainly a generic line of $\mathbb{D}(L)$, we see that ϵ_x (extended to L_E as in the previous paragraph) is an automorphism of $\mathbb{D}(L)$

if and only if $(xa)(bx)$ is equal to $((ab)^{-1})^{\epsilon_x}$ for all a, b. That is, if and only if

$$(xa)(bx) = (x((ab)^{-1})^{-1})x = (x(ab))x$$

for all a, b. □

3.3. Moufang loops

We begin with a result that could well have been in the previous section.

Theorem 3.12. *For the loop L, the following are equivalent:*

(1) *for each of its points p, the Latin square design $\mathbb{D}(L)$ admits a central automorphism with center p;*
(2) *$\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all $x \in L$ and L has the right inverse property;*
(3) *$\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all $x \in L$ and L has the left inverse property;*
(4) *L is an inverse property loop with $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for all $x \in L$;*
(5) *L is right Bol and $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(6) *L is left Bol and $\epsilon_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(7) *L is right Bol and $\rho_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(8) *L is left Bol and $\kappa_x \in \mathrm{Aut}(\mathbb{D}(L))$ for some $x \in L$;*
(9) *L is right Bol and has the anti-automorphic inverse property;*
(10) *L is left Bol and has the anti-automorphic inverse property;*
(11) *L is right Bol and has the left inverse property;*
(12) *L is left Bol and has the right inverse property;*
(13) *L is an inverse property loop that is is right Bol;*
(14) *L is an inverse property loop that is is left Bol;*
(15) *L is right Bol and left Bol.*

Proof. By previous results, each of the conditions (2) – (15) is equivalent to there being a fiber F of $\mathbb{D}(L)$ and at least one additional point $p \notin F$ such that $\mathbb{D}(L)$ admits central automorphisms with center p and each f of F. This condition is clearly a consequence of (1), so it remains to prove that conversely this condition implies (1).

Let the fibers of $\mathbb{D}(L)$ be F, G, and H with $p \in G$. Then τ_p switches F and H, and so

$$\mathrm{Aut}(\mathbb{D}(L)) \supset \{\, \tau_h \,|\, h \in H \,\} = \{\, \tau_f \,|\, f \in F \,\}^{\tau_p}.$$

Next for $q \in H$ we have

$$\mathrm{Aut}(\mathbb{D}(L)) \supset \{\, \tau_g \,|\, g \in G \,\} = \{\, \tau_f \,|\, f \in F \,\}^{\tau_q}.$$

This gives (1). □

Theorem 3.13. *Let L be a loop. Then each of the following conditions is equivalent to the others and to all the condition of Theorem* 3.12.

(M1) $(xa)(bx) = (x(ab))x$ *for all* x, a, b *in* L.
(M2) $(xa)(bx) = x((ab)x)$ *for all* x, a, b *in* L.
(M3) $((ax)b)x = a(x(bx))$ *for all* x, a, b *in* L.
(M4) $((xa)x)b = x(a(xb))$ *for all* x, a, b *in* L.
(M5) *For each of its points* p, *the Latin square design* $\mathbb{D}(L)$ *admits a central automorphism with center* p.

Proof. Condition (M5) is, of course, condition (1) of Theorem 3.12.

If we substitute $a = 1$ into conditions (M1) and (M3) and $b = 1$ into (M2) and (M4), then we get the flexible law $(xc)x = x(cx)$, for all $c, x \in L$. In particular conditions (M1) and (M2) are equivalent, since they differ only by an application of the flexible law on the righthand side.

By Proposition 3.11, being an inverse property loop with condition (M1) is equivalent to condition (4) of Theorem 3.12. So we show that condition (M1) forces a loop to be an inverse property loop.

With $x = {}^{-1}b$ in (M1), an application of the flexible law gives

$$ {}^{-1}ba = ({}^{-1}ba)(b({}^{-1}b)) = ({}^{-1}b(ab))({}^{-1}b) = {}^{-1}b((ab)({}^{-1}b)) \,.$$

We cancel ${}^{-1}b$ on the left to get the right inverse property $a = (ab)({}^{-1}b)$. Similarly, setting $x = a^{-1}$, we find

$$ ba^{-1} = (a^{-1}a)(ba^{-1}) = (a^{-1}(ab))a^{-1} \,.$$

The two righthand a^{-1}'s cancel to give $b = a^{-1}(ab)$ for all a, b, and this is the left inverse property. Therefore conditions (M1) and (M2) are equivalent to all the conditions of Theorem 3.12.

Next consider condition (M3). An application of the flexible law gives $((ax)b)x = a((xb)x))$, the right Bol identity. Also $x = {}^{-1}a$ in (M3) yields

$$ b({}^{-1}a) = ((a({}^{-1}a))b)({}^{-1}a) = a({}^{-1}a(b({}^{-1}a))) \,,$$

which for $z = b({}^{-1}a)$ reads $z = a({}^{-1}az)$, a version of the left inverse property. Therefore (M3) implies condition (11) of Theorem 3.12. Conversely, assume as in (11) of Theorem 3.12 that the loop L is a right Bol loop with the left inverse property. (In particular, inverses are two-sided.) Set $a = x^{-1}$ in the right Bol identity to get

$$ bx = ((x^{-1}x)b)x = x^{-1}((xb)x)) \,.$$

The left inverse property then gives $x(bx) = (xb)x$, the flexible law. But given the flexible law, condition (M3) and the right Bol identity are equivalent. Therefore (M3) is equivalent to condition (11) of Theorem 3.12.

A similar argument to that of the previous paragraph shows that condition (M4) is equivalent to being a left Bol loop with the right inverse property, condition (12) of Theorem 3.12. (Alternatively, (M4) is (M3) in the opposite loop.) □

Loops that satisfy all the conditions of the two theorems above are called *Moufang loops* after Ruth Moufang [21] who first studied the four conditions (M1) – (M4) of Theorem 3.13. Bol [2] first proved the equivalence of these four conditions, and the further equivalence with conditions (9) – (15) is well-known. (See, for instance, [26, II.3.10,IV.6.9].) The identity (M4) was Moufang's original condition, but various authors choose any one of the four conditions to define Moufang loops. Bruck [3, p. 116] and Pflugfelder [26, p. 89] prefer (M1).

Here we are particularly interested in condition (M5). 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 seen in the proofs above), goes back to Veblen and Young [33] (who considered automorphisms of projective planes and their relationship to Desargues' configurations) and to Reidermeister [29], Thomsen [31], Bol [2], and their collaborators who worked on 3-nets (3-webs) of parallel classes of lines in the projective plane. See also Bruck [3] and Pickert [27]. Tits [32] studied automorphisms of nets and groups with triality specifically in the context of the octonions and Cartan's triality groups. The geometric study has been revived more recently, particularly in the paper of Funk and P. Nagy [9] which describes in detail the relationships between Bol reflections on a 3-net (the dual of central automorphisms of a Latin square design) and coordinatizing Bol loops. See also [16, 24].

As before, several of the well-known properties of Moufang loops are immediate from the Theorem 3.13.

Theorem 3.14.

(*a*) *All loop isotopes of a Moufang loop are Moufang loops* [26, IV.4.2].

(*b*) *The loop L is a Moufang loop if and only if all its loop isotopes are inverse property loops* [3, VII.2.3], [26, IV.4.3]. □

3.4. Multiplication groups

If L is a loop (indeed a quasigroup) then for all $x \in L$ the maps

$$\mathrm{R}(x)\colon L \longrightarrow L \quad \text{given by} \quad a^{\mathrm{R}(x)} = ax$$

and

$$\mathrm{L}(x)\colon L \longrightarrow L \quad \text{given by} \quad a^{\mathrm{L}(x)} = xa$$

are permutations of L. We then define within $Sym(L)$ the *right multiplication group*

$$\mathrm{M_R}(L) = \langle\, \mathrm{R}(x) \,|\, x \in L \,\rangle\,,$$

the *left multiplication group*

$$\mathrm{M_L}(L) = \langle\, \mathrm{L}(x) \,|\, x \in L \,\rangle\,,$$

and the *multiplication group*

$$\mathrm{M}(L) = \langle\, \mathrm{R}(x), \mathrm{L}(x) \,|\, x \in L \,\rangle = \langle\, \mathrm{M_R}(L), \mathrm{M_L}(L) \rangle.$$

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

$$\mathrm{I}(L) = \{\, \alpha \in \mathrm{M}(L) \,|\, 1^\alpha = 1 \,\}\,.$$

These groups are often useful. Indeed, in our proof of Lemma 3.9 we verified and made good use of the fact that the automorphism $\kappa_z\kappa_1$ acted as the permutation $\mathrm{R}(z)$ in its action on the fiber L_R:

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

Following on from this we easily find

Proposition 3.15. *Let L be a loop.*

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

$$\kappa_1\kappa_z \in Sym(L_R) \times Sym(L_C) \times Sym(L_E)$$

with

$$\kappa_1\kappa_z = (\,\mathrm{R}(z^{-1}),\, \mathrm{L}(z)\mathrm{R}(z),\, \mathrm{R}(z)\,)\,.$$

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

$$\rho_1\rho_z \in Sym(L_R) \times Sym(L_C) \times Sym(L_E)$$

with

$$\rho_1\rho_z = (\,\mathrm{R}(z)\mathrm{L}(z),\, \mathrm{L}(z^{-1}),\, \mathrm{L}(z)\,)\,. \qquad \square$$

We thus have

Theorem 3.16.

(*a*) *If L is a right Bol loop, then the automorphism group*

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

acts as the right multiplication group $\mathrm{M_R}(L)$ *on the fibers L_R and L_E.*

(*b*) *If L is a left Bol loop, then the automorphism group*

$$\langle\, \rho_1\rho_z \,|\, z \in L \,\rangle = \langle\, \rho_x\rho_y \,|\, x, y \in L \,\rangle$$

acts as the left multiplication group $\mathrm{M_L}(L)$ *on the fibers L_C and L_E.*

(*c*) *If L is a Moufang loop, then the automorphism group*

$$\langle\, \rho_x\rho_y, \kappa_x\kappa_y \,|\, x, y \in L \,\rangle$$

acts as the multiplication group $\mathrm{M}(L)$ *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 [9]; and they went on to explore many of its consequences, particularly for Bol loops.

The maps of the lemma and theorem are special cases of autotopisms of the loop L. An *autotopism* of L is a triple

$$(\alpha, \beta, \gamma) \in Sym(L_R) \times Sym(L_C) \times Sym(L_E)$$

with

$$x \cdot y = z \iff x^\alpha \cdot y^\beta = z^\gamma \,.$$

So an autotopism is a self-isotopy (see Section).

It is immediate that the autotopism group of L is canonically isomorphic to $\mathrm{BAut}(\mathbb{D}(L))$, the normal base subgroup of $\mathrm{Aut}(\mathbb{D}(L))$ consisting of all automorphisms of $\mathbb{D}(L)$ that leave each fiber globally fixed.

Let $\mathrm{Aut}(\mathbb{D}(L))^0$ be the normal subgroup of $\mathrm{Aut}(\mathbb{D}(L))$ that is generated by all central automorphisms. Its base subgroup

$$\mathrm{BAut}(\mathbb{D}(L))^0 = \mathrm{Aut}(\mathbb{D}(L))^0 \cap \mathrm{BAut}(\mathbb{D}(L))$$

is in turn normal in $\mathrm{Aut}(\mathbb{D}(L))$. This is the subgroup of Theorem 3.16(c).

A permutation α of the loop L is called a *pseudo-automorphism* [2] of L if $1^\alpha = 1$ and there is an autotopism (α, β, γ). We thus have by Theorem 3.16(c)

Proposition 3.17. [3, Lemma VII.3.2], [26, IV.1.6]. *If L is a Moufang loop, then the inner mapping group $\mathrm{I}(L)$ is a normal subgroup of the group of all pseudo-automorphisms of L.* □

4. Wreath products and groups with triality

4.1. Wreath products

Let Ω be a finite set and K a group. For each $x \in \Omega$, let K_x be a copy of K and set $B = \bigotimes_x K_x$, the *base group*. The symmetric group $Sym(\Omega)$ acts on B via

$$k_x^g = k_{x.g}\,,$$

for each $g \in Sym(\Omega)$. The *full wreath product* $K \wr Sym(\Omega)$ is then the extension $B.Sym(\Omega)$.

The *projection homomorphism* is the map $\pi : K \wr Sym(\Omega) \longrightarrow Sym(\Omega)$ with kernel B. The *augmented wreath product* $\mathrm{Wr}(K, \Omega)$ is the normal subgroup of the full wreath product generated by the conjugacy class $T = (a, b)^{K \wr Sym(\Omega)}$ containing the 2-cycle class of $Sym(\Omega)$. We call T the set of *transpositions* of $K \wr Sym(\Omega)$. The quotient of $K \wr Sym(\Omega)$ by $\mathrm{Wr}(K, \Omega)$ is small – the largest abelian quotient of K. Therefore we can think of $K \wr Sym(\Omega)$ and $\mathrm{Wr}(K, \Omega)$ as essentially the same group.

Two distinct transpositions of $Sym(\Omega)$ have product of order 2 or 3. Surprisingly this restricted set of product orders maintains in the full wreath product. This is made precise in the following observation of Zara [34] and Doro [8]. (See also [14, Theorem 1.1].)

Theorem 4.1. *Let T be the transposition class of the full wreath product $K \wr Sym(\Omega)$ with $|\Omega| \geqslant 3$. Let the associated projection homomorphism be $\pi : K \wr Sym(\Omega) \longrightarrow Sym(\Omega)$. Then, for all $t, r \in T$, we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,. \qquad \square$$

[2] This definition is equivalent to the usual equational definition for a pseudo-automorphism of a loop; see [26, Theorem III.4.14].

That is, the product of two transpositions remains of order 2 or 3 in the full wreath product unless the transpositions are in the same coset of the base group. A nearly complete converse of this result was given in [14, Theorem 1.2]:

Theorem 4.2. *Let T be a conjugacy class of elements of order 2 in the group $G = \langle T \rangle$; and let $\pi : G \longrightarrow Sym(\Omega)$, with $|\Omega| \geq 4$, be a homomorphism in which $\pi(T)$ is the transposition class of $Sym(\Omega)$. Further assume, for all $t, r \in T$, that we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,.$$

Then there is a group K with

$$G/Z(G) \simeq \mathrm{Wr}(K, \Omega)/Z(\mathrm{Wr}(K, \Omega))\,. \qquad \square$$

4.2. Groups with triality

The case of Theorem 4.1 that is missing from the characterization Theorem 4.2 is that of $|\Omega| = 3$. The groups satisfying the hypotheses of Theorem 4.2 with $|\Omega| = 3$ have in fact been studied extensively, starting with Glauberman [12] and Doro [8], under the name of *groups with triality*; see [9, 16, 24, 32], for instance. Such groups need not arise from wreath products, Cartan's triality groups $\mathrm{P}\Omega_8^+(\mathbb{F}) : Sym(3)$, for $\mathbb{F}$ a field, furnishing the canonical example (and the name).

We have a version of Theorem 4.2 for groups with triality. (In that case the hypotheses can be streamlined somewhat.) This presents Glauberman and Doro's correspondence between groups with triality and Moufang loops.

Theorem 4.3. *Let T be a conjugacy class of elements of order 2 in the group $G = \langle T \rangle$, and let $\pi : G \longrightarrow Sym(3)$ be a surjective homomorphism. Further assume, for all $t, r \in T$, that we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = 3.$$

Then there is a Moufang loop L (unique up to isotopy) with

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

where the class T of size $3|L|$ 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.

Conversely if L is a Moufang loop, then the group $G = \mathrm{Aut}(\mathbb{D}(L))^0$ generated by the size $3|L|$ conjugacy class T of central automorphisms is a group with triality and has the above properties with respect to the projection map π given by

$$\pi(\rho_k) = (2,3), \quad \pi(\kappa_k) = (1,3), \quad \pi(\epsilon_k) = (1,2)\,,$$

for all $k \in L$.

Proof. Given the group G with triality (as in the hypothesis), we form a partial linear space $\mathbb{D}$ whose points are the members of the class T and whose lines are the various triples of elements of T in a subgroup $S \simeq Sym(3)$ generated by members of T and having $\pi(S) = Sym(3)$. Then $\mathbb{D}$ is a Latin square design whose fibers are the three sets

$$T_R = T \cap \pi^{-1}((2,3)), \quad T_C = T \cap \pi^{-1}((1,3)), \quad T_E = T \cap \pi^{-1}((1,2))\,.$$

G acts naturally by conjugation on $\mathbb{D}$, the kernel of the action being $Z(G)$, the center of G. Each element $t \in T$ acts on $\mathbb{D}$ as the central automorphism τ_t with center t. Therefore by Theorem 3.13 there is a Moufang loop L, unique up to isotopy, with $\mathbb{D}$ isomorphic to $\mathbb{D}(L)$.

The converse follows from Proposition 2.3 and Theorem 3.13. □

In particular, we see that the Zara-Doro Theorem 4.1 in the case $|\Omega| = 3$ is associated with the fact that a group is a special type of Moufang loop. In the split octonions over the field $\mathbb{F}$, the units of norm 1 form a Moufang loop whose associated group with triality is Cartan's triality group $\mathrm{P}\Omega_8^+(\mathbb{F}) : Sym(3)$.

The previous two theorems show that there are uniquely determined minimal groups with triality (and "Ω-ality"), namely those with trivial center. There are also uniquely determined maximal (universal) groups, those with the largest possible center compatible with the hypotheses. This comes from intermediate results in [14] that also emphasize the connection between Theorems 4.2 and 4.3. (See also [11, Prop. 2.5].) We first need a definition.

Definition 4.4. For a loop L and finite set Ω of size at least 3, the group $\mathrm{UWr}(L, \Omega)$ has the following presentation:

Generators:

$\langle\langle k\,;\, a\,, b\rangle\rangle$ for arbitrary $k \in L$ and distinct $a, b \in \Omega$;

Relations:

for arbitrary $k, h \in L$ and distinct $a, b, c, d \in \Omega$ (as possible):

(1) $\langle\langle k\,;\,a\,,b\rangle\rangle^2 = 1$;
(2) $\langle\langle k\,;\,a\,,b\rangle\rangle = \langle\langle k^{-1}\,;\,b\,,a\rangle\rangle$;
(3) $\langle\langle k\,;\,a\,,b\rangle\rangle^{\langle\langle h\,;\,b\,,c\rangle\rangle} = \langle\langle kh\,;\,a\,,c\rangle\rangle$;
(4) $\langle\langle k\,;\,a\,,b\rangle\rangle^{\langle\langle h\,;\,c\,,d\rangle\rangle} = \langle\langle k\,;\,a\,,b\rangle\rangle$.

The relation (4) is empty when $|\Omega| = 3$.

By (3) the set $T = \{\,\langle\langle k\,;\,a\,,b\rangle\rangle \mid k \in L, a, b \in \Omega\,\}$ is a conjugacy class of $\mathrm{UWr}(L,\Omega)$. The class need not be in bijection with the set of the various $(k,\{a,b\})$ (for instance, by (2) if L does not have two-sided inverses).

It is routine to check that $\mathrm{UWr}(L,\Omega)$ satisfies the hypotheses of Theorem 4.2 (for $|\Omega| \geqslant 3$) with respect to the class T and $\pi(\langle\langle k\,;\,a\,,b\rangle\rangle) = (a,b) \in Sym(\Omega)$. Indeed, if L is a group, then $\mathrm{Wr}(L,\Omega)$ is a quotient of $\mathrm{UWr}(L,\Omega)$ (as suggested by Theorem 4.1) with the transposition class and T in bijection (and so the kernel is central).

If L is a Moufang loop and $\Omega = \{R, C, E\}$ then, by Proposition 2.3 and Theorem 3.13, $\mathrm{Aut}(\mathbb{D}(L))^0$ is a homomorphic image of the group with triality $\mathrm{UWr}(L,\Omega)$ and the class T of $\mathrm{UWr}(L,\Omega)$ is in bijection with the class of central automorphisms (so again the kernel is central). The homomorphism and bijection are given by

$$\langle\langle k\,;\,2\,,3\rangle\rangle \mapsto \rho_k, \quad \langle\langle k\,;\,1\,,3\rangle\rangle \mapsto \kappa_k, \quad \langle\langle k\,;\,1\,,2\rangle\rangle \mapsto \epsilon_k\,.$$

(This also explains why we do not need relations describing the conjugations $\langle\langle k\,;\,a\,,b\rangle\rangle^{\langle\langle h\,;\,a\,,b\rangle\rangle}$; by Corollary 2.4 such relations are consequences of those already specified.)

These two classes of examples are essentially all there are.

Theorem 4.5. *Let T be a conjugacy class of elements of order 2 in the group $G = \langle T\rangle$; and let $\pi : G \longrightarrow Sym(\Omega)$, with $|\Omega| \geqslant 3$, be a homomorphism in which $\pi(T)$ is the transposition class of $Sym(\Omega)$. Further assume, for all $t, r \in T$, that we have*

$$\text{if } \pi(t) \neq \pi(r), \text{ then } |\pi(t)\pi(r)| = |tr|\,.$$

Then there is a Moufang loop L (unique up to isotopy) and a central subgroup Z of $\mathrm{UWr}(L,\Omega)$ with

$$G \simeq \mathrm{UWr}(L,\Omega)/Z\,.$$

Here the class T has size $3|L|$ and is in bijection with the class $\{\langle\langle k\,;\,a\,,b\rangle\rangle\}$ of $\mathrm{UWr}(L,\Omega)$. The map π factors through the natural map that takes each $\langle\langle k\,;\,a\,,b\rangle\rangle$ to $(a,b) \in Sym(\Omega)$.

If additionally $|\Omega| \geqslant 4$, then the Moufang loop L is a group. □

For $|\Omega| \geqslant 4$ this is essentially [14, Theorem 3.7], which is the major step in the proof of Theorem 4.2 (that is, [14, Theorem 1.2]). For $|\Omega| = 3$ this is essentially [14, Theorem 4.1] and is an easy consequence of Theorem 4.3 above and intermediate results proven in [14].

For $|\Omega| = 3$ this theorem can also be thought of as locating a unique largest Moufang quotient of a given loop or, equivalently, for each Latin square design giving the unique maximal quotient design (possibly of order 1) that admits all possible central automorphisms (as promised at the end of Section 2).

4.3. Generalized dihedral loops

The previous section suggests that one way of finding nice Moufang loops is to find nice groups with triality.[3]

A dihedral group G is one that has a normal cyclic subgroup H of index 2 such that every element g of $G \setminus H$ has order 2 and by conjugation inverts all elements h of H; that is, $gh = h^{-1}g$.

We say that the loop L is *generalized dihedral* precisely when it has a subloop H of index 2 such that every element g of $L \setminus H$ has order 2 and by conjugation inverts all elements h of H via $gh = h^{-1}g$. Dihedral groups provide examples of generalized dihedral Moufang loops.

A result of Chein [4, Theorem 1] gives

Theorem 4.6. *If L is a generalized dihedral Moufang loop, then the subloop H is a group. For any group H there is a generalized dihedral Moufang loop L with H as its distinguished subloop of index 2, and such an L is uniquely determined up to isomorphism.* □

A construction equivalent to Chein's was given by R.T. Curtis [6] but was not published. Chein and Curtis gave the Cayley table of L in a simple form which is derived from that of H.

Here the crucial but elementary observation is this:

> The symmetric group $Sym(3) = Sym(\{1,2,3\})$ is a homomorphic image of $Sym(4) = Sym(\{1,2,3,4\})$ with transpositions mapped to transpositions.

Therefore by Theorem 4.1 for any group H the augmented wreath product group $\mathrm{Wr}(H, \{1,2,3,4\})$ is a group with triality and so is associated as

[3] Equally well, nice groups with triality can be found from nice Moufang loops. Witness the unit octonions and Cartan's triality groups.

in the previous section with a Moufang loop L. The loop turns out to be generalized dihedral.

Theorem 4.7. [14, Theorem 4.4] *Let H be a group. Then the group* $\mathrm{UWr}(H, \{1,2,3,4\})$ *is isomorphic to* $\mathrm{UWr}(L, \{1,2,3\})$*, the universal group with triality associated with the generalized dihedral Moufang loop L having H as its distinguished subloop of index* 2. □

The theorem says that generalized dihedral Moufang loops come up naturally, namely as those Moufang loops arising from groups with triality that are full wreath products by the symmetric group of degree 4.

5. 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 octonions 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 [25].

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 and $\ker \pi = G$.

Lemma 5.1. [8, Cor.1.1] *Let L be a Moufang loop. Then L is simple if and only if* $\mathrm{BAut}(\mathbb{D}(L))^0$ *is triality-simple.* □

Lemma 5.2. [8, 23] *Let G be a nonabelian triality-simple group. Then one of:*

(a) *$G.S \simeq N \wr Sym(3)$ for a nonabelian simple group N,*

(b) *G is simple.* □

In the second lemma, since $S \simeq Sym(3)$ and G is nonabelian and S-simple, there must be a nonabelian simple group N with G the direct product of k copies of N for $k \in \{1,2,3,6\}$. The case $k = 1$ is conclusion (b). Doro showed that, for a triality-simple group, $k = 6$ is not possible and $k = 3$ leads to conclusion (a). He also showed that in the special case of finite nonabelian triality-simple groups $k = 2$ cannot occur. Nagy and Valsecchi later proved that for arbitrary nonabelian triality-simple groups $k = 2$ leads to a contradiction.

5.1. Finite simple Moufang loops

Liebeck [19], using the classification of finite simple groups, proved

Theorem 5.3. *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 $\mathbb{F}$.* □

With Lemmas 5.1 and 5.2 this yields

Theorem 5.4. [19, 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 $\mathbb{F}$.* □

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 [5] that Lagrange's Theorem remains true for finite Moufang loops. A result of Bruck [3, 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 5.4 it remained to check whether or not Lagrange's Theorem holds in finite Paige loops. This was recently done by several groups of people independently, the first being Grishkov and Zavarnitsine [13]. Therefore we have

Theorem 5.5. [10, 11, 13, 20] *Every subloop of the finite Moufang loop L has order that divides the order of L.* □

All of the proofs relate subloops of the octonions 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.

Just a few years ago, it was possible to say [5] that the two most important problems in loop theory were the Lagrange Property for finite Moufang loops and the existence of finite simple Bol loops that are not Moufang. Now both problems have been resolved positively. Nevertheless, as pointed out by the referee, it is still open as to whether all finite Bol loops have the Lagrange Property. Bruck's result [3, Lemma V.2.1] again reduces this to the case of simple loops. But Nagy's examples [22] of finite simple Bol loops that are not Moufang show that much remains to be done. In particular, the corresponding result to Doro's Lemma 5.1 is false, since Nagy's smallest example L (of order 24) has $\mathrm{Aut}(\mathbb{D}(L))^0$ solvable.

5.2. Locally finite simple Moufang loops

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.

A great deal of work has been done in the last twenty-five years on the classification and properties of locally finite simple groups (for instance, [15, 18]). Certain techniques go over to Moufang loops, allowing us to extend Liebeck's theorems by replacing every instance of "finite" by "locally finite."

Theorem 5.6. *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 $\mathbb{F}$.* □

Theorem 5.7. *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 $\mathbb{F}$.* □

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

Corollary 5.8. *An uncountable locally finite simple Moufang loop is associative and so is a locally finite simple group.* □

The proofs will appear elsewhere. A crucial initial observation is that the Moufang loop L is locally finite if and only if the associated universal group with triality $\mathrm{UWr}(L, 3)$ is locally finite. This is proven using Theorem 4.5 above. The rest of the argument then uses the techniques of locally finite group theory as found in [15, 18].

References

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

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

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

[4] **O. Chein**: *Moufang loops of small order. I*, Trans. Amer. Math. Soc. **188** (1974), 31 – 51.

[5] **O. Chein, M. K. Kinyon, A. Rajah and P. Vojtěchovský**: *Loops and the Lagrange property*, Results Math. **43** (2003), 74 – 78.

[6] **R. T. Curtis**: *Rayleigh Prize essay*, University of Cambridge, 1970.

[7] **A. Devillers and J. I. Hall**: *Rank* 3 *Latin square designs*, J. Combin. Theory, Ser. A, **113** (2006), 894 – 902.

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

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

[10] **S. M. Gagola III**: *Subloops of the unit octonions*, Acta Sci. Math. (Szeged) **72** (2006), 837 – 861.

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

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

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

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

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

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

[17] **M. Hall, Jr.**: *Combinatorial Theory*, Second edition, John Wiley & Sons, Inc., New York, 1986.

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

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

[20] **G. E. Moorhouse**: personal communication, August 2004.

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

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

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

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

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

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

[27] **G. Pickert**: *Projektive Ebenen*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.

[28] **C. E. Praeger**: *A note on group Latin squares*, J. Combin. Math. Combin. Comput. **5** (1989), 41 – 42.

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

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

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

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

[33] **O. Veblen and J. W. Young**: *Projective Geometry*, Ginn and Co., Boston, 1916, 1917.

[34] **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

Received June 8, 2007

Quasigroups and Related Systems **15** (2007), 47 – 76

Loops related to geometric structures

Helmut Karzel

Abstract

There are many connections between loops and geometries:

- one can derive loops from several geometries and then use these loops for a "coordinatization" of the geometries,
- one can start from loops with certain properties and associate to them geometric structures or
- one can use geometric structures – for instance "chain structures" or "graphs" – in order to represent loops.

Some of these relations I like to discuss here.

1. Introduction and historical remarks

In many geometries we observe the following situation. There is a set P of geometric objects (like points, lines, planes, circles etc.) and a distinct set Γ of permutations of P (like collineations, motions, automorphisms etc.) such that for any two objects $a, b \in P$ there is exactly one permutation in Γ – denoted by $[a \to b]$ – mapping a onto b. Thus the pair (P, Γ) is a *regular permutation set*. Such a situation we obtain for instance if we take for P the set of all points of an Euclidean, or more generally an absolute geometry, and for Γ all reflections in points. More precisely, many geometries $(P, \mathfrak{L}, \equiv)$ (P denotes the set of points, $\mathfrak{L}$ the set of lines and $\equiv$ the congruence relation) in particular absolute and some unitary geometries have the properties:

1. For all $a \in P$ there exists exactly one involutory motion $\tilde{a}$ with $Fix\,\tilde{a} = \{a\}$.
2. Any two points $a, b \in P$ have exactly one midpoint $m \in P$ hence $\widetilde{m}(a) = b$.

2000 Mathematics Subject Classification: Primary 20N05.
Keywords: loop, quasigroup, Bol loop, loop derivation, reflection structure, tranversal.

3. For all a,b $\in P$ it holds $\widetilde{\tilde{a}(b)} = \tilde{a} \circ \tilde{b} \circ \tilde{a}$.

Now if (P, Γ) is a regular permutation set and if we fix an arbitrary element $o \in P$, then the set P becomes with respect to the binary operation,

$$a + b := [o \to a] \circ [o \to o]^{-1}(b)$$

a loop $(P, +)$. This construction we call *loop derivation of* (P, Γ) *in the element* o. On the other side, for a given loop $(P, +)$ we obtain a regular permutation set. For $a \in P$ let $a^+(x) := a + x$, hence a^+ is a permutation of P. Let $P^+ := \{p^+ \mid p \in P\}$, $\nu : P \to P;\ x \mapsto (x^+)^{-1}(o)$ and $a^\circ := a^+ \circ \nu$. Then the pair (P, P°) with $P^\circ := \{p^\circ \mid p \in P\}$ is a regular permutation set – called the *permutation derivation of* $(P, +)$ – having the property that p° interchanges the elements o and p. The loop derivation of (P, P°) in the element o reproduces the loop $(P, +)$.

With these derivations we can translate properties of one structure in properties of the other.

Any arbitrary permutation set (E, Γ) (i.e., we claim only that Γ is a subset of the symmetric group $Sym\, E$ of the set E) can be represented as a chain structure $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ (cf. section 7, 8, 9) and so also any loop $(E, +)$ via the permutation set (E, E^+) and we have inter alia:

Let (E, Γ) *be a permutation set and* $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ *the corresponding chain structure, then* (E, Γ) *is regular* (*sharply* 2*-transitive; sharply* 3*-transitive*) *if and only if* $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ *is a web* (2*-structure; hyperbola structure*).

Of particular interest are invariant reflection structures (P, Γ) and their corresponding K-loops (= Bruck loops) (cf. section 6). Among these structures there are the ordinary point reflection spaces $(P, \widetilde{P})$ characterized by the "three reflection properties" (R1) and (R2) which allow us to define lines such that P together with the set $\mathfrak{L}$ of all lines forms an incidence space $(P, \mathfrak{L})$. Examples are the set P of points and the set $\widetilde{P}$ of all point reflections of a hyperbolic space. If we fix a point $o \in P$ in an ordinary point reflection spaces $(P, \widetilde{P})$ and consider the loop derivation $(P, +)$ in o, then each line $L \in \mathfrak{L}$ passing through o is a commutative subgroup of the loop $(P, +)$. Taking the loop $(P, +)$ and the set $\mathfrak{F} := \{F \in \mathfrak{L} \mid o \in F\}$ of all lines containing o we obtain a "coordinatization" $(P, +, \mathfrak{F})$ of the point reflection space $(P, \widetilde{P})$ like in analytic geometry where $(P, +)$ is a vector space and $\mathfrak{F}$ the set of one dimensional vector subspaces. The points of the corresponding point reflection space or affine space, respectively, are the

elements of P and the lines are in both cases the cosets $a + F$ with $a \in P$ and $F \in \mathfrak{F}$ (cf. Theorems 10.1, 11.5, 11.6).

Now we give some historical remarks on incidence groups and the generalisation to geometric spaces with a loop structure. A tripel $(P, \mathfrak{L}, \cdot)$ consisting of a group $(P, \cdot)$ and an incidence space $(P, \mathfrak{L})$ such that for each $a \in P$ the map

$$a^{\cdot} : P \to P; \quad x \mapsto a \cdot x$$

is a collineation of the incidence space $(P, \mathfrak{L})$ is called *incidence group*. Of interest there are the following subclasses. An incidence group $(P, \cdot, \mathfrak{L})$ is called:

fibered	if any line $L \in \mathfrak{L}$ containing the neutral element e of the group $(P, \cdot)$ is a subgroup of $(P, \cdot)$,
2-*sided*	if for all $a \in P$ also the map $^{\cdot}a : P \to P; \quad x \mapsto x \cdot a$ is a collineation of the incidence spacs $(P, \mathfrak{L})$,
kinematik space	if $(P, \mathfrak{L}, \cdot)$ is fibered and 2-sided.

If $(P, \mathfrak{L}, \cdot)$ is an incidence group then the set $\mathfrak{F} := \{L \in \mathfrak{L} \mid e \in L\}$ is a *bundle in* e, i.e., $\bigcup \mathfrak{F} = P$ and for all $A, B \in \mathfrak{F}$ with $A \neq B$ it holds $A \cap B = \{e\}$, and we have $\mathfrak{L} = \{a \cdot F \mid a \in P, \ F \in \mathfrak{F}\}$. If $(P, \mathfrak{L}, \cdot)$ is fibered then $\mathfrak{F}$ is a *fibration* (*partition*) of the group $(P, \cdot)$, i.e., $\mathfrak{F}$ is a bundle and a set of proper subgroups of the group $(P, \cdot)$. If $(P, \mathfrak{L}, \cdot)$ is even a kinematik space then $\mathfrak{F}$ is a *kinematik fibration*, i.e., $\mathfrak{F}$ has the additional property that for all $X \in \mathfrak{F}$ and for all $a \in P$ it holds $a \cdot X \cdot a^{-1} \in \mathfrak{F}$. On the other hand, if $\mathfrak{F}$ is a bundle of a group $(P, \cdot)$ in the neutral element e of $(P, \cdot)$ and if we set $\mathfrak{L} := \{a \cdot F \mid a \in P, \ F \in \mathfrak{F}\}$ then $(P, \mathfrak{L}, \cdot)$ is an incidence group if and only if the following condition is satisfied:

$$(f) \qquad \forall a \in P \ \forall X \in \mathfrak{F} \ \ e \in a \cdot X \ \Rightarrow \ a \cdot X \in \mathfrak{F}.$$

Clearly if $\mathfrak{F}$ is a fibration of the group $(P, \cdot)$ then $\mathfrak{F}$ satisfies the condition (f) and so there is a one to one correpondence between fibered incidence groups (kinematik spaces) and fibrations (kinematik fibrations) of groups.

The notion of incidence group was generalized by weakening the assumptions concerning the algebraic structure. The group $(P, \cdot)$ was replaced by a loop or even a groupoid by H. Wähling, G. Kist, M. Marchi, E. Zizioli and the author (cf. [8], [26], [18], [22], [11], [27]). In [11] the concepts "fibration" and "kinematic fibration" were used also for loops. In 1987 Elena Zizioli found out that for a general loop these notions are not enough to produce

a fibered incidence loop. She showed that the conditions $(f) = (F4)$ and $(F5)$ (cf. section 11) are necessary and sufficient. Such fibrations (satisfying $(F4)$ and $(F5)$) are called *incidence fibrations* (cf. [27], [16], [18] Sec. 8).

E. Kolb and A. Kreuzer [19] defined in a loop $(P,+)$ with the help of the defect function $\delta_{a,b}$ (cf. section 5) the binary relation "$a \sim b \Leftrightarrow \delta_{a,b} = id$". Under the assumption that $\sim$ is an equivalence relation, they showed that the equivalence classes form an incidence fibration.

2. Notations and known results

Permutation sets. In this paper P will always denote a non empty set, $Sym\,P$ the group of all permutations of the set P, $J := \{\sigma \in Sym\,P \mid \sigma^2 = id\}$ and $J^* := J \setminus \{id\}$. A pair (P,Γ) with $\Gamma \subseteq Sym\,P$ is called *permutation set* and we call a permutation set

Bol set	if for each $\gamma \in \Gamma$, $\gamma \circ \Gamma \circ \gamma = \Gamma$,
symmetric	if for each $\gamma \in \Gamma$, $\gamma \circ \Gamma^{-1} \circ \gamma = \Gamma$,
invariant	if for each $\gamma \in \Gamma$, $\gamma \circ \Gamma \circ \gamma^{-1} = \Gamma$,
involution set	if $\Gamma \subseteq J$.

For a permutation set (P,Γ) we define for $a,b \in P$:

$$[a \to b] := \{\gamma \in \Gamma \mid \gamma(a) = b\}.$$

Then we call a point $p \in P$ *semiregular* (*transitive*), if for each $x \in P$ we have $|[p \to x]| \leqslant 1$ ($|[p \to x]| \geqslant 1$), and we call $p \in P$ *regular* if $|[p \to x]| = 1$.

By P_s (P_t) we denote the set of all semiregular (transitive) points and by P_r or $(P,\Gamma)_r$ the set of all regular points of (P,Γ). The pair (P,Γ) is called *regular permutation set* if $P = P_r$.

2.1. *Let (P,Γ) be a permutation set. Then:*

(1) *(P,Γ) is a Bol set if and only if (P,Γ) is symmetric and $\Gamma = \Gamma^{-1}$.*

(2) *If (P,Γ) is symmetric and $\sigma \in Sym\,P$ then $(P,\sigma \circ \Gamma)$ is symmetric.*

(3) *If (P,Γ) is symmetric and $\sigma \in \Gamma$ then $(P,\sigma^{-1} \circ \Gamma)$ is a Bol set with $id \in \sigma^{-1} \circ \Gamma$.*

(4) *If (P,Γ) is a Bol set and $\sigma \in Sym\,P$ with $\sigma \circ \Gamma \circ \sigma = \Gamma$, in particular if $\sigma \in \Gamma$, then $(P,\sigma \circ \Gamma)$ is a Bol set.*

(5) *If (P,Γ) is an involution set then the notions "symmetric", "Bol set" and "invariant" coincide.*

Proof. (1) If (P,Γ) is a Bol set and $\gamma \in \Gamma$ then $\gamma \circ \Gamma \circ \gamma = \Gamma$ implies $\gamma^{-1} \circ \Gamma \circ \gamma^{-1} = \Gamma$ hence $\gamma^{-1} \circ \gamma \circ \gamma^{-1} = \gamma^{-1} \in \Gamma$, i.e., $\Gamma^{-1} = \Gamma$ and so $\gamma \circ \Gamma^{-1} \circ \gamma = \gamma \circ \Gamma \circ \gamma = \Gamma$.

(2) Let $\gamma \in \Gamma$ then $(\sigma \circ \gamma) \circ (\sigma \circ \Gamma)^{-1} \circ (\sigma \circ \gamma) = \sigma \circ \gamma \circ \Gamma^{-1} \circ \sigma^{-1} \circ \sigma \circ \gamma = \sigma \circ (\gamma \circ \Gamma^{-1} \circ \gamma) = \sigma \circ \Gamma$ hence $(P, \sigma \circ \Gamma)$ is symmetric.

(3) By (2) $\sigma^{-1} \circ \Gamma$ is symmetric and $\sigma \circ \Gamma^{-1} \circ \sigma = \Gamma$ implies $\sigma^{-1} \circ \Gamma = \Gamma^{-1} \circ \sigma = (\sigma^{-1} \circ \Gamma)^{-1}$, i.e., by (1) $(P, \sigma^{-1} \circ \Gamma)$ is a Bol set.

(4) follows in the same way as (2). □

Binary operation. If P is provided with a binary operation " $+$ ", we define for $a \in P$:

$$a^+ : P \to P; \quad x \mapsto a + x,$$

$$^+a : P \to P; \quad x \mapsto x + a,$$

$$P^+ := \{a^+ \mid a \in P\} \quad \text{and} \quad {}^+P := \{{}^+a \mid a \in P\}.$$

An element $o \in P$ is called *left* (*right*) *zero element* if $o^+ = id$ ($^+o = id$), and *zero element* if $o^+ = {}^+o = id$. $(P,+)$ is called *left* (*right*) *quasigroup* if $P^+ \subseteq Sym\, P$ (${}^+P \subseteq Sym\, P$) and *quasigroup* if $P^+ \cup {}^+P \subseteq Sym\, P$, and *left* (*right*) *loop* or *loop*, respectively, if moreover $(P,+)$ has a zero element.

If $(P,+)$ is a left loop, hence $P^+ \subseteq Sym\, P$, then for all $a, b \in P$ also

$$\delta_{a,b} := ((a+b)^+)^{-1} \circ a^+ \circ b^+ \in Sym\, P$$

is a permutation fixing the element o. Therefore to each left loop $(P,+)$ there corresponds the subgroup $\Delta := \langle \{\delta_{a,b} \mid a, b \in P\} \rangle$ of $Sym\, P$, generated by all these maps. We have:

2.2. *$(P,+)$ is a quasigroup if and only if (P, P^+) is a regular permutation set.*

2.3. *Let (P,Γ) be a permutation set with $P_r \neq \emptyset$, let $o \in P_r$ be fixed and for $a, b \in P$ we define $a^\bullet := [o \to a]$, $P^\bullet := \{a^\bullet \mid a \in P\}$ and*

$$a \oplus b := [o \to a](b) = a^\bullet(b),$$

$$a + b := [o \to a] \circ [o \to o]^{-1}(b) = a^\bullet \circ (o^\bullet)^{-1}(b).$$

Then

(1) $P^\bullet = \Gamma$.

(2) *$(P, \oplus)$ is a left quasigroup with the property "$\forall a \in P : a \oplus o = a$".*

(3) *$(P,+)$ is a left loop with o as zero element.*

(4) *If (P,Γ) is invariant then (P,Γ) is a regular permutation set, hence*

$P = P_r$.

(5) *If* (P, Γ) *is a regular permutation set then* $(P, \oplus)$ *is a quasigroup with the right zero element* o*, and* $(P, +)$ *is a loop with the zero element* o.

Proof. (4) Let $a, b \in P$ be given, let $c := [o \to a]^{-1}(b)$, $\gamma := [o \to a] \circ [o \to c] \circ [o \to a]^{-1}$ and $d := \gamma(o)$ then (by the invariance) $\gamma \in \Gamma$, hence (by $o \in P_r$) $\gamma = [o \to d]$ and $\gamma(a) = [o \to a] \circ [o \to c](o) = [o \to a](c) = b$. Therefore γ is the unique element in Γ mapping a onto b. □

Definition 1. If (P, Γ) is a permutation set with $P_r \neq \emptyset$ and $p \in P_r$, let $\tilde{p} := [p \to p]$, $\widetilde{P_r} := \{\tilde{p} \mid p \in P_r\}$. Then for each $p \in P_r$ the binary operation

$$+_p : P \times P \to P; \quad (a, b) \mapsto a + b := [p \to a] \circ \tilde{p}^{-1}(b)$$

is called the *loop derivation of* (P, Γ) *in the point* p. Moreover if (P, Γ) is regular and $o \in P$ we set:

$$\nu = \nu_o : P \to P; \quad x \mapsto \widetilde{o} \circ [o \to x]^{-1}(o),$$

$$\omega = \omega_o := \widetilde{o}^{-1} \circ \nu : P \to P; \quad x \mapsto [o \to x]^{-1}(o),$$

$$P^\circ := \Gamma \circ \omega = \{a^\circ := [o \to a] \circ \omega \mid a \in P\}.$$

We remark that $\nu(x) = [o \to o] \circ [o \to x]^{-1}(o) = (x^+)^{-1}(o)$ and we denote

$$-x := \nu(x) = (x^+)^{-1}(o).$$

For $a, b \in P$ we write $a - b := a + (-b)$.

2.4. *If* $(P, +)$ *is a left loop and* $\mu \in Sym\, P$ *any permutation with* $\mu(o) = o$*, then* $(P, P^+ \circ \mu)$ *is a permutation set with* $o \in (P, P^+ \circ \mu)_r$ *and the loop derivation of* $(P, P^+ \circ \mu)$ *in the point* o *gives us back the original left loop* $(P, +)$.

Definition 2. Let $(P, +)$ be a left loop with $-x = \nu(x)$. If $\nu \in Sym\, P$, let $P^\circ := P^+ \circ \nu = \{x^\circ := x^+ \circ \nu \mid x \in P\}$. Then (P, P°) is called *permutation derivation of the left loop* $(P, +)$. If $(P, +)$ is a loop and $p \in P$, let $2'p$ be the solution of the equation $x - p = p$. Then $\widetilde{p} := (2'p)^\circ$ (recall that $\widetilde{p}$ is the unique permutation of P° fixing p) and $\widetilde{\widetilde{p}} := p^+ \circ \nu \circ (p^+)^{-1}$.

2.5. *If $(P,+)$ is a left loop then:*

(1) $\nu \in Sym\, P \Leftrightarrow o \in (P,(P^+)^{-1})_r$.

(2) *If $(P,+)$ is obtained by the loop derivation of a permutation set (P,Γ) in a point $o \in (P,\Gamma)_r$ then* $\nu \in Sym\, P \Leftrightarrow o \in (P,\tilde{o}\circ\Gamma^{-1})_r$.

(3) *If $(P,+)$ is a loop then $\nu \in Sym\, P$ hence we can form the permutation derivation (P,P°) and the loop derivation of (P,P°) in o reproduces the original loop $(P,+)$.*

Definition 3. A loop $(P,+)$ is called:

(*)-loop	if (*) $\forall a,b \in P : a-(a-b)=b$;
Bol loop	if for all $a,b \in P$ we have $a^+\circ b^+\circ a^+ \in P^+$, i.e., $a+(b+(a+x))=(a+(b+a))+x$ and (P,P^+) is a Bol set;
Bruck loop or *K-loop*	if $(P,+)$ is a Bol loop and if $\nu \in Aut(P,+)$, i.e., $-(a+b)=(-a)+(-b)$.

2.6. *Let (P,Γ) be a Bol set with $P_r \neq \emptyset$ and $(P,+)$ the loop derivation in any point $o \in P_r$ then $(P,+)$ is a Bol loop. If $(P,+)$ is any Bol loop then the permutation derivation (P,P°) is a Bol set.*

Proof. Let $o \in P_r$, $(P,+)$ the loop derivation of (P,Γ) in o and let $a,b \in P$ then (cf. 2.3) $a^+ = a^\bullet\circ(o^\bullet)^{-1}$, $b^+ = b^\bullet\circ(o^\bullet)^{-1}$ and $a^+\circ b^+\circ a^+ = a^\bullet\circ(o^\bullet)^{-1}\circ b^\bullet\circ(o^\bullet)^{-1}\circ a^\bullet\circ(o^\bullet)^{-1}$. Since (P,Γ) is a Bol set, $o^\bullet\circ\Gamma\circ o^\bullet=\Gamma$ hence $\Gamma = (o^\bullet)^{-1}\circ\Gamma\circ(o^\bullet)^{-1}$ and so $(o^\bullet)^{-1}\circ b^\bullet\circ(o^\bullet)^{-1} \in (o^\bullet)^{-1}\circ\Gamma\circ(o^\bullet)^{-1} = \Gamma$, i.e., by 2.3(1) there is a $c \in P$ with $c^\bullet = (o^\bullet)^{-1}\circ b^\bullet\circ(o^\bullet)^{-1}$ and so $a^+\circ b^+\circ a^+ = a^\bullet\circ C^\bullet\circ a^\bullet\circ(o^\bullet)^{-1}$. Again since (P,Γ) is a Bol set there is a $d \in P$ with $a^\bullet\circ C^\bullet\circ a^\bullet = d^\bullet$ thus $a^+\circ b^+\circ a^+ = d^\bullet\circ(o^\bullet)^{-1} \in P^+$. Therefore (P,P^+) is a Bol set. Moreover by 2.1(1), $\Gamma=\Gamma^{-1}$ and so there is an $a' \in P$ with $a'^\bullet = o^\bullet\circ(a^\bullet)^{-1}\circ o^\bullet$. Hence $(a^+)^{-1} = (a^\bullet\circ(o^\bullet)^{-1})^{-1} = o^\bullet\circ(a^\bullet)^{-1}\circ o^\bullet\circ(o^\bullet)^{-1} = a'^\bullet\circ(o^\bullet)^{-1} = a'^+ \in P^+$. By [17] (3.10.3), $(P,+)$ is a Bol loop. □

2.7. *Let $(P,+)$ be a left loop with $\nu \in Sym\, P$ and $P^\circ := P^+\circ\nu$ then $o \in (P,P^\circ)_r$ and:*

(1) $a \in (P,P^\circ)_r \Leftrightarrow \forall x \in P\ \exists_1 x' \in P$ *such that* $x = x'-a$.

(2) *If $a \in (P,P^\circ)_r$ and if $+_a$ is the loop derivation of (P,P°) in the point a then for all $p,q \in P$ it holds* $p+_a q = p' + (a'^+)^{-1}(q)$.

(3) *If $(P,+)$ is a Bol loop then $(P,P^\circ)_r = P$ and for all $a \in P$ it holds $p+_a q = p'+(-a'+q)$ and $x' = a+((-a+x)+a)$, in particular, $a' = a+a =: 2a$ and moreover, $(P,+_a)$ is a Bol loop.*

Proof. (1) is a consequence of $p^\circ(a) = p^+ \circ \nu(a) = p + (-a) = p - a$.

