Chapter III

CHAPTER III

DIFFERENT TYPES OF QUASIGROUPS

There are different types of quasigroups which will be useful for Cryptographical applications. Many interesting quasigroups were introduced and studied by many researchers. This chapter is devoted to the study different types of quasigroups.

SECTION - 3.1

MEDIAL QUASIGROUPS AND IDEMPOTENT MEDIAL QUASIGROUPS

Definition: 3.1.1

A quasigroup $(Q,\cdot)$ is **medial,** if for $a,b,c,d \in (Q,\cdot)$ the identity $ab\cdot cd = ac\cdot bd$ holds.

Example: 3.1.2

The quasigroup $(Q,\cdot)$ is given in the following Table 3.1.1, is a medial quasigroup.

.	a	b	c	d	e	f	g
a	a	d	g	c	f	b	e
b	c	f	b	e	a	d	g
c	e	a	d	g	c	f	g
d	g	c	f	b	e	a	d
e	b	e	a	d	g	c	f
f	d	g	c	f	b	e	a
g	f	b	e	a	d	g	c

Table 3.1.1

Definition: 3.1.3

By a **formula** we mean any expression built up from a number of variables using the operations $\cdot, \backslash$ and $/$. More precisely:

1. the variables $x, y, \ldots$ are formulae;
2. if φ, ψ are formulae, then so are $\varphi \cdot \psi$, $\varphi \backslash \psi$ and φ / ψ.

Notation: 3.1.4

A formula φ containing (at most) two variables gives rise to a new binary operation $Q \times Q \rightarrow Q$, which we will also denote by the letter φ.

Theorem: 3.1.5

Let φ, ψ be the binary operations defined by any two formulae in a medial quasigroup Q. Then the following identity holds:

$$\varphi(\psi(a, b), \psi(c, d)) = \psi(\varphi(a, c), \varphi(b, d)).$$

Proof:

It is easily verified that the operations $\cdot, \backslash$ and $/$ are mutually medial, i.e. the identities $ab \backslash cd = (a \backslash c)(b \backslash d)$, $ab / cd = (a / c)(b / d)$ and $(a \backslash b)/(c \backslash d) = (a / c) \backslash (b / d)$ hold.

For example, if we denote $x = a \backslash c$ and $y = b \backslash d$, then $ax = c$ and $by = d$. Using mediality we get

$$cd = ax \cdot by = ab \cdot xy$$

$$\Rightarrow ab \backslash cd = xy = (a \backslash c)(b \backslash d).$$

A binary operation defined by a formula φ is mutually medial with multiplication, left and right division:

$$\varphi(ab, cd) = \varphi(a, c) \cdot \varphi(b, d), \tag{1}$$

$$\varphi(a \backslash b, c \backslash d) = \varphi(a, c) \backslash \varphi(b, d), \tag{2}$$

$$\varphi(a / b, c / d) = \varphi(a, c) / \varphi(b, d). \tag{3}$$

This is obvious for $\varphi(a, b) = a$ and $\varphi(a, b) = b$, and follows by induction for more complicated formulae. Supposing the identities are true for φ_1 and φ_2, we see that they also hold for $\varphi = \varphi_1 \cdot \varphi_2$:

$$\begin{aligned}\varphi(ab, cd) &= \varphi_1(ab, cd) \cdot \varphi_2(ab, cd) \\ &= \varphi_1(a, c)\varphi_1(b, d) \cdot \varphi_2(a, c)\varphi_2(b, d) \\ &= \varphi_1(a, c)\varphi_2(a, c) \cdot \varphi_1(b, d)\varphi_2(b, d) \\ &= \varphi(a, c) \cdot \varphi(b, d)\end{aligned}$$

The argument is similar for identities (2), (3) and formulae $\varphi = \varphi_1 \setminus \varphi_2$, $\varphi = \varphi_1 / \varphi_2$.

Finally, mutual mediality of φ and ψ is obtained by induction on ψ :

$$\begin{aligned}\varphi(\psi(a, b), \psi(c, d)) &= \varphi(\psi_1(a, b)\psi_2(a, b), \psi_1(c, d)\psi_2(c, d)) \\ &\overset{(1)}{=} \varphi(\psi_1(a, b), \psi_1(c, d)) \cdot \varphi(\psi_2(a, b), \psi_2(c, d)) \\ &= \psi_1(\varphi(a, c), \varphi(b, d)) \cdot \psi_2(\varphi(a, c), \varphi(b, d)) \\ &= \psi(\varphi(a, c), \varphi(b, d)).\end{aligned}$$

Identity (2) is used if $\psi = \psi_1 \setminus \psi_2$, and identity (3) if $\psi = \psi_1 / \psi_2$.

Corollary: 3.1.6

If $(Q, \cdot)$ is a medial quasigroup, then the binary operation defined by a formula φ is also medial.

Definition: 3.1.7

The points $a, b, c, d \in Q$ are said to form a **parallelogram,** denoted by **Par(a, b, c, d)**, if there are points $p, q \in Q$ such that $pa = qb$ and $pd = qc$.

Remark: 3.1.8

The relation $pa = qb$ and $pd = qc$, for $p, q \in Q$ satisfies the axioms of parallelogram space.

1. For any three points a, b, c there is a unique point d such that Par (a, b, c, d).
2. Par (a, b, c, d) implies Par (e, f, g, h), where (e, f, g, h) is any cyclic permutation of (a, b, c, d) or (d, c, b, a).
3. Par (a, b, c, d) and Par(c, d, e, f) imply Par (a, b, f, e).

Result: 3.1.9 [62]

The statement Par (a, b, c, d) holds. For any point p there is the unique point q and for any point q there is the unique point p such that $pa = qb$, $pd = qc$.

Definition: 3.1.10

A quasigroup $(Q, \cdot)$ is called **idempotent** if the identity $x \cdot x = x$ is satisfied for all $x \in Q$.

