Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 20, Number 2 (2024), pp. 313-321

http://www.ripublication.com

Distributive quasigroups And Their Parastrophs

Mengue Mengue David Joel

Mathematics Department-Faculty of Science-University of Ebolowa-Cameroon.

Abstract

Long overshadowed by general group theory, quasigroups and loops theory have become increasingly important in combinatorics, cryptography, algebra and physics, covering key research problems.In this paper, we give a detail study of quasigroups that satisfies the distributive laws, and prove the claim that whenever a quasigroup $(Q,\cdot) = (Q,F)$ satisfy the left and right distributive laws, the following algebraic structures$(\mathrm{Q}, \mathrm{F}^{-1})$; $(\mathrm{Q},{}^{-1}\mathrm{F})$;$(\mathrm{Q},{}^{-1}(F^{-1}))$;$(Q,({}^{-1}F)^{-1})$and $(Q,({}^{-1}(F^{-1}))^{-1})$ called parastrophs of (Q,F) are quasigroups, furthermore we prove that all the parastrophs of (Q,F) are also distributive quasigroups.

Keywords: Distributive quasigroups, parastrophs, normal subquasigroups, cosets, isotopic.

INTRODUCTION

A non empty set Q on which a binary operation$(\cdot)$ is defined is called a groupoid if for all $a, b \in Q$, $a \cdot b \in Q$. We denote it by $(Q,\cdot)$. A groupoid $(Q,\cdot)$ is called a right quasigroup if for all $a, b \in Q$, there exists a unique solution $x \in Q$ to the equation $x \cdot a = b$, that is in this case any right translation denoted by $R(a)$ of the groupoid $(Q,\cdot)$ is a permutation on the set Q. Similarly a groupoid $(Q,\cdot)$ is called a left quasigroup if for all $a, b \in Q$, there exists a unique solution $y \in Q$, to the equation $a \cdot y = b$, that is in this case any left translation denoted $L(a)$ for all $a \in Q$ of the groupoid $(Q,\cdot)$ is a permutation of the set Q. A left and right quasigroups$(Q,\cdot)$ is called a quasigroup. If also there is an element $e \in Q$ called identity element and such that $e \cdot a = a = a \cdot e$ for every $a \in Q$, then the quasigroup is called a loop. A binary closed operation $\circ$ on a non empty set Q is said to be left distributive (resp right distributive) over another binary operation $\perp$ on the same set Q if for all $a, b, c \in Q$ we have $a \circ (b \perp c) = (a \circ b) \perp (a \circ c)$ $(\text{resp}(a \perp b) \circ c = (a \circ c) \perp (b \circ c))$. A binary operation $\circ$ on Q is said to be distributive over $\perp$ if it is both left and right distributive on $\perp$. For any

quasigroup$(Q,\cdot) = (Q,F)$ it is possible to associate five other algebraic structures called parastrophs of $(Q,\cdot)$. If we denote the quasigroup operation (function) by the letter F, then with the quasigroup operation F, we can associate the following binaries operations for x_1, x_2 and x_3 elements of Q.

$$F(x_1,x_2) = x_1 \cdot x_2 = x_3 \Leftrightarrow F^{(12)}(x_2,x_1) = x_2 \circ x_1 = x_3 \Leftrightarrow F^{(13)}(x_3,x_2) = x_3/x_2 = x_1 \Leftrightarrow F^{(23)}(x_1,x_3) = x_1 \backslash x_3 = x_2 \Leftrightarrow F^{(123)}(x_2,x_3) = x_2 * x_3 = x_1 \Leftrightarrow F^{(132)}(x_3,x_1) = x_3 \times x_1 = x_2.$$

In other words $F^{\sigma}(x_{1\sigma}, x_{2\sigma}) = x_{3\sigma} \Leftrightarrow F(x_1,x_2) = x_3 \ where\ \sigma \in S_3$. For example, $F^{(132)}(x_3,x_1) = x_2 \Leftrightarrow F(x_1,x_2) = x_3$: that is,

$F^{(132)}\left(x_{1(132)}, x_{2(132)}\right) = x_{3(132)} \Leftrightarrow F(x_1,x_2) = x_3$. We shall also find it convenient to employ the alternative notation$x_1 \cdot x_2 = x_3 \Leftrightarrow x_{1\sigma} \cdot^{\sigma} x_{2\sigma} = x_{3\sigma}$where $\sigma \in S_3$, for parastrophic operations.

