

A finite quandle is therefore connected if, for every $a, b \in A$, there exist $x_1, \dots, x_n \in A$ such that

$b = x_1 * (x_2 * (\dots (x_n * a)))$ (compare to unique right division!). Connected quandles are arguably the most important class of quandles, both from the algebraic and topological points of view. Indeed, Latin quandles are connected, and the class of connected quandles is a very natural generalization of left distributive quasigroups: many structural properties of left distributive quasigroups extend to connected quandles.

To illustrate the power of connectedness, let us prove the following implication for quandles that are (both left and right) distributive.

Proposition 3.1 [3] Finite connected distributive quandles are quasigroups.

Proof. Assume the contrary, and let $(Q, *)$ be the smallest counter example. Right distributivity says that every right translation R_a is a homomorphism, hence, its image, $R_a(Q)$, forms a subquandle that is also connected and distributive (both properties project to homomorphic images). For every $a, b \in Q$, the subquandles $R_a(Q)$ and $R_b(Q)$ are isomorphic: connectedness of $(Q, *)$ provides an automorphism $\alpha \in \text{LMlt}(Q, *)$ such that $\alpha(a) = b$, and it follows from $\alpha(x * a) = \alpha(x) * \alpha(a) = \alpha(x) * b$ that α restricts to an isomorphism between $R_a(Q)$ and $R_b(Q)$. Therefore, by minimality, all subquandles $R_a(Q)$ are proper subquasigroups. Now we prove that $R_a(Q) \subseteq R_x * a(Q)$ for every $x, a \in Q$. Let $y * a \in R_a(Q)$. Since $R_a(Q)$ is a quasigroup, there is $z * a \in R_a(Q)$ such that $y * a = (z * a) * (x * a)$. Hence $y * a \in R_x * a(Q)$. By induction, $R_a(Q) \subseteq R_{x_1} * a(Q) \subseteq R_{x_2} * (x_1 * a)(Q) \subseteq \dots$, and thus, from connectedness, $R_a(Q) \subseteq R_b(Q)$ for every $a, b \in Q$. Hence all subquasigroups $R_a(Q)$ are equal, and since $x \in R_x(Q)$ for every $x \in Q$, all of them are equal to Q , a contradiction.

3.2 Loops. A loop is a quasigroup (Q, \cdot) with a unit element 1, i.e. $1 \cdot a = a \cdot 1 = a$ for every $a \in A$. Loops will be denoted multiplicatively. To avoid parenthesizing, we shortcut $x \cdot yz = x \cdot (y \cdot z)$ etc., and we remove parentheses whenever the elements associate, that is we shall write xyz whenever we know that $x \cdot yz = xy \cdot z$. For all unproved statements, we refer to any introductory book on loops, such as [4, 11].

Let (Q, \cdot) be a loop. Inner mappings are those elements of the multiplication group $\text{Mlt}(Q, \cdot)$ that fix the unit element. For example, the conjugation mappings $T_x(z) = xz/x$ are inner and, in a way, measure the non-commutativity in the loop. The left inner mappings are defined by $L_{x,y}(z) = (xy) \setminus (x \cdot yz)$ and measure the non-associativity from the left.

The most common example of loops are groups (i.e. associative loops), and most classes of loops studied in literature are those satisfying a weak version of associativity or commutativity.

We list a few weak associative laws (note that all the conditions hold in groups): a loop is called

- diassociative if all 2-generated sub loops are associative;
- left alternative if $x \cdot x y = x_2 y$;
- power-associative if all 1-generated subloops are associative;
- Moufang if $(xy \cdot x)z = x(y \cdot xz)$ (the dual law is equivalent in loops);
- left Bol if $(x \cdot yx)z = x(y \cdot xz)$;
- automorphic if all inner mappings are automorphisms.
- left automorphic if all left inner mappings $L_{x,y}$ are automorphisms.

Moufang's theorem [13] says that in a Moufang loop, every subloop generated by three elements that associate, is associative. In particular, Moufang loops are diassociative, since $a(ba) = (ab)a$ for every a, b , as directly follows from the Moufang law. Bol loops are power-associative.

The nucleus of a loop (Q, \cdot) is the set of all elements $a \in Q$ that associate with all other elements, That is $N = \{a \in Q : a \cdot x y = a x \cdot y, x \cdot a y = x a \cdot y, x \cdot y a = x y \cdot a \text{ for all } x, y \in Q\}$.

