DISCRETE STRUCTURE

LECTURE-18

GROUP & RING,SUBGROUP

Topics covered

- Introduction to Groups
- Rings
- Abelian groups

INTRODUCTION TO GROUP

- When we consider the behaviour of permutations under the composition operation we noticed certain underlying structures.
- Permutations are closed under this operation, they exhibit associativity, an identity element exists and an inverse exists for each permutation
- These properties define a general type of algebraic structure called a group.

GROUPS

A group $\langle G, \bullet \rangle$ or $(G, \bullet)$ is a set G with binary operation $\bullet$ which satisfies the following properties

1. $\bullet$ is a closed operation i.e. if $a \in G$ and $b \in G$ then $a \bullet b \in G$
2. $\forall a, b, c \in G \; a \bullet (b \bullet c) = (a \bullet b) \bullet c$ this is the associative law
3. G has an element e, called the identity, such that $\forall a \in G \; a \bullet e = e \bullet a = a$
4. $\forall a \in G$ there corresponds an element $a^{-1} \in G$ such that $a \bullet a^{-1} = a^{-1} \bullet a = e$

Examples: (1) The set of all permutations of a set *A* onto itself is group (called the *symmetric group* S_n for n elements).
(2) The set consisting of all (nxn) matrices that have inverses is a group under ordinary matrix multiplication(it is called GL(n)).

Two show that an algebraic system is a group we must show that it satisfies all the axioms of a group.

Question: Let $\langle A, \wedge, \vee, \bar{\ } \rangle$ be a Boolean algebra so that A is a set of propositional elements, $\vee$ is like 'or', $\wedge$ is like 'and' and $\bar{\ }$ is like 'not'. Show that $\langle A, \oplus \rangle$ is an abelian group where

$$\forall a, b \in A \; a \oplus b = \left(a \wedge \bar{b}\right) \vee \left(\bar{a} \wedge b\right)$$

Answer:

(1) Associative since $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
prove this ?

(2) Has an identity element 0 (false) since

$$\forall a \; a \oplus 0 = \left(a \wedge \bar{0}\right) \vee \left(\bar{a} \wedge 0\right) = (a \wedge 1) \vee 0$$

$$= a \vee 0 = a$$

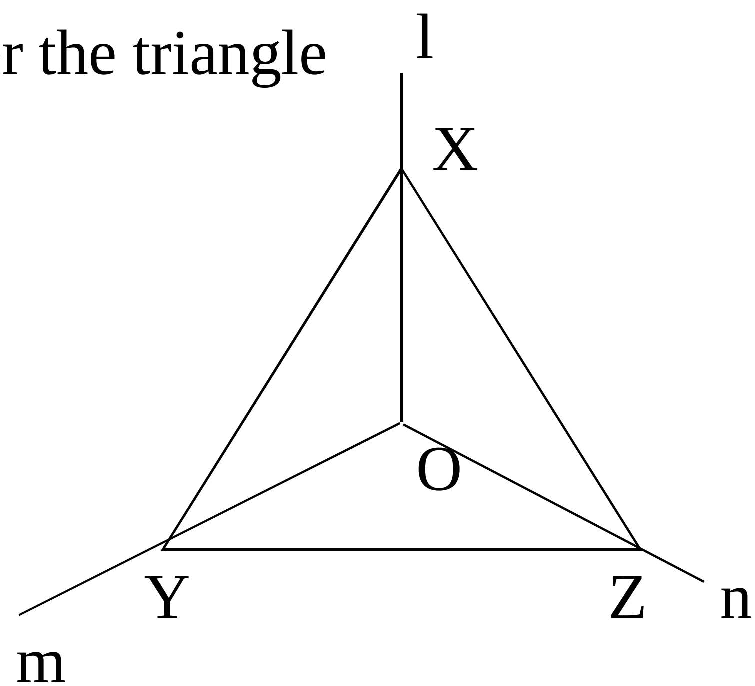
(3) Each element is its own inverse

$$a \oplus a = (a \wedge \bar{a}) \vee (\bar{a} \wedge a) = 0 \vee 0 = 0$$

(4) The operation commutes $a \oplus b = b \oplus a$
prove this ?