Definition: 3.1.11

An **IM-quasigroup (Idempotent Medial Quasigroup)** is a solvable and cancellative groupoid $(Q, \cdot)$ satisfying the identities of idempotency and mediality:

$$a \cdot a = a \tag{4}$$

$$ab \cdot cd = ac \cdot bd \tag{5}$$

for $a, b, c, d \in Q$.

Example: 3.1.12

Let $q \neq 0, 1$ be a complex number and define a binary operation on C by $a \cdot b = (1-q)a + qb$. It is known that $(C, \cdot)$ is an IM-quasigroup, i.e. satisfies the laws of idempotency and mediality:

$$a \cdot a = a$$

$$ab \cdot cd = ac \cdot bd$$

Theorem: 3.1.13

Let $(Q, \cdot)$ be an IM quasigroup and $a, b, c, d \in Q$. Then, Par (a, b, c, d) holds if and only if there are $x, y \in Q$ such that $xb = a$, $by = c$ and $xy = d$.

Proof:

Let $x, y \in Q$ be elements satisfying $xb = a$, $by = c$ and $xy = d$. By taking $p = a$ and $q = x$, we see that $pa = qb$ and $pd = xb \cdot xy = x \cdot by = qc$, i.e. Par (a, b, c, d) holds.

Now suppose Par (a, b, c, d) holds and denote $x = a / b$, $y = b \setminus c$. Then, $xb = a$ and $by = c$.

According to Result 3.1.9, for any $p \in Q$ there is a unique $q \in Q$ such that $pa = qb$ and $pd = qc$.

Specially, for $p = a$ we see that

$$a = qb \Rightarrow q = x$$

and

$$ad = qc = xc = x \cdot by = xb \cdot xy = a \cdot xy.$$

Cancelling a from the left yields $xy = d$.

SECTION - 3.2

HEXAGONAL QUASIGROUPS

Definition: 3.2.1

A qusigroup $(Q, \cdot)$ is said to be **semisymmetric** if it has the following properties;

$$ab = c \Leftrightarrow a = bc, \tag{1}$$

$$ab \cdot a = b, \tag{2}$$

$$a \cdot ba = b. \tag{2}'$$

Theorem: 3.2.2

In a semisymmetric quasigroup $(Q,\cdot)$ any two of the following three identities are equivalent;

$$ab\cdot cd = ac\cdot bd \tag{3}$$

$$a(bc\cdot d) = b(ac\cdot d) \tag{4}$$

$$(a\cdot bc)d = (a\cdot bd)c. \tag{4}'$$

Proof:

The identities (4) and (4)' are mutually dual with respect to the exchange of the left and right factors in every product, while the identity (3) is dual to itself. Therefore, it is enough to prove the equivalence (3) $\Leftrightarrow$ (4).

We shall use this kind of facilitations several times. According to (1), the equality $a(bc\cdot d) = e$ is equivalent to $bc\cdot d = ea$ and then to $ea\cdot bc = d$.

Similarly, the equality $b(ac\cdot d) = e$ is equivalent to $eb\cdot ac = d$. Therefore, (4) is valid iff it holds $ea\cdot bc = eb.ac$. But, this is mediality.

Definition: 3.2.3

A quasigroup is said to be **hexagonal** if it is idempotent, medial and semisymmetric, i.e., if the equalities

$$a\cdot a = a, \tag{5}$$

$$ab\cdot cd = ac\cdot bd \tag{6}$$

$$a\cdot ba = ab\cdot a = b \tag{7}$$

hold for all its elements.

Example: 3.2.4

Let $(G,+)$ be a commutative group with an automorphism φ such that for every $a\in G$ it holds

$$(\varphi\bullet\varphi)(a) - \varphi(a) + a = 0. \tag{8}$$

If $(\cdot)$ is a binary operation on the set G defined by

$$ab = a + \varphi(b-a), \tag{9}$$

Then $(G, \cdot)$ is a hexagonal quasigroup.

Proof :

For every $a, b \in G$ the equations $ax = b$ and $ya = b$ are equivalent (because of (9)) to the equations $a + \varphi(x - a) = b$ and $y + \varphi(a) - \varphi(y) = b$.

First of these equations has the unique solution $x = a + \varphi^{-1}(b - a)$ and, owing to (8), the second equation can be written in the form $(\varphi \bullet \varphi)(y) = \varphi(a) - b$.

Therefore, it has the unique solution $y = \varphi^{-1}(\varphi^{-1}(\varphi(a) - b))$.

The idempotency of the quasigroup $(G, \cdot)$ is obvious.

By (9) we obtain after some simplifications

$$a(bc \cdot d) = a - \varphi(a) + \varphi(bc) + (\varphi \bullet \varphi)(d) - (\varphi \bullet \varphi)(bc).$$

But, because of (8) and (9) we have

$$\varphi(bc) - (\varphi \bullet \varphi)(bc) = bc = b + \varphi(c) - \varphi(b),$$

and finally we obtain

$$a(bc \cdot d) = a + b - \varphi(a) - \varphi(b) + \varphi(c) + (\varphi \bullet \varphi)(d).$$

The symmetry of the right side of this equality in the variables a and b proves the identity $a(bc \cdot d) = b(ac \cdot d)$.

Result: 3.2.5

A hexagonal quasigroup has all mentioned properties (1) - (5), (2)', (4)'.

Theorem: 3.2.6

In a hexagonal quasigroup $(Q, \cdot)$ the identities of left and right distributivity

$$a \cdot bc = ab \cdot ac, \qquad (10)$$

$$ab \cdot c = ac \cdot bc, \qquad (10)'$$

and the identities

$$(ab\cdot c)d = b(c\cdot da), \tag{11}$$

$$(ab\cdot c)d = (a\cdot bd)\cdot ca, \tag{12}$$

$$b(c\cdot da) = ac\cdot(bd\cdot a). \tag{12}'$$

Proof:

If we put $b = a$ in $ab\cdot cd = ac\cdot bd$, then by idempotency it follows $a\cdot cd = ac\cdot bd$, i.e. the identity $a\cdot bc = ab\cdot ac$.