The following notation is also equivalent and appropriate:

$$F = \binom{123}{123}, \text{ and } x_1 \cdot x_2 = x_3 = F(x_1,x_3),$$

$$F^{-1} = \binom{123}{213}, \text{ and } x_2/x_1 = x_3 = F^{-1}(x_2,x_1),$$

$$^{-1}F = \binom{123}{132}, \text{ and } x_1 * x_3 = x_2 = {}^{-1}F(x_1,x_3),$$

$$^{-1}(F^{-1}) = \binom{123}{231}, \text{ and } x_2 \circledcirc x_3 = x_1 = {}^{-1}(F^{-1})(x_2,x_3),$$

$$(^{-1}F)^{-1} = \binom{123}{312}, \text{ and } x_3 \circledast x_1 = x_2 = (^{-1}F)^{-1}(x_3,x_1),$$

$$(^{-1}(F^{-1}))^{-1} = \binom{123}{321}, \text{ and } x_3 \circ x_2 = x_1 = (^{-1}(F^{-1}))^{-1}(x_3,x_2).$$

It is natural to ask if the five above algebraic structures are quasigroups? And furthermore, do they satisfy the distributive identities? In briefare they also distributive quasigroups? The study of parastrophs of quasigroup has receive attention from authors like Fisher and Yates (1934), who called them adjugates, Stein (1957) and (1959), and Belousov (1965) called them conjugates. Sade in (1959) called them parastrophes. They have been studies also by Artzy (1963), Charles Linder and Dwight Steedley in (1975) other contribution to the field include Pflugfelder (1990), Chein, Pflugfelder and Smith (1990) and Dene and Keedwell (1974). The most recent study of the parastrophs of quasigroup are by Sokhatski (1995), Duplak (2000), Shchukin and Gushan (2004), Jaiyeola (2008) and MengueMengue and Ajala (2010). But none of the above contribution cares about distributive quasigroups.

Definition:1 A quasigroup$(Q,\cdot)$ is called distributive if it satisfied the following identities relations

$$x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z) \qquad \textbf{(1)}$$

and

$$(y \cdot z) \cdot x = (y \cdot x) \cdot (z \cdot x) \quad \textbf{(2)}$$

For all $x, y, z \in Q$.

Separately, the identities (1) and (2) are called the left distributive and the right distributive law, respectively.

A well known way to construct a distributive quasigroup is by way of dividing an interval of a given proportion.

Example:1 If $(\mathbb{R}, +, \cdot)$ is the field of real numbers, and $x, y \in \mathbb{R}$are ssuch that$x + y = 1$, then $(\mathbb{R}, \circ)$where $a \circ b = xa + yb$ is a commutative distributive quasigroup;

Usingthis method , one can construct a distributive quasigroup starting with any commutative ring with unity. Taking $(\mathbb{R}, \circ) = (\mathbb{Z}_5, +)$ the following is an operation table $(\mathbb{R}, \circ)$such that $a \circ b = 2a + 4b$.

$\circ$	**0**	**1**	**2**	**3**	**4**
0	0	4	3	2	1
1	2	1	0	4	3
2	4	3	2	1	0
3	1	0	4	3	2
4	3	2	1	0	4

In example 1 above, if $x = y = \frac{1}{2}$, then $a \circ b = \frac{x+y}{2}$ is the arithmetic mean of x and y. Thus, the distributive quasigroup are closely related to arithmetic means on sets of numbers, and the study of distributive quasigroups can be applied for generalization of means.

Example:2 Consider the binary operation $*$ on Euclidian plan P define by:$*: P \times P \to P$ with$A * B = C$ If and only if B is the middle of the segment $[\![AC]\!]$ Operation $*$ is called the central symmetric and $A * B$ is read the symmetric of point A with respect to point B .One observe that $(P, *)$ is a distributive quasigroup (Well known in Geometry).

We begin our study of distributive quasigroups with some properties which follow directly from it definition.

Theorem:1 If $(Q, \cdot)$ is a distributive quasigroup,the following is true for all $x, y, z \in Q$.