(2) If $[a \to p]_\circ$ denotes the permutation of P° mapping a onto p then $[a \to p]_\circ = p'^+ \circ \nu$ in particular, $\tilde{a} = [a \to a]_\circ = a'^+$ and so by Definition 1, $p +_a q = [a \to p]_\circ \circ \tilde{a}^{-1}(q) = p'^+ \circ \nu \circ (\nu)^{-1} \circ (a'^+)^{-1}(q) = p' + (a'^+)^{-1}(q)$.

(3) For each loop we have $(P, P^\circ)_r = P$ and in a Bol loop, $(-a)^+ = (a^+)^{-1}$, $(2a)^+ = (a+(o+a))^+ = a^+ \circ a^+$ and so $(a+((-a+x)+a)) - a = a^+ \circ (-a+x)^+ \circ a^+(-a) = a^+ \circ (-a+x)^+(o) = a^+(-a+x) = x$ implying $x' = a+((-a+x)+a)$. Consequently, $p +_a q = p' + (a'^+)^{-1}(q) = p' + (-a' + q) = (a+((-a+p)+a)) + (-2a+q)$ and therefore $p^{+_a} = a^+ \circ (-a+p)^+ \circ (a^+)^{-1}$ implying $p^{+_a} \circ q^{+_a} \circ p^{+_a} = a^+ \circ (-a+p)^+ \circ (-a+q)^+ \circ (-a+p)^+ \circ (a^+)^{-1} \in a^+ \circ P^+ \circ (a^+)^{-1}$. Thus if $r := a + ((-a+p) + ((-a+q) + (-a+p)))$ then $p^{+_a} \circ q^{+_a} \circ p^{+_a} = r^{+_a}$ showing that $(P, +_a)$ is a Bol loop. □

2.8. *Let (P, Γ) be a regular permutation set, let $o \in P$ be fixed and $(P, +)$ the loop derivation in o then:*

(1) *(P, P°) (cf. Definition 1) is a regular permutation set and for each $a \in P$, a° interchanges the points o and a.*

(2) $P^\circ = \Gamma \Leftrightarrow \forall x \in P : \ [o \to x] = [x \to o]$.

(3) *If (P, Γ) is invariant then $\widetilde{o} \circ \nu = \nu \circ \widetilde{o}$ and so $\omega = \widetilde{o}^{-1} \circ \nu = \nu \circ \widetilde{o}^{-1}$ and moreover:*

P° is invariant $\Leftrightarrow \forall \alpha \in \Gamma : \alpha \circ \omega \circ \Gamma = \Gamma \circ \omega \circ \alpha \Leftrightarrow \Gamma \cup \{\nu\} \subseteq N(P^\circ)$.

(4) *If P° is invariant then $P^\circ \subseteq J$.*

Proof. (1) By 2.3(5) and 2.5(3), $\nu \in Sym\, P$ and so $\omega = \widetilde{o}^{-1} \circ \nu \in Sym\, P$ hence $P^\circ = \Gamma \circ \omega$ is a regular permutation set. Finally $\omega(o) = [o \to o]^{-1}(o) = o$, $\omega(a) = [o \to a]^{-1}(o)$ and so $a^\circ(o) = [o \to a] \circ \omega(o) = [o \to a](o) = a$ and $a^\circ(a) = [o \to a] \circ \omega(a) = [o \to a] \circ [o \to a]^{-1}(o) = o$.

(2) By Definition 1, $P^\circ = \Gamma \Leftrightarrow \omega = id \Leftrightarrow \nu = \widetilde{o} \Leftrightarrow \forall x \in P : \nu(x) = (x^+)^{-1}(o) = \widetilde{o} \circ [o \to x]^{-1}(o) = \widetilde{o}(x) \Leftrightarrow \forall x \in P : \ [o \to x](x) = o \Leftrightarrow \forall x \in P : \ [o \to x] = [x \to o]$ (since (P, Γ) is a regular permutation set).

(3) Let $x \in P$ then $\nu(x) = \widetilde{o} \circ [o \to x]^{-1}(o) = \widetilde{o} \circ [o \to x]^{-1} \circ \widetilde{o}^{-1}(o) = [o \to \widetilde{o}(x)]^{-1}(o)$ (since Γ is invariant) hence $\widetilde{o} \circ \nu(x) = \widetilde{o} \circ [o \to \widetilde{o}(x)]^{-1}(o) = \nu(\widetilde{o}(x))$ and so $\widetilde{o} \circ \nu = \nu \circ \widetilde{o}$.

Let $P^\circ = \Gamma \circ \omega = \Gamma \circ \widetilde{o}^{-1} \circ \nu$ be invariant and let $\alpha \in \Gamma$ then $\alpha \circ \omega \circ P^\circ = \alpha \circ \omega \circ \Gamma \circ \omega = P^\circ \circ \alpha \circ \omega = \Gamma \circ \omega \circ \alpha \circ \omega$ hence $\alpha \circ \omega \circ \Gamma = \Gamma \circ \omega \circ \alpha$. For $\alpha := \widetilde{o}$ and using the commutativity of $\widetilde{o}$ and ν we obtain $\nu \circ \Gamma = \Gamma \circ \nu$ hence $\omega \circ \Gamma = \widetilde{o}^{-1} \circ \nu \circ \Gamma = \widetilde{o}^{-1} \circ \Gamma \circ \nu = \Gamma \circ \widetilde{o}^{-1} \circ \nu = \Gamma \circ \omega = P^\circ$. Together, $\alpha \circ P^\circ = \alpha \circ \omega \circ \Gamma = \Gamma \circ \omega \circ \alpha = P^\circ \circ \alpha$.

Now let $\Gamma \cup \{\nu\} \subseteq N(P^\circ)$. Then $\nu \circ P^\circ = \nu \circ \Gamma \circ \omega = \nu \circ \Gamma \circ \widetilde{o}^{-1} \circ \nu = P^\circ \circ \nu = \Gamma \circ \omega \circ \nu$ hence (using the commutativity), $\nu \circ \Gamma \circ \widetilde{o}^{-1} = \Gamma \circ \widetilde{o}^{-1} \circ \nu = \Gamma \circ \nu \circ \widetilde{o}^{-1}$ and so $\nu \circ \Gamma = \Gamma \circ \nu$. This implies $\omega \circ \Gamma = \widetilde{o}^{-1} \circ \nu \circ \Gamma = \widetilde{o}^{-1} \circ \Gamma \circ \nu = \Gamma \circ \widetilde{o}^{-1} \circ \nu = \Gamma \circ \omega = P^\circ$ and so $\omega \circ P^\circ = \omega \circ \Gamma \circ \omega = P^\circ \circ \omega$. Therefore if $\alpha \circ \omega \in P^\circ$ then by $\alpha \in N(P^\circ)$, $\alpha \circ \omega \circ P^\circ = \alpha \circ P^\circ \circ \omega = P^\circ \circ \alpha \circ \omega$ showing that P° is invariant.

(4) If $a, b \in P$ we denote the map of P° mapping a onto b by $[a \to b]'$. Now let $\varphi \in P^\circ$, $a \in P$ and $b := \varphi(a)$ hence $\varphi = [a \to b]'$. Since P° is invariant we have $(a^\circ)^{-1} \circ [a \to b]' \circ a^\circ = [o \to (a^\circ)^{-1}(b)]'$. By (1) this is equal $[(a^\circ)^{-1}(b) \to o]' = (a^\circ)^{-1} \circ [b \to a]' \circ a^\circ$. Together we obtain, $\varphi = [b \to a]'$ hence $\varphi(b) = a$, i.e., $\varphi \in J$. □

3. Isomorphisms

Let (P, Γ) and (P', Γ') be permutation sets and let $\psi : P \to P'$ be a bijection. Then ψ is called *isomorphism* between (P, Γ) and (P', Γ') and (P, Γ), (P', Γ') are called *isomorphic*, if $\Gamma' = \psi \circ \Gamma \circ \psi^{-1}$. An isomorphism φ is called *automorphism* of (P, Γ) if $(P, \Gamma) = (P', \Gamma')$, hence $\Gamma = \varphi \circ \Gamma \circ \varphi^{-1}$. Thus the automorphism group $Aut(P, \Gamma)$ is exactly the normalizer of Γ in $Sym\, P$. We call (P, Γ) *homogeneous* if $Aut(P, \Gamma)$ acts transitively on P and *self homogeneous* if for all $a, b \in P$ it holds $[a \to b] \cap Aut(P, \Gamma) \neq \emptyset$. Clearly if (P, Γ) is homogeneous and $(P, \Gamma)_r \neq \emptyset$ then (P, Γ) is a regular permutation set, and if (P, Γ) is invariant with $(P, \Gamma)_r \neq \emptyset$, then (P, Γ) is homogeneous (cf. 2.3(4)).

3.1. *Let $\psi : P \to P'$ be an isomorphism from (P, Γ) onto (P', Γ'), let $(P, \Gamma)_r \neq \emptyset$ and $o \in (P, \Gamma)_r$ then $o' := \psi(o) \in \psi((P, \Gamma)_r) = (P', \Gamma')_r$ and we have:*

(1) $\forall a, b \in P \quad \psi \circ [a \to b] \circ \psi^{-1} = [\psi(a) \to \psi(b)]$.

(2) $\forall x \in P \quad \psi \circ [o \to x] \circ \tilde{o}^{-1} = [o' \to \psi(x)]' \circ \widetilde{o'}^{-1} \circ \psi$.

(3) *If $(P, +)$, $(P', +')$ are the loop derivations of (P, Γ) and (P', Γ') in o and o', respectively, then ψ is an isomorphism from $(P, +)$ onto $(P', +')$ and also from the permutation derivation (P, P°) onto the permutation derivation $(P', p'^{\circ'})$ (We have the formula: If $a \in P$ then $\psi \circ a^\circ \circ \psi^{-1} = (\psi(a))^{\circ'}$).*

(4) *If (P, Γ) is invariant then for all $a, b \in P$ and for each $\gamma \in \Gamma$:*

$$\gamma \circ [a \to b] \circ \gamma^{-1} = [\gamma(a) \to \gamma(b)].$$

Proof. Since ψ is an isomorphism we have for all $a, b \in P$: $\psi \circ [a \to b] \circ \psi^{-1} = [\psi(a) \to \psi(b)]$ and so by $o' = \psi(o)$, $\psi(a+b) = \psi([o \to a] \circ [o \to o]^{-1}(b)) = \psi[o \to a] \circ \psi^{-1} \circ \psi \circ [o \to o]^{-1} \circ \psi(b)[\psi(o) \to \psi(a)] \circ [\psi(o) \to \psi(o)]^{-1}(\psi(b)) = \psi(a) +' \psi(b)$. □

3.2. *Let $o \in (P, \Gamma)_r$, $o' \in (P', \Gamma')_r$, let $(P, +)$ and $(P', +')$, resp., be the loop derivations of (P, Γ) in o, and (P', Γ') in o', resp., and let φ be an isomorphism from $(P, +)$ onto $(P', +')$. Then:*

(1) *φ is also an isomorphism from (P, Γ) onto (P', Γ') if and only if $\varphi \circ \tilde{o} = \widetilde{o'} \circ \varphi$.*

(2) *If $\nu \in Sym\, P$, then $\nu' \in Sym\, P'$ and φ is an isomorphism from the permutation derivation $(P, P^\circ = P^+ \circ \nu)$ of $(P, +)$ onto the permutation derivation (P', P'°) of $(P', +')$.*

Proof. (1) For each $a \in P$ we have $a^+ = [o \to a] \circ \tilde{o}^{-1}$ and $(\varphi(a))^{+'} = [o' \to \varphi(a)]' \circ \widetilde{o'}^{-1}$, and since φ is an isomorphism, $\varphi \circ a^+ = (\varphi(a))^{+'} \circ \varphi$. Together we obtain, $\varphi \circ [o \to a] \circ \varphi^{-1} \circ \varphi \circ \tilde{o}^{-1} = [o' \to \varphi(a)]' \circ \widetilde{o'}^{-1} \circ \varphi$. This implies for $a = o$, $[o' \to \varphi(o)]' = \widetilde{o'}$ and so $o' = \varphi(o)$, i.e., φ is only an isomorphism from (P, Γ) onto (P', Γ') if $\varphi \circ \tilde{o} = \widetilde{o'} \circ \varphi$ and then $\varphi \circ [o \to a] \circ \varphi^{-1} = [o' \to \varphi(a)]'$ showing $\Gamma' = \varphi \circ \Gamma \circ \varphi^{-1}$ since $\Gamma = \{[o \to a] \mid a \in P\}$ and $\Gamma' = \{[o \to \varphi(a)]' \mid a \in P\}$.

(2) From $o' = \varphi(o) = \varphi(x + \nu(x)) = \varphi(x) +' \varphi(\nu(x))$ we obtain $\nu'(\varphi(x)) = \varphi(\nu(x))$ and finally, since $\tilde{o} = o^\circ = o^+ \circ \nu = \nu$ and $\widetilde{o'} = \nu'$ the equation $\varphi \circ \tilde{o} = \widetilde{o'} \circ \varphi$. Hence by 3.2(1), φ is an isomorphism from (P, P°) onto (P', P'°). □

From 3.1 and 3.2 one obtains:

3.3. *Let φ be an isomorphism between the permutation sets (P, Γ) and (P', Γ'), let $o \in (P, \Gamma)_r$ (then $\varphi(o) \in (P', \Gamma')_r$) and let $(P, +)$ resp. $(P', +')$ be the loop derivation in o resp. $\varphi(o)$. If $\nu \in Sym\, P$ (then also $\nu' \in Sym\, P'$), let $P^\circ := P^+ \circ \nu$ and $P'^\circ := P'^+ \circ \nu'$ then φ is an isomorphism between $(P, +)$ and $(P', +')$ and between the permutation sets (P, P°) and (P', P'°).*

3.4. *Let $(P, \Gamma)_r \neq \emptyset$, $a \in (P, \Gamma)_r$, $\psi \in Aut(P, \Gamma)$ and $b := \psi(a)$ then:*

(1) *$\forall x \in P \quad \psi \circ [a \to x] \circ \tilde{a}^{-1} = [b \to \psi(x)] \circ \tilde{b}^{-1} \circ \psi$,*

(2) *ψ is an isomorphism between the left loops $(P, +_a)$ and $(P, +_b)$ obtained by the loop derivations of (P, Γ) in the points a and b.*

3.5. *Let $(P,+)$ be a left loop with $\nu \in Sym\, P$, (P,P°) with $P^\circ = P^+ \circ \nu$ the permutation derivation of $(P,+)$ and let $\varphi \in Sym\, P$ and $f := \varphi\circ\nu\circ\varphi^{-1}(o)$. Then for $c \in P$:*

(1) $\varphi \in Aut(P,P^\circ) \Leftrightarrow \forall a \in P \;\; \varphi \circ a^+ \circ \varphi^{-1} \circ f^+ = (\varphi(a+\varphi^{-1}(f)))^+$.

(2) *If $\varphi(o) = o$ then: "$\varphi \in Aut(P,P^\circ) \Leftrightarrow \varphi \in Aut(P,+)$".*

(3) $\nu \in Aut(P,P^\circ) \Leftrightarrow \nu \in Aut(P,+)$.

(4) $c^+ \in Aut(P,P^\circ) \Leftrightarrow \forall a \in P \;\; c^+ \circ a^+ \circ (c^+)^{-1} \circ (c-(-c))^+ = (c+(a-(-c)))^+$.

(5) $c^\circ \in Aut(P,P^\circ) \Leftrightarrow \forall a \in P \;\; c^+ \circ \nu \circ a^+ \circ \nu^{-1} \circ (c^+)^{-1} \circ (c-(-c))^+ = (c-(a-c))^+$.

Proof. By definition, $\varphi \in Aut(P,P^\circ)$ if and only if $\varphi\circ a^+ \circ \nu \circ \varphi^{-1} \in P^+ \circ \nu$ for each $a \in P$. For $a = o$ we obtain that there has to be an $f \in P$ with $\varphi \circ \nu \circ \varphi^{-1} = f^+ \circ \nu$ and so $\varphi \circ \nu \circ \varphi^{-1}(o) = f^+ \circ \nu(o) = f^+(o) = f$. Thus $\varphi \circ a^+ \circ \nu \circ \varphi^{-1} = \varphi \circ a^+ \circ \varphi^{-1} \circ \varphi \circ \nu \circ \varphi^{-1} = \varphi \circ a^+ \circ \varphi^{-1} \circ f^+ \circ \nu \in P^+ \circ \nu$, i.e., $\varphi \circ a^+ \circ \varphi^{-1} \circ f^+ \in P^+$. Since $\varphi \circ a^+ \circ \varphi^{-1} \circ f^+(o) = \varphi(a+\varphi^{-1}(f))$ we have proved (1). If $\varphi(o) = o$ then $f = o$ and condition (1) assumes the form

$$\varphi \in Aut(P,P^\circ) \Leftrightarrow \forall a \in P \;\; \varphi \circ a^+ \circ \varphi^{-1} = (\varphi(a))^+.$$

But this tells us that φ is an automorphism of the left loop $(P,+)$. Since $\nu(o) = (o^+)^{-1}(o) = id(o) = o$, (3) is a consequence of (2).

Since $f := c^+ \circ \nu \circ (c^+)^{-1}(o) = c-(-c) = c^\circ(-c) = c^\circ \circ \nu \circ (c^\circ)^{-1}(o)$ and so $c^+(a+(c^+)^{-1}(f)) = c+(a-(-c))$ and $c^\circ(a+(c^\circ)^{-1}(f)) = c^\circ(a-c) = c-(a-c)$, (4) and (5) are consequences of (1). □

From 3.2 we obtain:

3.6. *Let $(P,+)$ be a left loop with $\nu \in Sym\, P$, then:*

(1) $P^+ \subseteq Aut(P,P^\circ) \Leftrightarrow \forall a,b \in P \;\; a^+ \circ b^+ = (a+(b-(-a)))^+ \circ (-a)^+$.

(2) *If $P^+ \subseteq Aut(P,P^\circ)$ then $(P,+)$ is a loop and for the structure group $\Delta := \langle \{\delta_{a,b} \mid a,b \in P\} \rangle$ of the loop generated by the permutations $\delta_{a,b} := ((a+b)^+)^{-1} \circ a^+ \circ b^+$ we have $\Delta \leq Aut(P,+)$ and therefore $Aut(P,P^\circ) = P^+ \rtimes_Q Aut(P,+)$ is equal the quasidirect product of the loop $(P,+)$ with the automorphism group of the loop.*

(3) $P^\circ \subseteq Aut(P,P^\circ) \Leftrightarrow \forall a,b \in P \;\; a^+ \circ (-b)^+ = (a-(b-a))^+ \circ (-a)^+$.

(4) $P^\circ \subseteq Aut(P,P^\circ) \Leftrightarrow P^+ \cup \{\nu\} \subseteq Aut(P,P^\circ)$.

Proof. (1) We have: "$P^+ \subseteq Aut(P,P^\circ) \Leftrightarrow$ the functional equation of 3.5(4) is valid for all $c,a \in P$". For $a = -c$ we obtain $(c^+)^{-1} \circ (c-(-c))^+ = ((-c)^+)^{-1}$ and so 3.5(4) takes on the form $(c+(a-(-c)))^+ \circ (-c)^+ = c^+ \circ a^+$.

(2) By 2.4, since $\nu \in Sym\, P$, (P, P°) is a permutation set with $o \in (P, P^\circ)_r$ and so by $P^+(o) = P$ and $P^+ \subseteq Aut(P, P^\circ)$, (P, P°) is a regular permutation set. With (P, P°) also $(P, P^+ = P^\circ \circ \nu^{-1})$ is regular and so by 2.2, $(P, +)$ is a loop. By $P^+ \subseteq Aut(P, P^\circ)$ we have $\Delta \leq Aut(P, P^\circ)$ and since $\delta_{a,b}(o) = ((a+b)^+)^{-1} \circ a^+ \circ b^+(o) = ((a+b)^+)^{-1}(a+b) = o$ each element $\delta \in \Delta$ fixes o and so by 3.5(2), $\Delta \leq Aut(P, +)$.

(3) Again, "$P^\circ \subseteq Aut(P, P^\circ) \Leftrightarrow$ the functional equation of 3.5(5) is valid $\forall c, a \in P$". For $c = o$ we obtain $\nu \circ a^+ \circ \nu^{-1} = (-a)^+$ and so 3.5(5) takes on the form $c^+ \circ (-a)^+ \circ (c^+)^{-1} \circ (c-(-c))^+ = (c-(a-c))^+$. Now by $a = c$, we obtain $(-c)^+ \circ (c^+)^{-1} \circ (c-(-c))^+ = id$, i.e., $(c-(-c))^+ = c^+ \circ ((-c)^+)^{-1}$ and finally $c^+ \circ (-a)^+ = (c-(a-c))^+ \circ (-c)^+$.

(4) Clearly if $P^\circ \subseteq Aut(P, P^\circ)$, then $\nu = o^\circ \in Aut(P, P^\circ)$ and $P^+ = P^\circ \circ \nu^{-1} \subseteq Aut(P, P^\circ)$. If $P^+ \cup \{\nu\} \in Aut(P, P^\circ)$ then $P^\circ = P^+ \circ \nu \subseteq Aut(P, P^\circ)$. □

3.7. *For a loop $(P, +)$ the following conditions are equivalent:*

(1) *(P, P°) is selfhomogeneous.*

(2) $\forall a, b \in P \quad a^+ \circ (-b)^+ \circ ((-a)^+)^{-1} = (a-(b-a))^+$.

(3) *(P, P°) is an invariant regular involution set.*

(4) *$(P, +)$ is a K-loop (= Bruck loop).*

Proof. Let $a, b \in P$ and $c \in P$ the solution of $x - a = b$ then $[a \to b]_\circ = c^\circ$ and so by 3.6(3) the conditions (1) and (2) are equivalent. From the equation (2) we obtain $a^+ \circ (-b)^+ = (a-(b-a))^+ \circ ((-a)^+)$ hence $a + (-b+x) = (a-(b-a)) + (-a+x)$ and so for $x := -(-a)$, $a + (-b-(-a)) = a-(b-a)$, i.e., $-b-(-a) = -(b-a)$, showing that ν is an automorphism of $(P, +)$. Now observing $\nu \in Aut(P, +)$ we obtain for $x := --(b-a)$: $a+(-b--(b-a)) = (a-(b-a))+(-a--(b-a)) = o$ hence $a = b-(b-a) = b^+ \circ \nu \circ b^+ \circ \nu(a) = b^\circ \circ b^\circ(a)$, i.e., $b^\circ \in J$ in particular, $o^\circ = o^+ \circ \nu = \nu \in J$. Consequently $P^\circ \subseteq J$. Finally $a^\circ = a^+ \circ \nu = (a^\circ)^{-1} = \nu \circ (a^+)^{-1}$ hence $(a^+)^{-1}(x) = \nu \circ a^+ \circ \nu(x) = -(a-x) = -a--x = -a+x = (-a)^+(x)$ and $\nu \circ a^+ \circ \nu = (-a)^+$. Therefore the equation (2) assumes the form $a^+ \circ b^+ \circ a^+ = (a+(b+a))^+$ saying that $(P, +)$ is a Bol loop hence together with $\nu \in Aut(P, +)$, $(P, +)$ is a Bruck loop and moreover, $a^\circ \circ b^\circ \circ a^\circ = a^+ \circ \nu \circ b^+ \circ \nu \circ a^+ \circ \nu = a^+ \circ (-b)^+ \circ a^+ \circ \nu = (a+(-b+a))^+ \circ \nu \in P^+ \circ \nu = P^\circ$. Consequently (P, P°) is an invariant regular involution set.

By [10], (3) and (4) are equivalent. Now let $(P, +)$ be a Bruck loop. Since $(P, +)$ is also a Bol loop, we have $a^+ \circ b^+ \circ a^+ = (a + (b + a))^+$ and obtain by substituting $a := -b$, $(-b)^+ = (b^+)^{-1}$ and so $(- - b)^+ =$

$((-b)^+)^{-1} = ((b^+)^{-1})^{-1} = b^+$ hence $--b = b$, i.e., $\nu^2 = id$. Then (since $\nu \in Aut(P,+)$) $a^+ \circ (-b)^+ \circ a^+ = (a+(-b+a))^+ = (a+(\nu(b)+\nu(\nu(a))^+ = (a+\nu(b+\nu(a))^+ = (a-(b-a))^+$ and this is equation (2). □

3.8. *For a left loop $(P,+)$ with $\nu \in Sym\, P$ the following conditions are equivalent:*

(1) $P^+ \subseteq Aut(P,P^\circ)$ *and* $P^+ = (P^+)^{-1}$,

(2) $(P,+)$ *is a Bol loop.*

Proof. (1) $\Rightarrow$ (2) Let $a,b \in P$ then there is a $c \in P$ with $(a^+)^{-1} = c^+$ hence $c = c^+(o) = (a^+)^{-1}(o)$ implying $a + c = a^+(c) = o$, i.e., $c = -a$ hence $(a^+)^{-1} = (-a)^+$ and so $-(-a) = a$. By 3.6(1), $a^+ \circ b^+ = (a + (b - (-a)))^+ \circ (-a)^+$ and by observing the previous facts we obtain $a^+ \circ b^+ = (a + (b + a))^+ \circ (a^+)^{-1}$ or $a^+ \circ b^+ \circ a^+ = (a + (b + a))^+$ telling us that $(P,+)$ is a Bol loop.

(2) $\Rightarrow$ (1) Since in a Bol loop, for each $a \in P$, $(a^+)^{-1} = (-a)^+$ and $-(-a) = a$ the characterizing functional equation $a^+ \circ b^+ \circ a^+ = (a+(b+a))^+$ of the Bol loop can be written in the form of the equation of 3.6(1) and therefore the statements of (1) are verified. □

Remark 1. By 3.8, if $(P,+)$ is a Bol loop then the permutation derivation (P,P°) of $(P,+)$ is a homogeneous Bol set (cf. 2.6) and so by 3.4(2), if $(P,+_a)$ is the loop derivation of (P,P°) in an arbitrary point $a \in P$, then $(P,+_a)$ and $(P,+)$ are isomorphic. This supplements 2.7(3) and more precisely we have: The map $(-a)^+$ is an isomorphism from the Bol loop $(P,+_a)$ onto the Bol loop $(P,+)$.

4. Involution sets

By [14] we have:

4.1. *Let $(P,+)$ be a left loop then the following statements are equivalent:*

(1) $\nu \in Sym\, P$ *and* $P^\circ \subseteq J$, *i.e.,* (P,P°) *is an involution set with* $o \in (P,P^\circ)_r$.

(2) $(P,+)$ *satisfies the condition* (*) $\forall\, a,b \in P \;\; a - (a-b) = b$.

4.2. *Let (P,Γ) be a permutation set with $P_r := (P,\Gamma)_r \neq \emptyset$, let $o \in P_r$ be fixed and let $+ := +_o$ be the loop derivation of (P,Γ) in o. Then:*

(1) $\Gamma = \Gamma^{-1} \Leftrightarrow \widetilde{P}_r \subseteq J$ *and* $\tilde{o} \circ (P^+)^{-1} \circ \tilde{o} = P^+$.

(2) *If there is a* $\nu' \in J$ *with* $\nu' \circ (P^+)^{-1} \circ \nu' = P^+$ *then* $\Gamma = \Gamma^{-1}$.

(3) *If* (P,Γ) *is an involution set then* $(P,+)$ *satisfies the condition* (*).
(4) *If* (P,Γ) *is an invariant involution set then* $(P,+)$ *is a K-loop.*

Proof. (1) If $a \in P_r$ then $\tilde{a} := [a \to a]$ is the unique element of Γ fixing a and also $\tilde{a}^{-1}(a) = a$. Therefore if $\Gamma = \Gamma^{-1}$ then $\tilde{a} = \tilde{a}^{-1}$, i.e., $\tilde{a} \in J$, in particular $\tilde{o} = o^\circ \in J$. By $P^+ = \{x^+ = [o \to x] \circ (o^\circ)^{-1} = x^\circ \circ \tilde{o} \mid x \in P\} = P^\circ \circ \tilde{o} = \Gamma \circ \tilde{o}$ hence $\Gamma = P^+ \circ \tilde{o}$ we have:

$$\Gamma = P^+ \circ \tilde{o} = \Gamma^{-1} = \tilde{o} \circ (P^+)^{-1} \Leftrightarrow \tilde{o} \circ (P^+)^{-1} \circ \tilde{o} = P^+.$$

(2) Let $\nu' \in J$ with $\nu' \circ (P^+)^{-1} \circ \nu' = P^+$ hence for each $a \in P$ $\exists b \in P$ with $\nu' \circ (a^\circ \circ (o^\circ)^{-1})^{-1} \circ \nu' = \nu' \circ o^\circ \circ (a^\circ)^{-1} \circ \nu' = b^\circ \circ o^\circ$. For $a = o$ we obtain $id = \nu' \circ \nu' = b^\circ \circ o^\circ$ hence $b^\circ = (o^\circ)^{-1}$. Consequently $\Gamma^{-1} = \tilde{o} \circ (P^+)^{-1} = \tilde{o} \circ \nu' \circ P^+ \circ \nu' = \Gamma = P^+ \circ \tilde{o}^{-1}$ if and only if $\nu' = \tilde{o}^{-1}$. □

5. Defect functions

Let (P,Γ) be a permutation set with $P_r \neq \emptyset$ then the map

$$\delta : P_r \times P \times \Gamma \to Sym\, P,$$
$$(a,b,\gamma) \mapsto \delta_{a;b,\gamma} = [a \to a] \circ [\gamma(b) \to a] \circ \gamma \circ [a \to b]$$

is called the *defect function of the permutation set* (P,Γ) *in the point* a.

We have $\delta_{a;b,\gamma}(a) = a$. If $P_r = P$ we set

$$\delta : P^3 \longrightarrow Sym\, P; \quad (a,b,c) \mapsto \delta_{a;b,c} := [a \to a] \circ [c \to a] \circ [b \to c] \circ [a \to b].$$

Three points $a,b,c \in P$ are called *defect free* if $\delta_{a;b,c} = id$.

If $(P,+)$ is a left loop then the map

$$\delta : P \times P \to Sym\, P; \quad (a,b) \mapsto \delta_{a,b} = ((a+b)^+)^{-1} \circ a^+ \circ b^+$$

is called the *defect function of the left loop* $(P,+)$ and $a,b \in P$ are called *defect free* if $\delta_{a,b} = id$, i.e., if $(a+b)^+ = a^+ \circ b^+$. Here o is the fixed point of $\delta_{a,b}$. We recall that the definition implies:

5.1. *If* $(P,+)$ *is a K-loop then* $\Delta := \langle \{\delta_{a,b} \mid a,b \in P\} \rangle \leq Aut\ (P,+)$.

6. Reflection structures and point reflection spaces

Let P be a non empty set. If there is a fixed point $o \in P$ and a map

$$^\circ : P \to J; \quad x \mapsto x^\circ \quad \text{with} \quad x^\circ(o) = x \quad \text{for each} \quad x \in P$$

then the tripel $(P,\ ^\circ, o)$ is called *reflection structure* (cf.[10]). If there is a map

$$\sim : P \to J;\quad x \mapsto \widetilde{x} \ \text{ with } \ Fix\ \widetilde{x} = \{x\} \ \text{ for each } \ x \in P$$

satisfying the property

(M) for all $a, b \in P\ \ \exists_1 m \in P$ with $\widetilde{m}(a) = b$

then the pair $(P, \sim)$ is called *point reflection structure* (cf. [6], [5]). A reflection structure (point reflection structure) is *invariant* if for all $a, b \in P$ there exists $c \in P$ with $a^\circ \circ b^\circ \circ a^\circ = c^\circ$, $(\widetilde{a} \circ \widetilde{b} \circ \widetilde{a} = \widetilde{c})$. An invariant reflection structure $(P,\ ^\circ, o)$ is a point reflection structure if for each $a \in P$, $|Fix\ a^\circ| = 1$.

By the definitions and 2.5 follows:

6.1. *Let $(P,\ ^\circ, o)$ be a reflection structure and $\Gamma := P^\circ := \{x^\circ \mid x \in P\}$. If (P, Γ) is regular, for each $p \in P$ we denote by $\widetilde{p} \in \Gamma$ the permutation with $\widetilde{p}(p) = p$. Let $\widetilde{P} := \{\widetilde{p} \mid p \in P\}$. Then:*

(1) *$(P,\ P^\circ)$ is an involution set, o a regular point hence $o \in (P, P^\circ)_r$ and the loop derivation of (P, P°) in the point o gives us a left loop $(P, +)$ satisfying the condition (*).*

(2) *$(P,\ ^\circ, o)$ is an invariant reflection structure $\Leftrightarrow$ (P, P°) is an invariant involution set with $(P, P^\circ)_r \neq \emptyset \Leftrightarrow (P, +)$ is a K-loop.*

(3) *$(P,\ ^\circ, o)$ is an invariant point reflection structure $\Leftrightarrow$ (P, P°) is an invariant involution set with $(P, P^\circ)_r \neq \emptyset$ and any two points $a, b \in P$ have exactly one midpoint $m \in P$, i.e., if $c^\circ \in P^\circ$ with $m \in Fix\, c^\circ$ then $c^\circ(a) = b \Leftrightarrow \widetilde{P} = P^\circ = \Gamma \Leftrightarrow (P, +)$ is a K-loop uniquely 2-divisible.*

(4) *If the reflection structure $(P,\ ^\circ, o)$ (the point reflection structure $(P, \sim)$) is invariant then for all $a, b \in P$ we have $a^\circ \circ b^\circ \circ a^\circ = (a^\circ \circ b^\circ(a))^\circ$, $(\widetilde{a} \circ \widetilde{b} \circ \widetilde{a} = \widetilde{\widetilde{a}(b)})$.*

Proof. All we have to show is that $\nu \in Sym\, P$. Let $x \in P$ then $x^+ = [o \to x] \circ [o \to o]^{-1} = x^\circ \circ (o^\circ)^{-1} = x^\circ \circ o^\circ$ hence $(x^+)^{-1} = o^\circ \circ x^\circ$ and so $\nu(x) = -x = (x^+)^{-1}(o) = o^\circ \circ x^\circ(o) = o^\circ(x)$. Therefore $\nu = o^\circ \in Sym\, P$. □

6.2. *If (P, Γ) is an involution set with $P_r = (P, \Gamma)_r \neq \emptyset$, $o \in P_r$ fixed and $x^\circ := [o \to x]$ for each $x \in P$ then $(P,\ ^\circ, o)$ is a reflection structure.*

6.3. *If $(P, +)$ is a left loop satisfying (*) and $x^\circ := x^+ \circ \nu$ for each $x \in P$ then $(P,\ ^\circ, o)$ is a reflection structure.*

Definition 4. Let $(P,\sim)$ be a point reflection structure and let $\rho := \{(a,b,c) \in P^3 \mid \tilde{a} \circ \tilde{b} \circ \tilde{c} \in J\}$ then $(P,\sim)$ is called *point reflection space* if:

$(R1)$ $\forall a,b,c \in \rho \ : \ \tilde{a} \circ \tilde{b} \circ \tilde{c} \in \widetilde{P}$,

$(R2)$ ρ is a *ternary equivalence relation*, i.e.,

$$(a,b,c) \in \rho \ \Rightarrow \ (b,c,a),(b,a,c) \in \rho \ \text{ and}$$
$$a \neq b \ \wedge (a,b,c),(a,b,d) \in \rho \ \Rightarrow \ (b,c,d) \in \rho.$$

Remark 2. If $(P,\mathfrak{L},\equiv,\alpha)$ is an absolute geometry (cf. [10]) and if $\sim$ is the map which associates to each point $p \in P$ the reflection in p then $(P,\sim)$ is a point reflection space.

From now on let $(P,\sim)$ be a point reflection space, let $\widetilde{P} := \{\widetilde{p} \mid p \in P\}$, and let $\mathbf{G} := \langle \widetilde{\mathbf{P}} \rangle$ be the group generated by the point reflections $\widetilde{p}$. Let the point $o \in P$ be fixed. From (R1) follows that $(P,\widetilde{P})$ is an invariant regular involution set. Therefore by 4.2(4) the loop derivation $(P,+)$ of $(P,\widetilde{P})$ in o is a K-loop. We call $(P,\sim)$ *singular* if $\rho = P^3$ and *ordinary* otherwise. Any two distinct points $a,b \in P$ determine an equivalence class

$$\overline{a,b} := \{x \in P \mid (a,b,x) \in \rho\}.$$

We have:

6.4. *A point reflection space $(P,\sim)$ is singular if one of the following equivalent conditions is satisfied:*

(1) *The set P of all points forms the only equivalence class of ρ,*

(2) $\widetilde{P} \circ \widetilde{P} \circ \widetilde{P} = \widetilde{P}$,

(3) $\widetilde{P} \circ \widetilde{P}$ *is a commutative subgroup of index* 2 *in* $\mathbf{G}$,

(4) *The K-loop $(P,+)$ is a commutative group (isomorphic with $\widetilde{P} \circ \widetilde{P}$).*

For the rest of this section let $(P,\sim)$ be an ordinary point reflection space. Then the set P together with the set $\mathfrak{L} := \{\overline{a,b} \mid a,b \in P, a \neq b\}$ of all equivalence classes of ρ – called *lines* – forms an incidence space $(P,\mathfrak{L})$ where the set $\mathfrak{L}$ contains more than one line. A subset $T \subseteq P$ is called *subspace of* $(P,\sim)$ if for all $a,b \in T$ with $a \neq b$ we have $\overline{a,b} \subseteq T$. Let $\mathfrak{T}$ be the set of all subspaces of $(P,\sim)$.

Remark 3. If $(P,\mathfrak{L},\equiv,\alpha)$ is an ordinary absolute geometry then the set of lines $\mathfrak{L}$ coincides with the set of equivalence classes of the relation ρ.

6.5. *An ordinary point reflection space $(P,\sim)$ has the following properties:*

(1) $(P,\mathfrak{L})$ *in an incidence space.*

(2) *If* $L \in \mathfrak{L}$, *then* $\forall a, b, c \in L\ \exists\ d \in L$ *with* $\widetilde{a} \circ \widetilde{b} \circ \widetilde{c} = \widetilde{d}$.
(3) *If* $a, b \in P$ *with* $a \neq b$, *then* $\overline{a, b} = \{x \in P \mid \widetilde{a} \circ \widetilde{b} \circ \widetilde{c} \in J\}$.
(4) *For each* $T \in \mathfrak{T}$, *and for each* $t \in T$ *it holds* $\widetilde{t}(T) = T$.
(5) *Let* $\sim_T : T \to Sym\, T;\ t \mapsto \widetilde{t}_{|T}$. *Then* $(T, \sim_T)$ *is a point reflection space and* $(T, \sim_T)$ *is singular if and only if* T *is a point or a line.*
(6) $\langle \widetilde{P} \rangle = \mathbf{G} \leq \mathbf{Aut}(\mathbf{P}, \sim) = \mathbf{Aut}(\mathbf{P}, \rho) = \mathbf{Aut}(\mathbf{P}, \mathfrak{L}) = \mathbf{Aut}(\mathbf{P}, \mathfrak{T})$ *and the automorphism group* $Aut(P, \sim)$ *acts transitively on the point set* P.

Since an absolute space $(P, \mathfrak{L}, \equiv, \alpha)$ is also an ordered space $(P, \mathfrak{L}, \alpha)$ and an ordered space is an exchange space (cf. [10] Theorem 1.5) there are ordinary point reflection spaces $(P, \sim)$ such that the corresponding incidence space $(P, \mathfrak{L})$ is an exchange space. For these spaces we can state:

6.6. *Let* $(P, \sim)$ *be an ordinary point reflection space such that the corresponding incidence space* $(P, \mathfrak{L})$ *is an exchange space. Then:*
(1) $(P, \mathfrak{L})$ *has a base* B, *two bases have the same cardinality and we define* $dim(P, \sim) := |B| - 1$ *as dimension of* $(P, \sim)$.
(2) *If* $dim(P, \sim) \geqslant 3$ *then* $(P, \sim)$ *is desarguesian.*
(3) *If* $dim(P, \sim) \geqslant 3$ *let* $\mathfrak{E} := \{T \in \mathfrak{T} \mid dim\, T = 2\}$ *be the set of all planes, for each* $p \in P$ *let* $\mathfrak{L}(p) := \{L \in \mathfrak{L} \mid p \in L\}$ *and* $\mathfrak{E}(p) := \{E \in \mathfrak{E} \mid p \in E\}$, *then* $(\mathfrak{L}(p), \mathfrak{E}(p), \subset)$ *is a projective space.*

7. Nets, chain structures, webs and their properties

Let $(P, \mathfrak{G}_1, \mathfrak{G}_2)$ be a 2-*net*, i.e., P is a non empty set and $\mathfrak{G}_1, \mathfrak{G}_2$ are subsets of the powerset of P called *generators* such that:

$(I1)$ $\forall p \in P,\ \forall i \in \{1, 2\}\ \exists_1\ [p]_i \in \mathfrak{G}_i$ with $p \in [p]_i$,

$(I2)$ $\forall X \in \mathfrak{G}_1, \forall Y \in \mathfrak{G}_2\ |X \cap Y| = 1$.

By $(I1)$, $(I2)$, if $A, B \in \mathfrak{G}_i$ then A and B have the same cardinality and there is a binary operation (cf. e.g. [4]):

$$\square : P \times P \to P;\quad (x, y) \mapsto xy := [x]_1 \cap [y]_2$$

which has the properties:

7.1. *Let* $a, b, c, d \in P$ *and let* $\{a, b\}^{\square} := \{ab, ba\}$ *and* $\{a, b; c, d\}^{\square} := \{ab, ba; cd, dc\}$. *Then:*
(1) $(ab)(cd) = ad$,

(2) "$ab = b \Leftrightarrow [a]_1 = [b]_1$", "$ab = a \Leftrightarrow [a]_2 = [b]_2$" *and* $aa = a$,
(3) $(\{a,b\}^{\square})^{\square} = \{ab, ba\}^{\square} = \{a,b\}$,
(4) $\{a,b\}^{\square} = \{a,b\} \Leftrightarrow ab = a \quad or \quad ab = b \Leftrightarrow |\{a,b\} \cup \{a,b\}^{\square}| < 4$,
(5) $(\{a,b;c,d\}^{\square})^{\square} = \{a,b;c,d\}$.

The set $\{a,b\}$ is called *parallel* (*joinable*) if $\{a,b\}^{\square} = \{a,b\}$, ($\{a,b\}^{\square} \neq \{a,b\}$) and a subset $A \subseteq P$ is called *joinable* if for all $\{a,b\} \in \binom{A}{2}$ we have $\{a,b\}^{\square} \neq \{a,b\}$. Let

$$\mathfrak{C} := \{C \in 2^P \mid \forall X \in \mathfrak{G}_1 \cup \mathfrak{G}_2 \quad |C \cap X| = 1\}$$

be the set of all *chains* of the 2-net $(P, \mathfrak{G}_1, \mathfrak{G}_2)$. If $\mathfrak{K} \subseteq \mathfrak{C}$ then $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is called *chain structure* and $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{C})$ *maximal chain structure*. We have:

$$\mathfrak{C} \neq \emptyset \Leftrightarrow \forall A \in \mathfrak{G}_1 \; \forall B \in \mathfrak{G}_2 \quad |A| = |B|.$$

If $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ satisfies the condition

(I_i) $\forall \{a_1, ..., a_i\} \in \binom{P}{i}$ which are joinable $\exists_1 K \in \mathfrak{K}$ with $\{a_1, ..., a_i\} \subseteq K$

for $i = 1, 2, 3$ then $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is called *web*, 2-*structure*, *hyperbola structure*, respectively. If $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is a web, for each $p \in P$ we denote the chain $K \in \mathfrak{K}$ which is uniquely determined by $p \in K$ with $[p]_3$, hence $[p]_3 \in \mathfrak{K}$ and $p \in [p]_3$.

For $A, B \in \mathfrak{C}$ and $p \in P$ let

$$pA := [p]_1 \cap A, \quad Ap := [p]_2 \cap A \quad \text{and} \quad \widetilde{AB} : P \to P; \quad x \mapsto (Bx)(xA).$$

Moreover we consider the 1- and 2-*perspectivities*:

$$[A \overset{1}{\to} B] : A \to B; \quad x \mapsto xB, \qquad [A \overset{2}{\to} B] : A \to B; \quad x \mapsto Bx.$$

We note:

7.2. *Let* $A, B, C \in \mathfrak{C}$ *then:*
(1) $\widetilde{AB} \in Sym\, P$ *with* $\widetilde{AB} \in Aut(P, \mathfrak{G}_1 \cup \mathfrak{G}_2)$ *and* $\widetilde{AB}(\mathfrak{G}_1) = \mathfrak{G}_2$, $\widetilde{BA} = (\widetilde{AB})^{-1}$, $Fix\, \widetilde{AB} = A \cap B$,
(2) $\widetilde{AB}(C) \in \mathfrak{C}$, $\widetilde{AB}(A) = B$, $\widetilde{AB}(B) = A$,
(3) $\widetilde{A} := \widetilde{AA}$ *is an involution with* $Fix\, \widetilde{A} = A$, *called* reflection in A,
(4) $\widetilde{AB} = \widetilde{CD} \Leftrightarrow (A, B) = (C, D)$,
(5) $\widetilde{A,B}_{|A} = [A \overset{2}{\to} B]$, $\widetilde{A,B}_{|B} = [B \overset{1}{\to} A]$,
(6) $\widetilde{A,B} \circ \widetilde{C} \circ \widetilde{B,A} = \widetilde{\widetilde{A,B}(C)}$, *in particular* $\widetilde{A} \circ \widetilde{C} \circ \widetilde{A} = \widetilde{\widetilde{A}(C)}$.

By 7.2(2) there is the following ternary operation:

$$\tau : \mathfrak{C} \times \mathfrak{C} \times \mathfrak{C} \to \mathfrak{C}; \quad (A, B, C) \mapsto \tau(A, B, C) := \widetilde{AC}(B).$$

Two chains $A, B \in \mathfrak{C}$ are called *orthogonal*, denoted by $A \perp B$, if $A \neq B$ and $\widetilde{A}(B) = B$. Then $A \perp B$ implies $B \perp A$. For a subset $\mathfrak{K} \subseteq \mathfrak{C}$ we denote by $\mathfrak{K}^{\perp} := \{C \in \mathfrak{C} \mid \forall K \in \mathfrak{K}\ \widetilde{C}(K) = K\}$ the *orthogonal complement* of the chain set $\mathfrak{K}$.

Definition 5. Let $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ be a chain structure, $T \in \mathfrak{C}$ and $X \in \mathfrak{G}_1 \cup \mathfrak{G}_2$. $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is called *covering* if $\bigcup \mathfrak{K} = P$. T is called *transversal* of $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ if for each $K \in \mathfrak{K}$

$$T \cap K \neq \emptyset \ \text{ and for each } \ t \in T\ \exists_1 K \in \mathfrak{K} \ \text{ such that } \ t \in K.$$

T is called *orthogonal transversal* of $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ if moreover for each $K \in \mathfrak{K}$ it holds $T \perp K$. X is called *transversal* (*quasi-transversal*) of $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ if the map

$$\mathfrak{K} \to X; \quad K \mapsto K \cap X$$

is a bijection (injection).

7.3. *Let $E \in \mathfrak{C}$ be fixed and for $A, B \in \mathfrak{C}$ let $A \cdot B := \widetilde{AB}(E)$. Then $(\mathfrak{C}, \cdot)$ is a group isomorphic to $\operatorname{Sym} E$ with the neutral element E and we have the representations:*

$$\tau(A, B, C) = \widetilde{AC}(B) = A \cdot B^{-1} \cdot C \quad \textit{and} \quad \widetilde{A}(B) = A \cdot B^{-1} \cdot A.$$

Definition 6. A subset $\mathfrak{S} \subseteq \mathfrak{C}$ is called *symmetric*, if for all $A, B \in \mathfrak{S}$ it holds $\tau(A, B, A) = \widetilde{A}(B) \in \mathfrak{S}$, and *double symmetric*, if for all $A, B, C \in \mathfrak{S}$ we have $\tau(A, B, C) = \widetilde{A, C}(B) \in \mathfrak{S}$.

Clearly each double symmetric subset $\mathfrak{S}$ is also symmetric, and the set of all symmetric and double symmetric subsets, respectively, is closed with respect to intersections. This allows us to define the two closure operations: if $\mathfrak{A}$ is an arbitrary subset of $\mathfrak{C}$ and if $\mathfrak{C}_S$ and $\mathfrak{C}_{SS}$, respectively, denotes the set of all symmetric and double symmetric subsets of $\mathfrak{C}$, let

$$\mathfrak{A}^{\sim} := \bigcap \{\mathfrak{S} \subseteq \mathfrak{C}_S \mid \mathfrak{A} \subseteq \mathfrak{S}\} \ \text{ and } \ \mathfrak{A}^{\sim\sim} := \bigcap \{\mathfrak{S} \subseteq \mathfrak{C}_{SS} \mid \mathfrak{A} \subseteq \mathfrak{S}\}\ ,$$

respectively, be the smallest symmetric and double symmetric subset of $\mathfrak{C}$ containing $\mathfrak{A}$.

Let $\widetilde{\mathfrak{A}} := \{\widetilde{A} \mid A \in \mathfrak{A}\}$ and $\widetilde{\widetilde{\mathfrak{A}}} := \{\widetilde{A, B} \mid A, B \in \mathfrak{A}\}$. Then:

7.4. *Let* $\mathfrak{A} \subseteq \mathfrak{C}$ *and* $\mathcal{M}(\mathfrak{A}) := \{\widetilde{AB}, \widetilde{AB} \circ \widetilde{C} \mid A, B, C \in \mathfrak{A}\}$. *Then:*

(1) $\mathfrak{A} = \mathfrak{A}^{\sim} \Leftrightarrow \widetilde{\mathfrak{A}}$ *is normal in* $\widetilde{\mathfrak{A}}$, (*i.e.,* $\forall\ \alpha, \beta \in \widetilde{\mathfrak{A}}\ \ \alpha \circ \beta \circ \alpha \in \widetilde{\mathfrak{A}}$),

(2) $\mathfrak{A} = \mathfrak{A}^{\sim\sim} \Leftrightarrow \widetilde{\mathfrak{A}}$ *is normal in* $\widetilde{\widetilde{\mathfrak{A}}}$,
(*i.e.,* $\forall\ \alpha \in \widetilde{\mathfrak{A}}\ \forall\ \beta \in \widetilde{\widetilde{\mathfrak{A}}}\ \ \beta \circ \alpha \circ \beta^{-1} \in \widetilde{\mathfrak{A}}$),

(3) *if an element* $E \in \mathfrak{A}$ *is fixed and the multiplication defined according to* 7.3, *then* $\mathfrak{A} = \mathfrak{A}^{\sim\sim}$, *i.e.,* $\mathfrak{A}$ *is double symmetric* $\Leftrightarrow \mathfrak{A} \leq \mathfrak{C}$,

(4) $\mathcal{M}(\mathfrak{A}) \leq Sym\, P \Leftrightarrow \mathfrak{A} \leq \mathfrak{C}$.