Group of Symmetries of a Triangle

Consider the triangle



We can perform the following transformations on the triangle

1=identity mapping from the plane to itself

p=rotation anticlockwise about O through 120 degrees

q=rotation clockwise about O through 120 degrees

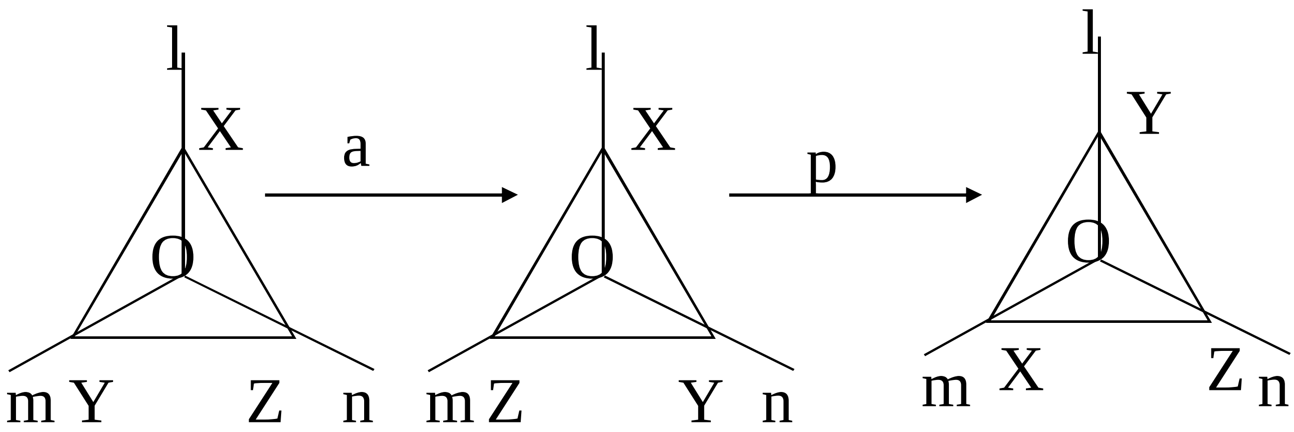
a=reflection in l

b=reflection in m

c=reflection in n

Let $x \bullet y$ denote transformation y followed by transformation x for x and y in {1,p,q,a,b,c}

So for example $p \bullet a = c$



$\bullet$	1	p	q	a	b	c
1	1	p	q	a	b	c
p	p	q	1	c	a	b
q	q	1	p	b	c	a
a	a	b	c	1	p	q
b	b	c	a	q	1	p
c	c	a	b	p	q	1

Notice the table is not symmetric

ABELIAN GROUPS

If $\langle G, \bullet \rangle$ is a group and $\bullet$ is also commutative then $\langle G, \bullet \rangle$ is referred to as an *Abelian group*

(the name is taken from the 19'th century mathematician N.H. Abel)

$\bullet$ is commutative means that

$$\forall a, b \in G, \; a \bullet b = b \bullet a$$

Examples: $\langle R, + \rangle, \langle Z, + \rangle$ and $\langle R - \{0\}, \times \rangle$ are abelian groups.

Why is $\langle R, \times \rangle$ not a group at all?

If $\forall a, b \in Z \; a \oplus b = a + b$ if $a + b < n$

$$= a + b - n \text{ if } a + b \geq n$$

then $\langle Z, \oplus \rangle$ is an abelian group and is usually referred to as the group of *integers modulo n*

RING

An algebraic system $\langle A, \oplus, \bullet \rangle$ is called a *ring* if the following conditions are satisfied:

(1) $\langle A, \oplus \rangle$ is an Abelian group

(2) $\langle A, \bullet \rangle$ is a semigroup

(3) The operation $\bullet$ is distributive over the operation $\oplus$

Example: $\langle Z, +, \times \rangle$ is a ring since

$\langle Z, + \rangle$ is an Abelian group

$\langle Z, \times \rangle$ is a semigroup

$\times$ distributes over $+$

A commutative ring is a ring in which $\bullet$ is commutative

A ring with unity contains an element 1 such that $\forall x \in A \; x \bullet 1 = 1 \bullet x = x$ where $1 \neq 0$
(0 is the identity of $\langle A, \oplus \rangle$)

Example: the ring of 2x2 matrices under matrix addition and multiplication is a ring with unity.
The element 1=I= $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Semigroup

An Abelian group is a strengthening of the notion of group (i.e. requires more axioms to be satisfied)

We might also look at those algebraic structures corresponding to a weakening of the group axioms

$\langle A, \bullet \rangle$ is a semigroup if the following conditions are satisfied:

1. $\bullet$ is a closed operation i.e. if $a \in A$ and $b \in G$ then $a \bullet b \in A$

2. $\bullet$ is associative

Example: The set of positive even integers {2,4,6,.....} under the operation of ordinary addition since

• The sum or two even numbers is an even number
• + is associative

The reals or integers are not semigroups under - why?

Application & Future Scope

- Coding Theory
- Cryptography