Chapter I

CHAPTER I

DEFINITIONS AND BASIC PROPERTIES OF QUASIGROUPS

Definition: 1.1

A non empty set Q on which a binary operation $(\cdot)$ is defined is called a **groupoid** if, for all $x, y \in Q$, $x \cdot y \in Q$.

Definition: 1.2

A groupoid $(Q, \cdot)$ is called a **left cancellation groupoid,** if the following implication is fulfilled:

$$a \cdot x = a \cdot y \Rightarrow x = y$$

for all $a, x, y \in Q$.

Definition: 1.3

A groupoid $(Q, \cdot)$ is called a **right cancellation groupoid,** if the following implication is fulfilled:

$$x \cdot a = y \cdot a \Rightarrow x = y$$

for all $a, x, y \in Q$.

Definition: 1.4

A groupoid $(Q, \cdot)$ is called a **cancellation groupoid,** if it is both a left and a right cancellation groupoid.

Definition: 1.5

A groupoid $(Q, \cdot)$ is called a **left solvable groupoid,** if the equation $x \cdot a = b$ has a solution x for every $x, a, b \in Q$.

Definition: 1.6

A groupoid $(Q, \cdot)$ is called a **right solvable groupoid,** if the equation $a \cdot y = b$ has a solution y for every $y, a, b \in Q$.

Definition: 1.7

A groupoid $(Q, \cdot)$ is called a **solvable groupoid,** if it is both a left and a right solvable groupoid.

Definition: 1.8

Let Q be a nonempty set, let n be natural number, $n \geq 2$. A map f that maps all n-tuples over Q into elements of the set Q is called an **n-ary operation,** i.e. $f(x_1, x_2, \ldots, x_n) = x_{n+1}$ for all $(x_1, x_2, \ldots, x_n) \in Q^n$ and $x_{n+1} \in Q$.

Definition: 1.9

A non-empty set A together with an n-ary operation $\alpha : A^n \to A$, $n \geq 2$ is called **n-groupoid** and is denoted by (A, α).

Definition: 1.10 [51]

A **Latin square of order n** is an n x n square matrix whose entries consist of n symbols such that each symbol appears exactly once in each row and each column. Example of a 4 x 4 Latin square is given below.

Order 4:

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

Definition: 1.11

The Latin square is called a **reduced Latin square,** if the elements in the first row and the first column are in monotonically increasing order. Example of a 3 x 3 reduced Latin square is given below.

Order 3:

1	2	3
2	3	1
3	2	1

Note: 1.12

Order 5:

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

This specific Latin square is **not a reduced Latin square** as the rows are not arranged in order.

Number of Latin Squares:

The total number of Latin squares N of order n are computed using the formula:

$$N(n, n) = n!\,(n-1)!\,L(n, n)$$

The number of reduced Latin squares

n	L(n , n)
1	1
2	1
3	1
4	4
5	56
6	9408
7	16 942 080
8	535 281 401 856
9	377 597 570 964 258 816

Here, L (n, n) is the number of reduced Latin squares of order n. For large values of n, the number of reduced Latin squares is difficult to compute and hence the total number of Latin squares of high order is unknown.

Definition: 1.13 [51]

A **Quasigroup** $(Q, *)$ is a set Q of elements along with a binary operation '$*$' having the following properties:

(a) For all $a, b \in Q$, $a * b \in Q$ (Q is closed under $*$)

(b) For all $a, b \in Q$, there exist unique $x, y \in Q$ so that

$a * x = b$ and $y * a = b$ i.e. ($(Q, *)$ has unique solubility of equations).

Remark: 1.14

Because of the unique solubility of equations, each element will appear exactly once in each row and exactly once in each column of the multiplication table of $(Q, *)$. That is, each row and column is a permutation of the elements of Q. If $|Q| = n$, then the interior of the Cayley table for $(Q, *)$ forms an n x n Latin square.

Example: 1.15

Let $Q = Z_5 = \{0, 1, 2, 3, 4\}$ and let $x * y = (x + y) \bmod 5$. Then $(Q, *)$ is addition modulo 5 on Z_5 and the Cayley table for $(Q, *)$ is given by,

$*$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 1.1

$(Q, *)$ is a quasigroup because its interior is a 5 x 5 Latin square. This quasigroup is also a group.

Note: 1.16

Every group is a quasigroup, but not every quasigroup is a group. Hence, groups are a special subset of the universe of quasigroups. Unlike groups, quasigroups are not required to obey the associative rule

$$a * (b * c) = (a * b) * c, \qquad \text{for all a, b and c.}$$

Definition: 1.17

The elements of Quasigroup $(Q, \cdot)$ are called **points.**

Lemma: 1.18

In any cancellative groupoid $(Q, \cdot)$ the identities

$$a(ab \cdot c) \cdot c = b,$$
$$a \cdot (a \cdot bc)c = b$$

are equivalent. Any cancellative groupoid with these two identities is a quasigroup.

Lemma: 1.19

In every quasigroup $(Q, \cdot)$ any two of the following three statements (one equivalence and two identities) are equivalent:

$$ab = c \Leftrightarrow a = bc,$$

$$ab \cdot a = b,$$

$$a \cdot ba = b.$$

Definition: 1.20

Consider a quasigroup $(Q, \cdot)$. We can introduce two new operations on the quasigroup, **left division and right division.**

Right division is the operation $/ : Q^2 \to Q \ ; \ (x, y) \mapsto x / y = xR(y)^{-1}$

Left division is the operation $\backslash : Q^2 \to Q \ ; \ (y, x) \mapsto y / x = xL(y)^{-1}$

Remark: 1.21

Right division undoes multiplication on the right, while left division undoes multiplication on the left. If Q is commutative, $x/y = y\backslash x$. But it is not true in general that $x/y = x\backslash y$.

Definition: 1.22

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 \, satisfying the identities:

$$y \backslash (y \cdot x) = x; \qquad x = (x \cdot y)/y;$$
$$y \cdot (y \backslash x) = x; \qquad x = (x/y) \cdot y.$$

Definition: 1.23

If $f(x) \cdot y = y$ for all $y \in Q$, then $f(x)$ is called **left identity element** of a quasigroups $(Q, \cdot)$.

Definition: 1.24

If $y \cdot e(x) = y$ for all $y \in Q$, then $e(x)$ is called **right identity element** of a quasigroups $(Q, \cdot)$.

Definition: 1.25

A quasigroup with an identity element is called **loop.**

Definition: 1.26

A quasigroup $(Q, \cdot)$ is **isotopic** to the quasigroup $(Q, *)$ if there exist permutations θ, ϕ, ψ of the set Q such that $(x \cdot y)\psi = x\theta * y\varphi$ for all $x, y \in Q$.

Theorem: 1.27

Every quasigroup is isotopic to some loop.

Definition: 1.28

A quasigroup $(Q,\cdot)$ has the **left inverse property** if for each $a \in Q$, there exists an $a_L^{-1} \in Q$ such that

$$a_L^{-1} \cdot (a \cdot b) = b, \qquad \text{for all } b \in Q.$$

Definition: 1.29

A quasigroup $(Q,\cdot)$ has the **right inverse property** if for each $a \in Q$, there exists an $a_R^{-1} \in Q$ such that

$$(b \cdot a) \cdot a_L^{-1} = b, \qquad \text{for all } b \in Q.$$

Definition: 1.30

A quasigroup $(Q,\cdot)$ has the **inverse property** if both left inverse property and right inverse property hold.