Remark 4. For a chain structure $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ the *General Rectangle Axiom*

$(R)\quad \forall A, B, C \in \mathfrak{K}\ :\ \{[[a]_1 \cap B]_2 \cap [[a]_2 \cap C]_1 \mid a \in A\} \in \mathfrak{K},$

formulated in [13] p.89, claims exactly that the set $\mathfrak{K}$ of chains is double symmetric, i.e., for all $A, B, C \in \mathfrak{K}$ it holds $A \cdot B^{-1} \cdot C \in \mathfrak{K}$. Therefore if a chain structure $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ satisfies the General Rectangle Axiom (R) then $\mathfrak{K}$ is symmetric. For a web $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ the axiom (R) is called *Reidemeister Condition.*

Remark 5. Another axiom formulated by W.Benz [3] for hyperbola structures $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ and called *Symmetry Axiom* is the following:

$(S)\quad \forall K, L \in \mathfrak{K}\ :\ |\widetilde{L}(K) \cap K| \geqslant 2\ \Rightarrow\ \widetilde{L}(K) = K.$

By [2] and [9] we have the result: *For a hyperbola structure* $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ *the Symmetry Axiom* (S) *implies the Rectangle Axiom* (R) *and so for a hyperbola structure* $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ *satisfying the Symmetry Axiom* (S) *the set of chains* $\mathfrak{K}$ *is symmetric.* But there are hyperbola structures $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ where $\mathfrak{K}$ is even double symmetric and the Symmetry Axiom (S) is violated (cf. [13] p. 90 ff).

7.5. *Let* $A, B, C, \dots \in \mathfrak{C}$, $E \in \mathfrak{C}$ *fixed and let* " $\cdot$ " *be defined according to* 7.3. *Then:*

(1) $Fix\, \widetilde{AB} = A \cap B, \quad Fix\, (\widetilde{AB} \circ \widetilde{C}) = (B \cap C)\square(A \cap C)$,

(2) $\widetilde{AB} \circ \widetilde{CD} \circ \widetilde{FG} = (AD^{-1}\widetilde{F})(\widetilde{GC^{-1}B})$,

(3) $\widetilde{AB} \circ \widetilde{CD} = (AD^{-1}\widetilde{U})(\widetilde{UC^{-1}B}) \circ \widetilde{U}$,

(4) $\widetilde{A} \circ \widetilde{B} \circ \widetilde{A} = \widetilde{AB^{-1}A} = \widetilde{\widetilde{A}(B)}$,

(5) $\widetilde{A} \circ \widetilde{BC} \circ \widetilde{A} = (AC^{-1}\widetilde{A})(\widetilde{AB^{-1}A}) = \widetilde{\widetilde{A}(C)}, \widetilde{A}(B)$,

(6) $\widetilde{AB} \circ \widetilde{E} \circ \widetilde{CD} \circ \widetilde{E} = (\widetilde{AC})(\widetilde{DB}) \circ \widetilde{E}$.

8. Symmetric chain structures as permutation sets

Let $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{C})$ be a maximal chain structure and let $\mathfrak{S} \subseteq \mathfrak{C}$ be a symmetric subset of chains, hence for all $S, T \in \mathfrak{S}$, $\widetilde{S}(T) \in \mathfrak{S}$. Therefore for each $S \in \mathfrak{S}$ the map

$$\widetilde{S} : \mathfrak{S} \to \mathfrak{S}; \quad X \mapsto \widetilde{S}(X)$$

is an involution of $Sym\,\mathfrak{S}$ and so $(\mathfrak{S}, \widetilde{\mathfrak{S}})$ with $\widetilde{\mathfrak{S}} := \{\widetilde{S} \mid S \in \mathfrak{S}\}$ is an involution set. By 7.2(6), $\widetilde{S} \circ \widetilde{T} \circ \widetilde{S} = \widetilde{\widetilde{S}(T)}$, hence $(\mathfrak{S}, \widetilde{\mathfrak{S}})$ is an invariant involution set. From 2.3 and 4.2 we obtain:

8.1. *Let $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{S})$ be a symmetric chain structure such that $(\mathfrak{S}, \widetilde{\mathfrak{S}})_r \neq \emptyset$ and let $E \in (\mathfrak{S}, \widetilde{\mathfrak{S}})_r$ then:*

(1) *$(\mathfrak{S}, \widetilde{\mathfrak{S}})$ is a regular invariant involution set,*

(2) *$\forall A, B \in \mathfrak{S}\ \exists_1 C \in \mathfrak{S}\ \ \widetilde{C}(A) = B$ (i.e., $[A \to B] = \widetilde{C}$),*

(3) *the loop derivation*

$$+ : \mathfrak{S} \times \mathfrak{S} \to \mathfrak{S}; \quad (A, B) \mapsto A + B := [E \to A] \circ \widetilde{E}(B)$$

of $(\mathfrak{S}, \widetilde{\mathfrak{S}})$ in E produces a K-loop $(\mathfrak{S}, +)$.

8.2. *Let $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{S})$ be a web with $\mathfrak{S}^\perp \neq \emptyset$, let $T \in \mathfrak{S}^\perp$ and for each $S \in \mathfrak{S}$ let $\widetilde{S}_{|T}$ be the restriction of $\widetilde{S}$ onto T then:*

(1) *$(T, \widetilde{\mathfrak{S}}_{|T})$ with $\widetilde{\mathfrak{S}}_{|T} := \{\widetilde{S}_{|T}) \mid S \in \mathfrak{S}\}$ is a regular involution set and for each $S \in \mathfrak{S}$ we have $S = \{x \square \widetilde{S}_{|T}(x) \mid x \in T\}$.*

(2) *The following statements are equivalent:*

(i) $\widetilde{\mathfrak{S}}$ is symmetric,

(ii) $(\mathfrak{S}, \widetilde{\mathfrak{S}})$ is a regular invariant involution set.

Proof. (1) Let $a, b \in T$ and $C := [ab]_3$ be the chain $C \in \mathfrak{S}$ of our web containing the point ab then $C \perp T$ and this implies $\widetilde{C}(T) = T$ and $\widetilde{T}(ab) = ba \in \widetilde{T}(C) = C$ hence $\widetilde{C}(a) = b$ and so $[a \leftrightarrow b] := \widetilde{C}_{|T}$ showing that $(T, \widetilde{\mathfrak{S}}_{|T})$ is a regular involution set.

(2) is a consequence of (1) and 8.1. □

9. Immersions of permutation sets in chain structures

We consider firstly the permutation set $(E, Sym\,E)$ where E is a not empty set. To $(E, Sym\,E)$ there corresponds the following maximal chain structure $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{C})$ (cf. e.g. [1]) with:

$$P := E \times E, \quad \mathfrak{G}_1 := \{E \times x \mid x \in E\}, \quad \mathfrak{G}_2 := \{x \times E \mid x \in E\}$$

and $\mathfrak{C}$ the set of all chains of the net $(P, \mathfrak{G}_1, \mathfrak{G}_2)$. If we identify E with the subset $\{(x,x) \mid x \in E\}$ of P then $E \in \mathfrak{C}$ and in that way we see that $\mathfrak{C}$ is not empty. Let

$$\kappa_E : Sym\, E \to \mathfrak{C}; \quad \sigma \mapsto \kappa_E(\sigma) := \{(x, \sigma(x)) \mid x \in E\}.$$

Then for each $\sigma \in Sym\, E$, $\kappa_E(\sigma)$ is a chain of $\mathfrak{C}$, the *graph* of σ, and the map κ_E is a bijection between $Sym\, E$ and $\mathfrak{C}$. The inverse map of κ_E is given by

$$\lambda_E : \mathfrak{C} \to Sym\, E; \quad C \mapsto \widetilde{CE} \circ \widetilde{CE}_{|E}.$$

Moreover if $\mathfrak{C}$ is turned into a group $(\mathfrak{C}, \cdot)$ according to 7.3 then κ_E is an isomorphism from the symmetric group $(Sym\, E, \circ)$ onto the group $(\mathfrak{C}, \cdot)$. Now let (E, Γ) be an arbitrary permutation set. Then $\mathfrak{K} := \kappa_E(\Gamma)$ is a subset of $\mathfrak{C}$ and $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ a chain structure called the *envelope* of (E, Γ). We write $\mathfrak{Ev}(E, \Gamma) := (P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$. Between a permutation set (E, Γ) and her envelope $\mathfrak{Ev}(E, \Gamma) := (P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ there are the following connections:

9.1. *Let (E, Γ) be a permutation set and $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K}) := \mathfrak{Ev}(E, \Gamma)$ her envelope then:*

(1) $\Gamma \leq Sym\, E \Leftrightarrow \mathfrak{K} \leq \mathfrak{C}$,

(2) *(E, Γ) is a regular permutation set $\Leftrightarrow$ $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is a web,*

(3) *(E, Γ) is a regular permutation group $\Leftrightarrow$ $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is a web with $\mathfrak{K} \leq \mathfrak{C}$, i.e., a web satisfying the Reidemeister Condition; in this case we call $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ a* webgroup,

(4) *(E, Γ) is a sharply 2-transitive permutation set $\Leftrightarrow$ $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is a 2-structure,*

(5) *(E, Γ) is a sharply 2-transitive permutation group $\Leftrightarrow$ $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is a 2-structure with $\mathfrak{K} \leq \mathfrak{C}$, i.e., a 2-structure satisfying the rectangle axiom (R) (cf. [7]); in this case we call $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ a* 2-group,

(6) *(E, Γ) is a sharply 3-transitive permutation set $\Leftrightarrow$ $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is a hyperbola structure,*

(7) *(E, Γ) is a sharply 3-transitive permutation group $\Leftrightarrow$ $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ is a hyperbola structure with $\mathfrak{K} \leq \mathfrak{C}$, i.e., a hyperbola structure satisfying the rectangle axiom; in this case we call $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ a* hyperbola group.

From now on we consider only permutation sets (E, Γ) with $(E, \Gamma)_r \neq \emptyset$.

9.2. *Let $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ be a chain structure with a transversal $X \in \mathfrak{G}_1$ of $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$, let $o \in X$ be fixed and let $E \in \mathfrak{K}$ with $o \in E$. Then for each $a \in E$, $o\square a$ is an element of X and so there is exactly one $A \in \mathfrak{K}$ with $o\square a \in A$. Therefore if we set $a^+ := \lambda_E(A)$ and $E^+ := \{a^+ \mid a \in E\}$ then (E, E^+) becomes a permutation set with $o \in (E, E^+)_r$, and $(E, +)$ with $a + b := a^+(b)$ becomes a left loop. Moreover we have $\kappa_E(a^+) = A$ hence $\mathfrak{K} = \kappa_E(E^+)$ and the following three propositions are equivalent:*

(i) $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$ *is a web,*

(ii) $\forall X \in \mathfrak{G}_1$ X *is a transversal of* $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$,

(iii) $\forall X \in \mathfrak{G}_2$ X *is a transversal of* $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$.

9.3. *Let $(E, +)$ be a left loop, $X := o\square E$, $\mathfrak{K} := \kappa_E(E^+)$ and for $a, b \in E$, $A := \kappa_E(a^+)$, $B := \kappa_E(b^+)$ then $\kappa_E(a^+ \circ b^+ \circ a^+) = A \cdot B \cdot A = \widetilde{A}(B^{-1})$ and we have:*

(1) $X \in \mathfrak{G}_1$ *is a transversal of* $(P, \mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{K})$,

(2) $a^+ \circ b^+ \circ a^+ \in E^+ \Leftrightarrow A \cdot B \cdot A = \widetilde{A}(B^{-1}) \in \mathfrak{K}$,

(3) $(E, +)$ *is a Bol loop* $\Leftrightarrow \mathfrak{K}$ *is symmetric.*

From 9.3 we obtain the theorems:

Theorem 9.4. *Let $(E, +)$ be a Bol loop and let $\mathfrak{K} := \kappa_E(E^+)$ then $\mathfrak{K}$ is symmetric hence (by section 8) $(\mathfrak{K}, \widetilde{\mathfrak{K}})$ is an invariant involution set and the following statements are equivalent:*

(i) $(\mathfrak{K}, \widetilde{\mathfrak{K}})$ *is regular,*

(ii) for all $a, b \in E$ *the equation* $b = x + (-a + x)$ *has exactly one solution* $x \in E$,

(iii) $(E, +)$ *is uniquely 2-divisible, i.e.,* $\forall a \in E$ $\exists_1 x \in E$ *with* $x + x = a$,

(iv) $\forall A \in \mathfrak{K}$ $\exists_1 A' \in \mathfrak{K}$ $A' \cdot A' = A$ *(this implies: if* $A + B := A' \cdot B \cdot A'$ *then* $(\mathfrak{K}, +)$ *is a K-loop),*

(v) $\mathfrak{K}^\perp \neq \emptyset$.

Proof. Let $A, B \in \mathfrak{K}$ and $a^+ := \lambda_E(A)$, $b^+ := \lambda_E(B)$. If there is a $C \in \mathfrak{K}$ such that $B = \widetilde{C}(A) = C \cdot A^{-1} \cdot C$ and if $c^+ := \lambda_E(C)$ then $b^+ = c^+ \circ (-a)^+ \circ c^+$ hence $b = c + (-a + c)$. If $c \in E$ is a solution of the equation $b = x + (-a + x)$ and $C := \kappa_E(C^+)$ then $\widetilde{C}(A) = B$. This shows the equivalence of (i) and (ii) and if we set $a := o$ in (ii) we see that (ii) implies (iii). Finally we assume (iii). For each $a \in E$ let $a' \in E$ such that $a' + a' = a$ then if $A := \kappa_E(a^+)$ and $A' := \kappa_E(a'^+)$ we have $\widetilde{A'}(E) = A' \cdot E \cdot A' = A' \cdot A' = \kappa_E(a'^+) \cdot \kappa_E(a'^+) = \kappa_E(a'^+ \circ a'^+) = \kappa_E(a^+) = A$. This

shows (iv) and $E \in (\mathfrak{K}, \widetilde{\mathfrak{K}})_r$ and so by 2.3(4), $(\mathfrak{K}, \widetilde{\mathfrak{K}})$ is a regular invariant involution set, i.e., (iv) implies (i).

The equivalence of (i) and (v) is a consequence of 8.1. □

We set $A + B := \widetilde{A'} \circ \widetilde{E}(B) = \widetilde{A'}(B^{-1}) = A' \cdot B \cdot A' = \kappa_E(a'^+) \cdot \kappa_E(b^+) \cdot \kappa_E(a'^+) = \kappa_E(a'^+ \circ b^+ \circ a'^+) = \kappa_E(a' + (b + a'))^+ \in \kappa_E(E^+) = \mathfrak{K}$ and so by 8.1(3), $(\mathfrak{K}, +)$ is a K-loop and moreover we have the result of P. T. Nagy and K. Strambach [23].

Theorem 9.5. *Let $(E, +)$ be a Bol loop uniquely 2-divisible and for $a \in E$ let $a' \in E$ such that $a' + a' = a$, then $(E, \oplus)$ with $a \oplus b := a' + (b + a')$ is a K-loop.*

10. Loops derived from point reflection spaces

In this section let $(P, \sim)$ be a point reflection space, let a point $o \in P$ be fixed and let $(P, +)$ be the loop derivation of $(P, \sim)$ in o. If $(P, \sim)$ is singular then by 6.4 the loop $(P, +)$ is a commutative group. Therefore we assume that $(P, \sim)$ is ordinary. Then by 9.4, $(P, +)$ is a proper K-loop uniquely 2-divisible. For $p \in P$ let $p' \in P$ such that $p' + p' = p$. We recall that the operation "+" is given by $a + b := \widetilde{a'} \circ \widetilde{o}(b)$ and that the pair $(P, \mathfrak{L})$, where $\mathfrak{L}$ denotes the set of equivalence classes of the relation ρ, is an incidence space (cf. section 6).

We show:

Theorem 10.1. *Let $\mathfrak{F} := \mathfrak{L}(o) := \{L \in \mathfrak{L} \mid o \in L\}$ be the set of all equivalence classes containing o and let $a, b \in P$. Then:*

(1) *if $a^+ \circ b^+ = b^+ \circ a^+$ then $a^+ \circ b^+ \in P^+$, more precisely, $a^+ \circ b^+ = (a + b)^+$,*

(2) *For each $F \in \mathfrak{F}$, F is a commutative subgroup of the loop $(P, +)$, and if $a \in F \setminus \{o\}$ then $F = \{x \in P \mid a^+ \circ x^+ = x^+ \circ a^+\}$,*

(3) *$\mathfrak{L} = \{a + F \mid a \in P,\ F \in \mathfrak{F}\}$,*

(4) *the collineation group $Aut(P, \mathfrak{L})$ contains P^+,*

(5) *the set $\mathfrak{F}$ is a fibration of the K-loop $(P, +)$ consisting of commutative subgroups of the loop $(P, +)$, i.e., for all $A, B \in \mathfrak{F}$ and for each $a \in P$:*

   (F.1) $|A| \geqslant 2$,

   (F.2) $\bigcup \mathfrak{F} = P$,

   (F.3) if $A \neq B$ then $A \cap B = \{o\}$.

Proof. (1) By $p^+ = \widetilde{p'} \circ \widetilde{o}$, the equation $a^+ \circ b^+ = \widetilde{a'} \circ \widetilde{o} \circ \widetilde{b'} \circ \widetilde{o} = b^+ \circ a^+ = \widetilde{b'} \circ \widetilde{o} \circ \widetilde{a'} \circ \widetilde{o}$ implies $\widetilde{a'} \circ \widetilde{o} \circ \widetilde{b'} = \widetilde{b'} \circ \widetilde{o} \circ \widetilde{a'}$, i.e., $\widetilde{a'} \circ \widetilde{o} \circ \widetilde{b'} \in J$ and so by (R1), there is a $c \in P$ such that $\widetilde{a'} \circ \widetilde{o} \circ \widetilde{b'} = \widetilde{c}$. Therefore $a^+ \circ b^+ = \widetilde{c} \circ \widetilde{o} \in P^+$ and since $a^+ \circ b^+(o) = a^+(b) = a + b$ this implies $a^+ \circ b^+ = (a+b)^+$.

(2) For $p \in P^+$ the equation $p = \widetilde{p'}(o)$ implies by 6.1(4), $\widetilde{p} = \widetilde{\widetilde{p'}(o)} = \widetilde{p'} \circ \widetilde{o} \circ \widetilde{p'}$ and $p' \neq o$ hence $\widetilde{o} \circ \widetilde{p'} \circ \widetilde{p} = \widetilde{p'} \in J$ and $\widetilde{o} \circ \widetilde{p} \circ \widetilde{p'} = \widetilde{o} \circ \widetilde{p'} \circ \widetilde{o} \in J$ and so by 6.5(3), $p' \in \overline{o,p}$ and $p \in \overline{o,p'}$ hence $\overline{o,p} = \overline{o,p'}$. Therefore: $x \in F = \overline{o,a} = \overline{o,a'} \Leftrightarrow x' \in F = \overline{o,a'} \Leftrightarrow \widetilde{x'} \circ \widetilde{o} \circ \widetilde{a'} = \widetilde{a'} \circ \widetilde{o} \circ \widetilde{x'} \Leftrightarrow x^+ \circ a^+ = \widetilde{x'} \circ \widetilde{o} \circ \widetilde{a'} \circ \widetilde{o} = \widetilde{a'} \circ \widetilde{o} \circ \widetilde{x'} \circ \widetilde{o} = a^+ \circ x^+ \;\Rightarrow\; x + a = x^+(a) = x^+ \circ a^+(o) = a^+ \circ x^+(o) = a + x$.

(3), (4) If $p \in P$ then by 6.5(6) $p^+ = \widetilde{p'} \circ \widetilde{o} \in Aut(P, \mathfrak{L})$, and therefore if $L \in \mathfrak{L}$, $p \in L$ then $F := (p^+)^{-1}(L) \in \mathfrak{L}$ and $o \in F$, i.e., $F \in \mathfrak{F}$ and $a + F = a^+(F) = L$. □

11. Loops with fibrations

In 1987 Elena Zizioli introduced for loops the notion of an *incidence fibration* (cf. [27], [16]) in the sense of the following definition:

Given a loop $(P,+)$ and a set $\mathfrak{F} \subseteq 2^P$, $\mathfrak{F}$ is called a *fibration* of $(P,+)$ if:

$(F1)$ $\forall X \in \mathfrak{F} \;\; |X| \geqslant 2$,

$(F2)$ $\bigcup \mathfrak{F} = P$,

$(F3)$ $\forall A, B \in \mathfrak{F} \; A \neq B \;\; A \cap B = \{o\}$.

If furthermore the following conditions

$(F4)$ $\forall a \in P \; \forall X \in \mathfrak{F} \;\; o \in a + X \Longrightarrow a + X \in \mathfrak{F}$,

$(F5)$ $\forall X \in \mathfrak{F} \; \forall \delta \in \Delta \;\; \delta(X) \in \mathfrak{F}$,

are valid then $\mathfrak{F}$ is called an *incidence fibration*.

Remark 6. If $(P, +, \mathfrak{F})$ is a fibered loop then to each $a \in P^*$ there is exactly one fiber $A \in \mathfrak{F}$ with $a \in A$ which we denote by $[a]$. Then $(F4)$ and $(F5)$ can be expressed in the form:

$(F4)'$ $\forall a \in P^* \;\; a + [-a] = [a]$,

$(F5)'$ $\forall a \in P^* \; \forall \delta \in \Delta \;\; \delta([a]) = [\delta(a)]$.

By [27] we have:

11.1. *If $\mathfrak{F}$ is an incidence fibration of a loop $(P,+)$ let $\mathfrak{L} := \{a + X \mid a \in P,\ X \in \mathfrak{F}\}$. Then $(P, \mathfrak{L}, +)$ is an incidence loop, i.e., $(P, \mathfrak{L})$ is an incidence space, $(P,+)$ is a loop and for each $a \in P$ the map a^+ is a collineation of $(P, \mathfrak{L})$.*

Remark 7. The fibration $\mathfrak{F}$ corresponding to an ordinary point reflection space $(P,\sim)$ according to 9.1 is an incidence fibration of the loop $(P,+)$ since the fiberes are subgroups of $(P,+)$ and the maps a^+ collineations of $(P,\mathfrak{L})$. Moreover if $A \in \mathfrak{F}$ and $a \in A \setminus \{o\}$ then $A = \{x \in P \mid x^+ \circ a^+ = a^+ \circ x^+\}$ is the centralizer of the element a in $(P.+)$.

Now we ask, when do the centralizers of an arbitrary loop form a fibration or an incidence fibration, respectively? To answer this, we consider the following two exchange conditions:

$(Z1)$ For all $a, b \in P^*$ if $b \in [a]$ then $[a] \subseteq [b]$.

$(Z2)$ For all $a, b \in P^*$ if $a^+ \circ b^+ = b^+ \circ a^+$ then $a^+ \circ b^+ \in P^+$.

11.2. *Let $(P,+)$ be a loop, for any $a \in P^*$ let $[a] := \{x \in P \mid a^+ \circ x^+ = x^+ \circ a^+\}$ be the centralizer of a and let $\mathfrak{Z} := \{[a] \mid a \in P^*\}$. Then:*

(1) *$\mathfrak{Z}$ is a fibration of $(P,+)$ if and only if the exchange condition $(Z1)$ is verified,*

(2) *$\mathfrak{Z}$ is an incidence fibration if and only if $(Z1)$ and the condition: "$\forall a \in P^*\ \forall \delta \in \Delta:\quad a + [-a] = [a]$ and $\delta([a]) = [\delta(a)]$" are valid,*

(3) *if $\mathfrak{Z}$ is a fibration then on each fiber $[a]$ the addition "$+$" is commutative,*

(4) *if $(P,+)$ satisfies $(Z1)$ and $(Z2)$ then each fiber $[a]$ is a commutative subsemigroup of $(P,+)$ and $[a]^+ := \{x^+ \mid x \in [a]\}$ is a commutative subsemigroup of $Sym\, P$,*

(5) *if $\Delta \leq Aut(P,+)$ (i.e., $(P,+)$ is an A_l-loop, cf. [17] p. 35) then $\mathfrak{Z}$ satisfies $(F5)$.*

Proof. (3), (4) Let $x, y \in [a] \setminus \{o\}$. Then $x+y = x^+ \circ y^+(o) = y^+ \circ x^+(o) = y + x$. If $(Z2)$ is valid then $(x+y)^+(o) = x + y = x^+ \circ y^+(o)$ implies $(x+y)^+ = x^+ \circ y^+$ and so $a^+ \circ (x+y)^+ = a^+ \circ x^+ \circ y^+ = x^+ \circ a^+ \circ y^+ = x^+ \circ y^+ \circ a^+ = (x+y)^+ \circ a^+$, i.e., $x + y \in [a]$ and moreover $(x+y)+z = (x+y)^+(z) = x^+ \circ y^+(z) = x + (y+z)$ showing that $[a]$ and $[a]^+$ are semigroups.

(5) Clearly if $a \in P^*$ and $\alpha \in Aut(P,+)$ then $\alpha([a]) = [\alpha(a)]$. □

If $\mathfrak{Z}$ is an incidence fibration we say that the loop $(P,+)$ has a *c(entralizer)-fibration*. In order to obtain more informations we claim from now on that our loop $(P,+)$ satisfies the *left inverse property*

$$\forall a \in P \quad a^+ \circ (-a)^+ = id.$$

11.3. *Let $(P,+)$ be a loop satisfying the left inverse property and $(Z1)$ then:*

(1) *$\nu \in Aut(P,\mathfrak{Z}) \cap J$, more precisely ν is the identity on $\mathfrak{Z}$,*

(2) *$(F4)' \Leftrightarrow \forall a \in P^*\ \ [a]+[a] \subseteq [a]$,*

(3) *if for each $a \in P^*\ \ [a]+[a] \subseteq [a]$ then $[a]$ is a commutative subgroup of the loop $(P,+)$,*

(4) *$(P,+)$ has a c-fibration if and only if $(Z1)$ and the condition: "$\forall a \in P^*\ \forall \delta \in \Delta\ \ [a]+[a]=[a]$ and $\delta([a])=[\delta(a)]$" are valid.*

Proof. Let $a \in P^*$ then $(-a)^+ = (a^+)^{-1}$ and so $a^+ \circ (-a)^+ = (-a)^+ \circ a^+$, hence by $(Z1)$, $[a]=[-a]$, i.e., $\nu \in Aut(P,\mathfrak{Z}) \cap J$ and $a+[-a] = a+[a] \subseteq [a]+[a] \subseteq [a]$. If $x \in [a]$ then $y := (a^+)^{-1}(x) = (-a)^+(x) = -a+x \in [a]+[a] \subseteq [a]$ hence $x \in a^+([a]) = a+[a]$. Together $a+[-a]=[a]$ and this shows the equivalence in (2). □

By 10.1, the loop $(P,+)$ derived from an ordinary point reflection space is a K-loop satisfying the exchange conditions $(Z1)$ and $(Z2)$. Since a K-loop is an A_l-loop with left inverse property, $(P,+)$ has a c-fibration.

11.4. *Let $(P,+)$ be a loop with left inverse property and where $\mathfrak{Z}$ is a c-fibration, let $(P,+,\mathfrak{L})$ (with $\mathfrak{L} := \{a+[b] \mid a \in P,\ b \in P^*\}$) the corresponding incidence loop (according 11.1) and let $a \in P^*$ then:*

(1) *the restriction of ν onto $[a]$ is an automorphism of the commutative group $([a],+)$,*

(2) *for each $p \in P\ \ \widetilde{\widetilde{p}} \in J$ and $\widetilde{\widetilde{p}}$ fixes the bundle $p+\mathfrak{Z}$ linewise,*

(3) *if $\nu \in Aut(P,+)$ then $P^\circ = P^+ \circ \nu \subseteq Aut(P,\mathfrak{L}) \cap J$ and for $p \in P$ $\nu \circ p^+ \circ \nu = (\nu(p))^+ = (-p)^+$, $\widetilde{\widetilde{p}} = p^+ \circ p^+ \circ \nu = p^+ \circ p^\circ$, hence $\widetilde{\widetilde{P}} \subseteq Aut(P,\mathfrak{L}) \cap J$.*

We summarize:

Theorem 11.5. *Let $(P,\sim)$ be an ordinary point reflection space (cf. Definition 4), let $o \in P$ be fixed and let $(P,+)$ the loop derivation of $(P,\sim)$ in o. Then $(P,+)$ is a proper K-loop uniquely 2-divisible, satisfying $(Z1)$ and $(Z2)$ and $\mathfrak{Z}$ is an incidence fibration.*

Theorem 11.6. *Let $(P,+)$ be a proper K-loop uniquely 2-divisible satisfying $(Z1)$ and $(Z2)$ and let*

$$\sim: P \to J; \quad p \mapsto \widetilde{p} := p^+ \circ \nu \circ (-p)^+.$$

Then:

(1) *$\mathfrak{Z}$ is an incidence fibration,*

(2) *$(P,\sim)$ is an ordinary point reflection space.*

Proof. (1) A K-loop is an A_l-loop with left inverse property. Therefore by 11.2 and 11.3, $(Z1)$ and $(Z2)$ enforce that $\mathfrak{Z}$ is an incidence fibration.

(2) Since in an uniquely 2-divisible K-loop, ν is an involutory automorphism of $(P,+)$ with $Fix\,\nu = \{o\}$ and $(-p)^+ = (p^+)^{-1}$, the map $\widetilde{p}$ is an involution fixing exactly the point p and $\widetilde{p} = (p+p)^+ \circ \nu = (p+p)^\circ$ showing $P^\circ = P^+ \circ \nu = \widetilde{P} := \{\widetilde{p} \mid p \in P\}$. By 3.7 and the 2-divisibility, $(P, P^\circ) = (P, \widetilde{P})$ is a selfhomogeneous invariant regular involution set satisfying (M). Hence $(P,\sim)$ is a point reflection structure and $\widetilde{p} = p^\circ \circ \nu \circ p^\circ$. If $(a,b,c) \in P^3$ are given and $a' := b^\circ \circ \widetilde{a} \circ b^\circ(o) = b^\circ \circ \widetilde{a}(b)$, $c' := b^\circ \circ \widetilde{c} \circ b^\circ(o) = b^\circ \circ \widetilde{c}(b)$ then $a'^\circ = b^\circ \circ \widetilde{a} \circ b^\circ$ and $c'^\circ := b^\circ \circ \widetilde{c} \circ b^\circ$ and we have: $(a,b,c) \in \rho \Leftrightarrow \widetilde{a} \circ \widetilde{b} \circ \widetilde{c} \in J \Leftrightarrow a'^\circ \circ \nu \circ c'^\circ \in J \Leftrightarrow a'^+ \circ c'^+ = c'^+ \circ a'^+$ implying by $(Z2)$, $d^\circ \circ \nu = d^+ = a'^+ \circ c'^+ = a'^\circ \circ \nu \circ c'^\circ \circ \nu$ for $d := a' + b'$ hence $d^\circ = b^\circ \circ \widetilde{a} \circ b^\circ \circ \nu \circ b^\circ \circ \widetilde{c} \circ b^\circ \Leftrightarrow \tilde{a} \circ \tilde{b} \circ \tilde{c} = b^\circ \circ d^\circ \circ b^\circ \in P^\circ = \tilde{P}$. Thus $(R1)$ is valid.

In order to show $(R2)$ we use the same notation as in the proof of $(R1)$. By the invariance of P° and $(R1)$, the relation ρ is symmetric. Therefore let $a \neq b$ and $(a,b,c),(a,b,d) \in \rho$ hence $a'^+ \circ c'^+ = c'^+ \circ a'^+$ and $a'^+ \circ d'^+ = d'^+ \circ a'^+$, i.e., $c', d' \in [a']$ and so $d'^+ \circ c'^+ = c'^+ \circ d'^+$ implying again by $(Z2)$ for $e := c' + d'$, $\tilde{c} \circ \tilde{b} \circ \tilde{d} = b^\circ \circ e^\circ \circ b^\circ \in P^\circ = \tilde{P}$. Consequently $(c,b,d) \in \rho$ and so also $(b,c,d) \in \rho$. Since $(P,+)$ is not commutative, $\rho \neq R^3$ and therefore $(P,\sim)$ is an ordinary point reflection space. □

References

[1] **B. Alinovi, H. Karzel and C. Tonesi**: *Halforders and automorphisms of chain structures*, J. Geometry **71** (2001), 1 – 18.

[2] **R. Artzy**: *A Pascal theorem applied to Minkowski geometry*, J. Geometry **9** (1973), 93 – 105.

[3] **W. Benz**: *Permutations and plane sections of ruled quadric*, Ist. Naz. Alta Mat., Symposia Matematica **5** (1971), 325 – 339.

[4] **E. Gabrieli, B. Im and H. Karzel**: *Webs related to K-loops and reflection structures*, Abh. Math. Semin. Univ. Hamburg **69** (1999), 89 – 102.

[5] **E. Gabrieli and H. Karzel**: *Point reflection geometries, geometric K-loops and unitary geometries*, Result. Math. **32** (1997), 66 – 72.

[6] **E. Gabrieli and H. Karzel**: *Reflection geometries over loops*, Result. Math. **32** (1997), 61 – 65.

[7] **H. Karzel**: *Zusammenhänge zwischen Fastbereichen, scharf zweifach transitiven Permutationsgruppen und 2-Strukturen mit Rechtecksaxiom*, Abh. Math. Semin. Univ. Hamburg **32** (1968), 191 – 206.

[8] **H. Karzel**: *Relations between incidence loops and normal quasi-fields*, J. Geometry **7** (1976), 9 – 10.

[9] **H. Karzel**: *Symmetrische Permutationsmengen*, Aequationes Math. **17** (1978), 83 – 90.

[10] **H. Karzel**: *Recent developments on absolute geometries and algebraization by K-loops*, Discrete Math. **208/209** (1999), 387 – 409.

[11] **H. Karzel and G. Kist**: *Kinematic algebras and their geometries*, Rings and geometry (Kaya et al. eds) NATO ASI series-C **160** (1985), 437 – 509.

[12] **H. Karzel and A. Konrad**: *Reflection groups and K-loops*, J. Geometry **52** (1995), 120 – 129.

[13] **H. Karzel and H.-J. Kroll**: *Geschichte der Geometrie seit Hilbert*, Wiss. Buchges., Darmstadt, 1988.

[14] **H. Karzel and S. Pianta**: *Left loops, bipartite graphs with parallelism and involution sets*, Abh. Math. Semin. Univ. Hamburg **75** (2005), 203 – 214.

[15] **H. Karzel, K. Sörensen and D. Windelberg**: *Einführung in die Geometrie*, Vandenhoeck, Göttingen, 1973.

[16] **H. Karzel and E. Zizioli**: *Extension of a class of fibered loops to kinematic spaces*, J. Geometry **65** (1999), 117 – 129.

[17] **H. Kiechle**: *Theory of K-loops*, Lecture notes in Mathematics vol.1778, Springer, 2000.

[18] **G. Kist**: *Theorie der verallgemeinerten kinematischen Räume*, Habilitationsschrift TU München, 1980.

[19] **E. Kolb and A. Kreuzer**: *Geometry of kinematic K-loops*, Abh. Math. Semin. Univ. Hamburg **65** (1995), 189 – 197.

[20] **A. Kreuzer**: *K-loops and Bruck-loops on* $\mathbb{R} \times \mathbb{R}$, J. Geometry **47** (1993), 86 – 93.

[21] **A. Kreuzer**: *Reflection loops and linear spaces with hyperbolic incidence structure*, Comment. Math. Univ. Carolinae **45** (2004), 303 – 320.

[22] **M. Marchi**: *Partition loops and affine geometries*, in *Procedings of the second Isle of Thorns Conference*, London Math. Soc. Lecture Notes **49** (1980), 226–243.

[23] **P. Nagy and K. Strambach**: *Loops in group theory and Lie Theory*, Expositions in Mathematics **35**, De Gruyter, Berlin, New York, 2002.

[24] **A. Ungar**: *Thomas rotation and the parametrisation of the Lorentz transformation group*, Found. Phys. Lett. **1** (1988), 57 – 89.

[25] **A. Ungar**: *The relativistic noncommutative nonassociative group of velocities and the Thomas rotation*, Results Math. **16** (1989), 168 – 179.

[26] **H. Wähling**: *Projektive Inzidenzgruppoide und Fastalgebren*, J. Geometry **9** (1977), 109 – 126.

[27] **E. Zizioli**: *Fibered incidence loops and kinematic loops*, J. Geometry **30** (1987), 144 – 151.

Zentrum Mathematik
T.U. München
D-80290 München
Germany

Received June 5, 2007

Quasigroups and Related Systems **15** (2007), 77 – 94

Computing with small quasigroups and loops

Gábor P. Nagy and Petr Vojtěchovský

Abstract

This is a companion to our lectures *GAP and loops*, to be delivered at the *Workshops Loops 2007*, Prague, Czech Republic. In the lectures we introduce the GAP [6] package LOOPS [15], describe its capabilities, and explain in detail how to use it. In this paper we first outline the philosophy behind the package and its main features, and then we focus on three particular computational problems: construction of loop isomorphisms, classification of small Frattini Moufang loops of order 64, and the search for loops of nilpotency class higher than two with an abelian inner mapping group.

In particular, this is not a user's manual for LOOPS, which can be downloaded from the distribution website of LOOPS.

1. Main features

On the one hand, since there is no useful representation theory for quasigroups and loops, we have decided to represent quasigroups and loops in LOOPS by their Cayley tables, thus effectively limiting the scope of the package to quasigroups of order at most 500 or so. (A future project is to implement other loop representations, notably by connected transversals in groups.)

On the other hand, to take advantage of the powerful methods for groups already present in GAP, most calculations in LOOPS are delegated to the permutation groups associated with quasigroups, rather than performed on the level of Cayley tables. For instance, to decide if a loop is simple, we check whether its multiplication group is a primitive permutation group.

2000 Mathematics Subject Classification: Primary 20N05.

Keywords: loop, quasigroup, GAP, computation in nonassociative algebra, loop isomorphism, Latin square, Csörgő loop, small Frattini Moufang loop, LOOPS package, code loop.

This paper was written during the Marie Curie Fellowship of the first author at the University of Würzburg. The second author supported by the PROF 2006 grant of the University of Denver.

To avoid repeated calculations, we store most information obtained for a given quasigroup as its attribute. In GAP, there is no syntactical difference between calling a method or retrieving an attribute. For instance, when Q is a quasigroup then `Center(`Q`)` calculates and stores the center $Z(Q)$ of Q when called for the first time, while it retrieves the stored attribute $Z(Q)$ when called anytime later.

Moreover, GAP uses simple deduction process—filters—to obtain additional information about an object without an explicit user's request. For instance, if LOOPS knows that Q is a left Bol loop that is also commutative, the built-in filter `(IsMoufangLoop, IsLeftBolLoop and IsCommutative)` automatically deduces that Q is a Moufang loop and stores this information for Q. This is a powerful tool, since many filters built into LOOPS are deep theorems.

1.1. Creating quasigroups and loops

A (*quasigroup*) *Cayley table* is an $n \times n$ Latin square with integral entries $x_1 < \cdots < x_n$. A *canonical Cayley table* is a Cayley table with $x_1 = 1, \ldots, x_n = n$.

When T is a Cayley table, `QuasigroupByCayleyTable(`T`)` creates a quasigroup whose Cayley table is the canonical Cayley table obtained from T by replacing x_i with i. Should T be *normalized*—the first row and first column reads $x_1, \ldots, x_n$—then `LoopByCayleyTable(`T`)` returns the corresponding loop. The Cayley table of a quasigroup Q can be retrieved by `CayleyTable(`Q`)`.

Throughout this paper, we illustrate the methods of LOOPS by examples, often without any comments for self-explanatory commands. The syntax is that of GAP.

```
gap> Q := QuasigroupByCayleyTable([[2,1],[1,2]]); Elements(Q);
<quasigroup of order 2>
[ q1, q2 ]
gap> L := LoopByCayleyTable([[3,5],[5,3]]); Elements(L); L.2;
<loop of order 2>
[ l1, l2 ]
l2
gap> CayleyTable(Q);
[ [ 2, 1 ], [ 1, 2 ] ]
gap> Print(L);
<loop with multiplication table
[ [  1,  2 ],
  [  2,  1 ] ]
>
```

It is also possible to create quasigroups and loops by reading Cayley tables from files (with very relaxed conditions on the form of the Cayley table), by converting groups to quasigroups, by taking subquasigroups, subloops, factor loops, direct products, etc. See the manual for details.

1.2. Conversions

Even if a quasigroup happens to have a neutral element, it is not considered a loop in LOOPS unless it is declared as a loop. Similarly, a group of GAP is not considered a loop. We therefore provide conversions between these types of algebras:

```
gap> G := Group((1,2,3),(1,2)); AsLoop(G);
Group([ (1,2,3), (1,2) ])
<loop of order 6>
gap> Q := QuasigroupByCayleyTable([[2,1],[1,2]]);  AsLoop(Q);
<quasigroup of order 2>
<loop of order 2>
```

The neutral element of any loop L in LOOPS is always the first element of L, i.e., `One(`L`) = `L`.1`.

Given a quasigroup Q and elements $f, g \in Q$, the principal loop isotope (Q, f, g) of Q is obtained from Q via the isotopism $(R_g^{-1}, L_f^{-1}, \mathrm{id})$, cf. [17, p. 60]. Then (Q, f, g) is a loop with neutral element fg.

The conversion `AsLoop(`Q`)` works as follows, starting with a quasigroup Q:

(i) When Q does not have a neutral element, it is first replaced by the principal loop isotope $(Q, Q.1, Q.1)$, thus turning Q into a loop with neutral element $(Q.1)(Q.1)$.

(ii) When Q has a neutral element k, it is replaced by its isomorphic copy via the transposition $(1, k)$.

1.3. Subquasigroups and subloops

A new quasigroup Q_2 is frequently obtained as a subquasigroup of an existing quasigroup Q_1. Since all information about Q_2 is already contained in the Cayley table of Q_1, and since it is often desirable to have access to the embedding of Q_2 into Q_1, we provide a mechanism in LOOPS for maintaining the inclusion of Q_2 and Q_1.

When Q_1 is a quasigroup and S is a subset of Q_1, `Subquasigroup(`Q_1`,` S`)` returns the subquasigroup Q_2 of Q_1 generated by S. At the same time, the attribute `Parent(`Q_2`)` is set to `Parent(`Q_1`)`, hence ultimately pointing to the largest quasigroup from which Q_2 has been created. The elements of Q_2 and the Cayley table of Q_2 are then calculated relative to the parent of Q_2.

```
gap> L := AsLoop(Group((1,2,3),(1,2))); S := Subloop(L,[3]);
<loop of order 6>
<loop of order 2>
gap> Parent( S ) = L; PosInParent( S ); Elements( S );
true
[ 1, 3 ]
[ l1, l3 ]
gap> HasCayleyTable( S ); CayleyTable( S );
false
[ [ 1, 3 ], [ 3, 1 ] ]
```

Note that the Cayley table of a subquasigroup is created only upon user's request.

1.4. Bijections as permutations on $\{1,\ldots,n\}$

When calculating isomorphisms, isotopisms, or other bijections of quasigroups of order n, the result is always returned as a permutation (triple of permutations) of $\{1,\ldots,n\}$. Equivalently, the quasigroups in question are first replaced by isomorphic copies with canonical Cayley tables, and only then the bijections are calculated. It is always possible to reconstruct the original bijection using the attribute `PosInParent`.

1.5. A few words about the implementation

One of the biggest strengths of the computer algebra system GAP is that most algebraic structures can be defined within it. In this subsection we briefly explain how the variety of quasigroups is implemented in LOOPS. In order to understand the implementation, we will need the following GAP terminology:

– A *filter*, such as `IsInteger` and `IsPermGroup`, is a special unary function on the set of GAP objects which returns either `true` or `false`. Roughly speaking, a filter is an *a priori* attribute of an object.

- A *category* is a class of objects defined by a collection of filters. An object can lie in several categories. For example, a row vector lies in the categories `IsList` and `IsVector`.
- All GAP objects are partitioned into *families.* The family of an object determines its relation to other objects. For instance, all permutations form a family, and groups presented by generators and relations form another family. However, a family is not a collection of objects, but abstract information about objects.
- Beside its name, a family can have further *labels.*
- Every GAP object has a *type.* The type of an object determines if a given operation can be performed with that object, and if so, how it is to be performed. The type of an object is derived from its family and its filters.
- A given data structure can be made into an *object* by specifying its type, that is, its family and its filters.

The following function constructs a quasigroup Q with Cayley table `ct`. First we define a family corresponding to the elements of Q and tell GAP that it will consist of quasigroup elements. Then we objectify the individual elements in this family, and label the family by the set of its elements, by the size of Q, and by the Cayley table. Then we objectify Q whose family will be the *collection* of its elements. Finally, we set some important attributes of Q.

```
function( ct )
    local F, Q, elms, n;
    # constructing the family of the elements of this quasigroup
    F := NewFamily( "QuasigroupByCayleyTableFam", IsQuasigroupElement );
    # installing data ("labels") for the family
    n := Length ( ct );
    F!.size := n;
    elms := Immutable( List( [1..n], i -> Objectify(
        NewType( F, IsQuasigroupElement and IsQuasigroupElmRep), [ i ] ) ) );
    F!.set := elms;
    F!.cayleyTable := ct;
    # creating the quasigroup by turning it into a GAP object
    # the family of Q is the collection of its elements
    Q := Objectify( NewType( FamilyObj( elms ),
        IsQuasigroup and IsAttributeStoringRep ), rec() );
    # setting some attributes for the quasigroup
    SetSize( Q, n );
    SetAsSSortedList( Q, elms );
```

```
    SetCayleyTable( Q, ct );
    return Q;
end;
```

Operations in GAP are overloaded, i.e., the same operation can be applied to different types of objects. In order to deal with this situation, GAP uses a method selection: When an operation is called, GAP first checks the types of the arguments, and then selects the appropriate method.

Here is how the multiplication of two quasigroup elements is implemented:

```
InstallMethod( \*, "for two quasigroup elements",
    IsIdenticalObj,
    [ IsQuasigroupElement, IsQuasigroupElement ],
function( x, y )
    local F;
    F := FamilyObj( x );
    return F!.set[ F!.cayleyTable[ x![ 1 ] ][ y![ 1 ] ] ];
end );
```

Note that the underlying quasigroup is easily accessed since the element x *knows* into which quasigroup it belongs.

2. What is in the package

Here is a very brief overview of the methods implemented in LOOPS, version 1.4.0. See the manual for (much) more details. Argument Q stands for a quasigroup, and L for a loop. Thus the methods with argument Q apply to both quasigroups and loops, while those with argument L apply only to loops. Any additional restrictions on the arguments are listed in parentheses. The symbol $\triangleright$ is a shortcut for *returns*.

2.1. Basic methods and attributes

Cayley tables and elements:

`Elements(`Q`)` $\triangleright$ list of elements of Q,
`CayleyTable(`Q`)` $\triangleright$ Cayley table of Q,
`One(`L`)` $\triangleright$ the neutral element of L,
`MultiplicativeNeutralElement(`Q`)` $\triangleright$ the neutral element of Q, or fail
`Size(`Q`)` $\triangleright$ the size of Q,
`Exponent(`L`)` $\triangleright$ the exponent of L (L power-associative).

Arithmetic operations:
`LeftDivision`(x, y) ▷ $x\backslash y$,
`RightDivision`(x, y) ▷ x/y,
`LeftDivisionCayleyTable`(Q) ▷ Cayley table of left division in Q,
`RightDivisionCayleyTable`(Q) ▷ Cayley table of right division in Q.

Powers and inverses:
`LeftInverse`(x) ▷ x^λ, where $x^\lambda x = 1$,
`RightInverse`(x) ▷ x^ρ, where $xx^\rho = 1$,
`Inverse`(x) ▷ the two-sided inverse of x, if it exists.

Associators and commutators:
`Associator`(x, y, z) ▷ the unique element u with $(xy)z = (x(yz))u$,
`Commutator`(x, y) ▷ the unique element v with $xy = (yx)v$.

Generators:
`GeneratorsOfQuasigroup`(Q) ▷ a generating subset of Q,
`GeneratorsOfLoop`(L) ▷ a generating subset of L,
`GeneratorsSmallest`$(\mathtt{Q})$ ▷ a generating subset of Q of size $\leqslant \log_2 |Q|$.

Subquasigroups:
`IsSubquasigroup`(Q, S) ▷ true if S is a subquasigroup of Q,
`IsSubloop`(L, S) ▷ true if S is a subloop of L,
`AllSubloops`(L) ▷ list of all subloops of L,
`RightCosets`(L, S) ▷ right cosets modulo S ($S \leq L$),
`RightTransversal`(L, S) ▷ a right transversal modulo S ($S \leq L$).

Translations and sections:
`LeftTranslation`(Q, x) ▷ the left translation L_x by x in Q ($x \in Q$),
`RightTranslation`(Q, x) ▷ the right translation R_x by x in Q ($x \in Q$),
`LeftSection`(Q) ▷ the set of all left translations in Q,
`RightSection`(Q) ▷ the set of all right translations in Q.

Multiplication groups:
`LeftMultiplicationGroup`(Q) ▷ the left multiplication group of Q,
`RightMultiplicationGroup`(Q) ▷ the right multiplication group of Q,
`MultiplicationGroup`(Q) ▷ the multiplication group of Q,
`RelativeLeftMultiplicationGroup`(L, S) ▷ the group generated by all left translations of L restricted to S ($S \leq L$),
`RelativeRightMultiplicationGroup`(L, S) ▷ the group generated by all right translations of L restricted to S ($S \leq L$),
`RelativeMultiplicationGroup`(L, S) ▷ the group generated by all translations of L restricted to S ($S \leq L$).

Inner mapping groups:

`InnerMappingGroup(`L`)` ▷ the inner mapping group of L,
`LeftInnerMappingGroup(`L`)` ▷ the group generated by $L_{yx}^{-1}L_yL_x$,
`RightInnerMappingGroup(`L`)` ▷ the group generated by $R_{xy}^{-1}R_yR_x$.

Nuclei:

`LeftNucleus(`Q`)` ▷ the left nucleus of Q,
`RightNucleus(`Q`)` ▷ the right nucleus of Q,
`MiddleNucleus(`Q`)` ▷ the middle nucleus of Q,
`Nuc(`Q`)`, `NucleusOfQuasigroup(`Q`)` ▷ the nucleus of Q.

Commutant, center and associator subloop:

`Commutant(`Q`)` ▷ $\{x \in Q;\ xy = yx \text{ for every } y \in Q\}$,
`Center(`Q`)` ▷ the center of Q,
`AssociatorSubloop(`L`)` ▷ the smallest $S \trianglelefteq L$ such that L/S is a group.