Now, let $(ab\cdot c)d = e$. Because of $ab = c \Leftrightarrow a = bc$, we obtain successively $ab\cdot c = de$, $ab = c\cdot de$, $b = (c\cdot de)a$ and by $(a\cdot bc)d = (a\cdot bd)c$ it follows $b = (c\cdot da)e$. Owing to $ab = c \Leftrightarrow a = bc$, we finally have $b(c\cdot da) = e$, which proves $(ab\cdot c)d = b(c\cdot da)$.

The identity $(ab\cdot c)d = (a\cdot bd)\cdot ca$ can be proved as follows:

$$\begin{aligned}(ab\cdot c)d &\overset{(2)}{=} (ab\cdot c)(ad\cdot a)\\ &\overset{(3)}{=} (ab\cdot ad)\cdot ca\\ &\overset{(10)}{=} (a\cdot bd)\cdot ca.\end{aligned}$$

Figure 3.2.1 also illustrates the proof of the identity (11) in the form $(ac\cdot d)e = c(d\cdot ea)$, where we have successively the equalities $(ac\cdot d)e = b$, $ac\cdot d = eb$, $ac = d\cdot eb$, $c = (d\cdot ea)b$, $c(d\cdot ea) = b$.

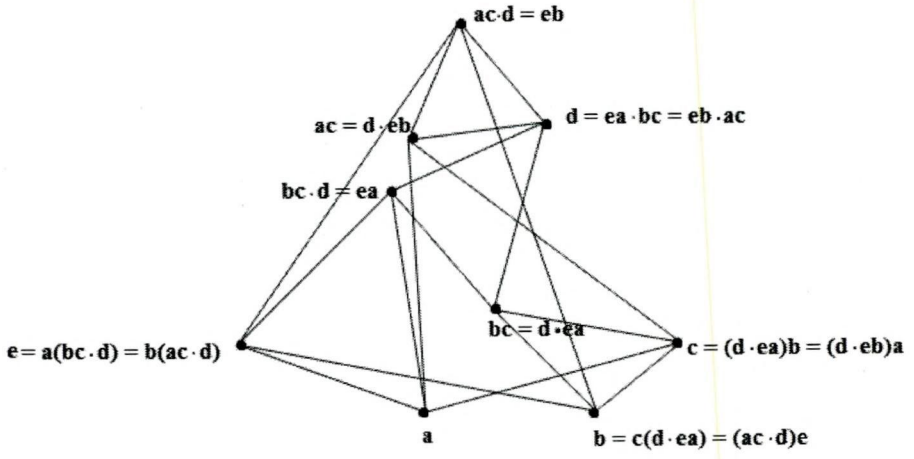

Figure 3.2.1

Theorem: 3.2.7

Par(a, b, c, bc · ab) for any points a, b, c. (Figure 3.2.2).

Proof:

It is sufficient to prove the equalities ap = bq, (bc · ab)p = cq with p = ba, q = b. We have successively

$$a \cdot ba \overset{(2)'}{=} b = bb \qquad (\because aa = a)$$

$$(bc \cdot ab) \cdot ba \overset{(3)}{=} (bc \cdot b)(ab \cdot a) \overset{(2)}{=} cb.$$

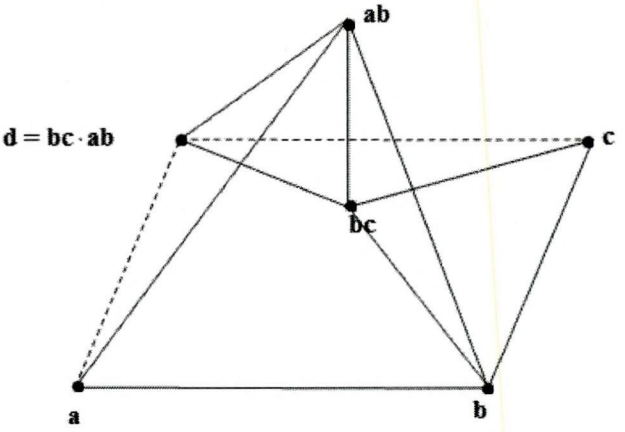

Figure 3.2.2

SECTION – 3.3

GS –QUASIGROUPS

Definition: 3.3.1

A quasigroup $(Q, \cdot)$ is said to be **Golden Section Quasigroup** or shortly **GS–Quasigroup** if it satisfies the (mutually equivalent) identities

$$a(ab \cdot c) \cdot c = b \qquad (1)$$

$$a \cdot (a \cdot bc)c = b \qquad (1)'$$

and moreover the identity of idempotency

$$aa = a \qquad (2)$$

Example: 3.3.2

Let (G,+) be a commutative group which possesses an automorphism φ such that

$$(\varphi \cdot \varphi)(a) - \varphi(a) - a = 0. \tag{3}$$

If we define an operation $\cdot$ on the set G by

$$ab = a + \varphi(b - a), \tag{4}$$

then $(G, \cdot)$ is a GS–quasigroup.

Proof:

Let us prove this statement. For any $a, b \in G$ the equations $ax = b$ and $ya = b$ are equivalent, because of (4), to the equations $a + \varphi(x - a) = b$ and $y + \varphi(a) - \varphi(y) = b$. The first equation has the unique solution $x = a + \varphi^{-1}(b - a)$ and the second equation can be written in the form $\varphi(y) + (\varphi \bullet \varphi)(a) - (\varphi \bullet \varphi)(y) = \varphi(b)$, i.e. by (3) in the form $(\varphi \bullet \varphi)(a) - y = \varphi(b)$, and has the solution $y = (\varphi \bullet \varphi)(a) - \varphi(b)$. Obviously (4) implies (2). By virtue of (4) we obtain after some arrangements

$$ab \cdot c = (\varphi \bullet \varphi)(a) - 2\varphi(a) + a - (\varphi \bullet \varphi)(b) + \varphi(b) + \varphi(c).$$

Because of (3) this becomes

$$ab \cdot c = 2a - \varphi(a) - b + \varphi(c).$$

Therefore, we have

$$a(ab \cdot c) \cdot c = 2a - \varphi(a) - [2a - \varphi(a) - b + \varphi(c)] + \varphi(c) = b.$$

Theorem: 3.3.3

If the operation $*$ on the set Q is defined by the equivalence

$$a * b = c \Leftrightarrow ba = c,$$

i.e. by the identity $a * b = ba$, then $(Q, *)$ is a GS–quasigroup if and only if $(Q, \cdot)$ is a GS–Quasigroup.

