Contd.

Monoid

A semigroup (G,o) containing the identity element is said to be a monoid. Thus an algebraic system (G,o) is said to be a monoid if

i) (a o b) o c = a o (b o c) ∀ a,b,c ϵ G &

ii) There exists an element e in G such that e o a = a o e = a ∀ a in G.

Ex. (Z,+) is a monoid, 0(zero) being the identity element.

Ex. (Z,.) is a monoid, 1 being the identity element.

Let E be the set of all even integers. Then (E,.) is a semigroup but not a monoid.

Contd.

Theorem In a monoid (G,o) if an element a be invertible then it has a unique inverse.

Proof: If possible let there be two inverse a', a'' of a in G. Then

$$a \circ a' = a' \circ a = e \quad \& \quad a \circ a'' = a'' \circ a = e$$

e being the identity element.

Now $(a' \circ a) \circ a'' = a' \circ (a \circ a'')$ since o is associative.

But, $(a' \circ a) \circ a'' = e \circ a'' = a''$ &

$$a' \circ (a \circ a'') = a' \circ e = a'$$

$$\therefore a' = a''$$

This proves the uniqueness of the inverse of a.

Contd.

Theorem In a monoid (G,o) if an element a be left invertible as well as right invertible then a is invertible & has unique inverse in the monoid.

Proof: Let e be the identity element & b be a left inverse, c be a right inverse of a.

Then $b \circ a = e$, $a \circ c = e$

Now $b \circ (a \circ c) = (b \circ a) \circ c$ since o is associative.

But $b \circ (a \circ c) = b \circ e = b$ &

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

$\therefore b = c$

Therefore $b \circ a = a \circ b = e$ & a is invertible & by previous theorem a has a unique inverse.

Contd.

Groups

A non empty set G is said to form a group w.r.t a binary composition o if

i) G is closed under the composition o

ii) o is associative

iii) there exists an element e in G such that

$e \circ a = a \circ e = a \ \forall \ a \in G$

iv) for each element a in G there exists an element a‘ in G such that a‘ o a = a o a‘ = e

The group is denoted by (G, o).

The element e is said to be an identity element in the group.

Contd.

Def^n: A group (G,o) is said to be commutative group or an abelian group if o is commutative.

Theorem: A group (G,o) contains only one identity element.

Proof: Let, e,f be two identity elements in the group.

Then e o a = a o e = a &

f o a = a o f = a $\forall$ a in G

Now, e o f = f by the property of e

also e o f = e by the property of f

Therefore e = f & this proves uniqueness of identity element.

Note: the identity element in (G,o) is denoted by ^eG.

Contd.

Theorem: In a group (G,o) each element has only one inverse.

Proof: Let, $a \epsilon G$ & a', a'' be two inverses of a.

Then $a' \circ a = a \circ a' = e$

$a'' \circ a = a \circ a'' = e$ being the identity.

Now $a' \circ (a \circ a'') = (a' \circ a) \circ a''$, since o is associative.

But $a' \circ (a \circ a'') = a' \circ e = a'$ &

$(a' \circ a) \circ a'' = e \circ a'' = a''$

Therefore $a' = a''$ & this proves that the inverse of a is unique.

Theorem: In a group (G,o)

i) $a \circ b = a \circ c$ implies $b=c$ (left cancellation law)

ii) $b \circ a = c \circ a$ implies $b=c$ (right cancellation law)

$\forall\, a,b,c \in G$.

Proof: i) Since $a \in G$, $a^{-1} \in G$

$a \circ b = a \circ c \Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$

$\Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$ (since o is associative)

$\Rightarrow e \circ b = e \circ c$, e being the identity

$\Rightarrow b=c$

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

$\Rightarrow (b \circ a) \circ a^{-1} = (c \circ a) \circ a^{-1}$

$\Rightarrow b \circ (a \circ a^{-1}) = c \circ (a \circ a^{-1})$ since o is associative

$\Rightarrow b \circ a = c \circ a$, c being the identity element

$\Rightarrow b = c$

Contd.

Theorem: In a group (G,o) ∀ a,b in G each of the equation a o x = b and y o a = b has a unique solution in G.

Proof: Since a,b ϵG, a^{-1}o b ϵG

Now a o (a^{-1}o b) = (a o a^{-1}) o b, since o is associative

= ^{e}G o b = b

This shows that a^{-1}o b is a sol^{n} of the eq^{n} a o x = b. Now we shall prove that this sol^{n} unique.

Let there be 2 sol^{n} x_1,x_2 in G of the eq^{n} a o x = b. Then

a o x_1 = a o x_2 & by previous theorem this implies x_1=x_2.

Again, b o a^{-1} ϵG. And (b o a^{-1}) o a = b o (a^{-1} o a) = b.

This shows that b o a^{-1} is a sol^{n} of the eq^{n} y o a = b. The uniqueness of the sol^{n} follows from the just previous theorem.