Normal subloops:

`IsNormal(`L, S`)` ▷ true if S is a normal subloop of L,
`NormalClosure(`L, S`)` ▷ the smallest normal subloop of L containing S,
`IsSimple(`L`)` ▷ true if L is a simple loop.

Factor loops:

`FactorLoop(`L, N`)` ▷ L/N (N normal subloop of L),
`NaturalHomomorphismByNormalSubloop(`L, N`)` ▷ the projection $L \to L/N$ (N normal subloop of L).

Central nilpotency and central series:

`NilpotencyClassOfLoop(`L`)` ▷ the (central) nilpotency class of L,
`IsNilpotent(`L`)` ▷ true if L is nilpotent,
`IsStronglyNilpotent(`L`)` ▷ true if the mult. group of L is nilpotent,
`UpperCentralSeries(`L`)` ▷ the upper central series of L,
`LowerCentralSeries(`L`)` ▷ the lower central series of L,

Solvability:

`IsSolvable(`L`)` ▷ true if L is solvable,
`DerivedSubloop(`L`)` ▷ the derived subloop of L,
`DerivedLength(`L`)` ▷ the derived length of L,
`FrattiniSubloop(`L`)` ▷ the Frattini subloop of L (L strongly nilpotent).

Isomorphisms and automorphisms:

`IsomorphismLoops(`L, M`)` ▷ an isomorphism of loops $L \to M$, or fail,
`LoopsUpToIsomorphism(`ls`)` ▷ filtered list ls of loops up to isomorphism,
`AutomorphismGroup(`L`)` ▷ the automorphism group of L,
`IsomorphicCopyByPerm(`Q, p`)` ▷ an isomorphic copy of Q via the permutation p,
`IsomorphicCopyByNormalSubloop(`L, S`)` ▷ an isomorphic copy of L in

which $S \trianglelefteq L$ occupies the first $|S|$ elements of L and where the remaining elements correspond to the cosets of S in L.

Isotopisms:

`IsotopismLoops`(L, M) ▷ an isotopism $L \to M$, or fail,
`LoopsUpToIsotopism`(ls) ▷ filtered list ls of loops up to isotopism.

2.2. Testing properties of quasigroups and loops

Associativity, commutativity and generalizations:

`IsAssociative`(Q) ▷ true if Q is associative,
`IsCommutative`(Q) ▷ true if Q is commutative,
`IsPowerAssociative`(L) ▷ true if L is power associative,
`IsDiassociative`(L) ▷ true if L is diassociative.

Inverse properties:

`HasLeftInverseProperty`(L) ▷ true if $x^\lambda(xy) = y$,
`HasRightInverseProperty`(L) ▷ true of $(yx)x^\rho = y$,
`HasInverseProperty`(L) ▷ true if $x^\lambda(xy) = y = (yx)x^\rho$,
`HasTwosidedInverses`(L) ▷ true if $x^\lambda = x^\rho$,
`HasWeakInverseProperty`(L) ▷ true if $(xy)^\lambda x = y^\lambda$,
`HasAutomorphicInverseProperty`(L) ▷ true if $(xy)^\lambda = x^\lambda y^\lambda$,
`HasAntiautomorphicInverseProperty`(L) ▷ true if $(xy)^\lambda = y^\lambda x^\lambda$.

Some properties of quasigroups:

`IsSemisymmetric`(Q) ▷ true if $(xy)x = y$,
`IsTotallySymmetric`(Q) ▷ true if Q is semisymmetric and commutative,
`IsIdempotent`(Q) ▷ true it $x^2 = x$,
`IsSteinerQuasigroup`(Q) ▷ true if Q is totally symm. and commutative,
`IsUnipotent`(Q) ▷ true if $x^2 = y^2$,
`IsLeftDistributive`(Q) ▷ true if $x(yz) = (xy)(xz)$,
`IsRightDistributive`(Q) ▷ true if $(xy)z = (xz)(yz)$,
`IsDistributive`(Q) ▷ true if Q is left and right distributive,
`IsEntropic`(Q), `IsMedial`(Q) ▷ true if $(xy)(uv) = (xu)(yv)$.

Loops of Bol-Moufang type:

`IsExtraLoop`(L) ▷ true if $x(y(zx)) = ((xy)z)x$,
`IsCLoop`(L) ▷ true if $x(y(yz)) = ((xy)y)z$,
`IsMoufangLoop`(L) ▷ true if $(xy)(zx) = (x(yz))x$,
`IsRCLoop`(L) ▷ true if $x((yz)z) = (xy)(zz)$,
`IsLCLoop`(L) ▷ true if $(xx)(yz) = (x(xy))z$,
`IsRightBolLoop`(L) ▷ true if $x((yz)y) = ((xy)z)y$,
`IsLeftBolLoop`(L) ▷ true if $x(y(xz)) = (x(yx))z$,

`IsFlexible(`Q`)` ▷ true if $x(yx) = (xy)x$,
`IsRightNuclearSquareLoop(`L`)` ▷ true if $x(y(zz)) = (xy)(zz)$,
`IsMiddleNuclearSquareLoop(`L`)` ▷ true if $x((yy)z) = (x(yy))z$,
`IsLeftNuclearSquareLoop(`L`)` ▷ true if $(xx)(yz) = ((xx)y)z$,
`IsRightAlternative(`Q`)` ▷ true if $x(yy) = (xy)y$,
`IsLeftAlternative(`Q`)` ▷ true if $(xx)y = x(xy)$,
`IsAlternative(`Q`)` ▷ true if it is both left and right alternative.

Power alternative loops:

`IsLeftPowerAlternative(`L`)` ▷ true if $x^n(x^m y) = x^{n+m}y$,
`IsRightPowerAlternative(`L`)` ▷ true if $(xy^n)y^m = xy^{n+m}$,
`IsPowerAlternative(`L`)` ▷ true if L is left and right power alternative.

Conjugacy closed loops:

`IsLCCLoop(`L`)` ▷ true if left translations are closed under conjugation,
`IsRCCLoop(`L`)` ▷ true if right translations are closed under conjugations,
`IsCCLoop(`L`)` ▷ true if L is left and right conjugacy closed.

Additional varieties of loops:

`IsLeftBruckLoop(`L`)`, `IsLeftKLoop(`L`)` ▷ true if L is left Bol and has the automorphic inverse property,
`IsRightBruckLoop(`L`)`, `IsRightKLoop(`L`)` ▷ true if L is right Bol and has the automorphic inverse property.

Here is a nice, albeit trivial illustration of the filters built into the LOOPS package:

```
gap> L := LoopByCayleyTable([[1,2],[2,1]]);
<loop of order 2>
gap> IsLeftBolLoop(L); L;
true
<left Bol loop of order 2>
gap> IsRightBolLoop(L); L;
true
<Moufang loop of order 2>
gap> IsAssociative(L); L;
true
<associative loop of order 2>
```

2.3. Libraries

Several libraries of small loops up to isomorphism are included in LOOPS. As of version 1.4.0, the libraries contain:

- all nonassociative left Bol loops of order $\leqslant 16$,
- all nonassociative Moufang loops of order $\leqslant 64$ and $= 81$,

- all nonassociative Steiner loops of order $\leqslant 16$,
- all (three) nonassociative conjugacy closed loops of order p^2, for every odd prime p,
- all (one) nonassociative conjugacy closed loops of order $2p$, for every odd prime p,
- the smallest nonassociative simple Moufang loop (of order 120),
- all nonassociative loops of order $\leqslant 6$.

There is also a library of all nonassociative loops of order $\leqslant 6$ up to isotopism.

The mth loop of order n in a given library can be retrieved via

$$\texttt{LeftBolLoop}(n,m), \quad \texttt{MoufangLoop}(n,m),$$

and so on.

We took great care to store the information in the libraries efficiently. For instance, the library of Moufang loops can be packed into less than 18 kilobytes, hence averaging about 4 bytes per loop.

Remark 2.1. All nonassociative Moufang loops of orderless than 64 can be found in [7]. Our numbering for these loops agrees with [7].

The 4262 nonassociative Moufang loops of order 64 were first constructed in [18], but it was proved (computationally) only in [16] that the list is complete.

The 2038 nonassociative left Bol loops of order 16 were enumerated for the first time by Moorhouse [12]. The first author obtained the same result by a different method, on which he will report in a separate paper [14].

The fact that for every odd prime p there are precisely three nonassociative conjugacy closed loops of order p^2 was established by Kunen [10]. Drápal and Csörgő derived simple formulas for multiplication in these three loops [4]. When p is an odd prime, Wilson [19] constructed a nonassociative conjugacy closed loop of order $2p$, and Kunen [10] showed there are no other such loops.

Our counts of small loops agree with the known results, e.g. [11].

The library of small Steiner loops is based on [2].

3. Constructing isomorphisms

There does not appear to be much research on the problem of finding an isomorphism between loops. In this section we explain the approach used in LOOPS. It works surprisingly well for many varieties of loops, including Moufang loops.

Let Q be a loop, and let $\mathcal{P}$ be a set of properties (of elements) invariant under isomorphisms. The nature of $\mathcal{P}$ depends on Q. For instance, when Q is power-associative, one of the invariant properties for an element x might be the order $|x|$.

Given $\mathcal{P}$ and a collection $\mathcal{C}$ of loops, define an equivalence on the (disjoint) union of $\mathcal{C}$ by $x \sim y$ if and only if $\varphi(x) = \varphi(y)$ for every $\varphi \in \mathcal{P}$. Then, if $f : Q \to L$ is an isomorphism and $\mathcal{C} = \{Q, L\}$, we must have $x \sim f(x)$ for every $x \in Q$. In other words, $\mathcal{P}$ partitions the elements into blocks invariant under isomorphism.

In order to find an isomorphism, we need a set of invariants $\mathcal{P}$ that is easy to calculate but results in a fine partition.

We have used the following invariants $\mathcal{P}$ for power-associative loops:

$$\begin{aligned}
\varphi_1(x) &= |x|,\\
\varphi_2(x) &= |\{y;\ y^2 = x\}|,\\
\varphi_3(x) &= |\{y;\ y^4 = x\}|,\\
\varphi_{4,k}(x) &= |\{y;\ xy = yx,\ |y| = k\}|,\ \text{for } k \geq 1.
\end{aligned}$$

The algorithm searching for an isomorphism $f : Q \to L$ first orders the equivalence classes of $\sim$ by increasing size on both Q and L. If the equivalence class sizes of Q and L do not match, it is clear that no isomorphism $f : Q \to L$ exists, and `fail` is returned. Otherwise, a backtrack search attempts to find an isomorphism respecting the partitions of $\sim$.

It would be an interesting project to analyze the speed of the algorithm depending on the choice of $\mathcal{P}$. We do not claim that the above $\mathcal{P}$ is optimized in any sense. Note, for instance, that the invariants φ_2, φ_3 are useless for many power associative loops of odd order, and $\varphi_{4,k}$ are useless for all commutative loops.

4. Classification of small Frattini Moufang loops of order 64

Let L be a loop and let the *Frattini subloop* $\Phi(L)$ be the normal subloop generated by all squares, commutators and associators of L. In other words, $\Phi(L)$ is the smallest normal subloop such that $L/\Phi(L)$ is an elementary abelian p-group. Following Hsu [9], we say that L is a *small Frattini p-loop* if $|\Phi(L)| \leqslant p$.

In this section, L will denote a small Frattini Moufang 2-loop of order 2^{n+1}. Moreover, in order to avoid trivialities, we assume that $|\Phi(L)| = 2$. Clearly, $\Phi(L) \leq Z(L)$, L is nilpotent of class 2, and it has a unique nontrivial square, commutator and associator element.

Remark 4.1. Small Frattini Moufang 2-loops are also called *code loops* due to their connection to doubly even linear binary codes. Some of these loops play an important role in the description of large sporadic simple groups.

We consider $V = L/\Phi(L)$ as a vector space over $\mathbb{F}_2$, and we identify $\Phi(L)$ and $\mathbb{F}_2$. In particular, we sometimes write the group operations additively.

Let us take arbitrary elements $u = x \mod \Phi(L)$, $v = y \mod \Phi(L)$, $w = z \mod \Phi(L)$ of V. Then, the following maps are well defined:

$$\begin{array}{ll} \sigma : V \to \mathbb{F}_2, & \sigma(u) = x^2, \\ \kappa : V \times V \to \mathbb{F}_2, & \kappa(u,v) = [x,y], \\ \alpha : V \times V \times V \to \mathbb{F}_2, & \alpha(u,v,w) = [x,y,z]. \end{array}$$

Moreover, α is an alternating trilinear form, κ is alternating, and we have

$$\begin{aligned} \sigma(u+v) &= \sigma(u) + \sigma(v) + \kappa(u,v), \\ \kappa(u+v,w) &= \kappa(u,w) + \kappa(v,w) + \alpha(u,v,w). \end{aligned}$$

Hence, by definition, V is a *symplectic cubic space*.

There are different ways in which a small Frattini Moufang 2-loop is obtained from a symplectic cubic space (cf. Griess [8], Chein and Goodaire [1], Hsu [9]). All of the above constructions induct on the dimension of V. In contrast, a new approach, [13], takes advantage of *groups with triality* and constructs the loop globally.

For this, let σ_i, κ_{ij} and α_{ijk} be the structure constants of σ, κ, α with respect to a fixed basis ov V. We define the group G with gerenators

g_i, f_i, h_i, $i \in \{1, \dots, n\}$, u and v by the following relations:

$$\begin{aligned}
&g_i^2 = u^{\sigma_i},\ f_i^2 = v^{\sigma_i},\ h_i^2 = u^2 = v^2 = 1,\\
&[g_i, g_j] = u^{\kappa_{ij}},\ [f_i, f_j] = v^{\kappa_{ij}},\\
&[g_i, f_j] = (uv)^{\kappa_{ij}} \prod_{k=1}^{n} h_k^{\alpha_{ijk}},\\
&[g_i, h_j] = u^{\delta_{ij}},\ [f_i, h_j] = v^{\delta_{ij}},\\
&[h_i, h_j] = [g_i, u] = [f_i, u] = [h_i, u] = [g_i, v] = [f_i, v] = [h_i, v] = 1.
\end{aligned}$$

Then, G is a group and the maps

$$\begin{aligned}
\tau &: g_i \leftrightarrow f_i,\ h_i \mapsto h_i,\ u \leftrightarrow v\\
\rho &: g_i \mapsto f_i,\ f_i \mapsto (g_i f_i)^{-1},\ h_i \mapsto h_i,\ u \mapsto v,\ v \mapsto uv
\end{aligned}$$

extend to *triality automorphisms* of G. The following function returns the Moufang loop associated to the group G with triality automorphisms τ, ρ:

```
TrialityGroupToLoop := function( G, tau, rho )
   local ccl, ct;
   ccl := Elements( ConjugacyClass( G, tau ) );
   ct := List( ccl, s1 ->
            List( ccl, s2 ->
               Position( ccl, s1^rho * s2^(rho^2) * s1^rho )
            )
         );
   return LoopByCayleyTable( NormalizedQuasigroupTable( ct ) );
end;
```

To complete the classification of small Frattini Moufang 2-loops of order 64, it now suffices to classify the symplectic cubic spaces of order 32. For a fixed basis, such a space is given by

$$\binom{5}{3} + \binom{5}{2} + 5 = 25$$

structure constants, which give rise to a 25-dimensional vector space W over $\mathbb{F}_2$.

Any linear map A of V defines a new symplectic cubic space with maps

$$\sigma^A(u) = \sigma(Au), \quad \kappa^A(u, v) = \kappa(Au, Av), \quad \alpha^A(u) = \alpha(Au, Av, Aw),$$

and hence A induces a linear map on W. This defines an action of $GL(5, 2)$ on W.

It is easy to show the 1-1 correspondence of loop isomorphisms and linear isomorphisms of symplectic cubic spaces. This implies that the orbits of $GL(5,2)$ on W will correspond precisely to the isomorphism classes of small Frattini Moufang 2-loops of order 64.

Since $|GL(5,2)|$ and 2^{25} are still too large for GAP to compute the needed orbits, one has to have a closer look at invariant subspaces of W. Once this is done, the classification is complete, with the result that there are precisely 80 nonisomorphic small Frattini Moufang loops of order 64.

5. An interesting Csörgő loop

One of the longer-standing problems in loop theory was the question if there is a loop with nilpotency class higher than two whose inner mapping group is abelian. In [3], Csörgő constructed such a loop (of order 128 and nilpotency class 3). The following GAP code returns this loop L. The code follows [3], where some insight is given.

```
# constructing a group of order 8192 by presenting relations
f := FreeGroup(13);
G := f/[ f.1^2, f.2^2, f.3^2, f.4^2, f.5^2, f.6^2, f.7^2, f.8^2, f.9^2, f.10^2,
f.11^2, f.12^2, f.13^2, (f.1*f.2)^2, (f.1*f.3)^2, (f.1*f.4)^2, (f.1*f.5)^2,
(f.1*f.6)^2, (f.1*f.7)^2, (f.1*f.8)^2, (f.1*f.9)^2, (f.1*f.10)^2, (f.1*f.11)^2,
(f.1*f.12)^2, (f.1*f.13)^2, (f.2*f.3)^2, (f.2*f.4)^2, (f.3*f.4)^2, (f.2*f.5)^2,
(f.2*f.6)^2, (f.2*f.7)^2, (f.3*f.5)^2, (f.3*f.6)^2, (f.3*f.7)^2, (f.4*f.5)^2,
(f.4*f.6)^2, (f.4*f.7)^2, (f.2*f.9)^2, (f.2*f.10)^2, (f.3*f.8)^2, (f.3*f.10)^2,
(f.4*f.8)^2, (f.4*f.9)^2, f.1*f.2*f.8*f.2*f.8, f.1*f.3*f.9*f.3*f.9,
f.1*f.4*f.10*f.4*f.10, (f.2*f.11)^2, (f.2*f.12)^2, (f.2*f.13)^2, (f.3*f.11)^2,
(f.3*f.12)^2, (f.3*f.13)^2, (f.4*f.11)^2, (f.4*f.12)^2, (f.4*f.13)^2, (f.5*f.6)^2,
(f.5*f.7)^2, (f.6*f.7)^2, (f.5*f.9)^2, (f.5*f.10)^2, (f.6*f.8)^2, (f.6*f.10)^2,
(f.7*f.8)^2, (f.7*f.9)^2, f.1*f.5*f.8*f.5*f.8, f.1*f.6*f.9*f.6*f.9,
f.1*f.7*f.10*f.7*f.10, (f.5*f.12)^2, (f.5*f.13)^2, (f.6*f.11)^2, (f.6*f.13)^2,
(f.7*f.11)^2, (f.7*f.12)^2, f.1*f.11*f.5*f.11*f.5, f.1*f.12*f.6*f.12*f.6,
f.1*f.13*f.7*f.13*f.7, f.2*f.5*f.9*f.10*f.9*f.10, f.3*f.6*f.8*f.10*f.8*f.10,
f.4*f.7*f.8*f.9*f.8*f.9, (f.8*f.11)^2, (f.9*f.12)^2, (f.10*f.13)^2,
f.8*f.12*f.8*f.4*f.12*f.7, f.8*f.13*f.8*f.3*f.13*f.6, f.10*f.11*f.10*f.3*f.11*f.6,
f.9*f.11*f.9*f.11*f.7, f.9*f.13*f.9*f.13*f.5, f.10*f.12*f.10*f.12*f.5,
(f.11*f.12)^2, (f.11*f.13)^2, (f.12*f.13)^2 ];
# auxiliary data
g := GeneratorsOfGroup(G);
N := Subgroup( G, [ g[5], g[6], g[7], g[1] ] );
W := Subgroup( G, [ g[5]*g[2], g[6]*g[3], g[7]*g[4], g[1] ] );
A_0 := [ One(G), g[8], g[9], g[10], g[8]*g[9], g[8]*g[10], g[9]*g[10]*g[2],
    g[8]*g[9]*g[10]*g[2] ];
B_0 := [ One(G), g[8]*g[11], g[9]*g[12], g[10]*g[13], g[8]*g[11]*g[9]*g[12],
    g[8]*g[11]*g[10]*g[13]*g[3], g[9]*g[12]*g[10]*g[13],
    g[8]*g[11]*g[9]*g[12]*g[10]*g[13]*g[3] ];
A := Union( List( Elements( N ), x -> A_0*x ) );
B := Union( List( Elements( W ), x -> B_0*x ) );
```

```
H := Subgroup( G, [ g[2], g[3], g[4], g[11], g[12], g[13] ] );
# constructing the loop
ListPosition := function( S, x )
    local i; i := 1; while not x in S[i] do i := i + 1; od; return i;
end;
m := MappingByFunction( Domain(Elements( G)), Domain([1..8192]),
    x -> Position( Elements(G), x ) );
CA := List( A, x -> x*Elements( H ) );
mCA := List( CA, c -> Set( c, x -> x^m ) );
T := List([1..128],i->[1..128]);
for ii in [1..128] do for jj in [1..128] do
    T[ii][jj] := ListPosition( mCA, (A[ii]*B[jj])^m );
od; od;
p := SortingPerm( T[1] );
T := List( T, r -> Permuted( r, p ) );
L := LoopByCayleyTable( T );
```

In addition, the following properties hold for L: (a) the nucleus of L is elementary abelian of order 16, (b) the left and middle nuclei have order 32, (c) the right nucleus has order 16, (d) the two-element center coincides with the associator subloop.

An interesting, more symmetric loop K is obtained from L by this greedy algorithm:

Given a groupoid Q, let $\mu(Q) = |\{(a,b,c) \in Q \times Q \times Q;\ a(bc) \neq (ab)c\}|$. Hence $\mu(Q)$ is a crude measure of (non)associativity of Q.

Let T be a multiplication table of L split into blocks of size 16×16 according to the cosets of the nucleus of L. Let h be the nontrivial central element of L.

(*) For $1 \leqslant i \neq j \leqslant 16$, let T_{ij} be obtained from T by multiplying the (i,j)th block and the (j,i)th block of T by h. Let (s,t) be such that $\mu(T_{st})$ is minimal among all $\mu(T_{ij})$. If $\mu(T_{st}) \geq \mu(T)$, stop, and return T. Else replace T by T_{st}, and repeat (*).

It turns out that the multiplication table T found by the above greedy algorithm yields another loop K of nilpotency class 3 whose inner mapping group is abelian. In addition, the following properties hold for K: (a) the nucleus is elementary abelian of order 16, (b) the left, middle, and right nuclei have order 64, (c) the two-element center coincides with the associator subloop. In particular, K is not isomorphic to L. Among other peculiar features, it contains a nonassociative power associative loop of order 64 that is the union of its nuclei.

The construction of L takes a minute or so in GAP, since calculations in free groups are slow. A more direct, systematic, and much faster construction of L and K will be presented elsewhere [5].

References

[1] **O. Chein and E. G. Goodaire**: *Moufang loops with a unique nonidentity commutator (associator, square)*, J. Algebra **130** (1990), 369 – 384.

[2] **C. J. Colbourn and A. Rosa**: Triple systems, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1999.

[3] **P. Csörgő**: *Abelian inner mappings and nilpotency class greater than two*, European J. Combin., to appear.

[4] **P. Csörgő and A. Drápal**: *Left conjugacy closed loops of nilpotency class two*, Results Math. **47** (2005), 242 – 265.

[5] **A. Drápal and P. Vojtěchovský**: *Explicit constructions of loops with commuting inner mappings*, submitted.

[6] **The GAP Group**: *GAP – Groups, Algorithms, and Programming, Version* 4.4.9; 2006. `http://www.gap-system.org`

[7] **E. G. Goodaire, S. May and M. Raman**: *The Moufang loops of order less than* 64, Commack, NY: Nova Science Publishers, 1999.

[8] **R. L. Griess, Jr.**: *Code loops*, J. Algebra **100** (1986), 224 – 234.

[9] **T. Hsu**:*Explicit constructions of code loops as centrally twisted products*, Math. Proc. Cambridge Philos. Soc. **128** (2000), 223 – 232.

[10] **K. Kunen**: *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352** (2000), 2889 – 2911.

[11] **B. D. McKay, A. Meynert and W. Myrvold**: *Small Latin squares, quasigroups and loops*, J. Combinatorial Designs, to appear.

[12] **G. E. Moorhouse**: *Bol loops of small order*, available at
http://www.uwyo.edu/moorhouse/pub/bol/

[13] **G. P. Nagy**: *Direct construction of code loops*, Discr. Math., to appear.

[14] **G. P. Nagy**: *Doubling of finite Bol loops*, in preparation, 2007.

[15] **G. P. Nagy and P. Vojtěchovský**: LOOPS – a GAP package, version 1.4.0, Feb. 2007, `http://www.math.du.edu/loops`

[16] **G. P. Nagy and P. Vojtěchovský**: *The Moufang loops of order* 64 *and* 81, submitted.

[17] **H. O. Pflugfelder**: *Quasigroups and Loops: Introduction*, Sigma Series in Pure Math. **8**, Heldermann Verlag, Berlin, 1990.

[18] **P. Vojtěchovský**: *Toward the classification of Moufang loops of order* 64, European J. Combin. **27**, issue **3** (April 2006), 444 – 460.

[19] **R. L. Wilson, Jr.**: *Quasidirect products of quasigroups*, Comm. Algebra **3** (1975), 835 – 850.

Received February 25, 2007

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

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

Quasigroups and Related Systems **15** (2007), 95 – 107

Connected transversals and multiplication groups of loops

Markku Niemenmaa and Miikka Rytty

Abstract

Several properties of loops and their multiplication groups can be reduced to the properties of connected transversals in groups. We discuss these transversals and prove group theoretical results which have direct loop theoretical consequences. We are particularly interested in the case where the inner mapping group is abelian and we show that it can never be a finite nontrivial cyclic group.

1. Introduction

The purpose of this paper is to explore the connection between loops and groups. The left and right translations of a loop Q generate a group $M(Q)$ called the multiplication group of the loop. The multiplication group can be characterized in purely group theoretical terms (Theorem 5.1 of this paper) and the notion of connected transversals to a subgroup H in a group G is central to this characterization. Here G corresponds to $M(Q)$ and H is the inner mapping group $I(Q)$ of Q.

The first three sections are devoted to H-connected transversals in a group G. We consider their basic properties and after that we are particularly interested in the case where H is abelian (the subcase where H is cyclic gets a very thorough treatment in section four). One of our goals is to show how loop theory is a source of interesting group theoretical problems – some of which are not easy at all to solve. Our results are not necessarily new but some of the proofs are and, in some cases, we have added some new spice to the old proofs. The reader should not be worried about the

2000 Mathematics Subject Classification: 20D10, 20N05
Keywords: loop, group, connected transversals

amount of group theory in this paper. After all, groups are nothing but associative loops.

In sections five and six we go to the other direction: we introduce the loop theoretic interpretations of the results that we have proved in the group theory sections. We see that the inner mapping group $I(Q)$ can never be a finite nontrivial cyclic group and we also see that finite loops with abelian inner mapping groups are centrally nilpotent. We also discuss the recent interesting results and constructions where the inner mapping group $I(Q)$ is an abelian p-group and the nilpotency class of Q equals either two or three.

As pointed out earlier, our approach is based on abstract group theory and the efficient use of connected transversals. Naturally, it is possible to deal with these problems by using permutation group theory combined with elementary (or advanced) loop theory (see Drápal [7]). We shall not go into the details of this approach in this paper and we also omit some other important questions like the relation between solvable loops and solvable multiplication groups or the structure of multiplication groups in the case of Moufang loops. The reader interested in these topics should consult Vesanen [16] and the excellent survey by Nagy and Vojtěchovský [13].

Some words about our notation. We bring with us some bad habits from abstract group theory: we write maps to the left of their arguments. If G is a group and x, y are two elements from G, the *commutator* $x^{-1}y^{-1}xy$ is denoted by $[x, y]$. If X, Y are nonempty subsets of G, then $[X, Y] = \langle [x, y] \mid x \in X, y \in Y \rangle$, the subgroup generated by all commutators $[x, y]$. The subgroup $G' = [G, G]$ is the *derived group* (or *commutator subgroup*) of G.

If H is a subgroup of G, then the largest normal subgroup of G contained in H is said to be the *core of H in G* and we denote it by H_G (thus $H_G = \bigcap_{x \in G} H^x$). The *conjugate of H* is the subgroup $x^{-1}Hx$ which we denote by H^x. The subgroup $N_G(H) = \{x \in G \mid H^x = H\}$ is the *normalizer of H in G*. A subgroup H is *subnormal in G*, if there are subgroups $H_0, H_1, \ldots, H_n$ of G such that $H_0 = H$, $H_n = G$ and H_{i-1} is normal in H_i for every $i = 1, 2, \ldots, n$. We say that H is a *characteristic subgroup of G*, if H is invariant under every automorphism of G. Naturally, if N is a normal subgroup of G and M is a characteristic subgroup of N, then M is normal in G. Finally, we assume that the reader is familiar with the Sylow theorems.

2. Connected transversals in groups

Let G be a group and $H \leq G$. A subset A of G is said to be *a left transversal to H in G* if it contains exactly one element from each left coset of H. A *right transversal* is defined similarly. If A and B are two left transversals to H in G and $[A, B] \leq H$, then we say that these two transversals are *H-connected*. In the case that $[A, A] \leq H$, we say that A is *H-selfconnected*. If A and B are H-connected transversals, then A and B are both left and right transversals to H in G (see [14], Lemma 2.1).

We shall now prove some elementary results about connected transversals. These results turn out to be very useful when we prove more substantial results which have interesting interpretations in loop theory. In the following lemmas A and B are H-connected transversals to H in G. Thus $a^{-1}b^{-1}ab \in H$ for every $a \in A$ and $b \in B$.

Lemma 2.1. *If $H_G = 1$, then $Z(G) \subseteq A \cap B$.*

Proof. Let $z \in Z(G)$ and assume that $z = ah$, where $a \in A$ and $h \in H$. Then $b^{-1}hb = b^{-1}a^{-1}zb = b^{-1}a^{-1}bz = b^{-1}a^{-1}bah \in H$ for every $b \in B$. Thus $h \in \bigcap_{b \in B} H^{b^{-1}} = 1$, hence $z = a \in A$. In similar way, we can show that $z \in B$. □

Remark 2.2. If $H_G = 1$, then by Lemma 2.1, $1 \in A \cap B$.

Lemma 2.3. *Let $C \subseteq A \cup B$ and $K = \langle H, C \rangle$. Then $C \subseteq K_G$.*

Proof. Let $c \in C$ and assume that $c \in A$ and $x = bh$, where $b \in B$ and $h \in H$. Now $x^{-1}c^{-1}x = h^{-1}b^{-1}c^{-1}bh = h^{-1}b^{-1}c^{-1}bcc^{-1}h$. As $b^{-1}c^{-1}bc \in H$, we may conclude that $x^{-1}c^{-1}x \in K$, hence $x^{-1}cx \in K$ and $c \in K_G$. If $c \in B$, then the same conclusion holds. □

In the proof of our following lemma, we need two results on commutators:

1. $[xy, z] = [x, z]^y [y, z]$ and
2. if $H \leq G$, then $[H, G]$ is a normal subgroup of G.

For the proofs, see [10], p. $253 - 255$.

Lemma 2.4. *If $H_G = 1$, then $N_G(H) = H \times Z(G)$.*

Proof. Let $K = N_G(H) = A_1H = B_1H$, where $A_1 \subseteq A$ and $B_1 \subseteq B$. As H is normal in K and K/H is abelian, we may conclude that $K' \leq H$. By Lemma 2.3, $\langle A_1, B_1\rangle \leq K_G$. Thus $[A_1, B_1] \leq K'_G \leq K' \leq H$. Now K'_G is normal in G and since $H_G = 1$, it follows that $K'_G = [A_1, B_1] = 1$.

If $g = ah \in G$ (here $a \in A$ and $b \in H$) and $b \in B_1$, then $[b, g] = b^{-1}h^{-1}a^{-1}bah = kb^{-1}a^{-1}bah$, where $k \in H$. Thus $[b, g] \in H$. As K_G is abelian and $a^{-1}b^{-1}a \in K_G$, we have $\left[b^{-1}, g\right] = bh^{-1}a^{-1}b^{-1}ah = dba^{-1}b^{-1}ah = da^{-1}b^{-1}abh \in H$ (here $d \in H$). Further, if $b, c \in B_1$, then $[bc, g] = [b, g]^c\,[c, g] \in H$. Thus $D = [\langle B_1\rangle, G] \leq H$ and since D is normal in G and $H_G = 1$, it follows that $[\langle B_1\rangle, G] = 1$ and $\langle B_1\rangle \leq Z(G)$. Now it is clear that $N_G(H) = H \times Z(G)$. □

Lemma 2.5. *If $H_G = 1$ and $[A, B] = 1$, then A and B are isomorphic subgroups of G.*

Proof. If we write $C = \langle A\rangle \cap H$, then $bc = cb$ for every $c \in C$ and $b \in B$. If $x \in G$, then $x = bh$, where $b \in B$ and $h \in H$. Thus $x^{-1}cx = (bh)^{-1}cbh = h^{-1}b^{-1}cbh = h^{-1}ch \in H$ whenever $c \in C$. This means that $c \in H^x$ for every $x \in G$ and, in fact, $c \in H_G = 1$. We have shown that $\langle A\rangle \cap H = 1$ and therefore $\langle A\rangle = A$. It is also clear that $\langle B\rangle = B$. For every $a \in A$ there exists a unique $f(a) \in B$ such that $a^{-1}H = f(a)H$. If $a, d \in A$, then $f(ad)H = (ad)^{-1}H = d^{-1}f(a)H = f(a)d^{-1}H = f(a)f(d)H$ and we see that $A \cong B$. □

We conclude this section by proving a result which deals with simple groups.

Lemma 2.6. *If G is a simple group and H is a proper subgroup of G, then H is maximal in G.*

Proof. Let $a \in (G \setminus H) \cap A$ and write $K = \langle a, H\rangle$. By Lemma 2.3, $a \in K_G$. As $K_G > 1$ and G is simple, it follows that $K_G = G$. But then $K = G$, and thus H is a maximal subgroup of G. □

3. Connected transversals to abelian subgroups

In this section we assume that $H \leq G$ is an abelian p-group (for a prime number p) and there exist H-connected transversals A and B in G. For the proof of our next theorem we need the following well-known result by Burnside (see [10], p. 419 – 420).

Lemma 3.1. *Let G be a finite group and P a Sylow p-subgroup of G such that $P \leq Z(N_G(P))$ (or $N_G(P) = C_G(P)$). Then there exists a normal subgroup K of G such that $G = KH$ and $K \cap H = 1$.* □

Now we are ready to prove

Theorem 3.2. *Let G be a finite group and $H \leq G$ an abelian p-group. Assume further that $H_G = 1$ and $G = \langle A, B \rangle$. Then $Z(G) > 1$.*

Proof. Assume that the claim is not true and $Z(G) = 1$. As $H_G = 1$, we can apply Lemma 2.4 and thus $N_G(H) = H \times Z(G) = H$. If $H < P \leq G$, where P is a p-group, then $H < N_P(H)$, a contradiction. We conclude that H is a Sylow p-subgroup of G. Now $N_G(H) = C_G(H)$ and by Lemma 3.1 there exists a normal subgroup K of G such that $G = KH$ and $K \cap H = 1$. As $G/K \cong H$ is abelian, it follows that $G' \leq K$. Thus $a^{-1}b^{-1}ab \in G' \cap H \leq K \cap H = 1$ and we get $ab = ba$ for every $a \in A$ and $b \in B$.

The subgroup $L = H \cap \langle A \rangle$ is normal in H and as $N_G(L) \supseteq B$, it follows that $N_G(L) \geq \langle H, B \rangle = G$. Since $H_G = 1$, we conclude that $L = 1$. This means that $\langle A \rangle = A$ is a normal subgroup of G. Similarly, B is a normal subgroup of G. Thus $K = A = B$ and as $G = \langle A, B \rangle$, we have a contradiction. We conclude that $Z(G) > 1$. □

Corollary 3.3. *Assume that the conditions of Theorem 3.2 hold for G and H. Then H is subnormal in G.* □

Remark 3.4. By using a similar but somewhat more complicated argumentation we could prove that the result of Theorem 3.2 also holds in the case that H is an abelian subgroup. Naturally, in this case H would be subnormal in G, too.

4. Connected transversals to cyclic subgroups

We first consider the situation that H is cyclic of order p (here p is a prime number) and then we proceed to more general cases. Naturally A and B are connected transversals to H in G.

Lemma 4.1. *Let H be a cyclic subgroup of order p. If $G = \langle A, B \rangle$, then $G' \leq H$.*

Proof. If $H_G > 1$, then $H = H_G$ is normal in G and $G' \leq H$. Thus we assume that $H_G = 1$. By Lemma 2.4 we know that $N_G(H) = H \times Z(G)$.

Let $a \in A$ and $b \in B$ such that $aH = bH$ and $a^{-1}b \neq 1$. Then $H = \langle a^{-1}b \rangle$ and $(a^{-1}b)^a = a^{-1}b^a = a^{-1}bb^{-1}a^{-1}ba \in H$. This means that $a \in N_G(H) = H \times Z(G)$, hence $a \in Z(G)$. By Lemma 2.1, it follows that $A = B$.

Let a and d be two elements from A. If $a, d \in Z(G)$, then $ad \in Z(G) \subseteq A$. Now assume that $a \notin Z(G)$ and write $ad = ch$, where $c \in A$ and $h \in H$. It follows that $d^{-1}a^{-1}da = d^{-1}a^{-1}a^{-1}ada = h^{-1}c^{-1}a^{-1}cha = h^{-1}c^{-1}a^{-1}caa^{-1}ha \in H$ and thus $h^a \in H$. If $h \neq 1$, then $a \in N_G(H)$, hence $a \in Z(G)$, a contradicting the choise of a. Thus $h = 1$ and $ad = c \in A$. Furthermore, let $a^{-1} = bh$ where $b \in A$ and $h \in H$. Then $h = b^{-1}a^{-1}$ and $h^{-1} = ab \in A \cap H = 1$. Thus $a^{-1} \in A$ and $A = B$ is a subgroup of G and this contradicts the condition $G = \langle A, B \rangle$. □

Now we proceed to the situation where H is a cyclic group of prime power order. In the following lemma we can very efficiently use the result of Theorem 3.2.

Lemma 4.2. *Let G be a finite group and $H \leq G$ a cyclic p-group. If $G = \langle A, B \rangle$, then $G' \leq H$.*

Proof. Let G be a minimal counterexample. If $H_G > 1$, then we consider the group G/H_G and the subgroup H/H_G. Then $(G/H_G)' \leq H/H_G$, hence $G' \leq H$.

Thus we may assume that $H_G = 1$. By Theorem 3.2, $Z(G) > 1$. Let $z \in Z(G)$ such that $|z| = q$, where q is a prime number. We now consider the groups $G/\langle z \rangle$ and $H\langle z \rangle/\langle z \rangle$ and conclude that $G' \leq H\langle z \rangle$. This means that $H\langle z \rangle$ is normal in G. If $p \neq q$, then H is a Sylow p-subgroup of $H\langle z \rangle$. As H is characteristic in $H\langle z \rangle$, it follows that H is normal in G and $G' \leq H$. Thus we may assume that $q = p$. We write $E = \langle x^p \mid x \in H\langle z \rangle \rangle$. Clearly, $E \leq H$ and as E is characteristic in $H\langle z \rangle$, it follows that E is normal in G. Since $H_G = 1$, we conclude that $E = 1$ and thus $|H| = p$. Now the claim follows from Lemma 4.1. □

We are now ready to prove our main result on connected transversals to cyclic subgroups.

Theorem 4.3. *Let G be a finite group and H a cyclic subgroup. If $G = \langle A, B \rangle$, then $G' \leq H$.*

Proof. Let G be a minimal counterexample. Clearly, we can assume that $H_G = 1$ and H is not of prime power order. If $N_G(H) > H$, then $Z(G) > 1$

by Lemma 2.1. Let $z \in Z(G)$ and $|z| = q$, where q is a prime number. Then $G' \leq H\langle z\rangle$ and H contains a Sylow p-subgroup P (with $p \neq q$) such that P is normal in G, a contradiction.

Thus we may assume that $N_G(H) = H$. Let P be a Sylow p-subgroup of H such that $N_G(P) > H$. Now $C_G(P)$ is normal in $N_G(P)$ and therefore $C_G(P) > H$. If $C_G(P) = G$, then P is normal in G, which is not possible. Thus G has a subgroup T such that $H < T \leq C_G(P) < G$. By Lemma 2.3, $T_G > 1$. We consider the groups G/T_G and $HT_G/T_G = T/T_G$ and get $G' \leq T$. It follows that T is normal in G. Now $P \leq Z(T)$ and $Z(T) \leq H$. Since $Z(T)$ is characteristic in T, we conclude that $Z(T)$ is normal in G. As $H_G = 1$, this is not possible.

Thus we may assume that $N_G(P) = C_G(P) = H$ for every Sylow subgroup P of H. All Sylow subgroups of H are also Sylow subgroups of G and by applying Lemma 3.1, we conclude that there exist a normal subgroup K of G such that $G = KH$ and $K \cap H = 1$. By standard arguments (as in the proof of Theorem 3.2), it follows that $K = A = B$ is a normal subgroup of G. But this contradicts $G = \langle A, B\rangle$ and our proof is ready. □

We shall next prove that the result of Theorem 4.3 also holds in the case that G is infinite. We first introduce a useful lemma (which was introduced to the first author by Tomáš Kepka some thirteen years ago).

Lemma 4.4. *Let H be a finite subgroup of G, $H_G = 1$ and $G = \langle A, B\rangle$. Then $G/Z(G)$ is finite.*

Proof. Let a be a fixed element of A, h fixed element of H and write $F(a,h) = \{b \in B \mid a^{-1}b^{-1}ab = h\}$. If $b, c \in F(a,h)$, then $bc^{-1} \in C_G(a)$ and $b \in C_G(a)c$. Thus $F(a,h) \subseteq C_G(a)b(h)$, where $b(h)$ is a fixed element from $F(a,h)$. Further, $B = \bigcup F(a,h)$, where h goes through all the elements of H. Now $G = BH \subseteq C_G(a)\{b(h) \mid h \in H\}H$, hence $[G : C_G(a)] \leq |H|^2$. As H is a finite subgroup of $\langle A, B\rangle$, we may conclude that $[G : C_G(H)]$ is finite. Then $[G : N_G(H)]$ is finite and since $N_G(H) = H \times Z(G)$, we have $G/Z(G)$ finite. □

Theorem 4.5. *Let H be a finite cyclic subgroup of G and let $G = \langle A, B\rangle$. Then $G' \leq H$.*

Proof. We proceed by induction on $|H|$. It is obvious that we may assume that $H_G = 1$. By using Lemma 4.4, we consider the finite group $G/Z(G)$ and its cyclic subgroup $HZ(G)/Z(G)$. By Theorem 4.3, $G' \leq HZ(G)$.

Let $p \mid |H|$ be a prime number and $E = \langle x \in HZ(G) \mid x^p = 1 \rangle$. Now E is characteristic in $HZ(G)$, hence E is normal in G. As $|HE/E| < |H|$, we apply induction and get $G' \leq HE$. Thus HE is normal in G. The group $L = \langle x^p \mid x \in HE \rangle$ is characteristic in HE and $L \leq H$ is normal in G. Since $H_G = 1$, it follows that $|H| = p$. But now the result follows from Lemma 4.1. □

Remark 4.6. By using Zorn's lemma and the result of the previous theorem it is possible to prove that $G' \leq H$ also in the case that H is an infinite cyclic group (for the details, see [12]).

Remark 4.7. Drápal [7] uses elementary loop theory combined with permutation group theory and proves results which are basicly the same as the preceding results of this section. In Drápal's article it also remains an open question whether it is necessary to use Zorn's lemma when proving the result of Theorem 4.5 for an infinite cyclic subgroup H.

We now have a very good understanding of the situation when H is a finite cyclic subgroup of G and $G = \langle A, B \rangle$. How does the situation change if $H \cong C_p \times C_p$?

Theorem 4.8. *Let $H \cong C_p \times C_p$ and $G = \langle A, B \rangle$. Then $G' \leq N_G(H)$.*

Proof. If $H_G > 1$, then $G' \leq H$ by Lemma 4.1. Thus we may assume that $H_G = 1$. By Lemma 2.4, $N_G(H) = H \times Z(G)$ and from Lemma 4.4 we conclude that $G/Z(G)$ is finite. Consider the subgroup $HZ(G)/Z(G)$ of $G/Z(G)$. If the core of $HZ(G)$ in G properly contains $Z(G)$, then $G' \leq HZ(G) = N_G(H)$ (again we use Lemma 4.1). We next assume that the core of $HZ(G)$ in G is $Z(G)$. By Lemma 2.4,

$$N_{G/Z(G)}(HZ(G)/Z(G)) = HZ(G)/Z(G) \times Z(G/Z(G)).$$

We write $M/Z(G) = Z(G/Z(G))$. Then $N_G(HZ(G)) = HM$, where M is normal in G and $H \cap M = 1$. By Theorem 3.2, $Z(G)$ is a proper subgroup of M. Then we write $HM = CH = DH$, where $C \subseteq A$ and $D \subseteq B$. By Lemma 2.1, $M/Z(G) \subseteq AZ(G)/Z(G) \cap BZ(G)/Z(G)$, which means that $M \subseteq CZ(G) \cap DZ(G)$. If $m \in M$, then $m = cz_1 = dz_2$, where $c \in C$, $d \in D$ and $z_1, z_2 \in Z(G)$. If $x \in A \cup B$, then $[x, m] \in M \cap H = 1$. Thus $C_G(m) \geq \langle A, B \rangle = G$ and consequently $m \in Z(G)$. But then $M = Z(G)$, a contradiction. □

If $H \cong C_p \times C_p \times C_p$, then things get more complicated. However, in 2006 Csörgő [5] managed to prove the following

Theorem 4.9. *If G is finite group, $H \cong C_p \times C_p \times C_p$ and $G = \langle A, B \rangle$, then $G' \leq N_G(H)$.* □

5. Multiplication groups of loops

Let Q be a loop (a groupoid with unique division and neutral element e). For each $a \in Q$ we have two permutations L_a (left translation) and R_a (right translation) on Q defined by $L_a(x) = ax$ and $R_a(x) = xa$ for every $x \in Q$. The set of all left and right translations generates a subgroup $M(Q)$ of S_Q called the *multiplication group of the loop Q*. The stabilizer of the neutral element e is called the *inner mapping group of the loop Q* and we denote it by $I(Q)$. The concept of multiplication groups was introduced by Albert in [1] and [2] and in his famous article [3], Bruck laid the foundation for the theory of multiplication and inner mapping groups. If Q is a group, then $I(Q)$ consists of the inner automorphims of Q. It is well-known that the inner mapping group is generated by the set

$$\{R_{yx}^{-1} R_x R_y, L_{xy}^{-1} L_x L_y, L_x^{-1} R_x \mid x, y \in Q\}.$$

If we write $A = \{L_a \mid a \in Q\}$ and $B = \{R_a \mid a \in Q\}$, then A and B are transversals to $I(Q)$ in $M(Q)$ and as $L_a^{-1} R_b^{-1} L_a R_b(e) = e$, we see that A and B are $I(Q)$-connected transversals in $M(Q)$. Now $M(Q)$ is transitive on Q and therefore, if $1 < N \leq I(Q)$, N is not normal in $M(Q)$ (thus the core of I(Q) in M(Q) is trivial). As a matter of fact, we have now introduced all the properties which completely characterize multiplication groups of loops. We state this characterization that was proved by Kepka and Niemenmaa [14] in 1990 as

Theorem 5.1. *A group G is isomorphic to the multiplication group of a loop if and only if there exist a subgroup H of G satisfying $H_G = 1$ and H-connected transversals A and B such that $G = \langle A, B \rangle$.*

Proof. Assume that the group G has a subgroup H and H-connected transversals A and B satisfying the conditions of the theorem. For each $x \in G$ there exists exactly one $f(x)$ of A such that $xH = f(x)H$. Let K be the set of left cosets of H. Now we define a binary operation $(*)$ on the set K by $(xH) * (yH) = f(x)yH$.

If $xH = uH$ and $yH = vH$, then $f(x) = f(u)$ and $f(x)yH = f(x)vH = f(u)vH$. We conclude that $(*)$ is well-defined. Now we shall show that the groupoid $(K, *)$ is a loop. By Lemma 2.1, we have that $1 \in A$. Therefore $(1H)*(yH) = f(1)yH = yH$ and $(xH)*(1H) = f(x)H = xH$, which means that $1H$ is the neutral element of K. If xH and yH are fixed elements in $(xH) * (yH) = zH$, then $yH = f(x)^{-1}zH$ is a unique element from the set K. Respectively let yH and zH be known elements in K and consider the equation $(xH) * (yH) = zH$. For every $y \in G$ there exists exactly one $g(y)$ of B such that $yH = g(y)H$. Since A and B are H-connected, we have $(xH) * (yH) = f(x)g(y)H = g(y)f(x)H = g(y)xH$. Thus $xH = g(y)^{-1}zH$ is the unique solution for the equation $(xH) * (yH) = zH$, so the groupoid $(K, *)$ is a loop.

Now we consider the action of G on K by left multiplication as its permutation representation is a homomorphism from G to $M(K)$ with the kernel $H_G = 1$. Since $G = \langle A, B \rangle$ and the left and right translations are of the form $L_{xH}(yH) = (xH) * (yH) = f(x)yH$ and $R_{xH}(yH) = (yH) * (xH) = f(y)g(x)H = g(x)f(y)H = g(x)yH$ where $f(x) \in A$ and $g(x) \in B$, we conclude that the image of the permutation representation is the whole $M(K)$. Therefore G is isomorphic to $M(K)$. □

When we combine Theorems 4.5 and 5.1, we immediately have

Theorem 5.2. *Let Q be a loop. If $I(Q)$ is a finite cyclic group, then $I(Q) = 1$ and Q is an abelian group.* □

From the previous result we see that a nontrivial finite cyclic group can never be in the role of $I(Q)$. On the other hand, there are finite abelian groups which are isomorphic to inner mapping groups of loops. Thus we pose

Problem 1. *Classify those finite abelian groups which are (are not) isomorphic to inner mapping groups of loops.*

6. Centrally nilpotent loops

The *centre $Z(Q)$ of a loop Q* consists of all elements a, which satisfy the equations $(ax)y = a(xy)$, $(xa)y = x(ay)$, $(xy)a = x(ya)$ and $ax = xa$ for all $x, y \in Q$. Thus $a \in Z(Q)$ if and only if $U(a) = a$ for every $U \in I(Q)$. Clearly, $Z(Q)$ is an abelian group and normal in Q. The following well-known result was first proved by Albert [1].

Lemma 6.1. *We have* $Z(Q) \cong Z(M(Q))$.