Theorem: 3.3.4

In any GS–quasigroup $(Q,\cdot)$ the mediality holds, i.e. we have the identity

$$ab \cdot cd = ac \cdot bd \tag{5}$$

Proof:

We have successively,

$$ac \cdot (ab \cdot cd)d \overset{(1)'}{=} a[ab \cdot (ab \cdot cd)d] \cdot (ab \cdot cd)d$$
$$\overset{(1)}{=} b$$
$$\overset{(1)'}{=} ac \cdot (ac \cdot bd)d,$$

which yields $ab \cdot cd = ac \cdot bd$.

Corollary: 3.3.5

In any GS-quasigroup $(Q,\cdot)$ the elasticity and left and right distributivity hold, i.e. we have the identities

$$ab \cdot a = a \cdot ba, \tag{6}$$
$$a \cdot bc = ab \cdot ac, \tag{7}$$
$$ab \cdot c = ac \cdot bc. \tag{7}'$$

Theorem: 3.3.6

In any GS – quasigroup $(Q,\cdot)$ the identities

$$a(ab \cdot b) = b, \tag{8}$$
$$(b \cdot ba)a = b, \tag{8}'$$
$$a(ab \cdot c) = b \cdot bc, \tag{9}$$
$$(c \cdot ba)a = cb \cdot b \tag{9}'$$

and the equivalencies

$$ab = c \Leftrightarrow a = c \cdot cb, \tag{10}$$
$$ab = c \Leftrightarrow b = ac \cdot c \tag{10}'$$

hold.

Proof:

We have successively

$$a(ab\cdot c)\cdot c \overset{(1)}{=} b \overset{(1)}{=} b(bb\cdot c)\cdot c \overset{(2)}{=} (b\cdot bc)c,$$

which implies (9). Now, (8) follows from (9) because of (2). The identities (8)' and (9)' follow from (8) and (9) by Theorem 3.3.3.

Moreover, by (8)' and (8) we have

$$(c\cdot cb)b = c \text{ and } a(ac\cdot c) = c$$

and therefore the equality $ab = c$ is equivalent to $a = c\cdot cb$ and $b = ac\cdot c$.

Theorem: 3.3.7

Any three of the four equalities

$$ab = d, \tag{11}$$

$$ae = f, \tag{12}$$

$$dc = e, \tag{13}$$

$$fc = b \tag{14}$$

imply the remaining equality (Figure 3.3.1).

Proof:

The substitutions $b \leftrightarrow e$, $d \leftrightarrow f$ imply the substitutions (11) $\leftrightarrow$ (12) and (13) $\leftrightarrow$ (14). Therefore, it is sufficient to prove the implications (12) & (13) & (14) $\Rightarrow$ (11) and (11) & (12) & (14) $\Rightarrow$ (13).

However, we have successively

$$ab \overset{(14)}{=} a\cdot fc \overset{(12)}{=} a(ae\cdot c) \overset{(13)}{=} a\cdot(a\cdot dc)c \overset{(1)'}{=} d,$$

$$dc \overset{(11)}{=} ab\cdot c \overset{(14)}{=} (a\cdot fc)c \overset{(12)}{=} a(ae\cdot c)\cdot c \overset{(1)}{=} e.$$

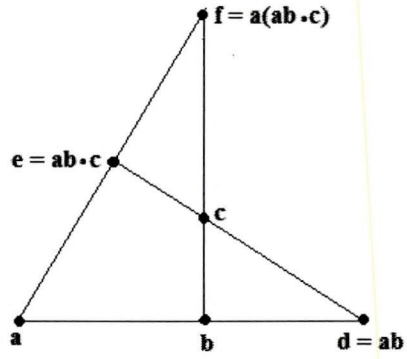

Figure 3.3.1

Definition: 3.3.8

Points a, b, c, d form a **parallelogram and** write **Par (a, b, c, d)** if the following identity $a \cdot b(ca \cdot a) = d$ holds (Figure 3.3.2).

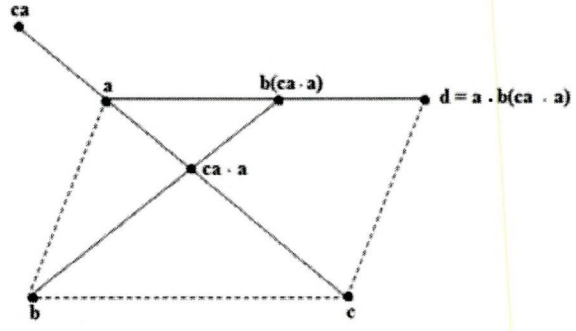

Figure 3.3.2

Definition: 3.3.9

Points a, b, c, d are said to be the vertices of the **Golden Section Trapezoid** which is denoted by **GST (a, b, c, d)** if the identity $a \cdot ab = d \cdot dc$ holds (Figure 3.3.3).

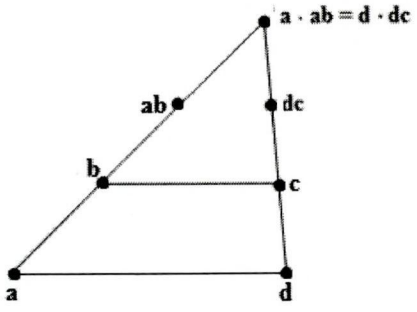

Figure 3.3.3

Definition: 3.3.10

Points a, b, c, d are said to be the vertices of a **Trapezoid of Double golden section** or shorter a **DGS - trapezoid** which is denoted by **DGST (a, b, c, d)** if the equality $ab = dc$ holds (Figure 3.3.4).