An element of a loop is called nuclear if it belongs to the nucleus. A mapping $f : Q \rightarrow Q$ is called k -nuclear if $x_k f(x) \in N$ for every $x \in Q$.

4.0 QUASIGROUPS AND LATIN QUANDLES

A Latin square is an $n \times n$ array on n symbols having the property that each symbol/ element appears exactly once in each row and column. A set with a binary operation that whose multiplication table is Latin square is called a quasigroup [Definition 2.10].

Smith [16], a quasigroup (Q, \cdot) is a set equipped with binary multiplication \cdot such that in the equation $x \cdot y = z$, (1)

Knowledge of any two of x, y, z specifies the third uniquely. It follows that for each element $x \in Q$, the right multiplication $R(x): Q \rightarrow Q; y \rightarrow y \cdot x$ (2)

And left multiplication $L(x): Q \rightarrow Q; y \rightarrow x \cdot y$ (3)

are permutations of Q . Therefore a quasigroup that is self distributive is a Latin quandle [3]. And for Latin quandles, the concept of left ($a \setminus b$) and the right (b / a) divisibility operations are unique which they inherit from their parent structure (quasigroup). Therefore, Latin quandles are special quandles. Axiomatically we will define Latin quandles below;

4.1 Definition: [3, 14] An algebraic structure $(Q, *)$ is called a Latin quandle if it obeys the following laws simultaneously:

- i. $x * x = x$ (idempotent law)
- ii. $a * x = b$ (left divisibility law)
- iii. $y * a = b$ (right divisibility law)
- iv. $a * (x * y) = (a * x) * (a * y)$ (left distributive law)
- v. $(x * y) * a = (x * a) * (y * a)$ (right distributive law)
- vi. $(x * y) * (u * v) = (x * u) * (y * v)$ (mediality property)
- vii. $x * (x * y) = y$ left involutory or (left symmetric) (hence we have unique left division with $x \setminus y = x * y$)

We observed that left distributive quasigroups are idempotent: $x * (x * x) = (x * x) * (x * x)$ by left distributivity and we can cancel from the right.

4.1 Remark. Every left distributive quasigroup that is idempotent is a Latin quandle.

Non – idempotent medial quasigroups exist indeed, abelian groups are examples. Also it is observed that idempotent trimedial binary algebras are distributive given $a, b, c \in A$, the sub algebra (a, b, c) is medial, hence $(a * b) * (a * c) = (a * a) * (b * c) = a * (b * c)$ and dually for right distributivity;

A binary algebra is called a left quandle, if it is idempotent, left distributive and has unique left division (remarkably, the three conditions correspond to the three Reidemeister moves in Knot Theory) [18]

Quandles that also have unique right division are called *Latin quandles*. Indeed Latin quandles and left distributive quasigroups and the very same things.

Alhamedadi [17] hence discussed that Latin quandles are right distributive quasigroups and left – distributive Latin Quandles are distributive quasigroups. Given a binary algebra $(A, *)$, it is natural to consider *left translations* $L_a(x) = a * x$, and $R_a(x) = x * a$, and the semigroups they generate, the left multiplication semi-group $LMlt(A, *) = (L_a : a \in A)$, the right multiplication semigroup $Mlt(A, *) = (L_a, R_a : a \in A)$. Unique left division turns left translations into permutations, thus the left multiplication semi group into a group (and usually for right translations). We observe that $L_a^{-1}(x) = a \setminus x$ and $R_a^{-1}(x) = x / a$. Also note that $(A, *)$ is left distributive if and only if L_a is an endomorphism for every $a \in A$. Hence, in quandles, $LMlt(A, *)$ is a subgroup of the automorphism group.

4.2 Remark: All Latin quandles are quasigroup but all quasigroups are not Latin quandles. Therefore Latin quandles generally obey the following;

$$a * (a \setminus b) = b \tag{4}$$

$$a \setminus (a * b) = b \tag{5}$$

Since $a * x = b \leftrightarrow x = a \setminus b \tag{6}$

And $x \setminus x = x = x / x \tag{7}$

For universal consideration, $(Q, *, \setminus)$ is quandle. But $(Q, *, /)$ is a Latin quandle.

Therefore, while quandle generally are equipped with two binary operations, Latin quandles are equipped with three binary operations. This structure is completely devoid of the identity element e such that $ae = ea = a$ otherwise, $(Q, *, e \setminus, /)$ is a loop.

4.3 Definition [3, 14] A finite quandle Q is therefore connected if for every $a, b \in Q$ there exists $x_1, * (x_2 * (\dots (\dots (x_n * a))))$.