Proof. Let $T \in Z(M(Q))$. Thus $L_x T(e) = TL_x(e)$ and it follows that $xT(e) = T(x)$ for every $x \in Q$. We see that $T = R_{T(e)}$. If $U \in I(Q)$, then $UT(e) = TU(e) = T(e)$ and so $T(e) \in Z(Q)$. We conclude that $Z(M(Q)) = \{R_c \mid c \in Z(Q)\}$. □

If we put $Z_0 = 1$, $Z_1 = Z(Q)$ and $Z_i/Z_{i-1} = Z(Q/Z_{i-1})$, then we obtain a series of normal subloops of Q. If Z_{n-1} is a proper subloop of Q and $Z_n = Q$, then Q is centrally nilpotent of class n.

Now the mapping $f : I(Q) \to I(Q/Z(Q))$ defined by $f(P)(xZ(Q)) = P(x)Z(Q)$ is a surjective homomorphism and

$$\mathrm{Ker}(f) = \{P \in I(Q) \mid P(x)Z(Q) = xZ(Q) \text{ for every } x \in Q\}.$$

We thus get

Lemma 6.2. *If* $K = \{P \in I(Q) \mid P(x) \in xZ(Q)$ *for every* $x \in Q\}$, *then* K *is a normal subgroup of* $I(Q)$ *and* $I(Q/Z(Q)) \cong I(Q)/K$. □

We combine the preceding lemma with Theorem 3.2.

Theorem 6.3. *Let* Q *be a finite loop and* $I(Q)$ *an abelian group of prime power order. Then* Q *is centrally nilpotent.*

Proof. By Theorem 3.2, $Z(M(Q)) > 1$ and thus $Z(Q) > 1$, by Lemma 6.1. If K is as in Lemma 6.2, we have $I(Q/Z(Q)) \cong I(Q)/K$. Again, $Z(Q/Z(Q)) > 1$. We continue like this and it follows that Q is centrally nilpotent. □

Remark 6.4. The result of Theorem 6.3 also holds if $I(Q)$ is abelian without any restrictions on the order of $I(Q)$ (for the details see [11] and [15]).

In the light of Theorem 6.3 is quite natural to pose the following problem.

Problem 2. *Assume that* Q *is a finite loop and* $I(Q)$ *is an abelian* p*-group whose structure is known. What can we say about the nilpotency class of a loop* Q*?*

We now recall a nilpotency criterion given by Bruck [3]. First write $I_0 = I(Q)$ and $I_i = N_{M(Q)}(I_{i-1})$ for each $i \geq 1$.

Theorem 6.5. *A necessary and sufficient condition that* Q *be centrally nilpotent of class* n *is that* $I_n = M(Q)$ *but* $I_{n-1} \neq M(Q)$. □

If Q is centrally nilpotent of class ≤ 2, then $N_{M(Q)}(I(Q)) = I(Q) \times Z(M(Q))$ is normal in $M(Q)$. It follows that $I(Q)'$ is normal in $M(Q)$, hence $I(Q)' = 1$ and $I(Q)$ is an abelian group.

The results given in Theorems 4.8 and 4.9 can now easily be interpreted in loop theory.

Theorem 6.6. *If Q is a finite loop and $I(Q) \cong C_p \times C_p$ or $I(Q) \cong C_p \times C_p \times C_p$, then Q is centrally nilpotent of class 2.* □

One is tempted to think that if $I(Q)$ is an elementary abelian p-group, then Q is centrally nilpotent of class 2. However, in a recent article Csörgő [4] has constructed an example of a finite group G of order 2^{13} such that G has an elementary abelian subgroup H of order 2^6 with H-connected transversals A and B, $G = \langle A, B\rangle$ and $G' \not\leq N_G(H)$. These conditions naturally imply the existence of a loop Q of order 2^7 with elementary abelian $I(Q)$ of order 2^6 and with nilpotency class greater than two.

Remark 6.7. Drápal and Vojtěchovský [9] have also constructed examples of loops Q with $I(Q)$ an abelian 2-group and Q centrally nilpotent of class 3 by means of a special group modification. It is interesting to note that in the case of a left conjugacy closed loop Q, it is centrally nilpotent of class 2 if and only if its inner mapping group is a nontrivial abelian group. This result is due to Csörgő and Drápal [6]. Finally, Drápal and Kinyon [8] have constructed a Buchsteiner loop of order 128 whose inner mapping group is abelian and nilpotency class is three.

We shall put an end to this article with the following

Problem 3. *Let Q be a loop such that $I(Q)$ is an abelian p-group. Is it possible that the nilpotency class of Q is greater than three?*

References

[1] **A. A. Albert**: *Quasigroups I*, Trans. Amer. Math. Soc. **54** (1943), 507−519.

[2] **A. A. Albert**: *Quasigroups II*, Trans. Amer. Math. Soc. **55** (1944), 401−419.

[3] **R. H. Bruck**: *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245 − 354.

[4] **P. Csörgő**: *Abelian inner mappings and nilpotency class greater than two*, European J. Comb. **28** (2007), 858 − 867.

[5] **P. Csörgő**: *On connected transversals to abelian subgroups and loop theoretical consequences*, Arch. Math. **86** (2006), 499 – 516.

[6] **P. Csörgő and A. Drápal**: *Left conjugacy closed loops of nilpotency class two*, Results Math. **47** (2005), 242 – 265.

[7] **A. Drápal**: *Orbits of inner mapping groups*, Monatsh. Math. **134** (2002), 191 – 206.

[8] **A. Drápal and M. Kinyon**: *Buchsteiner loops: associators and constructions*, to appear (2007).

[9] **A. Drápal and P. Vojtěchovský**: *Explicit constructions of loops with commuting inner mappings*, to appear (2007).

[10] **B. Huppert**: *Endliche Gruppen I*, Springer Verlag, 1967.

[11] **T. Kepka**: *On the abelian inner permutation groups of loops*, Comm. Algebra **26** (1998), 857 – 861.

[12] **T. Kepka and M. Niemenmaa**: *On loops with cyclic inner mapping groups*, Arch. Math. **60** (1993), 233 – 236.

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

[14] **M. Niemenmaa and T. Kepka**: *On multiplication groups of loops*, J. Algebra **135** (1990), 112 – 122.

[15] **M. Niemenmaa and T. Kepka**: *On connected transversals to abelian subgroups*, Bull. Austral. Math. Soc. **49** (1994), 121 – 128.

[16] **A. Vesanen**: *Solvable groups and loops*, J. Algebra **180** (1996), 862 – 876.

Department of Mathematical Sciences
University of Oulu
Pentti Kaiteran katu 1
PL 3000
90014 University of Oulu
Finland
E-mail: Markku.Niemenmaa@oulu.fi

Received April 2, 2007

Quasigroups and Related Systems **15** (2007), 109 – 140

Four lectures on quasigroup representations

Jonathan D. H. Smith

Abstract

These are notes for lectures in the Workshops Loops '07 series, held at the Czech Agricultural University, Prague, 13 August – 17 August, 2007. The initial lecture covers elementary topics and examples of quasigroups. The following lectures then introduce the three main branches of quasigroup representation theory: characters, permutation representations, and modules.

1. Quasigroups

1.1. Basic definitions.

1.1.1. *Combinatorial quasigroups.* A (*combinatorial*) *quasigroup* Q or $(Q, \cdot)$ is a set Q equipped with a binary operation of *multiplication*

$$Q \times Q \to Q; \quad (x, y) \mapsto xy \tag{1.1}$$

denoted by $\cdot$ or simple juxtaposition of the two arguments, in which specification of any two of x, y, z in the equation $x \cdot y = z$ determines the third uniquely.

1.1.2. *Equational quasigroups.* An (*equational*) *quasigroup*, written as Q or $(Q, \cdot, /, \backslash)$, is a set Q equipped with three binary operations of multiplication, *right division* $/$ and *left division* $\backslash$, satisfying the identities:

$$\begin{array}{llll} \text{(IL)} & y\backslash(y \cdot x) = x\,; & \text{(IR)} & x = (x \cdot y)/y\,; \\ \text{(SL)} & y \cdot (y\backslash x) = x\,; & \text{(SR)} & x = (x/y) \cdot y\,. \end{array}$$

Note the left-right symmetry of these identities.

2000 Mathematics Subject Classification: 20N05
Keywords: quasigroup, loop, multiplication group, centrality, character, association scheme, permutation representation, permutation group, transfomation group, split extension, module, group in category, combinatorial differentiation

1.1.3. *Quasigroups.* Suppressing the divisions, each equational quasigroup is a combinatorial quasigroup. For example, the unique solution y to $x \cdot y = z$ is $x\backslash z$. Conversely, each combinatorial quasigroup is equational: define $x\backslash z$ as the unique solution y to $x \cdot y = z$, and so on. We speak simply of *quasigroups*.

A subset P of a quasigroup $(Q, \cdot)$ is a *subquasigroup* of Q if P is closed under the multiplication and the divisions. If Q_1 and Q_2 are quasigroups, then their (*direct*) *product* is the product set $Q_1 \times Q_2$ equipped with componentwise multiplication and divisions.

1.1.4. *Homomorphisms and homotopies.* A map

$$f : (Q_1, \cdot, /, \backslash) \to (Q_2, \cdot, /, \backslash)$$

between quasigroups is a *homomorphism* if

$$xf \cdot yf = (x \cdot y)f$$

for all x, y in Q_1. It is an *isomorphism* if it is bijective. We then say that Q_1 and Q_2 are *isomorphic*, notation $Q_1 \cong Q_2$.

In quasigroup theory, the usual algebraic notion of homomorphism is often too strong. A triple of maps

$$(f, g, h) : (Q_1, \cdot, /, \backslash) \to (Q_2, \cdot, /, \backslash)$$

between quasigroups is a *homotopy* if

$$xf \cdot yg = (x \cdot y)h \tag{1.2}$$

for all x, y in Q_1. The triple is an *isotopy* if the maps f, g, h are bijective. We then say that Q_1 and Q_2 are *isotopic*, notation $Q_1 \sim Q_2$. (The concept of isotopy is often too weak. The right concept seems to be "central isotopy," as described in §1.5.5. Compare [5, §§4.2–3].)

1.1.5. *Exercises.*

1. If $f : Q_1 \to Q_2$ is a homomorphism between quasigroups, show $xf/yf = (x/y)f$ and $xf\backslash yf = (x\backslash y)f$ for all x, y in Q_1.
2. Show that a function $f : Q_1 \to Q_2$ between quasigroups is a homomorphism if and only if its *graph*

$$\{(x_1, x_2) \in Q_1 \times Q_2 \mid x_1 f = x_2\}$$

is a subquasigroup of the product $Q_1 \times Q_2$.

3. Show that isotopy is an equivalence relation.

4. Show that, if one of the three components f, g, h of a homotopy is bijective, then (f, g, h) is an isotopy.

5. Show that isotopic groups are isomorphic.

1.2. Basic examples.

1.2.1. *Groups.* Each group is a quasigroup, with $x/y = xy^{-1}$ and $x\backslash y = x^{-1}y$. The multiplication satisfies the associative law (although the divisions do not). Conversely, with the exception of the empty quasigroup, each associative quasigroup is a group. A quasigroup is *abelian* if it is commutative and associative, so is either empty or an abelian group.

1.2.2. *Subtraction.* If $(A, +)$ is an additive (abelian) group, then the set A forms a quasigroup $(A, -)$ under the nonassociative operation of subtraction. This operation is more fundamental than the associative operation of addition. For example, the integer 1 generates all integers using subtraction, since $0 = 1 - 1$, $-n = 0 - n$, $m + n = m - (-n)$. But 1 only generates the positive integers using addition.

1.2.3. *Isotopes.* If Q_2 is a quasigroup, and the maps $f, g, h : Q_1 \to Q_2$ are bijections, then there is a unique quasigroup structure on Q_1 so that (f, g, h) forms an isotopy. Using (1.2), we have $x \cdot y = (xf \cdot yg)h^{-1}$ for elements x, y in Q_1. For example, if $Q_1 = Q_2 = \mathbb{R}$, with Q_2 as the additive group $(\mathbb{R}, +, 0)$ of the real numbers, and the bijective maps $f, g, h : \mathbb{R} \to \mathbb{R}$ are the respective scalar multiplications by the invertible elements $1/2$, $1/2$, and 1, then the multiplication

$$x \cdot y = \frac{x + y}{2}$$

is the operation of taking arithmetic means.

1.2.4. *Latin squares.* A *Latin square*, such as that displayed on the left side of Figure 1, is an $n \times n$ square containing n copies of each of n symbols, arranged in such a way that no symbol is repeated in any row or column. The body of the multiplication table of a (finite) quasigroup is a Latin square, while each Latin square may be bordered to yield the multiplication table of a quasigroup. For example, labelling the rows and columns of the Latin square on the left side of Figure 1 by $1, \ldots, 6$ in order yields the multiplication table of a quasigroup Q with $3 \cdot 2 = 1$, etc., as displayed on the right side of Figure 1.

1	3	2	5	6	4
3	2	1	6	4	5
2	1	3	4	5	6
4	5	6	1	2	3
5	6	4	2	3	1
6	4	5	3	1	2

Q	1	2	3	4	5	6
1	1	3	2	5	6	4
2	3	2	1	6	4	5
3	2	1	3	4	5	6
4	4	5	6	1	2	3
5	5	6	4	2	3	1
6	6	4	5	3	1	2

Figure 1: A Latin square yields a multiplication table.

1.2.5. *Exercises.*

1. Define a multiplication operation $\circ$ on the additive group $\mathbb{Z}/3\mathbb{Z}$ of integers modulo 3 by $x \circ y = -x - y$. Set up the body of the multiplication table of $(\mathbb{Z}/3\mathbb{Z}, \circ)$ as a Latin square.

2. Show that the quasigroups $(\mathbb{Z}/3\mathbb{Z}, -)$, $(\mathbb{Z}/3\mathbb{Z}, +)$, and the quasigroup $(\mathbb{Z}/3\mathbb{Z}, \circ)$ of Exercise (1) are all isotopic.

3. Verify the nonassociativity of the quasigroup Q whose multiplication table appears in Figure 1.

1.3. Steiner systems.

1.3.1. *Steiner triple systems.* Steiner systems offer a rich source of quasigroups. A *Steiner triple system* $(S, \mathcal{B})$ is a finite set S together with a set $\mathcal{B}$ of *blocks*, 3-element subsets of S with the property that each pair of distinct elements of S is contained in exactly one block.

1.3.2. *Projective spaces over* $\mathsf{GF}(2)$. Suppose that S is the projective space $\mathsf{PG}(d, 2)$ of dimension d over the 2-element field $\mathsf{GF}(2)$. As a set, S consists of the nonzero elements of the $(d+1)$-dimensional vector space $\mathsf{GF}(2)^{d+1}$. The lines in the projective space are the intersection with S of 2-dimensional linear subspaces of $\mathsf{GF}(2)^{d+1}$. Taking $\mathcal{B}$ to be the set of lines yields a Steiner triple system $(S, \mathcal{B})$ which is also described as $\mathsf{PG}(d, 2)$. The points of S are specified by their coordinate vectors in $\mathsf{GF}(2)^{d+1}$, which in turn may be interpreted as length $d+1$ binary expansions of numbers from 1 to $2^{d+1}-1$. In the 2-dimensional case, illustrated in Figure 2, one obtains

$$\mathcal{B} = \{246, 145, 347, 123, 257, 167, 356\}$$

on writing each 3-element line $\{a, b, c\}$ in the abbreviated form *abc*. Note the curved "line" 356 in the figure.

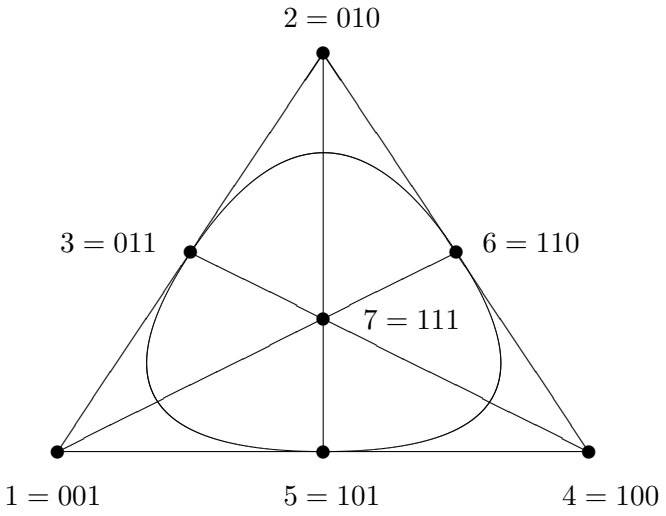


Figure 2: The projective space $\mathsf{PG}(2, 2)$.

Suppose that S is the projective space $\mathsf{PG}(d, 2)$ of dimension d over the 2-element field $\mathsf{GF}(2)$. As a set, S consists of the nonzero elements of the $(d+1)$-dimensional vector space $\mathsf{GF}(2)^{d+1}$. The lines in the projective space are the intersection with S of 2-dimensional linear subspaces of $\mathsf{GF}(2)^{d+1}$. Taking $\mathcal{B}$ to be the set of lines yields a Steiner triple system $(S, \mathcal{B})$ which is also described as $\mathsf{PG}(d, 2)$. The points of S are specified by their coordinate vectors in $\mathsf{GF}(2)^{d+1}$, which in turn may be interpreted as length $d + 1$ binary expansions of numbers from 1 to $2^{d+1} - 1$. In the 2-dimensional case, illustrated in Figure 2, one obtains

$$\mathcal{B} = \{246, 145, 347, 123, 257, 167, 356\}$$

on writing each 3-element line $\{a, b, c\}$ in the abbreviated form *abc*. Note the curved "line" 356 in the figure.

1.3.2. *Affine spaces over* $\mathsf{GF}(3)$. Suppose that S is the affine space $\mathsf{AG}(d, 3)$ of dimension d over the 3-element field $\mathsf{GF}(3)$. As a set, S is the vector space $\mathsf{GF}(3)^d$. The lines in the affine geometry are the cosets $L + v$ of 1-dimensional linear subspaces L of $\mathsf{GF}(3)^d$, with v as a vector from $\mathsf{GF}(3)^d$. Taking $\mathcal{B}$ to be the set of lines again yields a Steiner triple system $(S, \mathcal{B})$,

which is also described as $\mathsf{AG}(d,3)$. The points of S may be represented by Cartesian coordinates, which in turn may be interpreted as length d ternary expansions of numbers from 0 to 3^d-1. In the 2-dimensional case, one obtains

$$\mathcal{B} = \{012, 036, 048, 057, 138, 147, 156, 237, 246, 258, 345, 678\}$$

on writing each 3-element line $\{a,b,c\}$ in the abbreviated form abc.

1.3.4. *Totally symmetric quasigroups.* A Steiner triple system $(S,\mathcal{B})$ yields a quasigroup $(S,\cdot)$ on defining $x\cdot y = z$ whenever $x=y=z$ or $\{x,y,z\}\in\mathcal{B}$. Such a quasigroup is *idempotent*, satisfying the identity

$$x\cdot x = x\,. \tag{1.3}$$

It also possesses the property of *total symmetry* expressed by the identities

$$x\cdot y = x/y = x\backslash y. \tag{1.4}$$

Conversely, each idempotent, totally symmetric quasigroup $(S,\cdot)$ yields a Steiner triple system on defining

$$\mathcal{B} = \big\{\{x,y,x\cdot y\} \;\big|\; x\neq y\in S\big\}.$$

It is convenient to identify each Steiner triple system $(S,\mathcal{B})$ with the corresponding idempotent, totally symmetric quasigroup $(S,\cdot)$.

1.3.5. *Exercises.*

1. Construct the multiplication table for the idempotent, totally symmetric quasigroup $\mathsf{PG}(2,2)$.
2. Describe the quasigroup of Exercise 1.2.5 (1) as a Steiner triple system.
3. Show that for positive integers m and n, the totally symmetric quasigroups $\mathsf{AG}(m+n,3)$ and $\mathsf{AG}(m,3)\times\mathsf{AG}(n,3)$ are isomorphic.

1.4. Multiplication groups.

1.4.1. *Multiplications.* Let p be an element of a subquasigroup P of a quasigroup $(Q,\cdot)$. The (*relative*) *left multiplication* $L_Q(p)$ or $L(p)$ by p in Q is the map

$$L(p): Q\to Q;\quad x\mapsto p\cdot x\,.$$

Note that $L(p)$ is a permutation (bijective self-map) of Q. Indeed, the identity (IL) gives the injectivity of $L(p)$, while the identity (SL) gives the surjectivity. Similarly, the (*relative*) *right multiplication* $R_Q(p)$ or $R(p)$ by p in Q is the map

$$R(p) : Q \to Q; \quad x \mapsto x \cdot p\,.$$

1.4.2. *Multiplication groups.* Let P be a subquasigroup of a quasigroup Q. Let $Q!$ be the group of all permutations of the set Q. The (*relative*) *left multiplication group* of P in Q is the subgroup

$$\mathrm{LMlt}_Q P = \langle L_Q(p) \mid p \in P \rangle_{Q!}$$

of $Q!$ generated by all the relative left multiplications $L(p)$ by elements p of P. The (*relative*) *right multiplication group*

$$\mathrm{RMlt}_Q P = \langle R_Q(p) \mid p \in P \rangle_{Q!}$$

is defined similarly. The (*relative*) *multiplication group* of P in Q is the subgroup

$$\mathrm{Mlt}_Q P = \langle L_Q(p), R_Q(p) \mid p \in P \rangle_{Q!}$$

generated by both the left and right multiplications from P. Note that P is invariant under $\mathrm{Mlt}_Q P$. Finally, define the (*combinatorial*) *multiplication group* $\mathrm{Mlt}\, Q$ of Q as the relative multiplication group of Q in itself. (The adjective "combinatorial" distinguishes from the groups of §4.2.2.)

1.4.3. *Multiplication groups of groups.* Suppose that the quasigroup Q is a group (compare §1.2.1), with centre $Z(Q)$. The combinatorial multiplication group G of Q is given by the exact sequence

$$1 \to Z(Q) \xrightarrow{\Delta} Q \times Q \xrightarrow{T} G \to 1 \tag{1.5}$$

of groups with $\Delta : z \mapsto (z, z)$ and $T : (x, y) \mapsto L(x)^{-1} R(y)$. If the group Q is abelian, then the right multiplication map

$$R : Q \to G; \quad q \mapsto R(q)$$

is a group isomorphism.

1.4.4. *Multiplication groups as permutation groups.* Suppose that G is a relative multiplication group of a quasigroup Q. For elements x and y of Q, define

$$\rho(x, y) = R(x\backslash x)^{-1} R(x\backslash y) \tag{1.6}$$

in G. Note that $\rho(x,x) = 1$ for x in Q. The action of G on Q is transitive: given elements x and y of Q, we have

$$x\rho(x,y) = xR(x\backslash x)^{-1}R(x\backslash y) = xR(x\backslash y) = x(x\backslash y) = y$$

since $xR(x\backslash x) = x(x\backslash x) = x$. Consider the stabiliser

$$G_x = \{g \in G \mid xg = x\}$$

of each element x in Q. The stabilisers are all conjugate in G, indeed

$$(G_x)^{\rho(x,y)} = G_{x\rho(x,y)} = G_y$$

for x and y in Q.

1.4.5. *Exercises.*

1. Verify that Δ and T in (1.5) are group homomorphisms.

2. Verify the exactness of the sequence (1.5) — at each of the three interior nodes, the image of the arrow coming in is the group kernel of the arrow going out.

3. Let G be the combinatorial multiplication group of a group Q with identity element e. Show that the stabiliser G_e is the inner automorphism group $\operatorname{Inn} Q$ of Q.

4. For an integer $n > 1$, show that the dihedral group D_n of degree n is the multiplication group of the quasigroup $(\mathbb{Z}/n\mathbb{Z}, -)$ of integers modulo n under subtraction.

5. Let e be an element of a subquasigroup P of a quasigroup Q. Let G be the relative multiplication group of P in Q, and let G_e be the stabiliser of e in G. Using the notation (1.6), show that G decomposes as the disjoint union

$$G = \bigcup_{x \in P} G_e\rho(e,x)\,.$$

6. Let e be an element of a quasigroup Q with combinatorial multiplication group G. Show that Q is an abelian group if and only if the stabiliser G_e is a normal subgroup of G [7, III Prop.2.5.3].

1.5. Centrality.

1.5.1. *Congruences.* If $f : Q_1 \to Q_2$ is a quasigroup homomorphism, consider the kernel relation $\ker f$ of f, defined by

$$(x, y) \in \ker f \Leftrightarrow xf = yf\,.$$

This is a *congruence* (*relation*) on Q_1, an equivalence relation which, as a subset of $Q_1 \times Q_1$, is a subquasigroup of $Q_1 \times Q_1$. Conversely, given a congruence relation V on a quasigroup Q, the natural projection

$$\mathrm{nat}\, V : Q \to Q^V;\quad x \mapsto x^V\,,$$

mapping x in Q to its equivalence class $x^V = \{y \in Q \mid (x, y) \in V\}$ in the set $Q^V = \{x^V \mid x \in Q\}$ of all equivalence classes, is a quasigroup homomorphism.

1.5.2. *Uniformity of congruences.* Let V be a congruence on a quasigroup Q. Then for elements x and y of Q, the map $\rho(x, y) : x^V \to y^V$ is a well-defined bijection. To see that it is well defined, consider an element x' of x^V. Then

$$(y, x'\rho(x, y)) = \big(x\rho(x, y), x'\rho(x, y)\big) = \big((x, x')/(x\backslash x, x\backslash x)\big) \cdot (x\backslash y, x\backslash y)$$

is an element of V, since V is both a reflexive relation and a subquasigroup of Q^2. Summarizing, a quasigroup congruence is determined by any one of its congruence classes.

1.5.3. *Normal subquasigroups.* A subquasigroup P of a quasigroup Q is said to be a *normal* subquasigroup of Q, written $P \triangleleft Q$, if there is a congruence V on Q having P as a single congruence class. By the uniformity (§1.5.2), the congruence V is uniquely determined by P. Write Q/P for the quotient Q^V. Note that a normal subgroup N of a group Q is a class of the kernel congruence of the natural projection $Q \to Q/N$; $x \mapsto Nx$.

1.5.4. *Central congruences.* For a quasigroup Q, the *diagonal*

$$\widehat{Q} = \{(x, x) \in Q^2 \mid x \in Q\}$$

is a subquasigroup of Q^2. The diagonal is a subquasigroup of each congruence V on Q, since V is reflexive. The congruence V is said to be *central* if $\widehat{Q} \triangleleft V$. Each central congruence on Q is a subcongruence of a maximal central congruence, the *centre congruence* $\zeta(Q)$ of Q. For a group Q, the centre $Z(Q)$ is the $\zeta(Q)$-class of the identity element. A quasigroup Q is

said to be *central* if $\zeta(Q) = Q^2$. The class of central quasigroups is denoted by $\mathfrak{Z}$. Central groups are precisely the abelian groups.

1.5.5. *Central isotopy.* For a quasigroup Q, suppose that the diagonal $\widehat{Q}$ is a congruence class of a congruence W on $\zeta(Q)$. A quasigroup P is *centrally isotopic* to Q, written $P \simeq Q$, if there is a bijection $t : P \to Q$, a so-called *central shift*, and a pair (q, q') of elements of Q such that

$$(q, q')\ W\ \big((x \cdot y)t, xt \cdot yt\big) \tag{1.7}$$

for all x, y in P. In particular, it follows that the triple $\big(t, t, t\rho(q, q')\big)$ is an isotopy — Exercise 1.5.6 (4). Central isotopy is an equivalence relation, and centrally isotopic quasigroups have similar multiplication group actions (so in particular, their multiplication groups are isomorphic). A central quasigroup Q is centrally isotopic to the central quasigroup $Q^2/\widehat{Q}$. Note that the quotient $Q^2/\widehat{Q}$ has the class $\widehat{Q}$ as an idempotent element.

1.5.6. *Exercises.*

1. Show that a group Q is abelian if and only if $\widehat{Q} \lhd Q^2$.
2. Let $(A, +, 0)$ be an abelian group. For automorphisms R and L of $(A, +, 0)$, define $x \cdot y = xR + yL$. Show that $(A, \cdot)$ is a central quasigroup with 0 as an idempotent element. (In fact, each central quasigroup with an idempotent element is obtained in this way [1, Th. III.5.2], [6, §3.5].)
3. For the quasigroup $(A, \cdot)$ of Exercise (2), show that $\mathrm{Mlt}(A, \cdot)$ is the split extension of the abelian group $(A, +, 0)$ by the subgroup $\langle R, L\rangle$ of the automorphism group $\mathrm{Aut}(A, +, 0)$ generated by the automorphisms R and L.
4. Let a quasigroup P be centrally isotopic to a quasigroup Q. Use (1.7) to deduce that $\big(t, t, t\rho(q, q')\big) : P \to Q$ is an isotopy.
5. Amongst the quasigroups of Exercise 1.2.5 (2), determine which pairs are centrally isotopic.

2. Characters

2.1. The Bose-Mesner algebra.

2.1.1. *Conjugacy classes.* Let Q be a quasigroup, with multiplication group G. Recall that the action of G on Q is transitive, with a single orbit Q

(§1.4.4). The group G acts on $Q \times Q$ with the *diagonal action*

$$(q_1, q_2)g = (q_1 g, q_2 g)$$

for q_1, q_2 in Q and g in G. There are several orbits. In the general theory of transitive group actions, these orbits are described as *orbitals*. Here, they are defined as the (*quasigroup*) *conjugacy classes*. Since G acts transitively on Q, one orbital is the diagonal $\widehat{Q} = C_1$, the relation $\{(q_1, q_2) \mid q_1 = q_2\}$ of equality on Q. The complement of $\widehat{Q} = C_1$ in Q^2 is the *diversity relation* $\{(q_1, q_2) \mid q_1 \neq q_2\}$. If the diversity relation forms a single orbital, then Q is described as a *rank* 2 *quasigroup*. For a general finite quasigroup Q of order n, there is a finite set Γ or

$$\Gamma(Q) = \{\widehat{Q} = C_1, C_2, \ldots, C_s\} \tag{2.1}$$

of conjugacy classes, known as the *conjugacy class partition* of Q^2. The integer s is known as the *rank* of the quasigroup Q. For $1 \leqslant i \leqslant s$, the cardinality of the i-th conjugacy class is a multiple $|C_i| = nn_i$ of n. The factor n_i, known as the *valency* of C_i, is the cardinality of $C_i(x) := \{q \mid (x, q) \in C_i\}$ for each x in Q — Exercise 2.1.5 (1). Note that $n_1 = 1$ and $n_1 + \cdots + n_s = n$.

2.1.2. *Incidence matrices.* Suppose that Q is a finite quasigroup, with a positive order n. Then the elements of Q may be used to index the rows and columns of each $n \times n$ matrix (with entries from the field $\mathbb{C}$ of complex numbers). For a relation R on Q, the *incidence matrix* of R is the $n \times n$ matrix having an entry of 1 in the row labelled q_1 and column labelled q_2 whenever $(q_1, q_2) \in R$. The other entries of the incidence matrix of R are zero. Thus the incidence matrix of the universal relation $Q \times Q$ is the $n \times n$ matrix J or J_n, all of whose entries are 1. The incidence matrix of the equality relation $\widehat{Q} = C_1$ is the $n \times n$ identity matrix I or I_n. The incidence matrix of the diversity relation is $J_n - I_n$. If the incidence matrix of a relation R is A, then the incidence matrix of the converse relation

$$R^{-1} = \{(q_1, q_2) \mid (q_2, q_1) \in R\}$$

is the (conjugate) transpose A^* of A.

2.1.3. *The Bose-Mesner algebra.* Let Q be a quasigroup of positive finite order n, with conjugacy class partition (2.1). The converse of each conjugacy class C_i is a conjugacy class C_{i^*}. The respective incidence matrices

$$I_n = A_1, A_2, \ldots, A_s \tag{2.2}$$

of the quasigroup conjugacy classes are the *adjacency matrices*. Note that $A_i^* = A_{i^*}$ (for $1 \leqslant i \leqslant s$) and

$$\sum_{i=1}^{s} A_i = J_n \,.$$

The adjacency matrices (2.2) generate a subalgebra of the complex algebra $\mathbb{C}_n^n$ of all complex $n \times n$ matrices. This algebra is known as the *Bose-Mesner algebra*. If the multiplication group of Q is G, then the Bose-Mesner algebra is also known as the *centraliser ring* (or **Vertauschungsring**) $V(G,Q)$ of G on Q.

2.1.4. *Primitive idempotents.* The Bose-Mesner algebra $V(G,Q)$ of a finite quasigroup turns out to be just the s-dimensional $\mathbb{C}$-linear span of the set (2.2) of adjacency matrices, and moreover, $V(G,Q)$ is a commutative subalgebra of the complex matrix algebra [6, Th. 6.1]. Thus there are *structure constants* c_{ij}^k for $1 \leqslant i,j,k \leqslant s$ with

$$A_i A_j = \sum_{k=1}^{s} c_{ij}^k A_k$$

and $c_{ij}^k = c_{ji}^k$. Simultaneous diagonalisation of the set (2.2) of mutually commuting matrices shows that the vector space $V(G,Q)$ has a basis

$$\frac{1}{n} J_n = E_1, E_2, \ldots, E_s \tag{2.3}$$

of mutually orthogonal *primitive idempotent* matrices, satisfying

$$E_i E_j = \delta_{ij} E_i \qquad \text{and} \qquad \sum_{i=1}^{s} E_i = I_n \,.$$

Thus the Wedderburn decomposition of $V(G,Q)$ as a direct sum of matrix rings is

$$V(G,Q) \cong V(G,Q)E_1 \oplus \cdots \oplus V(C,Q)E_s \cong \mathbb{C} \oplus \cdots \oplus \mathbb{C} \,.$$

The matrices (2.3) are the projections onto the common eigenspaces of the adjacency matrices (2.2). They are also uniquely determined as the set of atoms of the finite Boolean algebra of idempotent elements of $V(G,Q)$. For $1 \leqslant i \leqslant s$, the traces f_i of the matrices E_i are the *multiplicities*. Note that $f_1 = 1$ and $f_1 + \cdots + f_s = n$.

2.1.5. *Exercises.*

1. Let C_i be a conjugacy class of a finite quasigroup of order n. For elements x, y of Q, show that $\rho(x,y) : C_i(x) \to C_i(y)$ is a bijection.
2. Let Q be a group with identity element e. Show that
$$\{e\} = C_1(e), C_2(e), \ldots, C_s(e)$$
are the usual group conjugacy classes — see Exercise 1.4.5 (3).
3. If Q is a group with identity element e, show that
$$C_{i^*}(e) = \{x^{-1} \mid x \in C_i(e)\}\,.$$
4. Show that a finite, nonempty quasigroup is abelian if and only if all the valencies are 1.
5. Show that, up to isomorphism, the additive group $(\mathbb{Z}/2\mathbb{Z}, +, 0)$ is the only finite rank 2 group. (HNN-extensions of countable torsion-free groups yield infinite rank 2 groups [2].)
6. Let Q be the additive group $(\mathbb{Z}/3\mathbb{Z}, +, 0)$ of integers modulo 3. Show that the adjacency matrices are
$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$
and the primitive idempotents are
$$E_1 = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \; E_2 = \frac{1}{3}\begin{bmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \\ \omega & \omega^2 & 1 \end{bmatrix}, \; E_3 = \frac{1}{3}\begin{bmatrix} 1 & \omega^2 & \omega \\ \omega & 1 & \omega^2 \\ \omega^2 & \omega & 1 \end{bmatrix}$$
with $\omega = \exp(2\pi i/3)$ as a primitive cube root of unity.

2.2. The character table.

2.1.1. *Change of basis.* For a quasigroup Q of finite order n, with multiplication group G, the Bose-Mesner algebra $V(G,Q)$ has two bases: the adjacency matrices (2.2), and the primitive idempotents (2.3). Each matrix from one basis is expressed uniquely as a linear combination of the matrices from the other:

$$A_i = \sum_{j=1}^{s} \xi_{ij} E_j \,, \qquad E_i = \sum_{j=1}^{s} \eta_{ij} A_j \,.$$

The coefficients in these linear combinations form mutually inverse $s \times s$ matrices

$$\Xi = [\xi_{ij}] \quad \text{and} \quad H = [\eta_{ij}] \,. \tag{2.4}$$

2.2.2. *Character tables.* The *character table* of Q is the $s \times s$ matrix $\Psi(Q)$ or $\Psi = [\psi_{ij}]$ with entries given as the normalised versions

$$\psi_{ij} = \tfrac{\sqrt{f_i}}{n_j}\, \xi_{ji} = \tfrac{n}{\sqrt{f_i}}\, \overline{\eta}_{ij}$$

of the entries of the change-of-basis matrices (2.4). This normalisation is used in the theory of finite groups. With a different normalisation, the *unitary character table* of Q is the $s \times s$ matrix $\Upsilon(Q)$ or $\Upsilon = [\upsilon_{ij}]$ with entries given as

$$\upsilon_{ij} = \sqrt{\frac{f_i}{nn_j}}\xi_{ji} = \sqrt{\frac{nn_j}{f_i}}\overline{\eta}_{ij}$$

in terms of the entries of the change-of-basis matrices (2.4). The so-called *orthogonality relations* satisfied by the character tables Ψ and Υ are best summarised by saying that the unitary character table Υ is a unitary $s \times s$ matrix: $\Upsilon^* \Upsilon = I_s$ — Exercise 2.2.5 (1).

2.2.3. *Duality.* In order to keep track of all the notation, see Table 1,

adjacency matrix A_i	primitive idempotent E_i
valency n_i	multiplicity f_i
$n_1 = 1$	$f_1 = 1$
$n_1 + \cdots + n_s = n$	$f_1 + \cdots + f_s = n$
$A_1 = I_n$	$E_1 = \frac{1}{n} J_n$
$\sum_{i=1}^{s} A_i = J_n$	$\sum_{i=1}^{s} E_i = I_n$
$A_i \circ A_j = \delta_{ij} A_i$	$E_i \cdot E_j = \delta_{ij} E_i$
$A_i = \sum_{j=1}^{s} \xi_{ij} E_j$	$E_i = \sum_{j=1}^{s} \eta_{ij} A_j$

Table 1: Duality.

illustrating the duality present. For two matrices $B = [b_{ij}]$ and $C = [c_{ij}]$ of the same shape, recall the *Hadamard product* $B \circ C = [b_{ij}c_{ij}]$.

2.2.4. *Class functions.* For a quasigroup Q with multiplication group G, a complex-valued function $\theta : Q \times Q \to \mathbb{C}$ is a *class function* if $\theta(q_1 g, q_2 g) = \theta(q_1, q_2)$ for all q_i in Q and g in G. In other words, θ is constant on each conjugacy class. The class functions form a complex vector space $\mathbb{C}\mathrm{Cl}(Q)$ under componentwise addition and scalar multiplication. If Q has finite order n, then an inner product $\langle \mid \rangle$ is defined on $\mathbb{C}\mathrm{Cl}(Q)$ by

$$\langle \theta | \varphi \rangle = \frac{1}{n^2} \sum_{(x,y) \in Q^2} \theta(x,y)\varphi(y,x)\,.$$

For $1 \leqslant i \leqslant s$, the i-th row $\psi_i = [\psi_{i1}, \ldots, \psi_{is}]$ of the character table $\Psi(Q)$ determines a class function ψ_i with $\psi_i(x,y) = \psi_{ij}$ for $(x,y) \in C_j$, known as a *basic character* of Q. As a result of the orthogonality relations, and the choice of the normalisation for Ψ, the basic characters $\psi_1, \ldots, \psi_s$ form an orthonormal basis for the space $\mathbb{C}\mathrm{Cl}(Q)$ of class functions. In particular, the *principal character* ψ_1 is the *zeta function* $\zeta : Q^2 \to \mathbb{C}$ taking the constant value 1 — Exercise 2.2.5 (3).

2.2.5. *Exercises.*

1. For a finite nonempty quasigroup Q, use $\Xi H = I_s$ to prove that $\Upsilon(Q)$ is a unitary matrix.

2. For a quasigroup Q of positive order n, show that $f_i = n\eta_{i1}$ for $1 \leqslant i \leqslant s$. Conclude that $\psi_{i1} = \sqrt{f_i}$ for $1 \leqslant i \leqslant s$.

3. For a quasigroup Q of positive order n, show that $\xi_{1j} = 1$ for $1 \leqslant j \leqslant s$. Conclude that $\psi_{1j} = 1$ for $1 \leqslant j \leqslant s$.

4. Compute the character table and the unitary character table for the additive group $(\mathbb{Z}/3\mathbb{Z}, +, 0)$ of integers modulo 3 — compare Exercise 2.1.5 (6).

5. Show that a finite nonempty quasigroup is abelian if and only if all the multiplicities are 1.

2.3. Examples and computations.

2.3.1. *Rank 2 quasigroups.* Let Q be a rank 2 quasigroup of finite order n. Now $f_2 = n_2 = n-1$, so $\Psi(Q)$ has the form

$$\begin{bmatrix} 1 & 1 \\ (n-1)^{1/2} & ? \end{bmatrix}.$$

Using the orthogonality relations, this is completed to

$$\Psi(Q) = \begin{bmatrix} 1 & 1 \\ (n-1)^{1/2} & -(n-1)^{-1/2} \end{bmatrix}.$$

In particular — compare Exercise 2.1.5 (5),

$$\Psi(\mathbb{Z}/2\mathbb{Z}, +) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.5}$$

Almost all finite quasigroups are rank 2 quasigroups [7, Cor.6.5].

2.3.2. *Groups.* Suppose that Q is a finite group of order n, with identity element e. By Exercise 2.1.5 (2), the valencies n_i are the orders of the group conjugacy classes $C_i(e)$ for $1 \leqslant i \leqslant s$. Consider the complex vector space $\mathbb{C}Q$ spanned by Q. Extending the multiplication of Q by linearity (including the distributive law) yields $\mathbb{C}Q$ as the (*complex*) *group algebra* of Q. The right and left multiplications of Q act as endomorphisms of the vector space $\mathbb{C}Q$, making $\mathbb{C}Q$ a faithful module over $\mathbb{C}G$. The centraliser ring $V(G,Q)$, as the ring $\mathrm{End}_{\mathbb{C}G}\mathbb{C}Q$ of endomorphisms of the vector space $\mathbb{C}Q$ that commute with the action of G, is the centre $Z(\mathbb{C}Q)$ of the group algebra. Choose a set $\{V_1, V_2, \ldots V_s\}$ of mutually nonisomorphic representatives for the ordinary irreducible Q-modules, with V_1 trivial. Suppose $\dim V_i = d_i$ for $1 \leqslant i \leqslant s$. The group algebra $\mathbb{C}Q$ decomposes as

$$\begin{aligned} \mathbb{C}Q &\cong \mathrm{End}_{\mathbb{C}Q}\mathbb{C}Q \\ &\cong \mathrm{End}_{\mathbb{C}Q}V_1 \oplus \mathrm{End}_{\mathbb{C}Q}(d_2V_2) \oplus \cdots \oplus \mathrm{End}_{\mathbb{C}Q}(d_sV_s) \\ &\cong \mathbb{C} \oplus \mathrm{Mat}_{d_2}(\mathbb{C}) \oplus \mathrm{Mat}_{d_s}(\mathbb{C}), \end{aligned}$$

a direct sum of matrix rings. (The latter isomorphism holds by Schur's Lemma). The centre decomposes as

$$V(G,Q) = Z(\mathbb{C}Q) \cong \mathbb{C}\pi_1 \oplus \mathbb{C}\pi_2 \oplus \cdots \oplus \mathbb{C}\pi_s$$

with the primitive idempotent π_i or E_i as the idempotent projection from $\mathbb{C}Q$ onto the d_i^2-dimensional subspace $\mathrm{Mat}_{d_i}(\mathbb{C})$. Thus the multiplicities are $f_i = d_i^2$ for $1 \leqslant i \leqslant s$. It turns out that for $1 \leqslant i, j \leqslant s$, the basic character value ψ_{ij} is the value of the irreducible group character χ_i (the character of the irreducible module V_i) at elements of the group conjugacy class $C_j(e)$. The character table of the symmetric group S_3 of degree 3 is

$$\Psi = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -1 & 0 \end{bmatrix}. \tag{2.6}$$

As usual for groups, the entries $\sqrt{f_i}$ in the first column, namely the dimensions d_i of the irreducible modules, are integral.

2.3.3. *Subtraction modulo* 4. By Exercise 1.4.5 (4), the multiplication group G of the quasigroup $Q = (\mathbb{Z}/4\mathbb{Z}, -)$ of the integers modulo 4 under subtraction is the 8-element dihedral group D_4 of degree 4. The adjacency matrices are

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix},$$

corresponding to the three respective relations of equality, diametric opposition, and adjacency in the square graph of Figure 3.

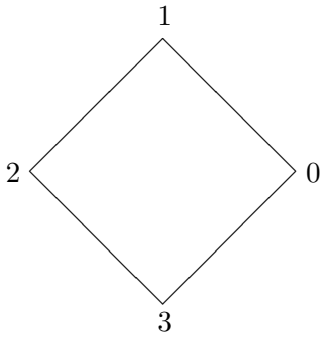


Figure 3: The square.

The centraliser ring $V(G,Q)$ is generated as a commutative complex algebra by the element $X = A_3$, since $A_3^2 = 2A_1 + 2A_2$, so $A_2 = \frac{1}{2}X^2 - 1$ (and, of course, $A_1 = 1$). Now $A_3^3 = 4A_3$, so

$$\begin{aligned} V(G,Q) &\cong \mathbb{C}[X]/\langle X^3 - 4X\rangle \\ &\cong \mathbb{C}[X]/\langle X-2\rangle \oplus \mathbb{C}[X]/\langle X+2\rangle \oplus \mathbb{C}[X]/\langle X\rangle\,. \end{aligned}$$

The isomorphism is obtained by the First Isomorphism Theorem for $\mathbb{C}$-algebras from the homomorphism

$$\mathbb{C}[X] \to \mathbb{C}^3;\quad f(X) \mapsto \big(f(2), f(-2), f(0)\big)\,.$$

Thus in the isomorphism $V(G,Q) \cong \mathbb{C}^3$,

$$\begin{aligned} A_1 = 1 &\mapsto (1,1,1)\,; \\ A_2 = \frac{X^2}{2} - 1 &\mapsto (1,1,-1)\,; \\ A_3 = X &\mapsto (2,-2,0)\,. \end{aligned}$$

The idempotent $E_1 = J/4 = (A_1 + A_2 + A_3)/4$, mapping to $(1,0,0)$, is projection onto the first component corresponding to $f(2)$. Let E_2 project to the second component $f(-2)$, and E_3 to the third $f(0)$. Then

$$\Xi = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 2 & -2 & 0 \end{bmatrix} \quad \text{and} \quad H = \begin{bmatrix} 1/4 & 1/4 & 1/4 \\ 1/4 & 1/4 & -1/4 \\ 1/2 & -1/2 & 0 \end{bmatrix}\,,$$

so $f_1 = f_2 = 1$ and $f_3 = 2$ — Exercise 2.2.5 (2). Finally

$$\Psi = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ \sqrt{2} & -\sqrt{2} & 0 \end{bmatrix} \tag{2.7}$$

— compare with the character table (2.6) of the symmetric group S_3.

2.3.4. *Exercises.*

1. Compute the character table of the Klein 4-group.
2. Compute the character table of the quasigroup $Q = (\mathbb{Z}/5\mathbb{Z}, -)$ of integers modulo 5 under subtraction. In your answer, use trigonometric functions rather than radicals as much as you can.

3. The character table (2.7) has the irrational entry $\sqrt{2}$ in the first column. Does the character table of a finite, nonassociative quasigroup always have at least one irrational entry somewhere in the first column?

4. (a) Using Exercise 1.5.6 (2) or otherwise, construct a central rank 2 quasigroup of order 5.
   (b) From the existence of non-central rank 2 quasigroups of order 5, conclude that the character table of a finite quasigroup Q cannot determine whether Q is central or not.
   (c) Since $\Psi(Q^2)$ does determine the centrality of Q [7, Cor. 7.2], conclude that $\Psi(Q)$ does not determine $\Psi(Q^2)$.

5. (a) Give an example of two isotopic quasigroups with distinct character tables.
   (b) Show that centrally isotopic quasigroups have the same character table.

3. Permutation representations

3.1. Cosets.

3.1.1. *Symmetry.* Consider a group Q, for example the group D_4 of symmetries of the square as illustrated in Figure 3. Let P be a *point stabiliser*, a subgroup of Q. In the square example, take the subgroup P to be the stabiliser $\{(0), (1\ 3)\}$ of the vertex 0. The subgroup P determines a (*group*) *homogeneous space*, the set

$$P\backslash Q = \{Px \mid x \in Q\}$$

of cosets. The cosets (including P itself) are considered as *points* of the homogeneous space. The group Q acts on the homogeneous space $P\backslash Q$ by

$$R_{P\backslash Q}(q) : P\backslash Q \to P\backslash Q; \quad Px \mapsto Pxq \tag{3.1}$$

for q in Q. Now in Figure 3, for a vertex v of the square, choose an element x of Q taking 0 to v. Each vertex v of the square corresponds to the coset Px, the set of permutations taking 0 to $0x = v$. The action of Q on the square is then similar (in the technical sense!) to the action of Q on the homogeneous space $P\backslash Q$.

3.1.2 *Cosets.* As described in §3.1.1., symmetry reduces to the action of a group on a homogeneous space, the set of cosets of a subgroup. Our goal is to examine symmetry within the theory of quasigroups. Let P be a subquasigroup of a quasigroup Q. The (*right*) *cosets* of P in Q are defined as the orbits of the relative left multiplication group $\mathrm{LMlt}_Q P$ (compare §1.4.2) in its action on Q. The (*quasigroup*) *homogeneous space* $P\backslash Q$ is defined as the set of cosets of P in Q. For a finite quasigroup Q, the *type* of a homogeneous space $P\backslash Q$ is the partition of $|P\backslash Q|$ given by the sizes of the orbits of the relative left multiplication group of P in Q. The type of a homogeneous space $P\backslash Q$, or the space itself, is said to be *uniform* if all the parts of the partition are equal.

If P is a subgroup of a group Q, then the right cosets

$$Px = \{px \mid p \in P\}$$

in the group sense are exactly the right cosets $x\mathrm{LMlt}_Q P$ in the quasigroup sense. Now in the group case, the maps (3.1) are bijections between the various right cosets. Thus for a finite group Q, every homogeneous space $P\backslash Q$ is uniform.