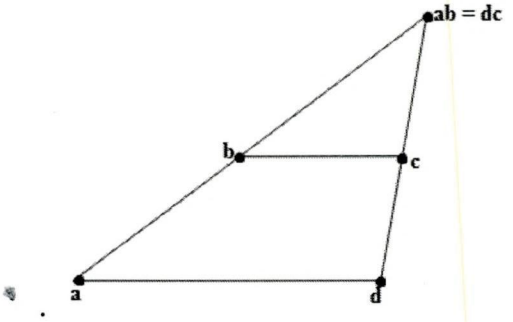

Figure 3.3.4

Definition: 3.3.11

Points a, b, c, d, e are said to be the vertices of the **Affine Regular Pentagon** and it is denoted by **ARP (a, b, c, d, e)** if any two (and then all five) of the five statements GST (a, b, c, d), GST (b, c, d, e), GST (c, d, e, a), GST (d, e, a, b), GST (e, a, b, c) are valid.

Definition: 3.3.12

Points o, a, b, c are said to be the vertices of a **Golden Section Deltoid** which is denoted by **GSD (o, a, b, c)** if and only if the identity $c = oa \cdot b$ is valid (Figure 3.3.5).

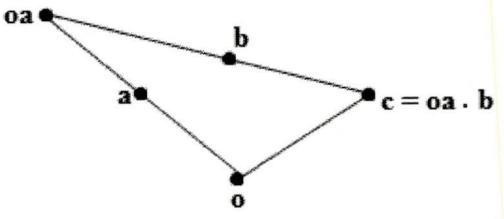

Figure 3.3.5

Theorem: 3.3.13

i. GST (a, b, c, d) implies GST (d, c, b, a).

ii. DGST (a, b, c, d) implies DGST (d, c, b, a).

iii. ARP (a, b, c, d, e) implies ARP (e, d, c, b, a).

iv. GSD (o, a, b, c) implies GSD (o, c, b, a).

Theorem: 3.3.14

i. Any two of the three statements Par (a, b, c, d), Par (e, f, g, h) and Par (ae, bf, cg, dh) imply the remaining statement (Figure 3.3.6).

ii. Any two of the three statements GST (a, b, c, d), GST (b, c, d, e) and GST (c, d, e, a) imply the remaining statement (Figure 3.3.7).

iii. Any two of the three statements DGST(a, b, c, d), DGST(e, f, g, h), DGST(ae, bf, cg, dh) imply the remaining statement (Figure 3.3.8).

iv. Any two of the three statements ARP(a, b, c, d, e), ARP(f, g, h, i, j), ARP(af, bg, ch, di, ej) imply the remaining statement (Figure 3.3.9).

v. Any two of the three statements GSD (o, a, b, c), GSD (o', a', b', c') and GSD (oo', aa', bb', cc') imply the remaining statement (Figure 3.3.10).

vi. If the statements GSD (o, a, b, c), GSD (o, b, c, d) hold, then ab = dc = e, i.e. DGST (a, b, c, d) and Par (o, a, e, d) hold (Figure 3.3.11).

vii. Any two of the three statements GSD (o, a, b, c), GSD (o, b, c, d), GST (o, a, b, d) imply the remaining statement (Figure 3.3.12).

viii. Any two of the three statements GSD (o, a, b, c), GSD (o, b, c, d), GST (o, d, c, a) imply the remaining statement (Figure 3.3.12).

ix. From GSD (o, a, b, c), GSD (o, b, c, d), GSD (o, c, d, e) it follows ARP (o, a, b, d, e) (Figure 3.3.13).

Proof of (i):

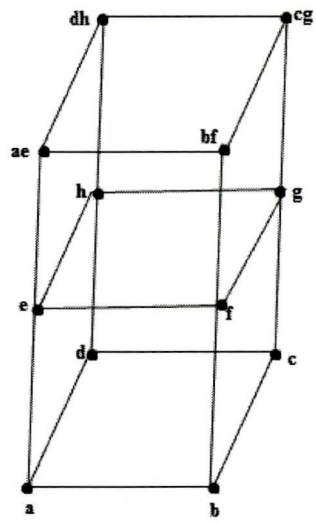

Figure 3.3.6

By (5) we obtain successively

$$\begin{aligned} ae\cdot[bf\cdot(cg\cdot ae)(ae)] &= ae\cdot[bf\cdot(ca\cdot ge)(ae)] \\ &= ae\cdot[bf\cdot(ca\cdot a)(ge\cdot e)] \\ &= ae\cdot[b(ca\cdot a)\cdot f(ge\cdot e)] \\ &= [a\cdot b(ca\cdot a)][e\cdot f(ge\cdot e)] \end{aligned}$$

and it becomes obvious that any two of the three equalities $a\cdot b(ca\cdot a)=d$, $e\cdot f(ge\cdot e)=h$ and $ae\cdot[bf\cdot(cg\cdot ae)(ae)]=dh$ imply the remaining equality.

Proof of (ii):

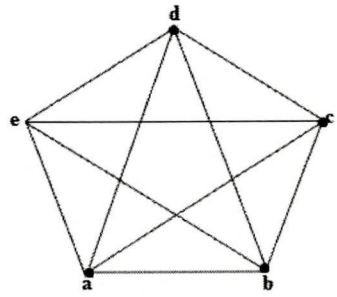

Figure 3.3.7

According to Theorem 3.3.13 (i) we have symmetry $b \leftrightarrow e$, $c \leftrightarrow d$, so it is sufficient to prove with the assumption GST (a, b, c, d) i.e. $d = (a \cdot ab)c$ the equivalency of the statements GST (b, c, d, e) and GST (c, d, e, a) i.e. the equivalency of the equalities $e = (b \cdot bc)d$ and $(c \cdot cd)e = a$.