The above definition however means that the inner mappings group of Q act transitively on Q .

Remark 4.3 Therefore All Latin Quandles are connected quandles, (proposition 3.1) since,

$L_{x/y}(y) = x$ [15]. That is if $(Q, *)$ is a Latin quandle, for all $x, y \in Q$, one can write $(x/y) * y = x$, or $x = y * (y \setminus x)$.

5.0 CONSTRUCTION OF LATIN QUANDLES:

5.1 Theorem. Let Q be a commutative quasigroup of order $2n + 1$; $n \geq 1$ such that

$$x + y = y^{-1} . xx \text{ for all } x, y \in Q.$$

Then $(Q, +)$ is a Latin quandle.

Proof:

Since Q is already a quasigroup, then the left and right division laws holds. We only show that idempotent and distributive laws hold in Q . Let $x, y, z \in Q$

- i) Let $x \in Q$, then $x + x = x^{-1} . xx = (x^{-1} x) = ex = x$ (idempotent law).
- ii) $(x + y) + z = (y^{-1} . xx) + z = z^{-1} . ((y^{-1} . xx)(y^{-1} . xx))$ (8)

Similarly

$$(x + z) + (y + z) = (z^{-1} . xx) + (z^{-1} . yy) = z(yy^{-1}) (z^{-1} . xx) (z^{-1} . xx) \quad (9)$$

Next we need to show that equation (8) = (9)

$$(z^{-1} . xx) + (z^{-1} . yy) = z(yy^{-1}) (z^{-1} . xx)(z^{-1} . xx) \text{ then}$$

$$z(yy^{-1}) (z^{-1} . xx)(z^{-1} . yy)^{-1} . (z^{-1} . xx)$$

$$((z^{-1})^{-1}(y)^{-1})(z^{-1} . xx) . ((z^{-1})^{-1}(y)^{-1})(z^{-1} . xx)$$

$$(1 . (y)^{-1})(z^{-1} . xx) . (1 . (y)^{-1})(z^{-1} . xx)$$

Recall that $(x + y) = (y^{-1} . xx)$ then

$$(z^{-1}(x + y) . (z^{-1}(x + y)$$

$$(z^{-1}(x + y)(x + y)) \quad (10)$$

This concludes the prove for the right distributive law.

Similarly, for the left distributive law $x + (y + z) = (x + y) + (x + z)$ holds.

Example 5.1 Quasigroup $(Q, .)$ order 5 in a Cayley Table representation

.	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	4	5	1	2
4	4	5	1	2	3
5	5	1	2	3	4

Table 1

Example 5.2 Latin quandle $(Q,+)$ order 5 generated from example 5.1 in a Cayley Table representation

+	1	2	3	4	5
1	1	5	4	3	2
2	3	2	1	5	4
3	5	4	3	2	1
4	2	1	5	4	3
5	4	3	2	1	5

Table 2

Theorem 5.2:

Let Q be a non- commutative self invertible Quasigroup of order $2n + 1$; $n \geq 1$

Such that $x + y = y x^{-1} y$ for all $x, y \in Q$.

Then $(Q, +)$ is a Latin Quandle of order $2n + 1$.



Proof:

Let $x, y, z \in Q$ then,

- i) $x + x = x x^{-1} x = x$ (idempotent law)
- ii) Left and right distributive laws
 - a) $x + (y + z) = (x + y) + (x + z)$
 - b) $(x + y) + z = (x + z) + (y + z)$
- iii) Since Q is already a quasigroup, then the left and right division laws holds. We only show that idempotent and distributive laws hold in Q .

Next we show that Let $x \in Q$, then $x + x = x x^{-1} x = (x x^{-1} x) = ex = x$ (idempotent law).

For left distributive law we show that (ii a) holds.

Let $x, y, z \in Q$ then, $x + (y + z) = (x + y) + (x + z)$

Since Q is a quasigroup, $x + (y + z) = x + (z y^{-1} z) = z y^{-1} z x^{-1} z y^{-1} z$ (11)

Then $(x + y) + (x + z) = y x^{-1} y + z x^{-1} z$
 $= z x^{-1} z (y x^{-1} y)^{-1} + z x^{-1} z$ (12)

Next, we need to show that (11) = (12)

$$\begin{aligned} & z x^{-1} z (y x^{-1} y)^{-1} z x^{-1} z \\ & z x^{-1} z (y(x^{-1})^{-1} y) z x^{-1} z \\ & (z x^{-1} z y^{-1}) (y^{-1} z x^{-1} z) \\ & x^{-1} ((z y^{-1} z) (z y^{-1} z)) \\ & x^{-1} ((y + z) (y + z)) \end{aligned}$$

Therefore,

$$x + (y + z) = ((z y^{-1} z) x^{-1} (z y^{-1} z)) \tag{13}$$

Note equation (11) = (13) and we conclude that equation (11) = (12)

Similarly, for the right distributive law,

$$((z y^{-1} z) x^{-1} (z y^{-1} z)) = z x^{-1} z (y(x^{-1})^{-1} y) z x^{-1} z$$

This concludes the proof.