3.1.3. *The quasigroup case.* To see what can happen in the quasigroup case, it is helpful to consider an example: the quasigroup Q whose multiplication table is displayed in Figure 1. Let P be the singleton subquasigroup $\{1\}$. Note that $\mathrm{LMlt}_Q P$ is the cyclic subgroup of $Q!$ generated by $(23)(456)$. Thus

$$P\backslash Q = \big\{\{1\}, \{2,3\}, \{4,5,6\}\big\}. \tag{3.2}$$

The space (3.2) is certainly not uniform, its type being the partition $3+2+1$ of 6. On the other hand, the homogeneous space determined by the subquasigroup $N = \{1,2,3\}$ is

$$N\backslash Q = \big\{\{1,2,3\}, \{4,5,6\}\big\}.$$

This space is uniform, of type $3+3$.

In a general quasigroup Q, the *regular* homogeneous space is defined as $\varnothing\backslash Q$. The relative left multiplication group of the empty subquasigroup just consists of the identity permutation, so the regular space is the set $\big\{\{x\} \bigm| x \in Q\big\}$ of singletons, isomorphic to (and often identified with) the set Q itself. If Q is a group or a *loop* (a quasigroup with identity element 1 satisfying $1 \cdot x = x = x \cdot 1$), the regular space may also be realised as the homogeneous space $\{1\}\backslash Q$.

3.1.4. *Exercises.*

1. Let Q be the quasigroup of integers modulo 4 under subtraction. For each subquasigroup P of Q, determine the homogeneous space $P\backslash Q$ and its type.

2. Let P be a subgroup of a group Q. Show that the orbits of the relative right multiplication group $\mathrm{RMlt}_Q P$ of P in Q are the left cosets of P.

3. Let P be a subgroup of a group Q. Show that the orbits of the relative multiplication group $\mathrm{Mlt}_Q P$ of P in Q are the double cosets PxP of P.

4. Let e be an element of a quasigroup Q with multiplication group G, and let G_e be the stabiliser of e in G. Show that the double cosets $G_e x G_e$ of G_e in G are in 1–1 correspondence with the quasigroup conjugacy classes of Q.

3.2. Action on homogeneous spaces.

3.2.1. *Markov matrices.* If q is an element of a group Q with subgroup P, the action of q on the homogeneous space $P\backslash Q$ is given by the map $R_{P\backslash Q}(q)$ of (3.1). Under right multiplication by q in Q, each element of a given coset Px is taken to the same coset Pxq.

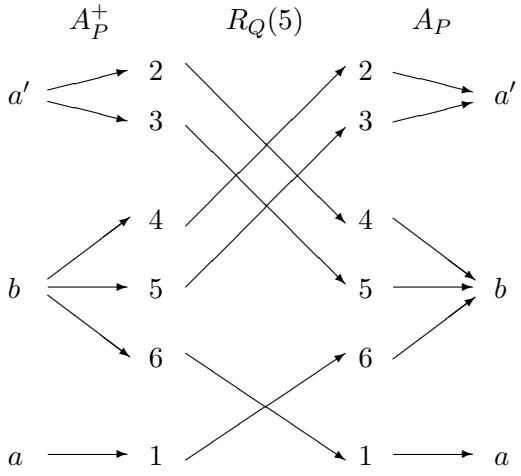


Figure 4: The action $R_{P\backslash Q}(5)$.

Now consider the quasigroup Q whose multiplication table is given in Figure 1, with the subquasigroup $P = \{1\}$. The homogeneous space $P\backslash Q$ is displayed in (3.2), and again on each side of Figure 4. Here the respective cosets are labelled as $a = \{1\}$, $a' = \{2, 3\}$, and $b = \{4, 5, 6\}$. Under the action of right multiplication by the element 5 of Q, the elements of the coset b are not all sent to the same coset. The elements 4 and 5 go to a', while 6 goes to a. The action is described by the Markov matrix

$$\begin{array}{c} \\ a \\ a' \\ b \end{array} \begin{array}{c} \begin{array}{ccc} a & a' & b \end{array} \\ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ \frac{1}{3} & \frac{2}{3} & 0 \end{bmatrix} \end{array} = R_{P\backslash Q}(5) \tag{3.3}$$

indexed by the points of the homogeneous space. Under the uniform probability distribution on Q, and hence on each coset, an element of the coset b is sent to a with probability $\frac{1}{3}$, and to a' with probability $\frac{2}{3}$. The Markov chain specified by the Markov matrix $R_{P\backslash Q}(5)$ has the homogeneous space $P\backslash Q = \{a, a', b\}$ as its state space. Each element of the state space on the left of Figure 4 has a uniform chance of transitioning along each of the arrows leading from it. After that, its path through Q and back to the state space $P\backslash Q$ is uniquely specified.

3.2.2. *Moore-Penrose inverses.* The analytical specification of Markov matrices such as (3.3) relies on the concept of the (*Moore-*)*Penrose inverse* or *pseudoinverse* A^+ of a (not necessarily square) complex matrix A. This is the unique matrix A^+ satisfying the equations

$$\begin{aligned} AA^+A &= A\ , \\ A^+AA^+ &= A^+, \\ (A^+A)^* &= A^+A\,, \\ (AA^+)^* &= AA^+ \end{aligned}$$

in which * denotes the conjugate transpose [4].

For a subquasigroup P of a finite, nonempty quasigroup Q, let A or A_P denote the incidence matrix for the homogeneous space $P\backslash Q$ of Q. This is a rectangular matrix, with rows indexed by Q and columns indexed by $P\backslash Q$. An entry indexed by an element q of Q and a coset X in $P\backslash Q$ is 1 if q lies in X, and 0 otherwise. The pseudoinverse A^+ or A_P^+ has its rows indexed by $P\backslash Q$ and columns indexed by Q. An entry indexed by a coset X in $P\backslash Q$ and an element q of Q is $|X|^{-1}$ if q lies in X, and 0 otherwise. For

the singleton subquasigroup $P = \{1\}$ of the quasigroup Q from Figure 1, these matrices become

$$A_P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} \text{ and } A_P^+ = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix} . \tag{3.4}$$

— compare the right and left sides of Figure 4.

3.2.3. *Action matrices.* If q is an element of a finite quasigroup Q with subquasigroup P, the action of q on the homogeneous space $P\backslash Q$ is given by the Markov matrix

$$R_{P\backslash Q}(q) = A_P^+ R_Q(q) A_P \tag{3.5}$$

obtained using the incidence matrix A_P described in §3.2.2. The matrix (3.5) is called the *action matrix* of the element q on the homogeneous space $P\backslash Q$. Note how Figure 4 illustrates the composition of the action matrix $R_{P\backslash Q}(5)$ in the example under consideration. If Q is a finite group, then (3.5) recovers the permutation matrix describing the action (3.1) of q on $P\backslash Q$ — Exercise 3.2.4 (4).

3.2.4. *Exercises.*

1. Confirm that the matrices in (3.4) are mutual pseudoinverses.
2. Let P be a subquasigroup of positive order m in a quasigroup Q of finite order n. Suppose $|P\backslash Q| = 2$. Show that for an element q of Q,

$$R_{P\backslash Q}(q) = \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \text{if } q \in P\,; \\ \\ \begin{bmatrix} 0 & 1 \\ \frac{m}{n-m} & \frac{n-2m}{n-m} \end{bmatrix} & \text{otherwise.} \end{cases}$$

3. (a) If $(Q, \cdot)$ is a quasigroup, show that $(Q, \backslash)$ is a quasigroup.
   (b) Show that the multiplication table of a finite quasigroup $(Q, \cdot)$ is the formal sum $\sum_{q \in Q} q R_S(q)$ of action matrices of the regular homogeneous space S of the quasigroup $(Q, \backslash)$.

4. If q is an element of a finite group Q with subgroup P, show that (3.5) recovers the permutation matrix describing the action (3.1) of q on $P\backslash Q$.

4. Modules

4.1. Groups in categories.

4.1.1. *Split extensions.* If Q is a group, a *Q-module* M is an abelian group $(M, +, 0)$ with a group homomorphism

$$Q \to \mathrm{Aut}(M, +, 0); \quad q \mapsto (m \mapsto mq)$$

from Q to the automorphism group of the abelian group $(M, +, 0)$. Since the composition of automorphisms is associative, this definition gives no possibility of extension to general quasigroups. Instead, it will be recast in more suitable form. Given a Q-module M, the *split extension* $E = Q \ltimes M$ is the set $Q \times M$ equipped with the product

$$(q_1, m_1)(q_2, m_2) = (q_1 q_2, m_1 q_2 + m_2)\,. \tag{4.1}$$

The split extension comes equipped with the projection

$$p : E \to Q; \quad (q, m) \mapsto q \tag{4.2}$$

and the insertion η_Q or

$$\eta : Q \to E; \quad q \mapsto (q, 0), \tag{4.3}$$

both of which are group homomorphisms.

4.1.1. *Slice categories.* If Q is an object of a category $\mathbf{C}$, an object in the *slice category* (or "comma category") $\mathbf{C}/Q$ is a $\mathbf{C}$-morphism $p : E \to Q$. For example, the projection (4.2) from the split extension is an object in the slice category $\mathbf{Gp}/Q$ of groups over Q, with $\mathbf{Gp}$ as the category of groups. A morphism in a slice category $\mathbf{C}/Q$ between two objects $p_1 : E_1 \to Q$ and $p_2 : E_2 \to Q$ is a $\mathbf{C}$-morphism $f : E_1 \to E_2$ for which the diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{f} & E_2 \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ Q & \xrightarrow[1_Q]{} & Q \end{array}$$

commutes. Such $\mathbf{C}/Q$-morphisms are often just denoted simply by the $\mathbf{C}$-morphism $f : E_1 \to E_2$. The identity morphism $1_Q : Q \to Q$ is the terminal object of $\mathbf{C}/Q$. If the category $\mathbf{C}$ has pullbacks, then the slice category $\mathbf{C}/Q$ has finite products. The product of two objects $p_1 : E_1 \to Q$ and $p_2 : E_2 \to Q$ is the pullback

$$\begin{array}{ccc} E_1 \times_Q E_2 & \xrightarrow{\pi_2} & E_2 \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ E_1 & \xrightarrow[p_1]{} & Q \end{array} \tag{4.4}$$

with the composite morphism $\pi_1 p_1 = \pi_2 p_2$ to Q. Recall that for categories of sets (possibly with algebraic structure), the pullback $E_1 \times_Q E_2$ is realised as $\{(e_1, e_2) \in E_1 \times E_2 \mid e_1 p_1 = e_2 p_2\}$, with the projections $\pi_i : E_1 \times_Q E_2 \to E_i;\ (e_1, e_2) \mapsto e_i$.

4.1.2. *Abelian groups.* The category **Set** of sets has all finite products, including the empty product as the terminal object T (the codomain of a unique morphism from each object). An abelian group $(A, +, 0)$ is an object A of **Set** with an addition morphism $+ : A^2 \to A$, a negation morphism $-1 : A \to A$, and a zero morphism $0 : A^0 \to A$ from the terminal object $T = A^0$, for which diagrams such as

$$\begin{array}{ccc} A & \xrightarrow{(1,-1)} & A^2 \\ \downarrow & & \downarrow{\scriptstyle +} \\ A^0 & \xrightarrow[0]{} & A \end{array} \tag{4.5}$$

(expressing the identities for abelian groups, in this case $a + (-a) = 0$) commute. An *abelian group A in a category* $\mathbf{C}$ with finite products is an object A of $\mathbf{C}$ with an addition morphism $+ : A^2 \to A$, a negation morphism $-1 : A \to A$, and a zero morphism $0 : A^0 \to A$ from the terminal object $T = A^0$, for which the diagrams (4.5) commute.

If M is a module over a group Q, the projection $p : E \to Q$ (4.2) is an abelian group in the slice category $\mathbf{Gp}/Q$. The addition is

$$+ : E \times_Q E \to E; \quad \big((q, m_1), (q, m_2)\big) \mapsto (q, m_1 + m_2)$$

and the zero morphism is given by the group homomorphism η of (4.3), determining the morphism

$$\begin{array}{ccc} Q & \xrightarrow{\eta} & E \\ {\scriptstyle 1_Q}\downarrow & & \downarrow{\scriptstyle p} \\ Q & \xrightarrow[1_Q]{} & Q \end{array} \tag{4.6}$$

from the terminal object $1_Q : Q \to Q$ of the slice category $\mathbf{Gp}/Q$.

4.1.3. *Modules.* Given a module M over a group Q, the split extension $p : Q \ltimes M \to Q$ (4.2) is an abelian group in the slice category $\mathbf{Gp}/Q$. For q in Q, the conjugation action of the element q^η on the normal subgroup $p^{-1}\{1\}$ of $Q \ltimes M$ is given by

$$(q,0)\backslash(1,m)(q,0) = (mq,0), \tag{4.7}$$

thereby reflecting the action of Q on the module M.

Conversely, suppose that $p : E \to Q$ is an abelian group in the slice category $\mathbf{Gp}/Q$, with addition $+ : E \times_Q E \to E$ and zero morphism as in (4.6). Let M denote the inverse image $p^{-1}\{1\}$ of the identity element 1 of Q under p. For elements m_1 and m_2 of M, the pair (m_1, m_2) lies in the pullback $E \times_Q E$, and the image $m_1 + m_2$ of the pair (m_1, m_2) under the addition again lies in M. In this way, the set M receives an abelian group structure. In analogy with (4.7), each element q of Q acts on M by

$$q : m \mapsto q^\eta \backslash m q^\eta,$$

making M a right Q-module.

In summary, it is seen that modules over a group Q are equivalent to abelian groups $p : E \to Q$ in the slice category $\mathbf{Gp}/Q$ of groups over Q. It is this module concept which allows itself to be extended to arbitrary quasigroups (§4.2.1).

4.1.5. *Exercises.*

1. Using the definition (4.1) of the product in the split extension, verify the formula (4.7).

2. The group $\mathbb{Z}/3\mathbb{Z}$ of integers modulo 3 acts as a nontrivial group of automorphisms of the Klein 4-group. The corresponding split extension is a group of order 12. Can you recognise this group?

3. Produce a full set of commuting diagrams like (4.5) to define abelian groups (associativity, commutativity, etc.).

4.2. Modules over quasigroups

4.2.1. *Quasigroup modules.* Let $\mathbf{V}$ be a *variety* of quasigroups, a class of quasigroups closed under homomorphic images, subquasigroups, and products. Equivalently (by Birkhoff's Theorem [7, IV Th. 2.3.3]), V is the class of all quasigroups satisfying a given set of identities. As examples, consider the variety $\mathbf{G}$ of associative quasigroups (§1.2.1), the variety $\mathbf{A}$ of abelian quasigroups, the variety $\mathbf{Q}$ of all quasigroups, or the variety **STS** of Steiner triple systems — idempotent (1.3) and totally symmetric (1.4) quasigroups (§1.3). The variety $\mathbf{V}$ may also be considered as a category. The class of quasigroups is the object class of the category, while the morphisms are the quasigroup homomorphisms between the quasigroups in the class. As a category, $\mathbf{V}$ has all limits and colimits, in particular all pullbacks, products and coproducts (free products) [7, IV §2.2].

For a quasigroup Q in $\mathbf{V}$, a *Q-module* in the variety $\mathbf{V}$ is defined as an abelian group $p : E \to Q$ in the slice category $\mathbf{V}/Q$ of $\mathbf{V}$-quasigroups over Q. If Q is a group, it is apparent from §4.1.4 that Q-modules in the variety $\mathbf{G}$ are equivalent to Q-modules in the usual sense.

Given two Q-modules $p_i : E_i \to Q$ in $\mathbf{V}$ (with $i = 1, 2$), a Q-module homomorphism is a $\mathbf{V}/Q$-morphism $f : E_1 \to E_2$ that commutes with the abelian group structures: $0f = 0$, $(-1)f = f(-1)$, and $+f = (f \times_Q f)+$. The Q-modules in $\mathbf{V}$ form a category $\mathbb{Z} \otimes \mathbf{V}/Q$.

4.2.2. *Universal multiplication groups.* The definition of modules over a quasigroup given in §4.2.1 is rather abstract. A direct description depends on certain groups associated with a quasigroup Q in a variety $\mathbf{V}$. Let $Q[X]_{\mathbf{V}}$ or $Q[X]$ be the free product (coproduct) of Q in $\mathbf{V}$ with the free quasigroup in $\mathbf{V}$ on a single generator X. The $\mathbf{V}$-quasigroup $Q[X]$ is analogous to a ring of polynomials, and is characterised by a similar universal property: for every quasigroup E in $\mathbf{V}$ that is the codomain of a $\mathbf{V}$-morphism $\eta : Q \to E$, and for every element x of E, there is a unique quasigroup homomorphism $Q[X] \to E$ restricting to η on the subquasigroup Q of $Q[X]$, and mapping the indeterminate X to x in E.

The *universal multiplication group* $\widetilde{G}$ or $U(Q, \mathbf{V})$ of Q in $\mathbf{V}$ is the relative multiplication group of Q in $Q[X]$. If Q is a subquasigroup of a quasigroup E in $\mathbf{V}$, the relative multiplication group of Q in E is a quotient of $\widetilde{G}$. In particular, the combinatorial multiplication group G of Q is a quotient of $\widetilde{G}$. In this way $\widetilde{G}$ acts on Q, and an element e of Q has its stabiliser in $\widetilde{G}$, the *universal stabiliser* $\widetilde{G}_e$.

4.2.3. *Examples of universal multiplication groups.*

1. The universal multiplication group $U(Q, \mathbf{Q})$ of a quasigroup Q in the variety $\mathbf{Q}$ of all quasigroups is the free group on the set $L(Q) + R(Q)$, the disjoint union of two copies of the set Q.

2. The universal multiplication group $U(Q, \mathbf{G})$ of a group Q in the variety $\mathbf{G}$ of all associative quasigroups is the direct square $Q \times Q$. Compare with §1.4.4, where the combinatorial multiplication group of Q is obtained from the direct square $Q \times Q$ by dividing out the diagonal copy of the centre $Z(Q)$.

3. For an abelian group Q in the variety $\mathbf{A}$ of all abelian quasigroups, $U(Q, \mathbf{A}) \cong Q$ — Exercise 4.2.6 (1).

4. The universal multiplication group $U(Q, \mathbf{STS})$ of a Steiner triple system Q in the variety $\mathbf{STS}$ of all Steiner triple systems is the free product (in the variety of groups) of $|Q|$ copies of the cyclic group of order 2. It is also described as the set $Q^{\times}$ of words in the alphabet Q without adjacent letters repeated. Each letter q from Q corresponds to $R(q)$ in $U(Q, \mathbf{STS})$. The product in the group is obtained from concatenation of words followed by cancellation of adjacent pairs of identical letters. For example, $q_1q_2q_3 \cdot q_3q_2 = q_1$. The identity element is the empty word.

4.2.4. *The Fundamental Theorem.* Let Q be a quasigroup, considered in the variety $\mathbf{Q}$ of all quasigroups. Let $\widetilde{G}$ be the universal multiplication group $U(Q, \mathbf{Q})$ of Q in $\mathbf{Q}$. Let e be an element of Q, with corresponding universal stabiliser $\widetilde{G}_e$. The *Fundamental Theorem of Quasigroup Representations* [6, Th. 10.1] states that modules over the quasigroup Q are equivalent to modules over the group $\widetilde{G}_e$.

Suppose that $p : E \to Q$ is an abelian group in $\mathbf{Q}/Q$. The inverse image $M = p^{-1}\{e\}$ forms an abelian group under the restriction of the addition morphism $+ : E \times_Q E \to E$. The zero morphism $0 : Q \to E$ embeds Q in E. The relative multiplication group $\mathrm{Mlt}_E(Q)$ is a quotient of $\widetilde{G}$. Then $\widetilde{G}$ acts on E via this quotient. The action restricts to an action of the universal stabilizer $\widetilde{G}_e$ on M. This action consists of automorphisms of the abelian group M. Thus the Q-module $p : E \to Q$ yields a $\widetilde{G}_e$-module $M = p^{-1}\{e\}$.

Conversely, for a $\widetilde{G}_e$-module M, a corresponding abelian group in $\mathbf{Q}/Q$ has to be constructed. For each element g of $\widetilde{G}$ and q of Q, there is a unique

element $s(q,g)$ of $\widetilde{G}_e$ such that

$$s(q,g)\rho(e,qg) = \rho(e,q)g \tag{4.8}$$

— Exercise 1.4.5 (5). Note that

$$s(e,g_e) = g_e \tag{4.9}$$

for g_e in $\widetilde{G}_e$. Now consider the $\widetilde{G}$-set $E = M \times Q$ with action

$$(m,q)g = \big(ms(q,g), qg\big)\,. \tag{4.10}$$

— compare Exercise 4.2.6 (2). Define local abelian group structures on E by

$$(m_1,q) - (m_2,q) = (m_1 - m_2, q) \tag{4.11}$$

for $m_i \in M$ and $q \in Q$. Let $\pi : E \to Q$ be projection onto the second factor. Then a quasigroup structure is defined on E by

$$\begin{cases} a \cdot b = aR(b\pi) + bL(a\pi)\,; \\ a/b = (a - bL(a\pi/b\pi))R(b\pi)^{-1}\,; \\ a\backslash b = (b - aR(a\pi\backslash b\pi))L(a\pi)^{-1}\,. \end{cases} \tag{4.12}$$

With this structure, $\pi : E \to Q$ becomes an abelian group object in the category $\mathbf{Q}/Q$. Note that by (4.9), the $\widetilde{G}_e$-modules M and $\pi^{-1}\{e\}$ are isomorphic.

4.2.5. *Differential calculus.* The Fundamental Theorem of Quasigroup Representations provides a *differentiation* process applying to quasigroup words and identities. Fix a quasigroup Q with element e and universal multiplication group $\widetilde{G} = U(Q,\mathbf{Q})$ in the variety of all quasigroups. The category of $\widetilde{G}_e$-modules is generated by the integral group algebra $\mathbb{Z}\widetilde{G}_e$, considered as a $\widetilde{G}_e$-module. Under the equivalence given by the Fundamental Theorem, the corresponding object is the Q-module $\pi : \mathbb{Z}\widetilde{G}_e \times Q \to Q$. Using (4.12), the action of a quasigroup word $x_1 \dots x_n w$ on this object is given by

$$(m_1,q_1)\dots(m_n,q_n)w = \Big(\sum_{h=1}^{n} m_h \rho(e,q_h)\frac{\partial w}{\partial x_h}\rho(e,w)^{-1}, q_1 \dots q_n w\Big) \tag{4.13}$$

for certain elements

$$\frac{\partial w}{\partial x_h} = \frac{\partial w}{\partial x_h}(q_1,\dots,q_n) \tag{4.14}$$

of $\mathbb{Z}\widetilde{G}$. Notational conventions similar to those of calculus are used. The functions

$$\frac{\partial w}{\partial x_h} : Q^n \to \mathbb{Z}\widetilde{G}; (q_1, \ldots, q_n) \mapsto \frac{\partial w}{\partial x_h}(q_1, \ldots, q_n) \tag{4.15}$$

for $1 \leqslant h \leqslant n$ are known as the *partial derivatives* of the quasigroup word $x_1 \ldots x_n w$. They are computed inductively using the parsing of the word $x_1 \ldots x_n w$. For $xw = x$, (4.13) simply gives

$$\frac{\partial x}{\partial x} = 1 \,. \tag{4.16}$$

More generally, the derivatives of the projection $x_1 \ldots x_i \ldots x_n \pi_i = x_i$ are given by

$$\frac{\partial \pi_i}{\partial x_j} = \delta_{ij} \,.$$

For $x_1 \ldots x_k x_{k+1} \ldots x_{k+l} w = x_1 \ldots x_k u \cdot x_{k+1} \ldots x_{k+l} v$, (4.12) and (4.13) give

$$\begin{aligned}
(m_1, q_1) \ldots (m_{k+l}, q_{k+l}) w &= \Big(\sum_{h=1}^{k+l} m_h \rho(e, q_h) \frac{\partial w}{\partial x_h} \rho(q_h, w)^{-1}, w \Big) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1}, u \Big) \cdot \Big(\sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1}, v \Big) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1}, u \Big) R(q_{k+1} \ldots q_{k+l} v) \\
&\quad + \Big(\sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1}, q_{k+1} \ldots q_{k+l} v \Big) L(q_1 \ldots q_k u) \\
&= \Big(\sum_{i=1}^{k} m_i \rho(e, q_i) \frac{\partial u}{\partial x_i} \rho(e, u)^{-1} s\big(u, R(v)\big) + \\
&\qquad \sum_{j=k+1}^{k+l} m_j \rho(e, q_j) \frac{\partial v}{\partial x_j} \rho(e, v)^{-1} s\big(v, L(u)\big), w \Big) \,,
\end{aligned}$$

leading to the *Product Rules*

$$\frac{\partial w}{\partial x_i} = \frac{\partial u}{\partial x_i} R(x_{k+1} \ldots x_{k+l} v)$$

for $1 \leqslant i \leqslant k$ and

$$\frac{\partial w}{\partial x_j} = \frac{\partial v}{\partial x_j} L(x_1 \dots x_k u)$$

for $k < j \leqslant k + l$. These may be summarized as

$$\frac{\partial (u \cdot v)}{\partial x_i} = \frac{\partial u}{\partial x_i} R(v)\,; \tag{4.17}$$

$$\frac{\partial (u \cdot v)}{\partial x_j} = \frac{\partial v}{\partial x_j} L(u)\,. \tag{4.18}$$

Note that if there are repeated arguments in the word w, say $q_i = q_j$ with $i \leqslant k < j$, then $\partial w/\partial x_i$ will include the sum of $\partial(u \cdot v)/\partial x_i$ as given by (4.17) and $\partial(u \cdot v)/\partial x_j$ as given by (4.18).

4.2.6. *Exercises.*

1. Let Q be an abelian group, considered in the variety $\mathbf{A}$ of abelian quasigroups.

   (a) Show that $Q[X]_{\mathbf{A}} = Q \oplus \mathbb{Z}$.

   (b) Show that $U(Q, \mathbf{A}) \cong Q$.

2. In the context of §4.2.4, let M be a $\widetilde{G}_e$-module.

   (a) Show that $s(q, g)s(qg, h) = s(q, gh)$ for $q \in Q$ and $g, h \in \widetilde{G}$.

   (b) Show that (4.10) does give a group action: for m in M, q in Q and g_1, g_2 in $\widetilde{G}$, show $(m, q)(g_1 g_2) = \big((m, q)g_1\big)g_2$.

3. In the context of §4.2.4, let M be a $\widetilde{G}_e$-module. Show that (4.12) defines a quasigroup structure on $E = M \times Q$.

4. Show that

$$\frac{\partial x^2}{\partial x} = R(x) + L(x)\,.$$

5. For nonassociative powers x^l and x^r, show that

$$\frac{\partial (x^l \cdot x^r)}{\partial x} = \frac{\partial x^l}{\partial x} R(x) + \frac{\partial x^r}{\partial x} L(x)\,.$$

   Conclude that nonassociative powers of x are indexed by their derivatives, which are noncommutative polynomials in $R(x)$ and $L(x)$ — the "index ψ-polynomials" of [3].

6. Derive the *Right Quotient Rules*

$$\frac{\partial(u/v)}{\partial x_i} = \frac{\partial u}{\partial x_i} R(v)^{-1};$$
$$\frac{\partial(u/v)}{\partial x_j} = -\frac{\partial v}{\partial x_j} L(u/v) R(v)^{-1};$$

and the *Left Quotient Rules*

$$\frac{\partial(u\backslash v)}{\partial x_i} = -\frac{\partial u}{\partial x_i} R(u\backslash v) L(u)^{-1};$$
$$\frac{\partial(u\backslash v)}{\partial x_j} = \frac{\partial v}{\partial x_j} L(u)^{-1}.$$

7. Let Q be a group, with identity element e. Take $\widetilde{G}$ to be the universal multiplication group $U(Q, \mathbf{G})$ of Q in the variety $\mathbf{G}$ of associative quasigroups. Show that Q-modules are equivalent to $\widetilde{G}_e$-modules.

References

[1] **O. Chein et al.:** *Quasigroups and Loops: Theory and Applications*, Heldermann, Berlin, 1990.

[2] **G. Higman, B.H. Neumann and H. Neumann:** *Embedding theorems for groups*, J. London Math. Soc. **24** (1949), 247 – 254.

[3] **H. Minc:** *Index polynomials and bifurcating root-trees*, Proc. Roy. Soc. Edin., A **65** (1957), 319 – 341.

[4] **R. Penrose:** *A generalised inverse for matrices*, Proc. Camb. Phil. Soc. **51** (1955), 406 – 413.

[5] **J. D. H. Smith:** *Mal'cev Varieties*, Springer, Berlin, 1976.

[6] **J. D. H. Smith:** *An Introduction to Quasigroups and their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

[7] **J. D. H. Smith and A. B. Romanowska:** *Post-Modern Algebra*, Wiley, New York, NY, 1999.

Department of Mathematics
Iowa State University Ames, Iowa 50011-2064
U.S.A.
E-mail: jdhsmith@math.iastate.edu
http://www.orion.math.iastate.edu/jdhsmith/

Received April 24, 2007

Quasigroups and Related Systems **15** (2007), 141 – 168

Gyrogroups, the grouplike loops in the service of hyperbolic geometry and Einstein's special theory of relativity

Abraham A. Ungar

Abstract

In this era of an increased interest in loop theory, the Einstein velocity addition law has fresh resonance. One of the most fascinating aspects of recent work in Einstein's special theory of relativity is the emergence of special grouplike loops. The special grouplike loops, known as *gyrocommutative gyrogroups*, have thrust the Einstein velocity addition law, which previously has operated mostly in the shadows, into the spotlight. We will find that Einstein (Möbius) addition is a gyrocommutative gyrogroup operation that forms the setting for the Beltrami-Klein (Poincaré) ball model of hyperbolic geometry just as the common vector addition is a commutative group operation that forms the setting for the standard model of Euclidean geometry. The resulting analogies to which the grouplike loops give rise lead us to new results in (i) hyperbolic geometry; (ii) relativistic physics; and (iii) quantum information and computation.

1. Introduction

The author's two recent books with the ambitious titles, *"Analytic hyperbolic geometry: Mathematical foundations and applications"* [56], and *"Beyond the Einstein addition law and its gyroscopic Thomas precession: The theory of gyrogroups and gyrovector spaces"* [53, 66], raise expectations for novel applications of special grouplike loops in hyperbolic geometry and in relativistic physics. Indeed, these books lead their readers to see what some

2000 Mathematics Subject Classification: 20N05, 51P05, 83A05
Keywords: Grouplike loops, gyrogroups, gyrovector spaces, hyperbolic geometry, special relativity.

special grouplike loops have to offer, and thereby give them a taste of loops in the service of the hyperbolic geometry of Bolyai and Lobachevsky and the special relativity theory of Einstein.

Seemingly structureless, Einstein's relativistic velocity addition is neither commutative nor associative. Einstein's failure to recognize and advance the rich, grouplike loop structure [52] that regulates his relativistic velocity addition law contributed to the eclipse of his velocity addition law of relativistically admissible 3-velocities, creating a void that could be filled only with the Lorentz transformation of 4-velocities, along with its Minkowski's geometry.

Minkowski characterized his spacetime geometry as evidence that *pre-established harmony* between pure mathematics and applied physics does exist [42]. Subsequently, the study of special relativity followed the lines laid down by Minkowski, in which the role of Einstein velocity addition and its interpretation in the hyperbolic geometry of Bolyai and Lobachevsky are ignored [5]. The tension created by the mathematician Minkowski into the specialized realm of theoretical physics, as well as Minkowski's strategy to overcome disciplinary obstacles to the acceptance of his reformulation of Einstein's special relativity is skillfully described by Scott Walter in [64].

According to Leo Corry [11], Einstein considered Minkowski's reformulation of his theory in terms of four-dimensional spacetime to be no more than "superfluous erudition". Admitting that, unlike his seemingly structureless relativistic velocity addition law, the Lorentz transformation is an elegant group operation, Einstein is quoted as saying:

> "If you are out to describe truth, leave elegance to the tailor."
>
> Albert Einstein (1879 – 1955)

One might, therefore, suppose that there is a price to pay in mathematical elegance and regularity when replacing ordinary vector addition approach to Euclidean geometry with Einstein vector addition approach to hyperbolic geometry. But, this is not the case since grouplike loops, called *gyrocommutative gyrogroups*, come to the rescue. It turns out that Einstein addition of vectors with magnitudes $< c$ is a gyrocommutative gyrogroup operation and, as such, it possesses a rich nonassociative algebraic and geometric structure. The best way to introduce the gyrocommutative gyrogroup notion that regulates the algebra of Einstein's relativistic velocity addition law is offered by Möbius transformations of the disc [29]. The subsequent transition from Möbius addition, which regulates the Poincaré ball

model of hyperbolic geometry, Fig. 1, to Einstein addition, which regulates the Beltrami-Klein ball model of hyperbolic geometry, Fig. 6, expressed in gyrolanguage, will then turn out to be remarkably simple and elegant [56, 57].

Evidently, the grouplike loops that we naturally call *gyrocommutative gyrogroups*, along with their extension to gyrovector spaces, form a new tool for the twenty-first century exploration of classical hyperbolic geometry and its use in physics.

2. Möbius transformations of the disc

Möbius transformations of the disc $\mathbb{D}$,

$$\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\} \tag{1}$$

of the complex plane $\mathbb{C}$ offer an elegant way to introduce the grouplike loops that we call *gyrogroups*. More than 150 years have passed since August Ferdinand Möbius first studied the transformations that now bear his name [35]. Yet, the rich structure he thereby exposed is still far from being exhausted

Ahlfors' book [1], *Conformal Invariants: Topics in Geometric Function Theory*, begins with a presentation of the Möbius self-transformation of the complex open unit disc $\mathbb{D}$,

$$z \mapsto e^{i\theta}\frac{a+z}{1+\overline{a}z} = e^{i\theta}(a\oplus_{\mathrm{M}} z) \tag{2}$$

$a, z \in \mathbb{D}$, $\theta \in \mathbb{R}$, where $\overline{a}$ is the complex conjugate of a [14, p. 211] [19, p. 185] [36, pp. 177–178]. Suggestively, the *polar decomposition* (2) of Möbius transformation of the disc gives rise to *Möbius addition*, $\oplus_{\mathrm{M}}$,

$$a\oplus_{\mathrm{M}} z = \frac{a+z}{1+\overline{a}z}\,. \tag{3}$$

Naturally, Möbius subtraction, $\ominus_{\mathrm{M}}$, is given by $a\ominus_{\mathrm{M}} z = a\oplus_{\mathrm{M}}(-z)$, so that $z\ominus_{\mathrm{M}} z = 0$ and $\ominus_{\mathrm{M}} z = 0\ominus_{\mathrm{M}} z = 0\oplus_{\mathrm{M}}(-z) = -z$. Remarkably, Möbius addition possesses the *automorphic inverse property*

$$\ominus_{\mathrm{M}}(a\oplus_{\mathrm{M}} b) = \ominus_{\mathrm{M}} a\ominus_{\mathrm{M}} b \tag{4}$$

and the *left cancellation law*

$$\ominus_{\mathrm{M}} a\oplus_{\mathrm{M}}(a\oplus_{\mathrm{M}} z) = z \tag{5}$$

for all $a, b, z \in \mathbb{D}$, [56, 53].

Möbius addition gives rise to the Möbius disc groupoid $(\mathbb{D}, \oplus_{\mathrm{M}})$, recalling that a groupoid $(G, \oplus)$ is a nonempty set, G, with a binary operation, $\oplus$, and that an automorphism of a groupoid $(G, \oplus)$ is a bijective self map f of G that respects its binary operation $\oplus$, that is, $f(a \oplus b) = f(a) \oplus f(b)$. The set of all automorphisms of a groupoid $(G, \oplus)$ forms a group, denoted $Aut(G, \oplus)$.

Möbius addition $\oplus_{\mathrm{M}}$ in the disc is neither commutative nor associative. To measure the extent to which Möbius addition deviates from associativity we define the *gyrator*

$$\mathrm{gyr} : \mathbb{D} \times \mathbb{D} \to Aut(\mathbb{D}, \oplus_{\mathrm{M}}) \tag{6}$$

by the equation

$$\mathrm{gyr}[a, b]z = \ominus_{\mathrm{M}}(a \oplus_{\mathrm{M}} b) \oplus_{\mathrm{M}} \{a \oplus_{\mathrm{M}} (b \oplus_{\mathrm{M}} z)\} \tag{7}$$

for all $a, b, z \in \mathbb{D}$.

The automorphisms

$$\mathrm{gyr}[a, b] \in Aut(\mathbb{D}, \oplus_{\mathrm{M}}) \tag{8}$$

of $\mathbb{D}$, $a, b \in \mathbb{D}$, called gyrations of $\mathbb{D}$, have an important hyperbolic geometric interpretation [63]. Thus, the gyrator in (6) generates the gyrations in (8). In order to emphasize that gyrations of $\mathbb{D}$ are also automorphisms of $(\mathbb{D}, \oplus_{\mathrm{M}})$, as we will see below, they are also called *gyroautomorphisms*.

Clearly, in the special case when the binary operation $\oplus_{\mathrm{M}}$ in (7) is associative, $\mathrm{gyr}[a, b]$ reduces to the trivial automorphism, $\mathrm{gyr}[a, b]z = z$ for all $z \in \mathbb{D}$. Hence, indeed, the self map $\mathrm{gyr}[a, b]$ of the disc $\mathbb{D}$ measures the extent to which Möbius addition $\oplus_{\mathrm{M}}$ in the disc $\mathbb{D}$ deviates from associativity.

One can readily simplify (7) in terms of (3), obtaining

$$\mathrm{gyr}[a, b]z = \frac{1 + a\overline{b}}{1 + \overline{a}b} z \tag{9}$$

$a, b, z \in \mathbb{D}$, so that the gyrations

$$\mathrm{gyr}[a, b] = \frac{1 + a\overline{b}}{1 + \overline{a}b} = \frac{a \oplus_{\mathrm{M}} b}{b \oplus_{\mathrm{M}} a} \tag{10}$$

are unimodular complex numbers. As such, gyrations represent rotations of the disc $\mathbb{D}$ about its center, as shown in (9).

Gyrations are invertible. The inverse, $\mathrm{gyr}^{-1}[a,b] = (\mathrm{gyr}[a,b])^{-1}$, of a gyration $\mathrm{gyr}[a,b]$ is the gyration $\mathrm{gyr}[b,a]$,

$$\mathrm{gyr}^{-1}[a,b] = \mathrm{gyr}[b,a] \tag{11}$$

Moreover, gyrations respect Möbius addition in the disc,

$$\mathrm{gyr}[a,b](c \oplus_{\mathrm{M}} d) = \mathrm{gyr}[a,b]c \oplus_{\mathrm{M}} \mathrm{gyr}[a,b]d \tag{12}$$

for all $a, b, c, d \in \mathbb{D}$, so that gyrations of the disc are automorphisms of the disc, as anticipated in (8).

Identity (10) can be written as

$$a \oplus_{\mathrm{M}} b = \mathrm{gyr}[a,b](b \oplus_{\mathrm{M}} a) \tag{13}$$

thus giving rise to the *gyrocommutative law* of Möbius addition. Furthermore, Identity (7) can be manipulated, by mean of the left cancellation law (5), into the identity

$$a \oplus_{\mathrm{M}} (b \oplus_{\mathrm{M}} z) = (a \oplus_{\mathrm{M}} b) \oplus_{\mathrm{M}} \mathrm{gyr}[a,b]z \tag{14}$$

thus giving rise to the *left gyroassociative law* of Möbius addition.

The gyrocommutative law, (13), and the left gyroassociative law, (14), of Möbius addition in the disc reveal the grouplike structure of Möbius groupoid $(\mathbb{D}, \oplus_{\mathrm{M}})$, that we naturally call a *gyrocommutative gyrogroup*. Taking the key features of Möbius groupoid $(\mathbb{D}, \oplus_{\mathrm{M}})$ as axioms, and guided by analogies with group theory, we thus obtain the following definitions of gyrogroups and gyrocommutative gyrogroups.

Definition 1. (Gyrogroups). A groupoid $(G, \oplus)$ is a *gyrogroup* if its binary operation satisfies the following axioms. In G there is at least one element, 0, called a *left identity*, satisfying

(G1) $\qquad 0 \oplus a = a$

for all $a \in G$. There is an element $0 \in G$ satisfying axiom $(G1)$ such that for each $a \in G$ there is an element $\ominus a \in G$, called a *left inverse* of a, satisfying

(G2) $\qquad \ominus a \oplus a = 0\,.$

Moreover, for any $a, b, c \in G$ there exists a unique element $\mathrm{gyr}[a,b]c \in G$ such that the binary operation obeys the *left gyroassociative law*

(G3) $\qquad a \oplus (b \oplus c) = (a \oplus b) \oplus \mathrm{gyr}[a,b]c\,.$

The map $\mathrm{gyr}[a,b] : G \to G$ given by $c \mapsto \mathrm{gyr}[a,b]c$ is an automorphism of the groupoid $(G, \oplus)$, that is,

(G4) $\qquad \mathrm{gyr}[a,b] \in Aut(G,\oplus)\,,$

and the automorphism $\mathrm{gyr}[a,b]$ of G is called the *gyroautomorphism*, or the *gyration*, of G generated by $a, b \in G$. The operator $\mathrm{gyr} : G \times G \to Aut(G,\oplus)$ is called the gyrator of G. Finally, the gyroautomorphism $\mathrm{gyr}[a,b]$ generated by any $a, b \in G$ possesses the *left loop property*

(G5) $\qquad \mathrm{gyr}[a,b] = \mathrm{gyr}[a\oplus b, b]\,.$

The gyrogroup axioms $(G1)-(G5)$ in Definition 1 are classified into three classes:

(1) The first pair of axioms, $(G1)$ and $(G2)$, is a reminiscent of the group axioms.

(2) The last pair of axioms, $(G4)$ and $(G5)$, presents the gyrator axioms.

(3) The middle axiom, $(G3)$, is a hybrid axiom linking the two pairs of axioms in (1) and (2).

The loop property $(G5)$ turns out to be equivalent to the gyration-free identity

$$x\oplus(y\oplus(x\oplus z)) = (x\oplus(y\oplus x))\oplus z \tag{15}$$

which loop theorists recognize as the *left Bol identity* [46, 47].

As in group theory, we use the notation $a\ominus b = a\oplus(\ominus b)$ in gyrogroup theory as well.

In full analogy with groups, gyrogroups are classified into gyrocommutative and non-gyrocommutative gyrogroups.

Definition 2. (Gyrocommutative gyrogroups). A gyrogroup $(G,\oplus)$ is *gyrocommutative* if its binary operation obeys the *gyrocommutative law*

(G6) $\qquad a \oplus b = \mathrm{gyr}[a,b](b \oplus a)$

for all $a, b \in G$.

Some first gyrogroup theorems, some of which are analogous to group theorems, are presented in [56, Chap. 2]. Thus, in particular, the gyrogroup left identity and left inverse are identical with their right counterparts, and the resulting identity and inverse are unique, as in group theory. Furthermore, the left gyroassociative law and the left loop property are associated with corresponding right counterparts.

A gyrogroup operation $\oplus$ comes with a dual operation, the *cooperation* (or, *co-operation*, for clarity) $\boxplus$ [56, Def. 2.7], given by the equation

$$a \boxplus b = a \oplus \mathrm{gyr}[a, \ominus b]b \tag{16}$$

so that

$$a \boxminus b = a \ominus \mathrm{gyr}[a, b]b \tag{17}$$

for all $a, b \in G$, where we define $a \boxminus b = a \boxplus (\ominus b)$. The gyrogroup cooperation shares with its associated gyrogroup operation remarkable duality symmetries as, for instance [56, Theorem 2.10],

$$\begin{aligned} a \boxplus b &= a \oplus \mathrm{gyr}[a, \ominus b]b \\ a \oplus b &= a \boxplus \mathrm{gyr}[a, b]b \end{aligned} \tag{18}$$

Interestingly, by [56, Theorem 3.4], a gyrogroup cooperation is commutative if and only if its corresponding gyrogroup is gyrocommutative.

The gyroautomorphisms have their own rich structure as we see, for instance, from the gyroautomorphism inversion property

$$(\mathrm{gyr}[a, b])^{-1} = \mathrm{gyr}[b, a] \tag{19}$$

from the loop property (left and right)

$$\begin{aligned} \mathrm{gyr}[a, b] &= \mathrm{gyr}[a \oplus b, b] \\ \mathrm{gyr}[a, b] &= \mathrm{gyr}[a, b \oplus a] \end{aligned} \tag{20}$$

and from the elegant nested gyroautomorphism identity

$$\mathrm{gyr}[a, b] = \mathrm{gyr}[\ominus \mathrm{gyr}[a, b]b, a] \tag{21}$$

for all $a, b \in G$ in any gyrogroup $G = (G, \oplus)$. More gyroautomorphism identities and important gyrogroup theorems, along with their applications, are found in [53, 56, 62] and in [6, 13, 25, 26, 30, 45, 46, 47, 63].

Thus, without losing the flavor of the group structure we have generalized it into the gyrogroup structure to suit the needs of Möbius addition in the disc and, more generally, in the open ball of any real inner product space [61], as we will show in Sec. 3. Gyrogroups abound in group theory, as shown in [15] and [16], where finite and infinite gyrogroups, both gyrocommutative and non-gyrocommutative, are studied. Plenty of gyrogroup theorems are found in [53, 56, 62]. Furthermore, any gyrogroup can be extended into a group, called a *gyrosemidirect product group* [56, Sec. 2.6] [28].

Hence, the generalization of groups into gyrogroups bears an intriguing resemblance to the generalization of the rational numbers into the real ones. The beginner is initially surprised to discover an irrational number, like $\sqrt{2}$, but soon later he is likely to realize that there are more irrational numbers than rational ones. Similarly, the gyrogroup structure of Möbius addition initially comes as a surprise. But, interested explorers may soon realize that in some sense there are more non-group gyrogroups than groups.

In our "gyrolanguage", as the reader has noticed, we attach the prefix "gyro" to a classical term to mean the analogous term in our study of grouplike loops. The prefix stems from Thomas gyration, which is the mathematical abstraction of the relativistic effect known as Thomas precession, explained in [53]. Indeed, gyrolanguage turns out to be the language we need to articulate novel analogies that the classical and the modern in this paper and in [53, 56, 62] share.

3. Möbius addition in the ball

If we identify complex numbers of the complex plane $\mathbb{C}$ with vectors of the Euclidean plane $\mathbb{R}^2$ in the usual way,

$$\mathbb{C} \ni u = u_1 + iu_2 = (u_1, u_2) = \mathbf{u} \in \mathbb{R}^2 \tag{22}$$

then the inner product and the norm in $\mathbb{R}^2$ are given by the equations

$$\begin{aligned} \bar{u}v + u\bar{v} &= 2\mathbf{u}\cdot\mathbf{v} \\ |u| &= \|\mathbf{u}\| \end{aligned} \tag{23}$$

These, in turn, enable us to translate Möbius addition from the complex open unit disc $\mathbb{D}$ into the open unit disc $\mathbb{R}^2_{s=1} = \{\mathbf{v}\in\mathbb{R}^2 : \|\mathbf{v}\| < s = 1\}$ of $\mathbb{R}^2$ [29]:

$$\begin{aligned} \mathbb{D} \ni u \oplus_{\mathrm{M}} v &= \frac{u+v}{1+\bar{u}v} \\ &= \frac{(1+u\bar{v})(u+v)}{(1+\bar{u}v)(1+u\bar{v})} \\ &= \frac{(1+\bar{u}v+u\bar{v}+|v|^2)u+(1-|u|^2)v}{1+\bar{u}v+u\bar{v}+|u|^2|v|^2} \\ &= \frac{(1+2\mathbf{u}\cdot\mathbf{v}+\|\mathbf{v}\|^2)\mathbf{u}+(1-\|\mathbf{u}\|^2)\mathbf{v}}{1+2\mathbf{u}\cdot\mathbf{v}+\|\mathbf{u}\|^2\|\mathbf{v}\|^2} \\ &= \mathbf{u}\oplus_{\mathrm{M}}\mathbf{v} \in \mathbb{R}^2_{s=1} \end{aligned} \tag{24}$$

for all $u, v \in \mathbb{D}$ and all $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2_{s=1}$. The last equation in (24) is a vector equation, so that its restriction to the ball of the Euclidean two-dimensional space $\mathbb{R}^2_{s=1}$ is a mere artifact. As such, it survives unimpaired in higher dimensions, suggesting the following definition of Möbius addition in the ball of any real inner product space.

Definition 3. (Möbius addition in the ball). Let $\mathbb{V}$ be a real inner product space [33], and let $\mathbb{V}_s$ be the s-ball of $\mathbb{V}$,

$$\mathbb{V}_s = \{\mathbb{V}_s \in \mathbb{V} : \|\mathbf{v}\| < s\} \tag{25}$$

for any fixed $s > 0$. *Möbius addition* $\oplus_M$ *in the ball* $\mathbb{V}_s$ is a binary operation in $\mathbb{V}_s$ given by the equation

$$\mathbf{u} \oplus_{\mathrm{M}} \mathbf{v} = \frac{(1 + \frac{2}{s^2}\mathbf{u}\cdot\mathbf{v} + \frac{1}{s^2}\|\mathbf{v}\|^2)\mathbf{u} + (1 - \frac{1}{s^2}\|\mathbf{u}\|^2)\mathbf{v}}{1 + \frac{2}{s^2}\mathbf{u}\cdot\mathbf{v} + \frac{1}{s^4}\|\mathbf{u}\|^2\|\mathbf{v}\|^2} \tag{26}$$

$\mathbf{u}, \mathbf{v} \in \mathbb{V}_s$, where $\cdot$ and $\|\cdot\|$ are the inner product and norm that the ball $\mathbb{V}_s$ inherits from its space $\mathbb{V}$.

Without loss of generality, one may select $s = 1$ in Definition 3. We, however, prefer to keep s as a free positive parameter in order to exhibit the result that in the limit as $s \to \infty$, the ball $\mathbb{V}_s$ expands to the whole of its real inner product space $\mathbb{V}$, and Möbius addition $\oplus_{\mathrm{M}}$ in the ball reduces to vector addition in the space. Remarkably, like the Möbius disc groupoid $(\mathbb{D}, \oplus_{\mathrm{M}})$, also the Möbius ball groupoid $(\mathbb{V}_s, \oplus_{\mathrm{M}})$ forms a gyrocommutative gyrogroup, called a Möbius gyrogroup.

Möbius addition in the ball $\mathbb{V}_s$ is known in the literature as a *hyperbolic translation* [2, 43]. Following the discovery of the gyrocommutative gyrogroup structure in 1988 [50], Möbius hyperbolic translation in the ball $\mathbb{V}_s$ now deserves the title *"Möbius addition"* in the ball $\mathbb{V}_s$, in full analogy with the standard vector addition in the space $\mathbb{V}$ that contains the ball.