However, we obtain

$$(c \cdot cd) \cdot (b \cdot bc)d = c[c \cdot (a \cdot ab)c] \cdot [(b \cdot bc) \cdot (a \cdot ab)c]$$

$$\overset{(6)}{=} c[c(a \cdot ab) \cdot c] \cdot [(b \cdot bc) \cdot (a \cdot ab)c]$$

$$\overset{(9)}{=} [(a \cdot ab) \cdot (a \cdot ab)c][(b \cdot bc) \cdot (a \cdot ab)c]$$

$$\overset{(7)'}{=} (a \cdot ab)(b \cdot bc) \cdot (a \cdot ab)c$$

$$\overset{(7)}{=} (a \cdot ab) \cdot (b \cdot bc)c$$

$$\overset{(8)'}{=} (a \cdot ab)b$$

$$\overset{(8)'}{=} a.$$

Proof of (iii):

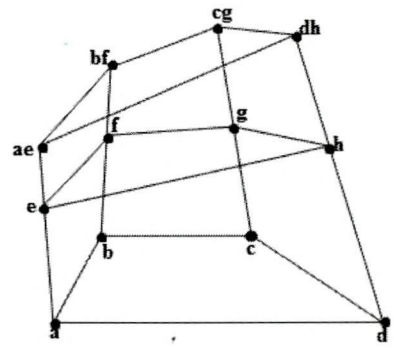

Figure 3.3.8

We must prove that any two of the three equalities $ab = dc$, $ef = hg$ and $ae \cdot bf = dh \cdot cg$ imply the remaining equality. This is obvious, because of (5) the third equality is equivalent to $ab \cdot ef = dc \cdot hg$.

Proof of (iv):

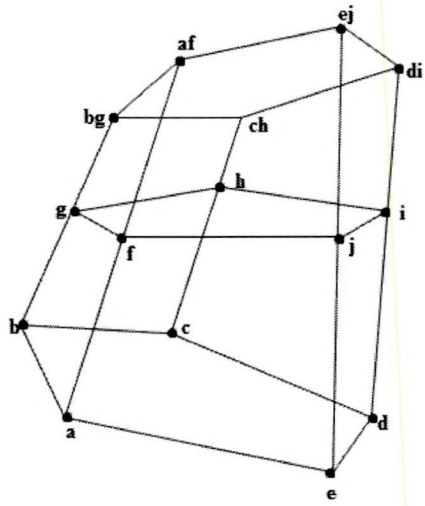

Figure 3.3.9

It is sufficient to prove that any two of three statements GST (a, b, c, d), GST (f, g, h, i), GST (af, bg, ch, di) imply the remaining statement. However, according to (5) we have successively

$$[(af)\cdot(af)(bg)](ch) = [(af)\cdot(ab\cdot fg)](ch)$$
$$= [(a\cdot ab)\cdot(f\cdot fg)](ch)$$
$$= (a\cdot ab)c\cdot(f\cdot fg)h$$

and then it is obvious that any two of the equalities $(a\cdot ab)c = d, (f\cdot fg)h = i$ and $[(af)\cdot(af)(bg)](ch) = di$ imply the remaining equality.

Proof of (v):

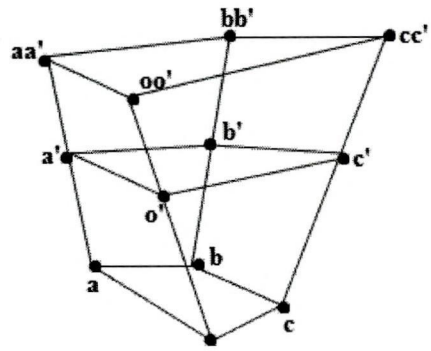

Figure 3.3.10

Because of (5) we have successively

$$(oo'\cdot aa')\cdot bb' = (oa\cdot o'a')\cdot bb'$$

$$= (oa\cdot b)(o'a'\cdot b')$$

and then it is obvious that any two of the three equalities $oa\cdot b = c$, $o'a'\cdot b' = c'$ and $(oo'\cdot aa')\cdot bb' = cc'$ and imply the remaining equality.

Proof of (vi):

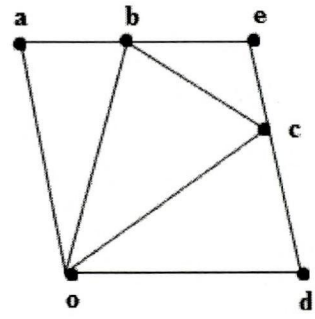

Figure 3.3.11

From $c = oa\cdot b$ and $d = ob\cdot c$ there follows $d = ob\cdot(oa\cdot b) \overset{(7)'}{=} (o\cdot oa)b$

which gives

$$dc = (ob\cdot c)c \overset{(10)'}{=} (oc\cdot b)b = [o(oab)b]b \overset{(1)}{=} ab$$

and the first statement is proved.

Because of

$$o\cdot d(eo\cdot o) = o[(o\cdot oa)b\cdot(ab\cdot o)o]$$

$$= o[(o\cdot oa)(ab\cdot o)\cdot bo]$$

$$\overset{(5)}{=} o[(o\cdot ab)(oa\cdot o)\cdot bo]$$

$$\overset{(6)}{=} o[(o\cdot ab)(o\cdot ao)\cdot bo]$$

$$\overset{(7)}{=} o[o(ab\cdot ao)\cdot bo]$$

$$\overset{(7)}{=} o[o(a\cdot bo)\cdot bo] \overset{(1)'}{=} a$$

Proof of (vii):

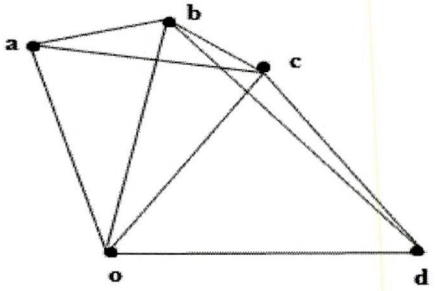

Figure 3.3.12

It is necessary to prove that any two of the three statements $oa \cdot b = c, ob \cdot c = d, \quad (o \cdot oa)b = d$ imply the remaining statement.

However, it becomes obvious because of (7)' we have the equality $ob \cdot (oa \cdot b) = (o \cdot oa)b$.

Proof of (viii):

The statement follows from Theorem 3.3.14 (vii) and Theorem 3.3.13 (iv).