- **a)** $(Q, \cdot)$is idempotent i.e $z^2 = z$ **(3)**
- **b)** $L(z)$ and $R(z)$ are automorphisms of $(Q, \cdot)$.
- **c)** $R(z)L(z) = L(z)R(z)$ **(4)**

d) If $(\backslash)$ and $(/)$ stand for the left and right division in $(Q,\cdot)$ then we have:

$$x \cdot (y \backslash z) = (x \cdot y) \backslash (x \cdot z) \quad \textbf{(5)}$$

$$(y/x) \cdot z = (y \cdot z) \,/\, (x \cdot z) \quad \textbf{(6)}$$

$$x \backslash (y \cdot z) = (x \backslash y) \cdot (x \backslash z) \quad \textbf{(7)}$$

$$(y \cdot x)/z = (y/z) \cdot (x/z) \quad \textbf{(9)}$$

Proof:

a) From (1) with $x = y = z$ we have $x \cdot (x \cdot x) = (x \cdot x) \cdot (x \cdot x)$Thus $x = x \cdot x$. Denoting $x \cdot x$by x^2, we get $z^2 = z$ for all $z \in Q$.

b) By definition $l(x)$ and $R(x)$ are translation bijective maps with the departure set equal to the arrival set and identities in relation (1) and (2) can be rewritten as $(y \cdot z)L(x) = yL(x) \cdot zL(x)$ and $(y \cdot z)R(x) = yR(x) \cdot zR(x)$ which means that $L(x)$ and $R(x)$ are automorphisms.

c) Setting $x = z$, from relation (1) and (2), we have $x \cdot (y \cdot x) = (x \cdot y) \cdot (x \cdot x) = (x \cdot y) \cdot x$. In terms of $L(x)$ and $R(x)$, we can write this as $yR(x)L(x) = yL(x)R(x)$ which give us relations (4).

d) To prove from (5) to (9) one need to recall the definition of $(\backslash)$ and $(/)$: $x \backslash y = z$ means that $y = x \cdot z$ and $x/y = z$ means that $x = z \cdot y$

To prove relation (5) we solve for t the equation $x \cdot (y \backslash z) = (x \cdot y) \backslash (x \cdot t)$ and show that $t = z$, $x \cdot t = (x \cdot y) \cdot \big(x \cdot (y \backslash z)\big) = x \cdot \big(y \cdot (y \backslash z)\big) = x \cdot z$, or $t = z$

To prove relation (7) we also solve for s the equation $x \backslash (y \cdot s) = (x \backslash y) \cdot (x \backslash z)$ and show that $s = z$, Thus $y \cdot s = x \cdot \big((x \backslash y) \cdot (x \backslash z)\big) = \big(x \cdot (x \backslash y)\big) \cdot \big(x \cdot (x \backslash z)\big) = x \cdot z \; or \; s = z$

To prove relation (6) we again solve for h the equation $(y/z) \cdot x = (y \cdot x)/(z \cdot x)$ that gives $(h \cdot x)/(z \cdot x) = (y/z) \cdot x$ imply that $h \cdot x = \big((y/z) \cdot x\big) \cdot (z \cdot x) = \big((y/z) \cdot z\big) \cdot x = y \cdot x$ or $h = y$.

To prove relation (9) we solve for r the equation $(r \cdot z)/x = (y/x) \cdot (z/x)$ we then have $r \cdot z = \big((y/x) \cdot (z/x)\big) \cdot x = \big((y/x) \cdot x\big) \cdot \big((z/x) \cdot x\big) = y \cdot z$ Thus $r = y$.

Proposition:1 Let $(Q,\cdot)$ be a distributive quasigroup. If $|Q| \geq 2$ then Q do not have the identity element

Proof: Assume that $(Q,\cdot)$ has an identity element say e then e is both left and right identity we then have $\forall x \in Q, e \cdot x = x$ but being a distributive quasigroup all it elements are idempotent i.e$\forall x \in Q, x = x \cdot x$ hence $e \cdot x = x \cdot x \; thus \; x = e \;\; \forall x \in Q$ hence $Q = \{e\}$ and $|Q| = 1$ This contradict our assumption hypothesis hence the proposition is true.

P**roposition:2** Let $(Q,\cdot)$ be a distributive quasigroup. $(Q,\cdot)$ is associative if and only if

$|Q| = 1$.

Proof: $(Q,\cdot)$ is a distributive quasigroup.