Möbius addition in the ball $\mathbb{V}_s$ satisfies the *gamma identity*

$$\gamma_{\mathbf{u}\oplus_{\mathrm{M}}\mathbf{v}} = \gamma_{\mathbf{u}}\gamma_{\mathbf{v}}\sqrt{1 + \frac{2}{s^2}\mathbf{u}\cdot\mathbf{v} + \frac{1}{s^4}\|\mathbf{u}\|^2\|\mathbf{v}\|^2} \tag{27}$$

for all $\mathbf{u}, \mathbf{v} \in \mathbb{V}_s$, where $\gamma_{\mathbf{u}}$ is the gamma factor

$$\gamma_{\mathbf{v}} = \frac{1}{\sqrt{1 - \dfrac{\|\mathbf{v}\|^2}{s^2}}} \tag{28}$$

in the s-ball $\mathbb{V}_s$.

Following (16), Möbius cooperation, also called Möbius coaddition, in the ball is commutative, given by the equation

$$\mathbf{u} \boxplus_{\mathrm{M}} \mathbf{v} = \frac{\gamma_{\mathbf{u}}^2 \mathbf{u} + \gamma_{\mathbf{v}}^2 \mathbf{v}}{\gamma_{\mathbf{u}}^2 + \gamma_{\mathbf{v}}^2 - 1} \tag{29}$$

for all $\mathbf{u}, \mathbf{v} \in \mathbb{V}_s$. Note that $\mathbf{v} \boxplus_{\mathrm{M}} \mathbf{0} = \mathbf{v}$ and $\mathbf{v} \boxminus_{\mathrm{M}} \mathbf{v} = \mathbf{0}$, as expected.

4. Gyrogroups are loops

A *loop* is a groupoid $(G, \oplus)$ with an identity element, 0, such that each of its two *loop equations* for the unknowns x and y,

$$\begin{aligned} a \oplus x &= b \\ y \oplus a &= b \end{aligned} \tag{30}$$

possesses a unique solution in G for any $a, b \in G$ [39, 40]. Any gyrogroup is a loop. Indeed, if $(G, \oplus)$ is a gyrogroup then the respective unique solutions of the gyrogroup *loop equations* (30) are [56, Sec. 2.4]

$$\begin{aligned} x &= \ominus a \oplus b \\ y &= b \boxminus a \end{aligned} \tag{31}$$

The *cogyrogroup* $(G, \boxplus)$, associated with any gyrogroup $(G, \oplus)$, is also a loop. The unique solutions of its two loop equations

$$\begin{aligned} a \boxplus x &= b \\ y \boxplus a &= b \end{aligned} \tag{32}$$

are [56, Theorem 2.38]

$$\begin{aligned} x &= \ominus(\ominus b \oplus a) \\ y &= b \ominus a \end{aligned} \tag{33}$$

Note that, in general, the two loop equations in (32) are identically the same equation if and only if the gyrogroup cooperation $\boxplus$ is commutative. Hence, their solutions must be, in general, identical if and only if the gyrogroup cooperation $\boxplus$ is commutative. Indeed, a gyrogroup $(G, \oplus)$ possesses the *gyroautomorphic inverse property*, $\ominus(a \oplus b) = \ominus a \ominus b$, if and

only if it is gyrocommutative [56, Theorem 3.2]. Hence, the two solutions, x and y, in (33) are, in general, equal if and only if the gyrogroup $(G, \oplus)$ is gyrocommutative. This result is compatible with the result that a gyrogroup is gyrocommutative if and only if its cooperation $\boxplus$ is commutative [56, Theorem 3.4].

The cogyrogroup is an important and interesting loop. Its algebraic structure is not grouplike, but it plays a crucial role in the study of the gyroparallelogram law of Einstein's special relativity theory and its underlying hyperbolic geometry, Figs. 4, 5 and 8.

It follows from the solutions of the loop equations in (30) and (32) that any gyrogroup $(G, \oplus)$ possesses the following cancellation laws [56, Table 2.1]:

$$\begin{aligned} a \oplus (\ominus a \oplus b) &= b \\ (b \boxminus a) \oplus a &= b \\ a \boxminus (\ominus b \oplus a) &= b \\ (b \ominus a) \boxplus a &= b \end{aligned} \tag{34}$$

The first (second) cancellation law in (34) is called the *left* (*right*) *cancellation law*. The last cancellation law in (34) is called the *second right cancellation law*. The two right cancellation laws in (34) form one of the duality symmetries that the gyrogroup operation and cooperation share, mentioned in the paragraph of (18). It is thus clear that in order to maintain analogies between gyrogroups and groups, we need both the gyrogroup operation and its associated gyrogroup cooperation.

In the special case when a gyrogroup is gyrocommutative, it is also known as (i) a *K-loop* (a term coined by Ungar in [51]; see also [27, pp. 1, 169-170]); and (ii) a *Bruck loop* [27, pp. 168]. A new term, (iii) "dyadic symset", which emerges from an interesting work of Lawson and Lim in [31], turns out, according to [31, Theorem 8.8], to be identical with a two-divisible, torsion-free, gyrocommutative gyrogroup [56, p. 71].

5. Möbius scalar multiplication in the ball

Having developed the Möbius gyrogroup as a grouplike loop, we do not stop at the loop level. Encouraged by analogies gyrogroups share with groups, we now seek analogies with vector spaces as well. Accordingly, we uncover the scalar multiplication, $\otimes_{\mathrm{M}}$, between a real number $r \in \mathbb{R}$ and a vector

$\mathbf{v}\in\mathbb{V}_s$, that a Möbius gyrogroup $(\mathbb{V}_s, \oplus_{\mathrm{M}})$ admits, so that we can turn the Möbius gyrogroup into a Möbius gyrovector space $(\mathbb{V}_s, \oplus_{\mathrm{M}}, \otimes_{\mathrm{M}})$. For any natural number $n\in\mathbb{N}$ we define and calculate $n\otimes_{\mathrm{M}}\mathbf{v} := \mathbf{v}\oplus_{\mathrm{M}} \ldots \oplus_{\mathrm{M}}\mathbf{v}$ (n-terms), obtaining a result in which we formally replace n by a real number r, suggesting the following definition of the Möbius scalar multiplication.

Definition 4. (Möbius scalar multiplication). Let $(\mathbb{V}_s, \oplus_{\mathrm{M}})$ be a Möbius gyrogroup. Then its corresponding Möbius gyrovector space $(\mathbb{V}_s, \oplus_{\mathrm{M}}, \otimes_{\mathrm{M}})$ involves the *Möbius scalar multiplication* $r\otimes_{\mathrm{M}}\mathbf{v} = \mathbf{v}\otimes_{\mathrm{M}} r$ in $\mathbb{V}_s$, given by the equation

$$\begin{aligned} r\otimes_{\mathrm{M}}\mathbf{v} &= s\frac{\left(1+\dfrac{\|\mathbf{v}\|}{s}\right)^r - \left(1-\dfrac{\|\mathbf{v}\|}{s}\right)^r}{\left(1+\dfrac{\|\mathbf{v}\|}{s}\right)^r + \left(1-\dfrac{\|\mathbf{v}\|}{s}\right)^r}\frac{\mathbf{v}}{\|\mathbf{v}\|} \\ &= s\tanh(r\,\tanh^{-1}\frac{\|\mathbf{v}\|}{s})\frac{\mathbf{v}}{\|\mathbf{v}\|} \end{aligned} \tag{35}$$

where $r\in\mathbb{R}$, $\mathbf{v}\in\mathbb{V}_s$, $\mathbf{v}\neq\mathbf{0}$; and $r\otimes_{\mathrm{M}}\mathbf{0} = \mathbf{0}$.

Extending Definition 4 by abstraction, we obtain the abstract gyrovector space, studied in [56, Chap. 6]. As we go through the study of gyrovector spaces, we see remarkable analogies with classical results unfolding. In particular, armed with the gyrovector space structure, we offer a gyrovector space approach to the study of hyperbolic geometry [56], which is fully analogous to the common vector space approach to the study of Euclidean geometry [24]. Our basic examples are presented in the sequel and shown in several figures.

6. Möbius gyroline and more

In full analogy with straight lines in the standard vector space approach to Euclidean geometry, let us consider the *gyroline* equation in the ball $\mathbb{V}_s$,

$$L_{AB} := A\oplus(\ominus A\oplus B)\otimes t \tag{36}$$

$t\in\mathbb{R}$, $A, B\in\mathbb{V}_s$, in a Möbius gyrovector space $(\mathbb{V}_s, \oplus, \otimes)$. For simplicity, we use in this section the notation $\oplus_{\mathrm{M}} = \oplus$ and $\otimes_{\mathrm{M}} = \otimes$. The gyrosegment AB is the part of the gyroline (36) that links the points A and B. Hence, it is given by (36) with $0\leqslant t\leqslant 1$, Fig. 1.

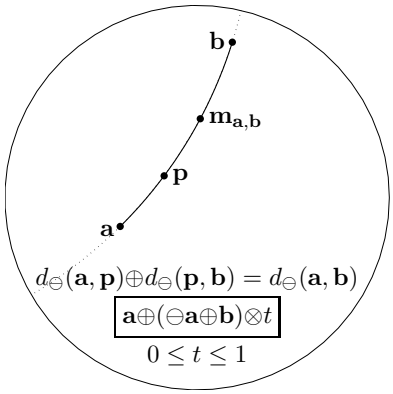


Figure 1. The gyrosegment that links the two points **a** and **b** in the Möbius gyrovector plane $(\mathbb{R}^2_s, \oplus, \otimes)$. **p** is a generic point between **a** and **b**, and $m_{\mathbf{a},\mathbf{b}}$ is the midpoint of the points **a** and **b**.

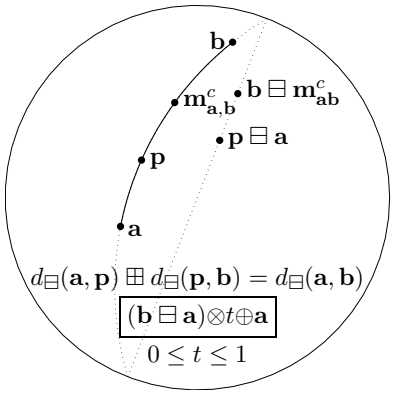


Figure 2. The cogyrosegment that links the two points **a** and **b** in the Möbius gyrovector plane $(\mathbb{R}^2_s, \oplus, \otimes)$. **p** is a generic point cobetween **a** and **b** and $m_{\mathbf{a},\mathbf{b}}$ is the comidpoint of the points **a** and **b**.

For any $t\in\mathbb{R}$ the point $P(t) = A\oplus(\ominus A\oplus B)\otimes t$ lies on the gyroline L_{AB}. Thinking of t as time, at time $t = 0$ the point P lies at $P(0) = A$ and, owing to the left cancellation law in (34), at time $t = 1$ the point P lies at $P(1) = B$. Furthermore, the point P reaches the *gyromidpoint* M_{AB} of the points A and B at time $t = 1/2$,

$$M_{AB} = A\oplus(\ominus A\oplus B)\otimes\tfrac{1}{2} = \tfrac{1}{2}\otimes(A\boxplus B) \tag{37}$$

[56, Sec. 6.5]. Here M_{AB} is the unique gyromidpoint of the points A and B in the gyrodistance sense, $d(A, M_{AB}) = d(B, M_{AB})$, the gyrodistance function being $d(A, B) = \|\ominus A\oplus B\| = \|B\ominus A\|$.

In the special case when $\mathbb{V}_s = \mathbb{R}^2_s$, the gyroline L_{AB}, shown in Fig. 1, is a circular arc that intersects the boundary of the s-disc $\mathbb{R}^2_s$ orthogonally. A study of the connection between gyrovector spaces and differential geometry [56, Chap. 7] [57] reveals that this gyroline is the unique geodesic that passes through the points A and B in the Poincaré disc model of hyperbolic geometry.

The *cogyroline* equation in the ball $\mathbb{V}_s$, similar to (36), is

$$L^c_{AB} := (B\boxminus A)\otimes t\oplus A \tag{38}$$

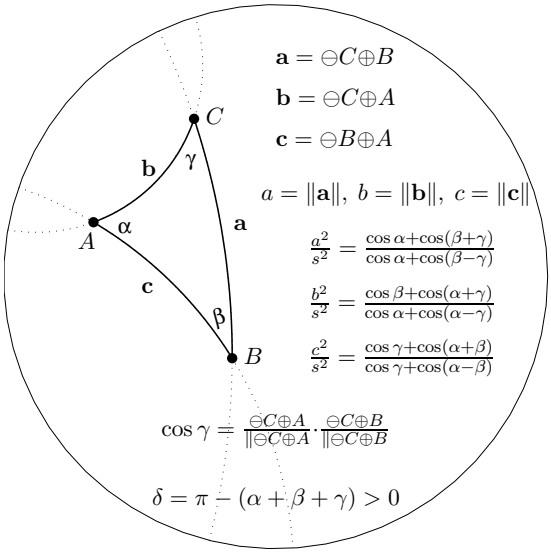


Figure 3. Möbius gyrotriangle and its standard notation and identities in a Möbius gyrovector space $(\mathbb{V}_s, \oplus, \otimes)$. Remarkably, in the limit as $s \to \infty$ the equations in the figure reduce to their Euclidean counterparts. Thus, for instance, in that limit we have $\cos\alpha + \cos(\beta+\gamma) = 0$ implying the Euclidean theorem according to which the triangle angle sum is π, $\alpha+\beta+\gamma = \pi$.

$t \in \mathbb{R}$, $A, B \in \mathbb{V}_s$, in a Möbius gyrovector space $(\mathbb{V}_s, \oplus, \otimes)$. The cogyrosegment AB is the part of the cogyroline (38) that links the points A and B. Hence, it is given by (38) with $0 \leqslant t \leqslant 1$, Fig. 2.

For any $t \in \mathbb{R}$ the point $P(t) = (B \boxminus A) \otimes t \oplus A$ lies on the cogyroline L^c_{AB} in (38). Thinking of t as time, at time $t = 0$ the point P lies at $P(0) = A$ and, owing to the right cancellation law in (34), at time $t = 1$ the point P lies at $P(1) = B$. Furthermore, the point P reaches the *cogyromidpoint* M^c_{AB} of the points A and B at time $t = 1/2$,

$$M^c_{AB} = (B \boxminus A) \otimes \tfrac{1}{2} \oplus A = \tfrac{1}{2} \otimes (A \oplus B) \tag{39}$$

[56, Theorem 6.34]. Here M^c_{AB} is the unique cogyromidpoint of the points A and B in the cogyrodistance sense, $d^c(A, M^c_{AB}) = d^c(B, M^c_{AB})$, the cogyrodistance function being $d^c(A, B) = \|\ominus A \boxplus B\| = \|B \boxminus A\|$.

In the special case when $\mathbb{V}_s = \mathbb{R}^2_s$, the cogyroline L^c_{AB}, shown in Fig. 2, is a circular arc that intersects the boundary of the s-disc $\mathbb{R}^2_s$ diametrically.

Let $A, B, C \in G$ be any three non-gyrocollinear points of a Möbius gyrovector space $G = (G, \oplus, \otimes)$. In Fig. 3 we see a gyrotriangle ABC whose vertices, A, B, and C, are linked by the gyrovectors $\mathbf{a}$, $\mathbf{b}$, and $\mathbf{c}$; and whose

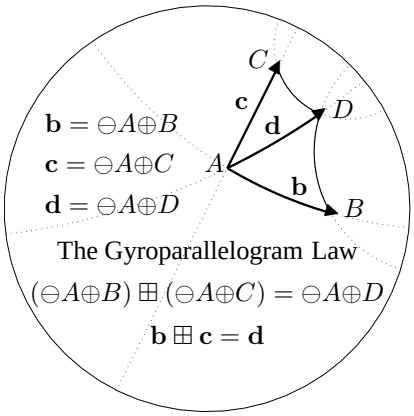


Figure 4. The Möbius gyroparallelogram $ABDC$ and its associated gyroparallelogram addition law of gyrovectors in a Möbius gyrovector space $(\mathbb{V}_s, \oplus, \otimes)$ is shown.

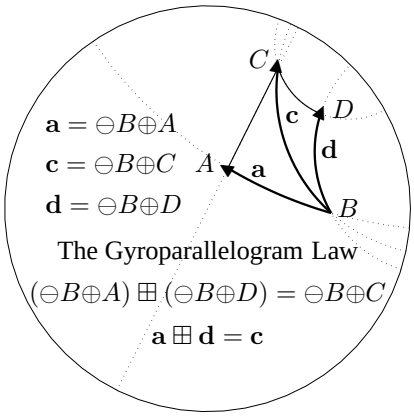


Figure 5. As a second example, the same Möbius gyroparallelogram $ABDC$ in Fig. 4 gives rise to a second gyroparallelogram addition of gyrovectors.

side gyrolengths are a, b, and c, given by the equations

$$\begin{aligned} \mathbf{a} &= \ominus C \oplus B, & a &= \|\mathbf{a}\| \\ \mathbf{b} &= \ominus C \oplus A, & b &= \|\mathbf{b}\| \\ \mathbf{c} &= \ominus B \oplus A, & c &= \|\mathbf{c}\| \end{aligned} \tag{40}$$

With the gyrodistance function $d(A, B) = \|\ominus A \oplus B\| = \|B \ominus A\|$, we have the gyrotriangle inequality [56, Theorem 6.9] $d(A, C) \leqslant d(A, B) \oplus d(B, C)$, in full analogy with the Euclidean triangle inequality.

A gyrovector $\mathbf{v} = \ominus A \oplus B$ in a Möbius gyrovector plane $(\mathbb{R}^2_s, \oplus, \otimes)$ and in a Möbius three-dimensional gyrovector space $(\mathbb{R}^3_s, \oplus, \otimes)$ is represented graphically by the directed gyrosegment AB from A to B as, for instance, in Figs. 4–5 and 8.

Two gyrovectors, (i) $\ominus A \oplus B$, from A to B, and (ii) $\ominus A' \oplus B'$, from A' to B', in a gyrovector space $G = (G, \oplus, \otimes)$ are equivalent if

$$\ominus A \oplus B = \ominus A' \oplus B' \tag{41}$$

In the same way that vectors in Euclidean geometry are equivalence classes of directed segments that add according to the parallelogram law,

gyrovectors in hyperbolic geometry are equivalence classes of directed gyrosegments that add according to the gyroparallelogram law. A gyroparallelogram, the hyperbolic parallelogram, sounds like a contradiction in terms since parallelism in hyperbolic geometry is denied. However, in full analogy with Euclidean geometry, but with no reference to parallelism, the gyroparallelogram is defined as a hyperbolic quadrilateral whose gyrodiagonals intersect at their gyromidpoints, as in Figs. 4 – 5. Indeed, any three non-gyrocollinear points A, B, C in a gyrovector space $(G, \oplus, \otimes)$ form a gyroparallelogram $ABDC$ if and only if D satisfied the *gyroparallelogram condition* $D = (B \boxplus C) \ominus A$ [56, Sec. 6.7].

An interesting contrast between Euclidean and hyperbolic geometry is observed here. In Euclidean geometry vector addition coincides with the parallelogram addition law. In contrast, in hyperbolic geometry gyrovector addition, given by Möbius addition, and the Möbius gyroparallelogram addition law are distinct.

7. Einstein operations in the ball

Definition 5. (Einstein addition in the ball). Let $\mathbb{V}$ be a real inner product space and let $\mathbb{V}_s$ be the s-ball of $\mathbb{V}$,

$$\mathbb{V}_s = \{\mathbf{v} \in \mathbb{V} : \|\mathbf{v}\| < s\} \tag{42}$$

where $s > 0$ is an arbitrarily fixed constant (that represents in physics the vacuum speed of light c). *Einstein addition* $\oplus_{\mathrm{E}}$ is a binary operation in $\mathbb{V}_s$ given by the equation

$$\mathbf{u} \oplus_{\mathrm{E}} \mathbf{v} = \frac{1}{1 + \frac{\mathbf{u} \cdot \mathbf{v}}{s^2}} \left\{ \mathbf{u} + \frac{1}{\gamma_{\mathbf{u}}} \mathbf{v} + \frac{1}{s^2} \frac{\gamma_{\mathbf{u}}}{1 + \gamma_{\mathbf{u}}} (\mathbf{u} \cdot \mathbf{v}) \mathbf{u} \right\} \tag{43}$$

where $\gamma_{\mathbf{u}}$ is the gamma factor, (28), in $\mathbb{V}_s$, and where $\cdot$ and $\|\cdot\|$ are the inner product and norm that the ball $\mathbb{V}_s$ inherits from its space $\mathbb{V}$.

We may note that the Euclidean 3-vector algebra was not so widely known in 1905 and, consequently, was not used by Einstein. Einstein calculated in his founding paper [12] the behavior of the velocity components parallel and orthogonal to the relative velocity between inertial systems, which is as close as one can get without vectors to the vectorial version (43).

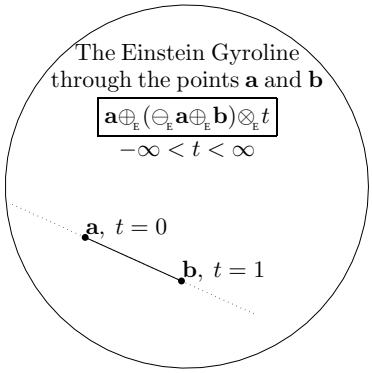


Figure 6. The unique gyroline in an Einstein gyrovector space $(\mathbb{V}_s, \oplus_{\mathrm{E}}, \otimes_{\mathrm{E}})$ through two given points **a** and **b**. The case of the Einstein gyrovector plane, when $\mathbb{V}_s = \mathbb{R}^2_s$ is the real open unit disc, is shown graphically.

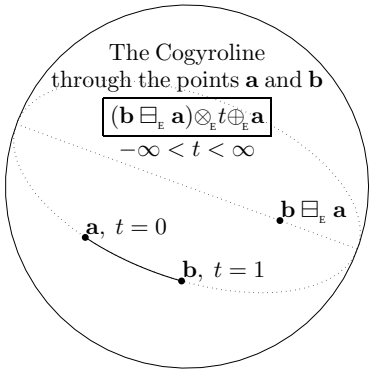


Figure 7. The unique cogyroline in an Einstein gyrovector space $(\mathbb{V}_s, \oplus_{\mathrm{E}}, \otimes_{\mathrm{E}})$ through two given points **a** and **b**. The case of the Einstein gyrovector plane, when $\mathbb{V}_s = \mathbb{R}^2_s$ is the real open unit disc, is shown graphically.

Seemingly structureless, Einstein velocity addition could not play in Einstein's special theory of relativity a central role. Indeed, Borel's attempt to "repair" the seemingly "defective" Einstein velocity addition in the years following 1912 is described in [65, p. 117]. Fortunately, however, there is no need to "repair" the Einstein velocity addition law since, like Möbius addition in the ball, Einstein addition in the ball is a gyrocommutative gyrogroup operation, which gives rise to the Einstein ball gyrogroups $(\mathbb{V}_s, \oplus_{\mathrm{E}})$ and gyrovector spaces $(\mathbb{V}_s, \oplus_{\mathrm{E}}, \otimes_{\mathrm{E}})$, Figs. 6 – 7 [53, 8]. Furthermore, Einstein's gyration turns out to be the Thomas precession of relativity physics [52], so that Thomas precession is a kinematic effect rather than a dynamic effect as it is usually portrayed [58]. A brief history of the discovery of Thomas precession is presented in [53, Sec. 1.1].

The gamma factor is related to Einstein addition by the *gamma identity*

$$\gamma_{\mathbf{u}\oplus_{\mathrm{E}}\mathbf{v}} = \gamma_{\mathbf{u}}\gamma_{\mathbf{v}}\left(1 + \frac{\mathbf{u}\cdot\mathbf{v}}{s^2}\right) \tag{44}$$

This gamma identity provided the historic link between Einstein's special theory of relativity and the hyperbolic geometry of Bolyai and Lobachevsky, as explained in [60].

Einstein scalar multiplication in the ball $\mathbb{V}_s$ is identical with Möbius scalar multiplication, (35), in the ball $\mathbb{V}_s$, $r\otimes_{\mathrm{E}}\mathbf{v} = r\otimes_{\mathrm{M}}\mathbf{v}$ for all $r\in\mathbb{R}$ and $\mathbf{v}\in\mathbb{V}_s$. Hence Einstein and Möbius scalar multiplication are denoted here, collectively, by $\otimes$.

The isomorphism between Einstein addition $\oplus_{\mathrm{E}}$ and Möbius addition $\oplus_{\mathrm{M}}$ in the ball $\mathbb{V}_s$ is surprisingly simple when expressed in gyrolanguage,

the language of gyrovector spaces. As we see from [56, Table 6.1], the gyrovector space isomorphism between $(\mathbb{V}_s, \oplus_{\rm E}, \otimes)$ and $(\mathbb{V}_s, \oplus_{\rm M}, \otimes)$ is given by the equations

$$\begin{aligned} \mathbf{u}\oplus_{\rm E}\mathbf{v} &= 2\otimes(\tfrac{1}{2}\otimes\mathbf{u}\oplus_{\rm M}\tfrac{1}{2}\otimes\mathbf{v}) \\ \mathbf{u}\oplus_{\rm M}\mathbf{v} &= \tfrac{1}{2}\otimes(2\otimes\mathbf{u}\oplus_{\rm E}2\otimes\mathbf{v}) \end{aligned} \tag{45}$$

Following (16), Einstein cooperation, also called Einstein coaddition, in the ball is commutative, given by the equation

$$\mathbf{u}\boxplus_{\rm E}\mathbf{v} = 2\otimes\frac{\gamma_{\mathbf{u}}\mathbf{u}+\gamma_{\mathbf{v}}\mathbf{v}}{\gamma_{\mathbf{u}}+\gamma_{\mathbf{v}}} \tag{46}$$

for all $\mathbf{u}, \mathbf{v}\in\mathbb{V}_s$. Clearly, $\mathbf{v}\boxminus_{\rm E}\mathbf{v} = \mathbf{0}$. Noting the *Einstein half*,

$$\tfrac{1}{2}\otimes\mathbf{v} = \tfrac{\gamma_{\mathbf{v}}}{1+\gamma_{\mathbf{v}}}\mathbf{v} \tag{47}$$

and the *scalar associative law* of gyrovector spaces [56, p. 138], it is clear from (46) – (47) that $\mathbf{v}\boxplus_{\rm E}\mathbf{0} = \mathbf{v}$, as expected.

Einstein noted in 1905 that

> "Das Gesetz vom Parallelogramm der Geschwindigkeiten gilt also nach unserer Theorie nur in erster Annäherung."
>
> A. Einstein [12], 1905

[Thus the law of velocity parallelogram is valid according to our theory only to a first approximation.]

We now see that with our gyrovector space approach to hyperbolic geometry, Einstein's noncommutative addition $\oplus_{\rm E}$ gives rise to an *exact* hyperbolic parallelogram addition $\boxplus_{\rm E}$, Fig. 8, which is commutative. The cogyrogroup $(\mathbb{V}_s, \boxplus)$ is thus an important commutative loop that regulates algebraically the hyperbolic parallelogram [59].

An interesting contrast between Euclidean and hyperbolic geometry is thus observed here. In Euclidean geometry and in classical mechanics vector addition coincides with the parallelogram addition law. In contrast, in hyperbolic geometry and in relativistic mechanics gyrovector addition, given by Einstein addition, $\mathbf{u}\oplus_{\rm E}\mathbf{v}$, and the gyroparallelogram addition, $\mathbf{u}\boxplus_{\rm E}\mathbf{v}$ in $\mathbb{V}_s$, are distinct. We thus face the problem of whether the ultimate relativistic velocity addition is given by the (i) non-commutative Einstein velocity addition law in (43), or by the (ii) commutative Einstein gyroparallelogram

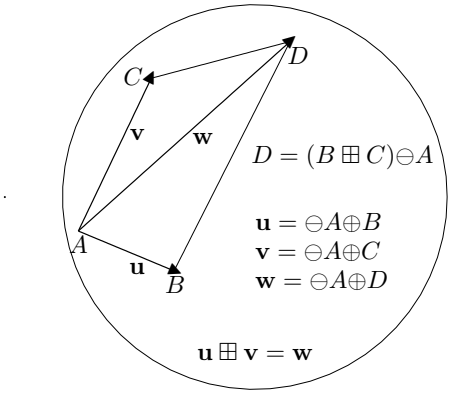


Figure 8. The Einstein gyroparallelogram addition law of relativistically admissible velocities. Let $A, B, C \in \mathbb{R}^3_s$ be any three nongyrocollinear points of an Einstein gyrovector space $(\mathbb{R}^3_s, \oplus, \otimes)$, giving rise to the two gyrovectors $\mathbf{u} = \ominus A \oplus B$ and $\mathbf{v} = \ominus A \oplus C$. Furthermore, let D be a point of the gyrovector space such that $ABDC$ is a gyroparallelogram, that is, $D = (B \boxplus C) \ominus A$. Then, Einstein coaddition of $\mathbf{u}$ and $\mathbf{v}$, $\mathbf{u} \boxplus \mathbf{v} = \mathbf{w}$, obeys the gyroparallelogram law, $\mathbf{w} = \ominus A \oplus D$, just as vector addition in $(\mathbb{R}^3, +)$ obeys the parallelogram law. Einstein coaddition, $\boxplus$, thus gives rise to the gyroparallelogram addition law of Einsteinian velocities, which is commutative and fully analogous to the parallelogram addition law of Newtonian velocities.

addition law in Fig. 8. Fortunately, a cosmic phenomenon that can provide the ultimate resolution of the problem does exist. It is the stellar aberration, illustrated classically and relativistically for particle aberration in Figs. 9 and 10.

A cosmic experiment in our cosmic laboratory, the Universe, that can validate the Einstein gyroparallelogram addition law, Fig. 8, and its associated gyrotriangle addition law of Einsteinian velocities shown in Fig. 10, is the *stellar aberration* [48]. Stellar aberration is particle aberration where the particle is a photon emitted from a star. Particle aberration, in turn, is the change in the apparent direction of a moving particle caused by the relative motion between two observers. The case when the two observers are E (at rest relative to the Earth) and S (at rest relative to the Sun) is shown graphically in Fig. 9 (classical interpretation) and Fig. 10 (relativistic interpretation). Obviously, in order to detect stellar aberration there is no need to place an observer at rest relative to the Sun since this effect varies during the year. It is this variation that can be observed by observers at rest relative to the Earth.

The classical interpretation of particle aberration is obvious in terms of the triangle law of Newtonian velocity addition (which is the common vector addition in Euclidean geometry), as demonstrated graphically in Fig. 9. The

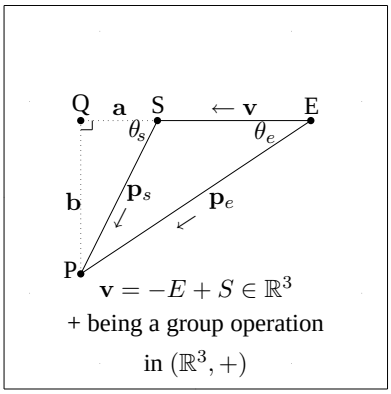


Figure 9. Particle Aberration: Classical interpretation in terms of the triangle law of addition of Newtonian velocities in the standard model of 3-dimensional Euclidean geometry $(\mathbb{R}^3, +)$. Two dimensions are shown for graphical clarity. Here + is the common vector addition in $\mathbb{R}^3$.
A particle P moves with Newtonian velocity $\mathbf{p}_e$ ($\mathbf{p}_s$) relative to the Earth E (the Sun S), making an angle θ_e (θ_s) with the Newtonian velocity $\mathbf{v}$ of the Sun S relative to the Earth E.
In order to calculate the Newtonian (classical) particle aberration $\theta_s - \theta_e$, the Euclidean triangle ESP is augmented into the Euclidean right-angled triangle EQP, allowing elementary trigonometry to be employed.
Points are given by their orthogonal Cartesian coordinates (x, y, z), $x^2 + y^2 + z^2 < \infty$. The coordinates are not shown.
The Euclidity of $(\mathbb{R}^3, +)$ is determined by the Euclidean metric in which the distance between two points A, B is $\| - A + B\|$.

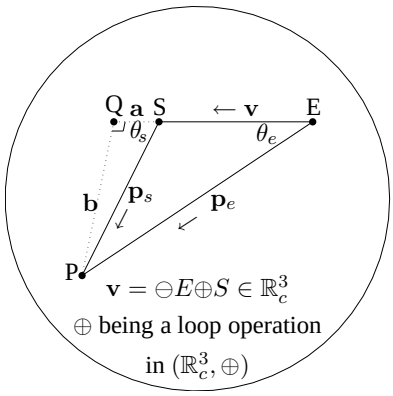


Figure 10. Particle Aberration: Relativistic interpretation in terms of the gyrotriangle law of addition of Einsteinian velocities in the Beltrami-Klein ball model of 3-dimensional hyperbolic geometry $(\mathbb{R}^3_c, \oplus)$. Here $\oplus$ is Einstein addition in the c-ball $\mathbb{R}^3_c \subset \mathbb{R}^3$.
A particle P moves with Einsteinian velocity $\mathbf{p}_e$ ($\mathbf{p}_s$) relative to the Earth E (the Sun S), making an angle θ_e (θ_s) with the Einsteinian velocity $\mathbf{v}$ of the Sun S relative to the Earth E.
In order to calculate the relativistic particle aberration $\theta_s - \theta_e$, the gyrotriangle ESP is augmented into the right-gyroangled gyrotriangle EQP, allowing elementary gyrotrigonometry to be employed [62].
Points are given by their orthogonal Cartesian coordinates (x, y, z), $x^2 + y^2 + z^2 < c^2$. The coordinates are not shown.
The hyperbolicity of $(\mathbb{R}^3_c, \oplus)$ is determined by the hyperbolic gyrometric in which the distance between two points A, B is given by $\| \ominus A \oplus B \|$.

relativistic interpretation of particle aberration is, however, less obvious.

Relativistic particle aberration is illustrated in Fig. 10 in terms of analogies that it shares with its classical interpretation in Fig. 9. These analogies are just analogies that gyrocommutative gyrogroups share with commutative groups and gyrovector spaces share with vector spaces. Remarkably, the resulting expressions that describe the relativistic stellar aberration phenomenon, obtained by our gyrovector space approach, agree with expressions that are obtained in the literature by employing the relativistic Lorentz transformation group. Our gyrovector space approach is thus capable of recovering known results in astrophysics, to which it gives new geometric

interpretations that are analogous to known, classical interpretations.

8. Dark matter of the universe

> What is the universe made of? We do not know. If standard gravitational theory is correct, then most of the matter in the universe is in an unidentified form that does not emit enough light to have been detected by current instrumentation. Astronomers and physicists are collaborating on analyzing the characteristics of this dark matter and in exploring possible physics or astronomical candidates for the unseen material.
>
> S. Weinberg and J. Bahcall [4, p. v]

Fortunately, our gyrovector space approach is capable of discovering a novel result in astrophysics as well, proposing a viable mechanism for the formation of the dark matter of the Universe.

We have seen in Sec. 8 that the cosmic effect of stellar aberration supports our gyrovector gyrospace approach guided by analogies that it shares with the common vector space approach. Another cosmic effect that may support a relativistic physical novel result obtained by our gyrovector space approach to Einstein's special theory of relativity is related to the elusive relativistic center of mass. The difficulties in attempts to obtain a satisfactory relativistic center of mass definition were discussed by Born and Fuchs in 1940 [7], but they did not propose a satisfactory definition. Paradoxically, "In relativity, in contrast to Newtonian mechanics, the centre of mass of a system is not uniquely determined", as Rindler stated with a supporting example [44, p. 89]. Indeed, in 1948 M.H.L. Pryce [41] reached the conclusion that "there appears to be no wholly satisfactory definition of the [relativistic] mass-centre." Subsequently, Pryce's conclusion was confirmed by many authors who proposed various definitions for the relativistic center of mass; see for instance [3, 17, 32] and references therein, where various approaches to the concept of the relativistic center of mass are studied. Consequently, Goldstein stated that "a meaningful center-of-mass (sometimes called center-of-energy) can be defined in special relativity only in terms of the angular-momentum tensor, and only for a particular frame of reference." [18, p. 320].

Fortunately, the spacetime geometric insight that our novel grouplike loop approach offers enables the elusive "manifestly covariant" relativistic

center of mass of a particle system with *proper time* to be identified. It turns out to be analogous to the classical center of mass to the mass of which a specified fictitious mass must be added so as to render it "manifestly covariant" with respect to the motions of hyperbolic geometry. Specifically, let $S = S(m_k, \mathbf{v}_k, \Sigma_{\mathbf{0}}, N)$, be an isolated system of N noninteracting material particles the k-th particle of which has mass $m_k > 0$ and velocity $\mathbf{v}_k \in \mathbb{R}^3_c$ relative to a rest frame $\Sigma_{\mathbf{0}}$, $k = 1, \ldots, N$. Then, classically, the system S of N particles can be viewed as a fictitious single particle located at the center of mass of S, with mass $m_0 = \sum_{k=1}^{N} m_k$ that equals the total mass of the constituent particles of S. Relativistically, however, symmetries are determined by gyrogroup, rather than group, symmetries. As in the classical counterpart, the system S can be viewed in Einstein's special theory of relativity as a fictitious single particle located at the relativistic center of mass of S (specified in [62]), with mass m_0 that we present in (48) below.

In order to obey necessary relativistic symmetries, the mass m_0 of the relativistic center of mass of S must exceed, in general, the total mass of the constituent particles of S according to the equation

$$m_0 \;=\; \sqrt{\left(\sum_{k=1}^{N} m_k\right)^2 + 2\sum_{\substack{j,k=1\\ j<k}}^{N} m_j m_k(\gamma_{\ominus\mathbf{v}_j\oplus\mathbf{v}_k} - 1)} \;\geq\; \sum_{k=1}^{N} m_k \qquad (48)$$

as explained in [62].

The additional, fictitious mass $m_0 - \sum_{k=1}^{N} m_k$ in (48) of the system S results from relative velocities, $\ominus\mathbf{v}_j\oplus\mathbf{v}_k$, $j, k = 1, \ldots, N$, between particles of the system S. The fictitious mass of a rigid particle system, therefore, vanishes. The fictitious mass of nonrigid galaxies does not vanish and, hence, could account for the dark matter needed to gravitationally "glue" each nonrigid galaxy together.

Indeed, the cosmic laboratory, our Universe, may support the existence of the predicted fictitious mass in (48) as the mass of the dark matter in the Universe that astrophysicists are forced to postulate but cannot detect [4, 34, 10, 37, 49]. Hence, in order to uncover a viable mechanism that accounts for the formation of dark matter that manifests itself only through gravitational interaction, there is no need to modify the laws of physics, as Milgrom proposed in [34]. Rather, one can find it in our grouplike loop approach that improves our understanding of Einstein's special theory of relativity and its underlying hyperbolic geometry of Bolyai and Lobachevsky [62].

9. The Bloch gyrovector of QIC

Bloch vector is well known in the theory of quantum information and computation (QIC). We will show that, in fact, Bloch vector is not a vector but, rather, a gyrovector [9, 54, 55]. It is easy to predict that in the present twenty-first century it is quantum mechanics that will increasingly influence our lives. Hence, it would be interesting to see what gyrovector spaces have to offer in QIC.

A *qubit* is a two state quantum system completely described by the qubit *density matrix* $\rho_{\mathbf{v}}$,

$$\rho_{\mathbf{v}} = \tfrac{1}{2}\begin{pmatrix} 1+v_3 & v_1 - iv_2 \\ v_1 + iv_2 & 1-v_3 \end{pmatrix} \tag{49}$$

parametrized by the vector $\mathbf{v} = (v_1, v_2, v_3) \in \mathbb{B}^3$ in the open unit ball $\mathbb{B}^3 = \mathbb{R}^3_{s=1}$ of the Euclidean 3-space $\mathbb{R}^3$. The vector $\mathbf{v}$ in the ball is known in QIC as the Bloch vector. However, we will see that it would be more appropriate to call it a gyrovector rather than a vector.

The density matrix product of the four density matrices in the following equation, which are parametrized by two distinct Bloch vectors $\mathbf{u}$ and $\mathbf{v}$, can be written as a single density matrix parametrized by the Bloch vector $\mathbf{w}$, multiplied by the trace of the matrix product,

$$\rho_{\mathbf{u}}\rho_{\mathbf{v}}\rho_{\mathbf{v}}\rho_{\mathbf{u}} = tr[\rho_{\mathbf{u}}\rho_{\mathbf{v}}\rho_{\mathbf{v}}\rho_{\mathbf{u}}]\rho_{\mathbf{w}} \tag{50}$$

$\mathbf{u}, \mathbf{v} \in \mathbb{B}^3$. Here $tr[m]$ is the trace of a square matrix m, and

$$\mathbf{w} = \mathbf{u} \oplus_{\mathrm{M}} (2 \otimes \mathbf{v} \oplus_{\mathrm{M}} \mathbf{u}) = 2 \otimes (\mathbf{u} \oplus_{\mathrm{M}} \mathbf{v}) \tag{51}$$

Identity (51) is one of several identities available in [9, 54, 55] that demonstrate the compatibility of density matrix manipulations and gyrovector space manipulations.

Two Bloch vectors $\mathbf{u}$ and $\mathbf{v}$ generate the two density matrices $\rho_{\mathbf{u}}$ and $\rho_{\mathbf{v}}$ that, in turn, generate the *Bures fidelity* $\mathcal{F}(\rho_{\mathbf{u}}, \rho_{\mathbf{v}})$ that we may also write as $\mathcal{F}(\mathbf{u}, \mathbf{v})$. The Bures fidelity $\mathcal{F}(\mathbf{u}, \mathbf{v})$ is a most important distance measure between quantum states $\rho_{\mathbf{u}}$ and $\rho_{\mathbf{v}}$ of the qubit in QIC, given by the equations

$$\mathcal{F}(\mathbf{u}, \mathbf{v}) = \left[\mathrm{tr}\sqrt{\sqrt{\rho_{\mathbf{u}}}\rho_{\mathbf{v}}\sqrt{\rho_{\mathbf{u}}}}\right]^2 = \tfrac{1}{2}\,\frac{1 + \gamma_{\mathbf{u} \oplus_{\mathrm{E}} \mathbf{v}}}{\gamma_{\mathbf{u}}\gamma_{\mathbf{v}}} \tag{52}$$

The first equation in (52) is well known [38, 67], and the second equation in (52) is a gyrovector space equation verified in [56, Eq. 9.69]. Identity (51)

and the second identity in (52) indicate that in density matrix manipulations in QIC, Bloch vectors appear to behave like gyrovectors in Möbius gyrovector spaces $(\mathbb{R}^3_{s=1}, \oplus_{\mathrm{M}}, \otimes)$ and in Einstein gyrovector spaces $(\mathbb{R}^3_{s=1}, \oplus_{\mathrm{E}}, \otimes)$.

Indeed, since the Bures fidelity has particularly wide currency today in QIC geometry, Nielsen and Chuang had to admit for their chagrin [38, p. 410] that

> "Unfortunately, no similarly [alluding to Euclidean geometric interpretation] clear geometric interpretation is known for the fidelity between two states of a qubit".

It is therefore interesting to realize that while Bures fidelity has no Euclidean geometric interpretation, as Nielsen and Chuang admit, it does have a hyperbolic geometric interpretation, which is algebraically regulated by our grouplike loops and their associated gyrovector spaces.

References

[1] **L. V. Ahlfors**: *Conformal invariants: topics in geometric function theory*, McGraw-Hill Book Co., New York, 1973.

[2] **L. V. Ahlfors**: *Möbius transformations in several dimensions*, Univ. of Minnesota School of Mathematics, Minneapolis, Minn., 1981.

[3] **D. Alba, L. Lusanna and M. Pauri**: *Centers of mass and rotational kinematics for the relativistic N-body problem in the rest-frame instant form*, J. Math. Phys. **43(4)** (2002), 1677 – 1727.

[4] **J. Bahcall, T. Piran and S. Weinberg (eds.)**: *Dark Matter in the Universe*, sec. ed. Kluwer Academic Publishers Group, Dordrecht, 2004.

[5] **J. F. Barrett**, *Special relativity and hyperbolic geometry*, Univ. Sunderland, Sunderland, UK, 1998. Physical Interpretations of Relativity Theory. Proceedings, London, UK, 11–14 September 1998.

[6] **G. S. Birman and A. A. Ungar**: *The hyperbolic derivative in the poincaré ball model of hyperbolic geometry*, J. Math. Anal. Appl. **254** (2001), 321 – 333.

[7] **M. Born and K. Fuchs**: *The mass centre in relativity*, Nature **145** (1940), 587.

[8] **J. L. Chen and A. A. Ungar**: *From the group* $\mathrm{sl}(2, \mathbf{C})$ *to gyrogroups and gyrovector spaces and hyperbolic geometry*, Found. Phys. **31(11)** (2001), 1611 – 1639.

[9] **J. L. Chen and A. A. Ungar**: *The Bloch gyrovector*, Found. Phys. **32(4)** (2002), 531 – 565.

[10] **D. B. Cline**: *The search for dark matter*, Sci. Amer., March 2003, 50 – 59.

[11] **L. Corry**: *The influence of David Hilbert and Hermann Minkowski on Einstein's views over the interrelation between physics and mathematics*, Endeavor **22(3)** (1998), 95 – 97.

[12] **A. Einstein**: *Zur Elektrodynamik Bewegter Körper* (*on the electrodynamics of moving bodies*), Ann. Physik (Leipzig) **17** (1905), 891 – 921.

[13] **T. Feder**: *Strong near subgroups and left gyrogroups*, J. Algebra **259** (2003), 177 – 190.

[14] **S. D. Fisher**: *Complex variables*, Dover Publications Inc., Mineola, NY, 1999, Corrected reprint of the second (1990) edition.

[15] **T. Foguel and A. A. Ungar**: *Involutory decomposition of groups into twisted subgroups and subgroups*, J. Group Theory **3** (2000), 27 – 46.

[16] **T. Foguel and A. A. Ungar**: *Gyrogroups and the decomposition of groups into twisted subgroups and subgroups*, Pac. J. Math. **197** (2001), 1 – 11.

[17] **R. P. Gaĭda, V. I. Tretyak and Yu. G. Yaremko**: *Center-of-mass variables in relativistic Lagrangian dynamics of a particle system*, Teoret. Mat. Fiz. **101** (1994), 402 – 416.

[18] **H. Goldstein**: *Classical mechanics*, Addison-Wesley Publishing Co., Reading, Mass., second edition, 1980.

[19] **R. E. Greene and S. G. Krantz**: *Function theory of one complex variable*, John Wiley & Sons Inc., New York, 1997.

[20] **H. Haruki and T. M. Rassias**: *A new invariant characteristic property of Möbius transformations from the standpoint of conformal mapping*, J. Math. Anal. Appl. **181** (1994), 320 – 327.

[21] **H. Haruki and T. M. Rassias**: *A new characteristic of Möbius transformations by use of Apollonius points of triangles*, J. Math. Anal. Appl. **197** (1996), 14 – 22.

[22] **H. Haruki and T. M. Rassias**: *A new characteristic of Möbius transformations by use of Apollonius quadrilaterals*, Proc. Amer. Math. Soc. **126** (1998), 2857 – 2861.

[23] **H. Haruki and T. M. Rassias**: *A new characterization of Möbius transformations by use of Apollonius hexagons*, Proc. Amer. Math. Soc. **128** (2000), 2105 – 2109.

[24] **M. Hausner**: *A vector space approach to geometry*, Dover Publications Inc., Mineola, NY, 1998. Reprint of the 1965 original.

[25] **A. N. Issa**: *Gyrogroups and homogeneous loops*,Rep. Math. Phys. **44** (1999), 345 – 358.

[26] **A. N. Issa**: *Left distributive quasigroups and gyrogroups*, J. Math. Sci. Univ. Tokyo **8** (2001), 1 – 16.

[27] **H. Kiechle**: *Theory of K-loops*, Springer-Verlag, Berlin, 2002.

[28] **M. K. Kinyon and O. Jones**: *Loops and semidirect products*, Comm. Algebra **28** (2000), 4137 – 4164.

[29] **M. K. Kinyon and A. A. Ungar**: *The gyro-structure of the complex unit disk*, Math. Mag. **73** (2000), 273 – 284.

[30] **E. Kuznetsov**: *Gyrogroups and left gyrogroups as transversals of a special kind*, Algebra Discrete Math. **3** (2003), 54 – 81.

[31] **J. Lawson and Y. Lim**: *Symmetric sets with midpoints and algebraically equivalent theories*, Results Math. **46** (2004), 37 – 56.

[32] **L. R. Lehner and O. M. Moreschi**: *On the definition of the center of mass for a system of relativistic particles*, J. Math. Phys. **36** (1995), 3377 – 3394.

[33] **J. E. Marsden**: *Elementary classical analysis*, W. H. Freeman and Co., San Francisco, 1974. With the assistance of M. Buchner, A. Erickson, A. Hausknecht, D. Heifetz, J. Macrae and W. Wilson, and with contributions by P. Chernoff, I. Fáry and R. Gulliver.

[34] **M. Milgrom**: *Is 95% of the universe really missing? an alternative to dark matter*, Sci. Amer. August 2002, 42 – 50.

[35] **D. Mumford, C. Series and D. Wright**: *Indra's pearls: The vision of Felix Klein*, Cambridge University Press, New York, 2002.

[36] **T. Needham**: *Visual complex analysis*, The Clarendon Press Oxford University Press, New York, 1997.

[37] **I. Nicolson**: *Dark side of the universe: dark matter, dark energy, and the fate of the cosmos*, John Hopkins University Press, Baltimore, MD, 2007.

[38] **M. A. Nielsen and I. L. Chuang**: *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[39] **H. O. Pflugfelder**: *Quasigroups and loops: introduction*, vol. 7 of *Sigma Series in Pure Mathematics*, Heldermann Verlag, Berlin, 1990.

[40] **H. Orlik Pflugfelder**: *Historical notes on loop theory*, Comment. Math. Univ. Carolin. **41** (2000), 359 – 370.

[41] **M. H. L. Pryce**: *The mass-centre in the restricted theory of relativity and its connexion with the quantum theory of elementary particles*, Proc. Roy. Soc. London. Ser. A. **195** (1948), 62 – 81.

[42] **L. Pyenson**: *Relativity in late Wilhelmian Germany: the appeal to a preestablished harmony between mathematics and physics*, Arch. Hist. Exact Sci. **27** (1982), 137 – 155.

[43] **J. G. Ratcliffe**: *Foundations of hyperbolic manifolds*, vol. 149 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1994.

[44] **W. Rindler**: *Introduction to special relativity*, The Clarendon Press Oxford University Press, New York, 1982.

[45] **K. Rózga**: *On central extensions of gyrocommutative gyrogroups*, Pacific J. Math. **193** (2000), 201 – 218.

[46] **L. V. Sabinin**: *On A. Ungar's gyrogroups*, Uspekhi Mat. Nauk **50(305)** (1995), 251 – 252.

[47] **L. V. Sabinin, L. L.Sabinina and L. V.Sbitneva**: *On the notion of gyrogroup*, Aequationes Math. **56** (1998), 11 – 17.