Proof of (ix):

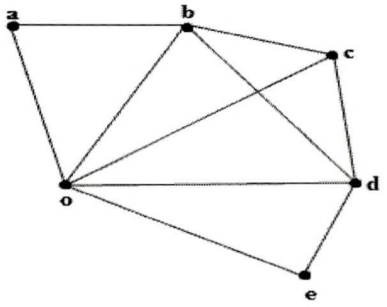

Figure 3.3.13

Because of Theorem 3.3.14 (vii) and the definition of an affine regular pentagon the following implications are valid

GSD (o, a, b, c) GSD (o, b, c, d) $\Rightarrow$ GST (o, a, b, d)

GSD (o, e, d, c) GSD (o, d, c, b) $\Rightarrow$ GST (o, e, d, b)

GST (o, a, b, d) GST (o, e, d, b) $\Rightarrow$ ARP (o, a, b, d, e).

SECTION – 3.4

CI – QUASIGROUPS

Definition: 3.4.1

A **finite quasigroup** $(Q, \cdot)$ of order n consist of a set Q of symbols on which a binary operation $\cdot$ is defined such that

i. for all pairs of elements $a, b \in Q, a \cdot b \in Q$ (closure) and

ii. for all pairs $a, b \in Q$, there exist unique elements $x, y \in Q$,

such that $x \cdot a = b$ and $a \cdot y = b$ (unique solubility of equations).

Definition: 3.4.2

A quasigroup is said to satisfy **left crossed inverse property,** if for each $a \in Q$, there exist an element $a'_L \in Q$ such that $a'_L \cdot (b \cdot a) = b$ for all $b \in Q$.

Definition: 3.4.3

A quasigroup is said to satisfy **right crossed inverse property,** if for each $a \in Q$, there exist an element $a'_R \in Q$ such that $(a \cdot b) \cdot a'_R = b$ for all $b \in Q$.

Lemma: 3.4.4

A quasigroup $(Q, \cdot)$ of finite order which has the left crossed-inverse property also has the right crossed-inverse property; and conversely.

Proof:

The left crossed-inverse property states that, for every element $a \in Q$, there exists an element $a'_L \in Q$ such that $a'_L \cdot (b \cdot a) = b$ for every $b \in Q$. To each $a \in Q$, there corresponds a unique a'_L because the equation $x \cdot (b \cdot a) = b$ has a unique solution $x = a'_L$. Also, distinct elements

$a_1, a_2 \in Q$ have distinct left inverses because $(a_1')_L = (a_2')_L = a_L'$ would imply $a_L' \cdot (b \cdot a_1) = b = a_L' \cdot (b \cdot a_2)$ and so, by the unique solubility of equations, $b \cdot a_1 = b \cdot a_2$ hence $a_1 = a_2$. It follows that, given $c \in Q$, there exists a unique $c' \in Q$ such that $c \cdot (b \cdot c') = b$ for all $b \in Q$.

Let d be an arbitrary element of Q. By the solubility of equations, there exists an element $b \in Q$ such that $d = b \cdot c'$. Then, $c \cdot d = c \cdot (b \cdot c') = b$ and so $(c \cdot d) \cdot c' = b \cdot c' = d$. That is, given $c \in Q$, there exists an element $c' \in Q$ such that $(c \cdot d) \cdot c' = d$ for all $d \in Q$. This is the right crossed-inverse property. The proof of the converse is similar.

Definition: 3.4.5

Non – commutative quasigroups of finite order which satisfy left crossed inverse property and consequently (by Lemma 3.4.4) also satisfy right crossed inverse property are called **CI-quasigroups.**

Lemma: 3.4.6

If a_L^{-1} is the left inverse of a in a quasigroup $(Q, \cdot)$ which has the left inverse property, then a is the left inverse of a_L^{-1} for that quasigroup. An analogous result holds for right inverses.

Proof:

By the left inverse property, $a_L^{-1} \cdot (a \cdot c) = c$ for all $c \in Q$. Let b be an arbitrary element of Q. Then, by the solubility of equations, there exists an element $c \in Q$ such that $b = a \cdot c$. So $a_L^{-1} \cdot b = a_L^{-1} \cdot (a \cdot c) = c$.

Hence $a \cdot (a_L^{-1} \cdot b) = a \cdot c = b$.

This proves the result because b was arbitrarily chosen.

Definition: 3.4.7

If $(Q,\cdot)$ is a CI-quasigroup in which a' is the right crossed-inverse of a, a'' is that of a', a''' is that of a'', and so on, then the cycle (a a'a''...) is called the **inverse cycle associated with the element a.**

Theorem: 3.4.8

Let $(G,\cdot)$ be an abelian group of order n such that n+1 is composite. Define a binary operation $(\bullet)$ on the elements of G by the relation $a \bullet b = a^r b^s$, where rs = n+1. Then $(G,\bullet)$ is a CI-quasigroup and the right crossed inverse of the element a is a^u, where $u = (-r)^3$.

Proof:

We first show that $(G,\bullet)$ is a quasigroup. Let $x \bullet a = b$. Then $x^r a^s = b$ so $x^r = ba^{-s}$ and $x = x^{rs} = (ba^{-s})^s$ which is an element of G. Similarly, if $a \bullet y = b$, then $a^r y^s = b$ so $y = y^{rs} = (a^{-r}b)^r$. Thus, equations are uniquely soluble and $(G,\bullet)$ is a quasigroup.

Also, $(a \bullet b) \bullet c = (a \bullet b)^r c^s = (a^r b^s)^r c^s = b^{sr} a^{rr} c^s = b$ if $a^{rr} c^s = e$, the identity element of $(G,\cdot)$: that is, if $c^s = a^{-rr}$ or if $c = c^{sr} = a^u$, where $u = (-r)^3$, as before. Thus, $(G,\bullet)$ is a CI-quasigroup and a^u, where $u = (-r)^3$, is the right crossed inverse of a. The result of the theorem follows.