Assume that $|Q| = 1$ Let take $Q = \{x\}$, we have $x \cdot (x \cdot x) = x^3 = (x \cdot x) \cdot x$ hence the law is associative.

Assume that $(Q,\cdot)$ is associative then for all $x, y \in Q$ we have $x \cdot (x \cdot y) = (x \cdot x) \cdot y$ but $x \cdot (x \cdot y) = (x \cdot x) \cdot y = (x \cdot y) \cdot (x \cdot y)$ hence $x = x \cdot y$ that is $x \cdot x = x \cdot y$ thus $x = y$ for all $x, y \in Q$ we then have $|Q| = 1$

Remark: An interesting property of distributive quasigroup is that a distributive quasigroup can never be a loop unless it consist of one element only. Indeed if $(Q,\cdot)$ is distributive and is a loop with identity element $e$then the left distributive property implies that $x \cdot y = x \cdot (y \cdot e) = (x \cdot y) \cdot x$, and $x = e$ for every $x \in Q$.

In fact a distributive quasigroup cannot even possess a one side identity $e_\lambda$or e_ρ.

Proposition:3 Let $(Q,\cdot)$ be a finite distributive quasigroup; If $(Q,\cdot)$ is commutative then $|Q|$ is odd.

Proof : Assume that $(Q,\cdot)$ is commutative, for all $a \in A$ take $B = \cup_{i\in I} \{\{x_i, y_i\}\, x_i, y_i \in A: x_i \neq a \; and \; x_I y_I = a\}$

Our main work:

Theorem: If $(Q,\cdot)$ is a distributive quasigroup, then all its parastrophs are also distributive:

Proof:

1-) We begin with the left distributive law for the parastroph$(Q,\backslash)$ i.e: we want to show that

$$a \setminus (b \setminus c) = (a \setminus b) \setminus (a \setminus c) \qquad \textbf{(1)}$$

Let $b \setminus c = x$; $a \setminus b = y; a \setminus c = z$ and $a \setminus x = t$ then we have that $c = b \cdot x, b = a \cdot y$, $c = a \cdot z$ and $x = a \cdot t$ hence the relation (1) can be rewrite as $a \setminus x = y \setminus z$ or $t = y\backslash z$ to solve (1) one need just to show that $z = y \cdot t$ so we have:

$$y \cdot t = (a\backslash b) \cdot (a\backslash x) = a\backslash(b \cdot x) = a\backslash c = z$$

We continuous with the right distributive law for (Q,\).

We want to show that

$$(a\backslash b)\backslash c = (a\backslash c)\backslash(b\backslash c) \qquad \textbf{(2)}$$

Let take $a\backslash b = q; a\backslash c = w; b\backslash c = r$ and $q\backslash c = t$ then we have that $b = a \cdot q; c = a \cdot w; c = b \cdot r$ and $c = q \cdot t$ hence the relation (2) can be rewrite as $q\backslash c =$

$w\backslash r \; or \; t = w\backslash r$ to solve (2) one need just to show that $r = w \cdot t$.

Now $w \cdot t = (a\backslash c) \cdot (q\backslash c) = (a \cdot q)\backslash c = b\backslash c = r$.

Hence by relations (1) and (2) : $(Q,\backslash)$ is distributive.

2-) We begin with the left distributive law for the parastroph $(Q,/)$ i.e: we want to show that

$a/(b/c) = (a/b)/(a/c)$ **(3)**

Let $b/c = x$; $a/b = y; a/c = z$ and $a/x = t$ then we have that $b = x \cdot c, a = y \cdot b$, $a = z \cdot c$ and $a = t \cdot x$ hence the relation (3) can be rewrite as $a/x = y/z$ or $t = y/z$ to solve (3) one need just to show that $y = t \cdot z$ so we have:

$t \cdot z = (a/x) \cdot (a/c) = a/(x \cdot c) = a/b = y$

$(a/b)/c = (a/c)/(b/c)$ **(4)**

Let take $a/b = q; a/c = w; b/c = r$ and $q/c = t$ then we have that $a = q \cdot b; a = w \cdot c; b = r \cdot c$ and $q = t \cdot c$ hence the relation (4) can be rewrite as $q/c = w/r \; or \; t = w/r$ to solve (4) one need just to show that $w = t \cdot r$

Now $t \cdot r = (q/c) \cdot (b/c) = (q \cdot b)/c = a/c = w$.