[48] **A. B. Stewart**: *The discovery of stellar aberration*, Sci. Amer. March 1964, 100 – 108.

[49] **V. Trimble**: *Existence and nature of dark matter in the universe*, Ann. Rev. Astron. Astrophys. **25** (1987), 425 – 472.

[50] **A. A. Ungar**: *Thomas rotation and the parametrization of the Lorentz transformation group*, Found. Phys. Lett. **1** (1988), 57 – 89.

[51] **A. A. Ungar**: *The relativistic noncommutative nonassociative group of velocities and the Thomas rotation*, Resultate Math. **16** (1989), 168 – 179.

[52] **A. A. Ungar**: *Thomas precession and its associated grouplike structure*, Amer. J. Phys. **59** (1991), 824 – 834.

[53] **A. A. Ungar**: *Beyond the Einstein addition law and its gyroscopic Thomas precession: The theory of gyrogroups and gyrovector spaces*, vol. 117 of *Fundamental Theories of Physics*, Kluwer Academic Publishers Group, Dordrecht, 2001.

[54] **A. A. Ungar**: *The density matrix for mixed state qubits and hyperbolic geometry*, Quantum Inf. Comput. **2** (2002), 513 – 514.

[55] **A. A. Ungar**: *The hyperbolic geometric structure of the density matrix for mixed state qubits*: Found. Phys. **32** (2002), 1671 – 1699.

[56] **A. A. Ungar**: *Analytic hyperbolic geometry: Mathematical foundations and applications*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

[57] **A. A. Ungar**: *Gyrovector spaces and their differential geometry*, Nonlinear Funct. Anal. Appl. **10** (2005), 791 – 834.

[58] **A. A. Ungar**: *Thomas precession: a kinematic effect of the algebra of Einstein's velocity addition law. Comments on: "Deriving relativistic momentum and energy. II. Three-dimensional case" by S. Sonego and M. Pin*, European J. Phys. **27(3)** (2006), $L17 - L20$.

[59] **A. A. Ungar**: *The relativistic hyperbolic parallelogram law*, in *Geometry, integrability and quantization*, Softex, Sofia, 2006, $249 - 264$.

[60] **A. A. Ungar**: *Einstein's velocity addition law and its hyperbolic geometry*, Comput. Math. Appl. **53** (2007), $1228 - 1250$.

[61] **A. A. Ungar**: *From Möbius to gyrogroups*, Amer. Math. Monthly, 2007 (in print).

[62] **A. A. Ungar**: *Analytic hyperbolic geometry and Einstein's special theory of relativity*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008.

[63] **J. Vermeer**: *A geometric interpretation of Ungar's addition and of gyration in the hyperbolic plane*, Topology Appl. **152(3)** (2005), $226 - 242$.

[64] **S. Walter**: *Minkowski, mathematicians, and the mathematical theory of relativity*, in *The expanding worlds of general relativity* Berlin, 1995, $45 - 86$. Birkhäuser Boston, Boston, MA, 1999.

[65] **S. Walter**: *The non-Euclidean style of Minkowskian relativity*: in *The symbolic universe* (J. J. Gray (ed.), M. Keynes, England), $91 - 127$, Oxford Univ. Press, New York, 1999.

[66] **S. Walter**: *Book Review: Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession: The Theory of Gyrogroups and Gyrovector Spaces*, by A. A. Ungar, Found. Phys. **32(2)** (2002), $327 - 330$.

[67] **X. B. Wang, L. C. Kwek and C. H. Oh**: *Bures fidelity for diagonalizable quadratic Hamiltonians in multi-mode systems*, J. Phys. A, **33(27)** (2000), $4925 - 4934$.

Received May 10, 2007

Department of Mathematics
North Dakota State University
Fargo, North Dakota 50105
United States of America
E-mail: Abraham.Ungar@ndsu.edu

Quasigroups and Related Systems **15** (2007), 169 – 190

Transversals in latin squares

Ian M. Wanless

Abstract

A latin square of order n is an $n \times n$ array of n symbols in which each symbol occurs exactly once in each row and column. A transversal of such a square is a set of n entries such that no two entries share the same row, column or symbol. Transversals are closely related to the notions of complete mappings and orthomorphisms in (quasi)groups, and are fundamental to the concept of mutually orthogonal latin squares.

Here we provide a brief survey of the literature on transversals. We cover (1) existence and enumeration results, (2) generalisations of transversals including partial transversals and plexes, (3) the special case when the latin square is a group table, (4) a connection with covering radii of sets of permutations. The survey includes a number of conjectures and open problems.

1. Introduction

A *latin square* of order n is an $n \times n$ array of n symbols in which each symbol occurs exactly once in each row and in each column. By a *diagonal* of such a square we mean a set of entries which contains exactly one representative of each row and column. A *transversal* is a diagonal in which no symbol is repeated.

Historically, interest in transversals arose from the study of orthogonal latin squares. A pair of latin squares $A = [a_{ij}]$ and $B = [b_{ij}]$ of order n are said to be *orthogonal mates* if the n^2 ordered pairs (a_{ij}, b_{ij}) are distinct. It is simple to see that if we look at all n occurrences of a given symbol in B, the corresponding positions in A must form a transversal. Indeed,

Theorem 1. *A latin square has an orthogonal mate iff it has a decomposition into disjoint transversals.* □

2000 Mathematics Subject Classifications: 05B15 20N05
Keywords: transversal, partial transversal, Latin square, plex, n-queens, turn-square, Cayley table, quasigroup, complete mapping, orthomorphism, covering radius

For example, below there are two orthogonal latin squares of order 8. Subscripted letters are used to mark the transversals of the left hand square which correspond to the positions of each symbol in its orthogonal mate (the right hand square).

$$\begin{array}{cccccccc} 1_a & 2_b & 3_c & 4_d & 5_e & 6_f & 7_g & 8_h \\ 7_b & 8_a & 5_d & 6_c & 2_f & 4_e & 1_h & 3_g \\ 2_c & 1_d & 6_a & 3_b & 4_g & 5_h & 8_e & 7_f \\ 8_d & 7_c & 4_b & 5_a & 6_h & 2_g & 3_f & 1_e \\ 4_f & 3_e & 1_g & 2_h & 7_a & 8_b & 5_c & 6_d \\ 6_e & 5_f & 7_h & 8_g & 1_b & 3_a & 2_d & 4_c \\ 3_h & 6_g & 2_e & 1_f & 8_c & 7_d & 4_a & 5_b \\ 5_g & 4_h & 8_f & 7_e & 3_d & 1_c & 6_b & 2_a \end{array} \qquad \begin{array}{cccccccc} a & b & c & d & e & f & g & h \\ b & a & d & c & f & e & h & g \\ c & d & a & b & g & h & e & f \\ d & c & b & a & h & g & f & e \\ f & e & g & h & a & b & c & d \\ e & f & h & g & b & a & d & c \\ h & g & e & f & c & d & a & b \\ g & h & f & e & d & c & b & a \end{array} \tag{1}$$

More generally, there is interest in sets of *mutually orthogonal latin squares* (MOLS), that is, sets of latin squares in which each pair is orthogonal in the above sense. The literature on MOLS is vast (start with [15, 16, 37]) and provides ample justification for an interest in transversals. Subsequent investigations have ranged far beyond the initial justification of Theorem 1 and have proved that transversals are interesting objects in their own right. Despite this, a number of basic questions about their properties remain unresolved, as will become obvious in the subsequent pages.

Orthogonal latin squares exist for all orders $n \notin \{2, 6\}$. For $n = 6$ there is no pair of orthogonal squares, but we can get close. Finney [25] gives the following example which contains 4 disjoint transversals indicated by the subscripts a, b, c and d.

$$\begin{array}{cccccc} 1_a & 2 & 3_b & 4_c & 5 & 6_d \\ 2_c & 1_d & 6 & 5_b & 4_a & 3 \\ 3 & 4_b & 1 & 2_d & 6_c & 5_a \\ 4 & 6_a & 5_c & 1 & 3_d & 2_b \\ 5_d & 3_c & 2_a & 6 & 1_b & 4 \\ 6_b & 5 & 4_d & 3_a & 2 & 1_c \end{array}$$

Table 1 shows the squares of order n, for $4 \leqslant n \leqslant 8$, counted according to their maximum number m of disjoint transversals. The entries in the table are counts of main classes (A *main class*, or *species* is an equivalence class of latin squares each of which has essentially the same structure. See [15, 37] for the definition.)

Evidence such as that in Table 1 led van Rees [54] to conjecture that, as $n \to \infty$, a vanishingly small proportion of latin squares have orthogonal

m	$n=4$	5	6	7	8
0	1	0	6	0	33
1	0	1	0	1	0
2	0	0	2	5	7
3	-	0	0	24	46
4	1	-	4	68	712
5	-	1	-	43	71330
6	-	-	0	-	209505
7	-	-	-	6	-
8	-	-	-	-	2024
Total	2	2	12	147	283657

Table 1: Number m of disjoint transversals in latin squares of order $n \leqslant 8$.

mates. However, the trend seems to be quite the reverse (see [57]), although no rigorous way of establishing this has yet been found.

A point that Table 1 raises is that some latin squares have no transversals at all. We now look at some results in this regard.

A latin square of order mq is said to be of *q-step type* if it can be represented by a matrix of $q \times q$ blocks A_{ij} as follows

$$\begin{array}{cccc} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mm} \end{array}$$

where each block A_{ij} is a latin subsquare of order q and two blocks A_{ij} and $A_{i'j'}$ contain the same symbols iff $i + j \equiv i' + j' \bmod m$. The following classical theorem is due to Maillet [39].

Theorem 2. *Suppose that q is odd and m is even. No q-step type latin square of order mq possesses a transversal.* □

As we will see in §4, this rules out many group tables having transversals. In particular, no cyclic group of even order has a transversal. By contrast, there is no known example of a latin square of odd order without transversals.

Conjecture 1. *Each latin square of odd order has at least one transversal.*

This conjecture is known to be true for $n \leqslant 9$ (see §3). It is attributed to Ryser [46] and has been open for forty years. In fact, Ryser's original conjecture was somewhat stronger: for every latin square of order n, the number of transversals is congruent to n mod 2. In [2], Balasubramanian proved the even case.

Theorem 3. *In any latin square of even order the number of transversals is even.* □

Despite this, it has been noted in [8] (and other places) that there are many counterexamples of odd order to Ryser's original conjecture. Hence the conjecture has now been weakened to Conjecture 1 as stated. One obstacle to proving this conjecture was recently revealed in [57].

Theorem 4. *For every $n > 3$ there exists a latin square of order n which contains an entry that is not included in any transversal.* □

Given Theorem 1, this latest theorem showed existence for all $n > 3$ of a latin square without an orthogonal mate. The same result was obtained in [24] without showing Theorem 4.

2. Partial transversals

We have seen in §1 that not all latin squares have transversals, which prompts the question of how close we can get to finding a transversal in such cases. We define a *partial transversal of length k* to be a set of k entries, each selected from different rows and columns of a latin square such that no two entries contain the same symbol. Note that in some papers (e.g. [50]) a partial transversal of length k is defined slightly differently to be a diagonal on which k different symbols appear.

Since not all squares of order n have a partial transversal of length n (i.e., a transversal), the best we can hope for is to find one of length $n-1$. The following conjecture has been attributed by Brualdi (see [15, p.103]).

Conjecture 2. *Every latin square of order n possesses a partial transversal of length $n-1$.*

A claimed proof of this conjecture by Derienko [18] contains a fatal error [8]. Recently, a paper [32] has appeared in the maths arXiv claiming a proof of Conjecture 2. However, given the history of the problem such a claim should be treated cautiously, at least until the paper has been refereed.

The best reliable result to date states that there must be a partial transversal of length at least $n - O(\log^2 n)$. This was shown by Shor [50], and the implicit constant in the 'big O' was very marginally improved by Fu et al. [26]. Subsequently Hatami and Shor [29] discovered an error in [50] (duplicated in [26]) and corrected the constant to a higher one. Nonetheless, the important thing remains that the bound is $n-O(\log^2 n)$. This improved on a number of earlier bounds including $\frac{2}{3}n+O(1)$ (Koksma [35]), $\frac{3}{4}n+O(1)$ (Drake [19]) and $n - \sqrt{n}$ (Brouwer et al. [4] and Woolbright [59]).

Erdős and Spencer [21] showed that any $n \times n$ array in which no entry occurs more than $(n-1)/16$ times has a transversal (in the sense of a diagonal with n different symbols on it). It has also been shown by Cameron and Wanless [8] that every latin square possesses a diagonal in which no symbol appears more than twice.

Conjecture 2 has been well known and open for decades. A much simpler problem is to consider the shortest possible length of a maximal partial transversal (maximal in the sense that it is contained in no partial transversal of greater length). It is easy to see that no partial transversal of length strictly less than $\frac{1}{2}n$ can be maximal, since there are not enough 'used' symbols to fill the submatrix formed by the 'unused' rows and columns. However, for all $n > 4$, maximal partial transversals of length $\lceil \frac{1}{2}n \rceil$ can easily be constructed using a square of order n which contains a subsquare S of order $\lfloor \frac{1}{2}n \rfloor$ and a partial transversal containing the symbols of S but not using any of the same rows or columns as S.

3. Number of transversals

In this section we consider the question of how many transversals a latin square can have. We define $t(n)$ and $T(n)$ to be respectively the minimum and maximum number of transversals among the latin squares of order n.

We have seen in §1 that some latin squares have no transversals but it is not settled for which orders such latin squares exist. Thus for lower bounds on $t(n)$ we cannot do any better than to observe that $t(n) \geqslant 0$, with equality occurring at least when n is even. A related question, for which no work seems to have been published, is to find an upper bound on $t(n)$ when n is odd.

Turning to the maximum number of transversals, it should be clear that $T(n) \leqslant n!$ since there are only $n!$ different diagonals. An exponential improvement on this trivial bound was obtained by McKay et al. [42]:

Theorem 5. *For $n \geqslant 5$,*

$$15^{n/5} \leqslant T(n) \leqslant c^n \sqrt{n}\, n!$$

where $c = \sqrt{\frac{3-\sqrt{3}}{6}}\, e^{\sqrt{3}/6} \approx 0.61354$. □

The lower bound in Theorem 5 is very simple and would not be too difficult to improve. The upper bound took considerably more work, although it too is probably far from the truth.

In the same paper the authors reported the results of an exhaustive computation of the transversals in latin squares of orders up to and including 9. Table 2 lists the minimum and maximum number of transversals over all latin squares of order n for $n \leqslant 9$, and the mean and standard deviation to 2 decimal places.

n	$t(n)$	Mean	Std Dev	$T(n)$
2	0	0	0	0
3	3	3	0	3
4	0	2	3.46	8
5	3	4.29	3.71	15
6	0	6.86	5.19	32
7	3	20.41	6.00	133
8	0	61.05	8.66	384
9	68	214.11	15.79	2241

Table 2: Transversals in latin squares of order $n \leqslant 9$.

Table 2 confirms Conjecture 1 for $n \leqslant 9$. The following semisymmetric squares (see [15] for a definition of semisymmetric) are representatives of the unique main class with $t(n)$ transversals for $n \in \{5, 7, 9\}$. In each case the largest subsquares are shown in **bold**.

1	**2**	**3**	**4**	**5**
2	**1**	4	5	3
3	5	**1**	2	4
4	3	5	**1**	2
5	4	2	3	**1**

3	**2**	**1**	5	4	7	6
2	**1**	**3**	6	7	4	5
1	**3**	**2**	7	6	5	4
5	6	7	4	1	2	3
4	7	6	1	5	3	2
7	4	5	2	3	6	1
6	5	4	3	2	1	7

2	**1**	**3**	6	7	8	9	5	4
1	**3**	**2**	5	4	9	**6**	**7**	**8**
3	**2**	**1**	4	9	5	**7**	**8**	**6**
9	5	4	3	2	1	**8**	**6**	**7**
8	4	6	2	5	7	1	9	3
4	**7**	**9**	**8**	3	6	5	1	2
5	**8**	**7**	**9**	6	**2**	**3**	**4**	1
6	**9**	**8**	**7**	1	**4**	**2**	**3**	5
7	6	5	1	8	**3**	**4**	**2**	9

n	Lower Bound	Upper Bound
10	5504	75000
11	37851	528647
12	198144	3965268
13	1030367	32837805
14	3477504	300019037
15	36362925	2762962210
16	244744192	28218998328
17	1606008513	300502249052
18	6434611200	3410036886841
19	87656896891	41327486367018
20	697292390400	512073756609248
21	5778121715415	6803898881738477

Table 3: Bounds on $T(n)$ for $10 \leqslant n \leqslant 21$.

In Table 3 we reproduce from [42] bounds on $T(n)$ for $10 \leqslant n \leqslant 21$. The upper bound is somewhat sharper than that given by Theorem 5, though proved by the same methods. The lower bound in each case is constructive and likely to be very close to the true value. When $n \not\equiv 2 \bmod 4$ the lower bound comes from the group with the highest number of transversals (see Table 4). When $n \equiv 2 \bmod 4$ the lower bound comes from a so-called turn-square, many of which were analysed in [42]. A *turn-square* is obtained by starting with the Cayley table of a group (typically a group of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_m$ for some m) and "turning" some of the intercalates (that is, replacing a subsquare of order 2 by the other possible subsquare on the same symbols). For example,

$$\begin{array}{ccccc|ccccc}
\mathbf{5} & \mathbf{6} & 2 & 3 & 4 & \mathbf{0} & \mathbf{1} & 7 & 8 & 9 \\
\mathbf{6} & 2 & 3 & 4 & 0 & \mathbf{1} & 7 & 8 & 9 & 5 \\
2 & 3 & 4 & 0 & 1 & 7 & 8 & 9 & 5 & 6 \\
3 & 4 & 0 & 1 & 2 & 8 & 9 & 5 & 6 & 7 \\
4 & 0 & 1 & 2 & 3 & 9 & 5 & 6 & 7 & 8 \\
\hline
\mathbf{0} & \mathbf{1} & 7 & 8 & 9 & \mathbf{5} & \mathbf{6} & 2 & 3 & 4 \\
\mathbf{1} & 7 & 8 & 9 & 5 & \mathbf{6} & 2 & 3 & 4 & 0 \\
7 & 8 & 9 & 5 & 6 & 2 & 3 & 4 & 0 & 1 \\
8 & 9 & 5 & 6 & 7 & 3 & 4 & 0 & 1 & 2 \\
9 & 5 & 6 & 7 & 8 & 4 & 0 & 1 & 2 & 3
\end{array} \tag{2}$$

achieves 5504 transversals. The 'turned' entries have been marked in **bold**.

The study of turn-squares was pioneered by Parker (see [5] and the references therein) in his unsuccessful quest for a triple of MOLS of order 10. He noticed that turn-squares often have many more transversals than is typical for squares of their order, and used this as a heuristic in the search for MOLS.

It is has long been suspected that $T(10)$ is achieved by (2). This suspicion was strengthened by McKay et al. [41] who examined several billion squares of order 10, including every square with a non-trivial symmetry, and found none had more than 5504 transversals. Parker was indeed right that the square (2) is rich in orthogonal mates (it has 12265168 of them [38], which is an order of magnitude greater than he estimated). However, using the number of transversals as a heuristic in searching for MOLS is not fail-safe. For example, the turn-square of order 14 with the most transversals (namely, 3477504) does not have any orthogonal mates [42]. Meanwhile there are squares of order n with orthogonal mates but which possess only the bare minimum of n transversals (the left hand square in (1) is one such).

Nevertheless, the number of transversals does provide a useful invariant for squares of small orders where this number can be computed in reasonable time (see, for example, [34] and [55]). It is straightforward to write a backtracking algorithm to count transversals in latin squares of small order, though this method currently becomes impractical if the order is much over 20. See [30], [31] for some algorithms and complexity theory results on the problem of counting transversals.

It seems very difficult to find theoretical estimates for the number of transversals (unless, of course, that number is zero). This difficulty is so acute that there are not even good estimates for z_n, the number of transversals of the cyclic group of order n. Vardi [52] makes the following prediction:

Conjecture 3. *There exist real constants* $0 < c_1 < c_2 < 1$ *such that*

$$c_1^n n! \leqslant z_n \leqslant c_2^n n!$$

for all odd $n \geqslant 3$.

Vardi makes this conjecture while considering a variation on the toroidal n-queens problem. The toroidal n-queens problem is that of determining in how many different ways n non-attacking queens can be placed on a toroidal $n \times n$ chessboard. Vardi considered the same problem using semiqueens in place of queens, where a semiqueen is a piece which moves like a toroidal queen except that it cannot travel on right-to-left diagonals. The solution to

Vardi's problem provides an upper bound on the toroidal n-queens problem. The problem can be translated into one concerning latin squares by noting that every configuration of n non-attacking semiqueens on a toroidal $n \times n$ chessboard corresponds to a transversal in a cyclic latin square L of order n, where $L_{ij} \equiv i - j \bmod n$. Note that the toroidal n-queens problem is equivalent to counting diagonals which simultaneously yield transversals in L and L', where $L'_{ij} = i + j \bmod n$.

As a corollary of Theorem 5 we can infer that the upper bound in Conjecture 3 is true (asymptotically) with $c_2 = 0.614$. This also yields an upper bound for the number of solutions to the toroidal n-queens problem. Theorem 5 is valid for all latin squares, but Conjecture 3 has also been attacked by methods which are specific to the cyclic square. Cooper and Kovalenko [12] first showed that Vardi's upper bound is asymptotically true with $c_2 = 0.9153$, and this was then improved to $c = 1/\sqrt{2} \approx 0.7071$ in [36]. Finding a lower bound of the form given in Conjecture 3 is still an open problem. However, [10] and [45] do give some lower bounds, each of which applies only for some n. Cooper et al. [11] estimated that perhaps the correct rate of growth for z_n is around $0.39^n\, n!$.

4. Finite Groups

By using the symbols of a latin square to index its rows and columns, each latin square can be interpreted as the Cayley table of a quasigroup. In this section we consider the important special case when that quasigroup is associative; in other words, it is a group.

Much of the study of transversals in groups has been phrased in terms of the equivalent concepts of complete mapping and orthomorphisms. Mann [40] introduced complete mappings for groups, but their definition works just as well for quasigroups. It is this: a permutation θ of the elements of a quasigroup $(Q, \oplus)$ is a *complete mapping* if $\eta : Q \mapsto Q$ defined by $\eta(x) = x \oplus \theta(x)$ is also a permutation. The permutation η is known as an *orthomorphism* of $(Q, \oplus)$, following terminology introduced in [33]. All of the results of this paper could be rephrased in terms of complete mappings and/or orthomorphisms because of our next observation.

Theorem 6. *Let $(Q, \oplus)$ be a quasigroup and L_Q its Cayley table. Then $\theta : Q \mapsto Q$ is a complete mapping iff we can locate a transversal of L_Q by selecting, in each row x, the entry in column $\theta(x)$. Similarly, $\eta : Q \mapsto Q$*

is an orthomorphism iff we can locate a transversal of L_Q by selecting, in each row x, the entry containing symbol $\eta(x)$. □

Having noted that transversals, complete mappings and orthomorphisms are essentially the same thing, we will adopt the practice of expressing our results in terms of transversals even when the original authors used one of the other notions.

As mentioned, this section is devoted to the case when our latin square is L_G, the Cayley table of a finite group G. The extra structure in this case allows for much stronger results. For example, suppose we know of a transversal of L_G that comprises a choice from each row i of an element g_i. Let g be any fixed element of G. Then if we select from each row i the element $g_i g$ this will give a new transversal and as g ranges over G the transversals so produced will be mutually disjoint. Hence

Theorem 7. *If L_G has a single transversal then it has a decomposition into disjoint transversals.* □

We saw in §1 that the question of which latin squares have transversals has not been settled. The same is true for group tables, but we are getting much closer to answering the question, building on the pioneering work of Hall and Paige.

Consider the following five propositions:

(i) L_G has a transversal.

(ii) L_G can be decomposed into disjoint transversals.

(iii) There exists a latin square orthogonal to L_G.

(iv) There is some ordering of the elements of G, say $a_1, a_2, \ldots, a_n$, such that $a_1 a_2 \cdots a_n = \varepsilon$, where ε denotes the identity element of G.

(v) The Sylow 2-subgroups of G are trivial or non-cyclic.

The fact that (i), (ii) and (iii) are equivalent comes directly from Theorem 1 and Theorem 7. Paige [43] showed that (i) implies (iv). Hall and Paige [28] then showed that (iv) implies (v). They also showed that (v) implies (i) if G is a soluble, symmetric or alternating group. They conjectured that (v) is equivalent to (i) for all groups.

It was subsequently noted in [17] that both (iv) and (v) hold for all non-soluble groups, which proved that (iv) and (v) are equivalent. A much more direct and elementary proof of this fact was given in [53].

To summarise:

Theorem 8. $(i) \iff (ii) \iff (iii) \implies (iv) \iff (v)$. □

Conjecture 4. $(i) \iff (ii) \iff (iii) \iff (iv) \iff (v)$.

As mentioned above, Conjecture 4 is known to be true for all soluble, symmetric and alternating groups. It has also been shown for many other groups including the linear groups $GL(2,q)$, $SL(2,q)$, $PGL(2,q)$ and $PSL(2,q)$ (see [23] and the references therein).

After decades of incremental progress on Conjecture 4 there has recently been what would appear to be a very significant breakthrough. In a preprint Wilcox [58] has claimed to reduce the problem to showing it for the sporadic simple groups (of which the Mathieu groups have already been handled in [13]). See [15], [22] or [58] for further reading and references on the Hall-Paige conjecture.

An immediate corollary of the proof of Theorem 7 is that for any G the number of transversals through a given entry of L_G is independent of the entry chosen. Hence (see Theorem 3.5 of [16]) we get:

Theorem 9. *The number of transversals in L_G is divisible by $|G|$, the order of G.* □

McKay et al. [42] also showed the following simple results, in the spirit of Theorem 3:

Theorem 10. *The number of transversals in any symmetric latin square of order n is congruent to n modulo 2.* □

Corollary 1. *Let G be a group of order n. If G is abelian or n is even then the number of transversals in G is congruent to n modulo 2.* □

Corollary 1 cannot be generalised to non-abelian groups of odd order, given that the non-abelian group of order 21 has 826814671200 transversals.

Theorem 11. *If G is a group of order $n \not\equiv 1 \bmod 3$ then the number of transversals in G is divisible by 3.* □

We will see below that the cyclic groups of small orders $n \equiv 1 \bmod 3$ have a number of transversals which is not a multiple of three.

The semiqueens problem in §3 led to an investigation of z_n, the number of transversals in the cyclic group of order n. Let $z'_n = z_n/n$ denote the number of transversals through any given entry of the cyclic square of order n. Since $z_n = z'_n = 0$ for all even n by Theorem 8 we shall assume for the following discussion that n is odd.

The initial values of z'_n are known from [47] and [48]. They are $z'_1 = z'_3 = 1$, $z'_5 = 3$, $z'_7 = 19$, $z'_9 = 225$, $z'_{11} = 3441$, $z'_{13} = 79259$, $z'_{15} = 2424195$, $z'_{17} = 94471089$, $z'_{19} = 4613520889$, $z'_{21} = 275148653115$, $z'_{23} = 19686730313955$ and $z'_{25} = 1664382756757625$. Interestingly, if we take these numbers modulo 8 we find that this sequence begins 1,1,3,3,1,1,3,3,1,1,3,3,1. We know from Theorem 10 that z'_n is always odd for odd n, but it is an open question whether there is any deeper pattern modulo 4 or 8. We also know from Theorem 11 that z'_n is divisible by 3 when $n \equiv 2 \bmod 3$. The initial terms of $\{z'_n \bmod 3\}$ are 1,1,0,1,0,0,2,0,0,1,0,0,2.

An interesting fact about z_n is that it is the number of *diagonally cyclic latin squares* of order n (in other words, the number of quasigroups on the set $\{1, 2, \ldots, n\}$ which have the transitive automorphism $(123\cdots n)$). See [56] for a survey on such objects.

We now discuss the number of transversals in general groups of small order. For groups of order $n \equiv 2 \bmod 4$ there can be no transversals, by Theorem 8. For each other order $n \leqslant 23$ the number of transversals in each group is given in Table 4. The groups are ordered according to the catalogue of Thomas and Wood [51]. The numbers of transversals in abelian groups of order at most 16 and cyclic groups of order at most 21 were obtained by Shieh et al [49]. The remaining values in Table 4 were computed by Shieh [47]. McKay et al. [42] then independently confirmed all counts except those for cyclic groups of order $\geqslant 21$, correcting one misprint in Shieh [47].

Bedford and Whitaker [3] offer an explanation for why all the non-cyclic groups of order 8 have 384 transversals. The groups of order 4, 9 and 16 with the most transversals are the elementary abelian groups of those orders. Similarly, for orders 12, 20 and 21 the group with the most transversals is the direct sum of cyclic groups of prime order. It is an open question whether such a statement generalises to all n.

By Corollary 1 we know that in each case covered by Table 4 (except the non-abelian group of order 21), the number of transversals must have

n	Number of transversals in groups of order n
3	3
4	0, 8
5	15
7	133
8	0, 384, 384, 384, 384
9	2025, 2241
11	37851
12	0, 198144, 76032, 46080, 0
13	1030367
15	36362925
16	0, 235765760, 237010944, 238190592, 244744192, 125599744, 121143296, 123371520, 123895808, 122191872, 121733120, 62881792, 62619648, 62357504
17	1606008513
19	87656896891
20	0, 697292390400, 140866560000, 0, 0
21	5778121715415, 826814671200
23	452794797220965

Table 4: Transversals in groups of order $n \leqslant 23$.

the same parity as the order of the square. It is remarkable though, that the groups of even order have a number of transversals which is divisible by a high power of 2. Indeed, any 2-group of order $n \leqslant 16$ has a number of transversals which is divisible by 2^{n-1}. It would be interesting to know if this is true for general n.

5. Generalised transversals

There are several ways to generalise the notion of a transversal. We have already seen one of them, namely the partial transversals in §2. In this section we collect results on another generalisation, namely plexes.

A *k-plex* in a latin square of order n is a set of kn entries which includes k representatives from each row and each column and of each symbol. A transversal is a 1-plex. The marked entries form a 3-plex in the following square:

$$\begin{array}{cccccc} 1^* & 2 & 3 & 4^* & 5 & 6^* \\ 2^* & 1 & 4 & 3^* & 6^* & 5 \\ 3 & 5^* & 1 & 6 & 2^* & 4^* \\ 4 & 6 & 2^* & 5 & 3^* & 1^* \\ 5^* & 4^* & 6^* & 2 & 1 & 3 \\ 6 & 3^* & 5^* & 1^* & 4 & 2 \end{array} \tag{3}$$

The name k-plex was coined in [55] only recently. It is a natural extension of the names duplex, triplex, and quadruplex which have been in use for many years (principally in the statistical literature, such as [25]) for 2, 3 and 4-plexes.

The entries not included in a k-plex of a latin square L of order n form an $(n-k)$-plex of L. Together the k-plex and its complementary $(n-k)$-plex are an example of what is called an *orthogonal partition* of L. For discussion of orthogonal partitions in a general setting see Gilliland [27] and Bailey [1]. For our purposes, if L is decomposed into disjoint parts K_1, $K_2, \ldots, K_d$ where K_i is a k_i-plex then we call this a $(k_1, k_2, \ldots, k_d)$-partition of L. A case of particular interest is when all parts are the same size, k. We call such a partition a *k-partition*. For example, the marked 3-plex and its complement form a 3-partition of the square in (3). By Theorem 1, finding a 1-partition of a square is equivalent to finding an orthogonal mate.

Some results about transversals generalise directly to other plexes, while others seem to have no analogue. Theorem 3 and Theorem 7 seem to be in the latter class, as observed in [42] and [55] respectively. However, Theorems 2 and 8 showed that not every square has a transversal, and exactly the same arguments work for any k-plex where k is odd [55].

Theorem 12. *Suppose that q and k are odd integers and m is even. No q-step type latin square of order mq possesses a k-plex.* □

Theorem 13. *Let G be a group of finite order n with a non-trivial cyclic Sylow 2-subgroup. The Cayley table of G contains no k-plex for any odd k but has a 2-partition and hence contains a k-plex for every even k in the range $0 \leqslant k \leqslant n$.* □

The situation for even k is quite different to the odd case. Rodney [9, p.105] conjectures that every latin square has a duplex. This conjecture was strengthened in [55] to the following:

Conjecture 5. *Every latin square has the maximum possible number of disjoint duplexes. In particular, every latin square of even order has a* 2*-partition and every latin square of odd order has a* $(2, 2, 2, \ldots, 2, 1)$*-partition.*

Note that this conjecture also strengthens Conjecture 1. It also implies that every latin square has k-plexes for every even value of k up to the order of the square.

Conjecture 5 is true for all latin squares of orders $\leqslant 8$ and for all soluble groups (see [53, 55]). Depending on whether a soluble group has a non-trivial cyclic Sylow 2-subgroup, it either has a k-plex for all possible k, or has them for all possible even k but no odd k. If the Hall-Paige conjecture could be proved it would completely resolve the existence question of plexes in groups, and these would remain the only two possibilities. It is worth noting that other scenarios occur for latin squares which are not based on groups. For example, the square in (3) has no transversal but clearly does have a 3-plex. It is conjectured in [55] that there exist arbitrarily large latin squares of this type.

Conjecture 6. *For all even* $n > 4$ *there exists a latin square of order* n *which has no transversal but does contain a* 3*-plex.*

Another possibility was shown by a family of squares constructed in [20].

Theorem 14. *For all even* n *there exists a latin square of order* n *which has* k*-plexes for every odd value of* k *between* $\frac{1}{4}n - \frac{1}{2}$ *and* $\frac{3}{4}n + \frac{1}{2}$*, but not for any odd value of* k *outside this range.* □

Interestingly, there is no known example of odd integers $a < b < c$ and a latin square which has an a-plex and a c-plex but no b-plex.

The union of an a-plex and a disjoint b-plex of a latin square L is an $(a + b)$-plex of L. However, it is not always possible to split an $(a + b)$-plex into an a-plex and a disjoint b-plex. Consider a duplex which consists of $\frac{1}{2}n$ disjoint intercalates (latin subsquares of order 2). Such a duplex does not contain a partial transversal of length more than $\frac{1}{2}n$, so it is a long way from containing a 1-plex.

We say that a k-plex is *indivisible* if it contains no c-plex for $0 < c < k$. The duplex just described is indivisible. Indeed, for every k there is a indivisible k-plex in some sufficiently large latin square. This was first shown in [55], but "sufficiently large" in that case meant quadratic in k. This was improved to linear in [6] as a corollary of the following result.

Theorem 15. *For every $k \geqslant 2$ there exists a latin square of order $2k$ which contains two disjoint indivisible k-plexes.* □

Theorem 15 means that some squares can be split in "half" in a way that makes no further division possible. Experience with latin squares suggests that they generally have a vast multitude of partitions into various plexes, which in one sense means that latin squares tend to be a long way from being indivisible. This makes Theorem 15 slightly surprising.

It is a wide open question for what values of k and n there is a latin square of order n containing an indivisible k-plex. However, Bryant et al. [6] found the answer when k is small relative to n.

Theorem 16. *Let n and k be positive integers satisfying $5k \leqslant n$. Then there exists a latin square of order n containing an indivisible k-plex.* □

So far we have essentially looked at questions where we start with a latin square and ask what sort of plexes it might have. To complete the section we consider the reverse question. We want to start with a plex and ask what latin squares it might be contained in. Strictly speaking this is a silly question, since we defined a plex in terms of its host latin square, which therefore is the only possible answer. However, suppose we define a *k-homogeneous partial latin square* of order n to be an $n \times n$ array in which each cell is either blank or filled (the latter meaning that it contains one of $\{1, 2, \ldots, n\}$), and which has the properties that (i) no symbol occurs twice within any row or column, (ii) each symbol occurs k times in the array, (iii) each row and column contains exactly k filled cells. (The standard definition of a homogeneous partial latin square is slightly more general. However, once empty rows and columns have been deleted, it agrees with ours.) We can then sensibly ask whether this k-homogeneous partial latin square is a k-plex. If it is then we say the partial latin square is *completable* because the blank entries can be filled in to produce a latin square.

Theorem 17. *If $1 < k < n$ and $k > \frac{1}{4}n$ then there exists a k-homogeneous partial latin square of order n which is not completable.* □

Burton [7], and Daykin and Häggkvist [14] independently conjecture that if $k \leqslant \frac{1}{4}n$ then every k-homogeneous partial latin square is completable. It seems certain that for k sufficiently small relative to n, every k-homogeneous partial latin square is completable. This has already been proved when $n \equiv 0 \bmod 16$ in [14]. The following partial extension result due to Burton [7]0 also seems relevant.

Theorem 18. *For $k \leqslant \frac{1}{4}n$ every k-homogeneous partial latin square of order n is contained in a $(k+1)$-homogeneous partial latin square of order n.* □

6. Covering radii for sets of permutations

A novel approach to Conjecture 1 and Conjecture 2 has recently been opened up by Andre Kézdy and Hunter Snevily. To explain this interesting new approach, we need to introduce some terminology.

Consider the *symmetric group* S_n as a metric space equipped with *Hamming distance*. That is, the distance between two permutations $g, h \in S_n$ is the number of points at which they disagree (n minus the number of fixed points of gh^{-1}). Let P be a subset of S_n. The *covering radius* $\mathrm{cr}(P)$ of P is the smallest r such that the balls of radius r with centres at the elements of P cover the whole of S_n. In other words every permutation is within distance r of some member of P, and r is chosen to be minimal with this property.

Theorem 19. *Let $P \subseteq S_n$ be a set of permutations. If $|P| \leqslant n/2$, then $\mathrm{cr}(P) = n$. However, there exists P with $|P| = \lfloor n/2 \rfloor + 1$ and $\mathrm{cr}(P) < n$.* □

This result raises an obvious question. Given n and s, what is the smallest m such that there is a set S of permutations with $|S| = m$ and $\mathrm{cr}(S) \leqslant n - s$? We let $f(n, s)$ denote this minimum value m. This problem can also be interpreted in graph-theoretic language. Define the graph $G_{n,s}$ on the vertex set S_n, with two permutations being adjacent if they agree in at least s places. Now the size of the smallest dominating set in $G_{n,s}$ is $f(n, s)$.

Theorem 19 shows that $f(n, 1) = \lfloor n/2 \rfloor + 1$. Since any two distinct permutations have distance at least 2, we see that $f(n, n-1) = n!$ for $n \geq 2$. Moreover, $f(n, s)$ is a monotonic increasing function of s (by definition).

The next case to consider is $f(n, 2)$. Kézdy and Snevily made the following conjecture in unpublished notes.

Conjecture 7. *If n is even, then $f(n, 2) = n$; if n is odd, then $f(n, 2) > n$.*

The Kézdy–Snevily conjecture has several connections with transversals. The rows of a latin square of order n form a *sharply transitive set* of permutations (that is, for any i and j, exactly one permutation carries i to j); and every sharply transitive set is the set of rows of a latin square.

Theorem 20. *Let S be a sharply transitive subset of S_n. Then S has covering radius at most $n-1$, with equality if and only if the corresponding latin square has a transversal.* □

Corollary 2. *If there exists a latin square of order n with no transversal, then $f(n,2) \leqslant n$. In particular, this holds for n even.* □

Hence Conjecture 7 implies Conjecture 1, as Kézdy and Snevily observed. In fact a stronger result holds:

Theorem 21. *If S is the set of rows of a latin square L of order n with no transversal, then S has covering radius $n-2$.* □

The following result is due to Kézdy and Snevily. See [8] for a proof.

Theorem 22. *Conjecture 7 implies Conjecture 2.* □

In other words, to solve the longstanding Ryser and Brualdi conjectures it may suffice to answer this: How small can we make a subset $S \subset S_n$ which has the property that every permutation in S_n agrees with some member of S in at least two places?

In Corollary 2 we used latin squares to find an upper bound for $f(n,2)$ when n is even. For odd n we can also find upper bounds based on latin squares. The idea is to choose a latin square with few transversals, or whose transversals have a particular structure, and add a small set of permutations meeting each transversal twice. For $n = 5, 7, 9$, we now give a latin square for which a single extra permutation suffices, showing that $f(n,2) \leqslant n+1$ in these cases.

1	2	3	4	5
2	1	4	5	3
3	5	1	2	4
4	3	5	1	2
5	4	2	3	1
1	3	4	2	5

1	2	3	4	5	6	7
2	3	1	5	4	7	6
3	1	2	6	7	4	5
4	5	6	7	1	2	3
5	4	7	1	6	3	2
6	7	4	2	3	5	1
7	6	5	3	2	1	4
3	2	1	7	6	5	4

1	3	2	4	6	5	7	9	8
2	1	3	5	4	6	8	7	9
3	2	1	7	9	8	4	6	5
4	6	5	9	8	7	1	3	2
5	4	6	8	7	9	3	2	1
6	5	4	2	1	3	9	8	7
7	9	8	1	3	2	5	4	6
8	7	9	3	2	1	6	5	4
9	8	7	6	5	4	2	1	3
5	4	6	1	3	2	9	8	7

In general, we have the following:

Theorem 23. $f(n,2) \leqslant \frac{4}{3}n + O(1)$ *for all n.* □

The reader is encouraged to seek out [8] and the survey by Quistorff [44] for more information on covering radii for sets of permutations.

7. Concluding Remarks

We have only been able to give the briefest of overviews of the fascinating subject of transversals in this survey. Space constraints have forced the omission of much worthy material, including proofs of the theorems quoted. However, even this brief skim across the surface has shown that many basic questions remain unanswered and much work remains to be done.

References

[1] **R. A. Bailey:** *Orthogonal partitions in designed experiments*, (Corrected reprint), Des. Codes Cryptogr. **8** (1996), 45 – 77.

[2] **K. Balasubramanian:** *On transversals in latin squares*, Linear Algebra Appl. **131** (1990), 125 – 129.

[3] **D. Bedford and R. M. Whitaker:** *Enumeration of transversals in the Cayley tables of the non-cyclic groups of order* 8, Discrete Math. **197/198** (1999), 77 – 81.

[4] **A. E. Brouwer, A. J. de Vries and R. M. A. Wieringa:** *A lower bound for the length of partial transversals in a latin square*, Nieuw Arch. Wisk. **26** (1978), 330 – 332.

[5] **J. W. Brown and E. T. Parker:** *More on order* 10 *turn-squares*, Ars Combin. **35** (1993), 125 – 127.

[6] **D. Bryant, J. Egan, B. M. Maenhaut and I. M. Wanless:** *Indivisible plexes in latin squares*, preprint.

[7] **B. Burton:**, *Completion of partial latin squares*, honours thesis, University of Queensland, 1997.

[8] **P. J. Cameron and I. M. Wanless:** *Covering radius for sets of permutations*, Discrete Math. **293** (2005), 91 – 109.

[9] **C. J. Colbourn and J. H. Dinitz (eds):** *The CRC handbook of combinatorial designs*, CRC Press, Boca Raton, FL, 1996.

[10] **C. Cooper:** *A lower bound for the number of good permutations, Data Recording, Storage and Processing*, Nat. Acad. Sci. Ukraine **2.3** (2000), 15 – 25.

[11] **C. Cooper, R. Gilchrist, I. Kovalenko and D. Novakovic:** *Deriving the number of good permutations, with applications to cryptography*, Cybernet. Systems Anal. **5** (2000), 10 – 16.

[12] **C. Cooper and I. M. Kovalenko:** *The upper bound for the number of complete mappings*, Theory Probab. Math. Statist. **53** (1996), 77 – 83.

[13] **F. Dalla Volta and N. Gavioli:** *Complete mappings in some linear and projective groups*, Arch. Math. (Basel), **61** (1993), 111 – 118.

[14] **D. E. Daykin and R. Häggkvist:** *Completion of sparse partial latin squares*, Graph theory and combinatorics, 127 – 132, Academic Press, London, 1984.

[15] **J. Dénes and A. D. Keedwell:** *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

[16] **J. Dénes and A. D. Keedwell:** *Latin squares: New developments in the theory and applications*, Ann. Discrete Math. **46**, North-Holland, Amsterdam, 1991.

[17] **J. Dénes and A. D. Keedwell:** *A new conjecture concerning admissibility of groups*, European J. Combin. **10** (1989), 171 – 174.

[18] **I. I. Derienko:** *On a conjecture of Brualdi*, (Russian), Mat. Issled. **102**, (1988), 53 – 65.

[19] **D. A. Drake:** *Maximal sets of latin squares and partial transversals*, J. Statist. Plann. Inference **1** (1977), 143 – 149.

[20] **J. Egan and I. M. Wanless:** *Latin squares with no small odd plexes*, preprint.

[21] **P. Erdős and J. Spencer:** *Lopsided Lovász local lemma and latin transversals*, Discrete Appl. Math. **30** (1991), 151 – 154.

[22] **A. B. Evans:** *The existence of complete mappings of finite groups*, Congr. Numer. **90** (1992), 65 – 75.

[23] **A. B. Evans:** *The existence of complete mappings of* $\mathrm{SL}(2,q)$*,* $q \equiv 3$ *modulo* 4, Finite Fields Appl. **11** (2005), 151 – 155.

[24] **A. B. Evans:** *Latin squares without orthogonal mates*, Des. Codes Cryptog. **40** (2006), 121 – 130.

[25] **D. J. Finney:** *Some orthogonal properties of the* 4×4 *and* 6×6 *latin squares*, Ann. Eugenics **12** (1945), 213 – 219.

[26] **H. Fu and S. Lin:** *The length of a partial transversal in a latin square*, J. Combin. Math. Combin. Comput. **43** (2002), 57 – 64.

[27] **D. C. Gilliland:** *A note on orthogonal partitions and some well-known structures in design of experiments*, Ann. Statist. **5** (1977), 565 – 570.

[28] **M. Hall and L. J. Paige:** *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541 – 549.

[29] **P. Hatami and P. W. Shor:** *Erratum to: A lower bound for the length of a partial transversal in a latin square*, J. Combin. Theory Ser. A (to appear).

[30] **J. Hsiang, D. F. Hsu and Y. P. Shieh:** *On the hardness of counting problems of complete mappings*, Disc. Math. **277** (2004), 87 – 100.

[31] **J. Hsiang, Y. Shieh and Y. Chen:** *The cyclic complete mappings counting problems*, PaPS: Problems and problem sets for ATP workshop in conjunction with CADE-18 and FLoC 2002, Copenhagen, 2002.

[32] **L. Hu and X. Li:** *Color degree condition for large heterochromatic matchings in edge-colored bipartite graphs*, http://arxiv.org/abs/math.CO/0606749.

[33] **D. M. Johnson, A. L. Dulmage and N. S. Mendelsohn:** *Orthomorphisms of groups and orthogonal latin squares I*, Canad. J. Math. **13** (1961), 356 – 372.

[34] **R. Killgrove, C. Roberts, R. Sternfeld, R. Tamez, R. Derby and D. Kiel:** *Latin squares and other configurations*, Congr. Numer. **117** (1996), 161 – 174.

[35] **K. K. Koksma:** *A lower bound for the order of a partial transversal in a latin square*, J. Combinatorial Theory **7** (1969), 94 – 95.

[36] **I. N. Kovalenko:** *Upper bound for the number of complete maps*, Cybernet. Systems Anal. **32** (1996), 65 – 68.

[37] **C. F. Laywine and G. L. Mullen:** *Discrete mathematics using latin squares*, Wiley, New York, 1998.

[38] **B. M. Maenhaut and I. M. Wanless:** *Atomic latin squares of order eleven*, J. Combin. Des. **12** (2004), 12 – 34.

[39] **E. Maillet:** *Sur les carrés latins d'Euler*, Assoc. Franc. Caen. **23** (1894), 244 – 252.

[40] **H. B. Mann:** *The construction of orthogonal latin squares*, Ann. Math. Statistics **13**, (1942), 418 – 423.

[41] **B. D. McKay, A. Meynert and W. Myrvold:** *Small latin squares, quasigroups and loops*, J. Combin. Des. **15**, (2007), 98 – 119.

[42] **B. D. McKay, J. C. McLeod and I. M. Wanless:** *The number of transversals in a latin square*, Des. Codes Cryptogr. **40** (2006), 269 – 284.

[43] **L. J. Paige:** *Complete mappings of finite groups*, Pacific J. Math. **1** (1951), 111 – 116.

[44] **J. Quistorff:** *A survey on packing and covering problems in the Hamming permutation Space*, Electron. J. Combin. **13** (2006), *A*1.

[45] **I. Rivin, I. Vardi and P. Zimmerman:** *The n-Queens Problem*, Amer. Math. Monthly **101** (1994), 629 – 639.

[46] **H. J. Ryser:** *Neuere Probleme der Kombinatorik*, Vortrage über Kombinatorik Oberwolfach, 24–29 Juli (1967), 69 – 91.

[47] **Y. P. Shieh:** *Partition strategies for #P-complete problem with applications to enumerative combinatorics*, PhD thesis, National Taiwan University, 2001.

[48] **Y. P. Shieh:** *private correspondence*, 2006.

[49] **Y. P. Shieh, J. Hsiang and D. F. Hsu:** *On the enumeration of abelian k-complete mappings*, Congr. Numer. **144** (2000), 67 – 88.

[50] **P. W. Shor:** *A lower bound for the length of a partial transversal in a latin square*, J. Combin. Theory Ser. A **33** (1982), 1 – 8.

[51] **A. D. Thomas and G. V. Wood:** *Group tables*, Shiva Mathematics Series 2, Shiva Publishing, Nantwich, 1980.

[52] **I. Vardi:** *Computational Recreations in Mathematics*, Addison-Wesley, Redwood City, CA, 1991.

[53] **M. Vaughan-Lee and I. M. Wanless:** *Latin squares and the Hall-Paige conjecture*, Bull. London Math. Soc. **35** (2003), $1-5$.

[54] **G. H. J. van Rees:** *Subsquares and transversals in latin squares*, Ars Combin. **29 B** (1990), $193-204$.

[55] **I. M. Wanless:** *A generalisation of transversals for latin squares*, Electron. J. Combin. **9(1)** (2002), $R12$.

[56] **I. M. Wanless:** *Diagonally cyclic latin squares*, European J. Combin. **25** (2004), $393-413$.

[57] **I. M. Wanless and B. S. Webb:** *The existence of latin squares without orthogonal mates*, Des. Codes Cryptog. **40** (2006), $131-135$.

[58] **S. Wilcox:** *Reduction of the Hall-Paige conjecture to sporadic simple groups*, http://www.math.harvard.edu/~stewartw/hallpaige2.pdf

[59] **D. E. Woolbright:** *An $n \times n$ latin square has a transversal with at least $n - \sqrt{n}$ distinct symbols*, J. Combin. Theory Ser. A **24** (1978), $235-237$.

School of Mathematical Sciences
Monash University
Vic 3800, Australia
E-mail: ian.wanless@sci.monash.edu.au

Received February 28, 2007