Suppose next that $u = (-r)^3$ is a primitive root of p. Then $(a\, a^u a^{uu} \ldots)$, of length p-l, is the inverse cycle of $(G,\bullet)$ which contains the element a since $u^{p-1} \equiv 1 \bmod p$ and $u^h \neq 1 \bmod p$ for $1 \leq h \leq p-2$.

Corollary: 3.4.9

If $(G,\cdot)$ is the cyclic group C_p of prime order p and there exists a divisor r of $p+1$ such that $(-r)^3$ is a primitive root of p, then the inverse

cycles of $(G,\bullet)$ are of lengths 1 and $p-1$.

Corollary: 3.4.10

If $(G,\cdot)$ is an elementary abelian group of order p^t (that is, an abelian group in which every element has the same prime order p) and there exists a divisor r of p^t+1 such that $(-r)^3$ is a primitive root of p, then the inverse cycles of $(G,\bullet)$, excepting that of the identity element e of $(G,\cdot)$, all have equal length $p-1$.

Example: 3.4.11

Let $(G,\cdot)$ be the cyclic group $C_5 = < c : c^5 = e >$ and define $a \bullet b = a^3 b^2$. We find that the multiplication table of the CI-quasigroup is as shown in Table 3.4.1, where the integers 0, 1, 2, 3, 4 represent the various powers of the generating element c of C_5. Since $u = (-3)^3 \equiv 3 \bmod 5, c^u = c^3$, $(c^3)^u = c^4, (c^4)^u = c^2$ and $(c^2)^u = c$, so the corresponding decomposition of G into inverse cycles is (0)(1 3 4 2). Thus,

$$(0 \bullet 3) \bullet 0 = 1 \bullet 0 = 3$$
$$(2 \bullet 4) \bullet 1 = 4 \bullet 1 = 4$$
$$(4 \bullet 2) \bullet 2 = 1 \bullet 2 = 2$$
$$(3 \bullet 3) \bullet 4 = 0 \bullet 4 = 3 \text{ etc.}$$

•	**0**	**1**	**2**	**3**	**4**
0	0	2	4	1	3
1	3	0	2	4	1
2	1	3	0	2	4
3	4	1	3	0	2
4	2	4	1	3	0

Table 3.4.1

Note: 3.4.12

The CI-quasigroup obtained by the method of Theorem 3.4.8 is unipotent only if $r + s = n$: that is, only if $n = 5$.

Definition: 3.4.13

For each element a in the CI-quasigroup, there exists another element a' such that $a' \cdot (b \cdot a) = b$ for all b in the quasigroup. The relation between a and a' is a permutation, $a'=\pi(a)$. This permutation is called the **CI - permutation.**

Note: 3.4.14

Groups are also Crossed-Inverse quasigroups must be commutative and have π (a) $=a^{-1}$. That is, the CI-permutation is merely the mapping from elements to their multiplicative inverses. If we iterate the mapping, π (π (a)), we get a. That is, two applications of the CI-permutation gives the "identity permutation" when working in a group.

SECTION - 3.5

TERNARY QUASIGROUPS

Definition: 3.5.1

An n-groupoid (Q, f) is said to be an **n-quasigroup** if the equation

$$f(a_1, a_2, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) = b \qquad (1)$$

has single solution x in Q for each $a_1, a_2, \ldots, a_n, b \in Q$ and for each $i = 1,2,...,n$.

In other words it means that (Q, f) is an n-quasigroup if knowledge of n elements of the n +1 elements in the equation (1), uniquely determine the remaining unknown element.

Remark: 3.5.2

In the special case when n = 1 the quasigroup is called a **unary quasigroup,** when n = 2, we have a **binary quasigroup** or only quasigroup and when n = 3, this kind of quasigroup is called a **ternary quasigroup.**

i.e. Let $Q = \{a_1, a_2, \ldots, a_k\}$ be a given finite set and $f : Q^3 \to Q$ is a ternary operation in Q. Then the quasigroup (Q, f) is called a ternary quasigroup.

Definition: 3.5.3

A **ternary quasigroup (or 3–quasigroup)** is a pair (Q, f) where Q is an n–set and $f(x, y, z)$ is a ternary operation on Q with unique solvability.

Lemma: 3.5.4

Let $(Q, f_1), (Q, f_2), \ldots, (Q, f_k)$ be k binary quasigroups and let $L_1, L_2, \ldots, L_k$ be the corresponding Latin squares. The binary quasigroups form ternary quasigroup (Q, f), if in the three-dimensional matrix $L = [a_{ijt}]_{k \times k \times k}$ constructed from the corresponding Latin squares placed one above the other, are satisfied the following implications

$$i \neq i' \Rightarrow a_{ijt} \neq a_{i'jt},$$
$$j \neq j' \Rightarrow a_{ijt} \neq a_{ij't},$$
$$t \neq t' \Rightarrow a_{ijt} \neq a_{ijt'}$$

for each $i, j, t \in \{1, 2, \ldots, k\}$.

Example: 3.5.5

Let $Q = \{1, 2, 3, 4\}$ and (Q, f_i) for $i = 1, 2, 3, 4$ are binary quasigroups with Cayley tables given in Table 3.5.1.

f_1	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

f_2	**1**	**2**	**3**	**4**
1	2	3	4	1
2	3	2	1	4
3	4	1	3	2
4	1	4	3	2

f_3	**1**	**2**	**3**	**4**
1	3	4	1	2
2	4	3	2	1
3	1	2	4	3
4	2	1	3	4

f_4	**1**	**2**	**3**	**4**
1	4	1	2	3
2	1	4	3	2
3	2	3	1	4
4	3	2	4	1

Table 3.5.1

Ternary quasigroups of order 4

All these quasigroups satisfy the condition that elements on the (i, j) position in all 4 quasigroups are different i.e the 4-tuple of all these elements is permutation of Q. So using them we can construct ternary quasigroup (Q, f) where $f(x_1, x_2, x_3) = f_{x_1}(x_2, x_3)$ for fixed x_1 from Q and x_1, x_2, x_3 also from Q. Also, using these quasigroups we can make 4! = 24 different ternary quasigroups depending on the order of their arrangement.