Example 5.3 Quasigroup (Q, .) of order 7 in a Cayley Table representation

.	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	7	1	2	3	4	5	6
3	6	7	1	2	3	4	5
4	5	6	7	1	2	3	4
5	4	5	6	7	1	2	3
6	3	4	5	6	7	1	2
7	2	3	4	5	6	7	1

Table 3

Example 5.4 Latin Quandle (Q, +) of order 7 generated from example 5.3 in a Cayley Table representation

+	1	2	3	4	5	6	7
1	1	3	5	7	2	4	6
2	7	2	4	6	1	3	5
3	6	1	3	5	7	2	4
4	5	7	2	4	6	1	3
5	4	6	1	3	5	7	2
6	3	5	7	2	4	6	1
7	2	4	6	1	3	6	7

Table 4

6.0 CONCLUSION

Quasigroups in general has been established with Theorem 5.1 and 5.2 as the parent algebraic structure of Latin Quandles which is very fruitful for future research work especially on investigation on some inverse properties peculiar to Latin quandles

REFERENCES.

- [1] Victor Shcherbacov A.: Elements of quasigroup theory and some its application in code theory 2003.www.karlin.mff.cuni.cz/drapal/speccurs.pdf.
- [2] C. Burstin and W. Mayer: Distributive Gruppen von endlicher ordnung, J, reineund angew Maths 160(1929), 111 -130.
- [3] David Stanovsky: A guide to self – distributive quasigroups, or latin quandles, quasigroups and related systems 23, (2015) 91 -128.
- [4] R. H. Bruck: A survey of binary systems. Ergebnisse der Mathematic undlher Grenzgebiete, Springer Verlag, Berlin – Gottingo – Heidelberg (1958),
- [5] R. H Bruck: Some results in the theory of quasigroups, Trans. Amer. Math. Soc. 55(1944), 19- 52
- [6] V. D. Belousov: Fundamentals of the theory of quasigroups and loops. (Russian) Nauka, Moskva (1967)
- [7] V. D. Belousov, and I. A Florya: On left distributive quasigroups (Russian). Bul Akad. Stiinte RSS Moldoven 7 (1965), 3-13.
- [8] D. Moskvich: Associativity vs. Distributivity low Dimensional Topology Blog July 21 (2014) <https://idtopology.wordpress.com/2014/07/21/associativity-vs-distributivity/>.
- [9] D. Joyce: Classifying invariant of Knots, the knot quandle, J Pure Appl.Algebra 23 (1982) 37 – 65.
- [10] S. V. Matveev: Distributive groupoids in knot theory, math.USSR. Sbornik 47 (1984), 73-83.
- [11] H. O Pflugfelder: Quasigroups and loops: introduction, Berlin , Helderm verlag 1990.
- [12] Clauwens F.J-B. J.: On small connected Quandles. Arxiv,1011.2430v(Math.GR)2018.
- [13] A Drapel: A simplified proof of moufang’s theorem, Proc Amer. Math Soc. 139 (2011) 93-98.
- [14] A.O.Isere, J. O. Adeniran, T. G. Jaiyeola (pre print): Latin quandles and Applications to cryptography(2020).

- [15] Indu R.U Churchill, M. Elhamdadi, M. Hiji and S. Nelson: Singular knots and Involutive Quandles, Journal of knot theory and its Ramifications, vol 26 (14)(2018) 1-10 DOI 10.1142/s0218216517500997.
- [16] Jonathan D.H. Smith: On Quasigroups and quandles Discrete Mathematics 109 (1992) 277- 282 North – Holland.
- [17] Mohamed Elhamdadi: Distributivity in Quandles and Quasigroups, DOI: 10. 10077978-3- 642- 55361 -5-14, 2012 source arxiv.
- [18] S. Nelson: The combinatorial revolution in knot theory. Notices Amer. Math. Soc. 58(2011) 155- 1561.