Hence by relations (3) and (4) : $(Q,/)$ is distributive.

3-) Knowing that for all $a, b \in Q, a \circ b = b \cdot a$, we want to first show that

$a \circ (b \circ c) = (a \circ b) \circ (a \circ c)$

$(a \circ b) \circ (a \circ c) = (b \cdot a) \circ (c \cdot a) = (c \cdot a) \cdot (b \cdot a) = (c \cdot b) \cdot a = a \circ (c \cdot b) = a \circ (b \circ c)$ For the right distributive law of $(Q,\circ)$ we have:

$(a \circ c) \circ (b \circ c) = (c \cdot a) \circ (c \cdot b) = (c \cdot b) \cdot (c \cdot a) = c \cdot (b \cdot a) = (b \cdot a) \circ c = (a \circ b) \circ c$

Hence (Q,∘) is distributive.

4-) To show that $(Q,*)$ is also distributive we need to recall that $a * b = b/a$ for all $a, b \in Q$. We are going to first show the left distributive law for $(Q,*)$ ..We then have the following

$$(a * b) * (a * c) = (b/a) * (c/a) = (c/a)/(b/a)$$
$$= (c/b)/a$$
$$= a * (c/b)$$
$$= a * (b * c)$$

For the right distributive law we have:

$$(a * c) * (b * c) = (c/a) * (c/b) = (c/b)/(c/a)$$

$$= c/(b/a)$$
$$= (b/a) * c$$
$$= (a * b) * c$$

Hence $(Q,*)$ is a distributive quasigroup.

5-) For the case of $(Q,\times)$ we have:

$$(a \times b) \times (a \times c) = (b\backslash a) \times (c\backslash a) = (c\backslash a)\backslash(b\backslash a)$$
$$= (c\backslash b)\backslash a$$
$$= a \times (c\backslash b)$$
$$= a \times (b \times c)$$

And

$$(a \times c) \times (b \times c) = (c\backslash a) \times (c\backslash b) = (c\backslash b)\backslash(c\backslash a)$$
$$= c\backslash(b\backslash a)$$
$$= (b\backslash a) \times c$$
$$= (a \times b) \times c$$

Hence $(Q,\times)$ is also distributive.

REFERENCES

[1] Albert A.A.. (1943) Quasigroups I, Trans. Amer.Math.Soc., 54.pp 507-519.
[2] Artzy.R`Isotopy of parastrophy quasigroups`Proc.Amer.Math.Soc.14(1963) 429-431p
[3] Belousov.V.D.`On the structure of distributive quasigroups`.Mat.Sb.50(1960),267-298.MR.22(1961)#11059
[4] Bruck.R.H.(1958) A Survey of binary system Sprinc-Verlag
[5] Chein.O, Pflugfelder.H.O.,and Smith.J.D.H.,`Quasigroups and loops. Theory and application,` Heldermann,Berlin,1990.
[6] Dene and Keedwell.`Latin square and their applications`.English University press.Lts (1974).pp549
[7] Duplak.J.`A parastrophic equivalence in quasigroups:quasigroups and related system (2000), 7-14p
[8] Fisher and Yates (1934)
[9] Jaiyeola.T.G.`Some necessary and sufficient conditions for parastrophic equivalence of the associative law in quasigroups`Fasc.Math.(2008),25-35p
[10] Linder and Dwight Steedley in (1975)
[11] Mengue Mengue.D.J.and Ajala.S.O.`Parastrophs of quasigroups`.Jour.of Math.Sc.Vol.21,N.3.(2010).339-344p.
[12] Pflugfelder.H.O, (1990), Quasigroups and loops; Introduction. Berlin; Sigma series pure Math 7.Heldermann Verlag.147p.

[13] Sade.A.`Quasigroupes parastrophiques`Math.Nachr.30 (1959),73-106p
[14] Shchukin.K.K. and Gushan.V.V..`A representation of parastrophs of loops and quasigroups.`J.Disc.Math. and appl.14(2004),535-542pp.
[15] Sokhatski.F.N`On isotope of a group`Jour.Ukrainian.Math.Journal (1995),1585-1590p
[16] Stein.S.K.,`On the foundation of quasigroup`. Trans.Amer.Math.Soc.85.(1957) 228-256p. MR.33.(1959)#922