GROUP – THEORY

Definition: Let A,B be two non-empty sets. A mapping or a function f is a rule that associates to each member of A with a unique member of B. Symbolically we write this as $f : A \to B$. If a member x of A associates with the unique member y of B, then we write y = f(x), y is called the image of x and x is said to be the pre-image of y and A is said to be the domain of the function, B is said to be the co-domain of the function f.

Definition: Let A be a non-empty set. A binary operation * is a mapping from AxA into A, which is symbolically written as $* : A \times A \to A$. For any element (a,b) $\in A \times A$ the image of (a,b) is generally written as *(a,b). As a special symbol we write this as (a * b). Obviously (a * b) $\in$ A. For any two elements a,b $\in$ A, (a * b) $\in$ A. This property is said to be the closure property.

Examples: The operation $+ : \square \times \square \to \square$ defined by +(a,b) = (a+b) is a binary operation on the set R of real numbers.

Definition: A non-empty set A together with a binary operation $*$ is said to be a semigroup if for all a,b,c $\in$ A $\Rightarrow$ a * (b * c) = (a * b) * c.

Definition: Let A be a non-empty set and $*$ be a binary operation on A. An element e $\in$ A is said to be an identity element of A if a * e = e * a = a for all a $\in$ A. A semigroup (A, $*$) is said to be a monoid if it contains an identity element.

Definition: Let (A, $*$) be a monoid with an identity element e. (A, $*$) is said to be a group if for each a $\in$ A there exists some $a' \in$ A such that

$a * a' = a' * a = e$. This a' is said to be an inverse of a which is denoted by

a^{-1}.

Definition: A group (G, $*$) is said to be a commutative group or an abelian group if for all elements a,b $\in$ G $\Rightarrow$ a * b = b * a.

Example: The set $G = \{1, w, w^2\}$, where w is a cube-root of unity with general multiplication is a group.

(R, +), (Q, +) are groups.

Some properties:

Let $(G, *)$ be a group, $a,b,c \in G$, then

i) The identity element e is unique
ii) For each $a \in G$, a^{-1} is unique
iii) $(a^{-1})^{-1} = a$ for all $a \in G$
iv) $(a*b)^{-1} = b^{-1}*a^{-1}$
v) $a*b = a*c \Rightarrow b = c$ and $b*a = c*a \Rightarrow b = c$

Proof :

i) Let e and f be two identity elements of G.
$a*e = e*a = a$ for all $a \in G$.
$\Rightarrow f*e = e*f = f$
$a*f = f*a = a$
$\Rightarrow e*f = f*e = e$
And hence e = f. So the identity element is unique.

ii) Let x and y be two inverses of a and e be the identity element of G.
So
$a*x = x*a = e$
$a*y = y*a = e$
Now $(x*a)*y = x*(a*y)$
$\Rightarrow e*y = x*e$
$\Rightarrow y = x$, i.e the inverse is unique.

iii) $a*a' = a'*a = e \Rightarrow a' = a^{-1}$
$a'*a = a*a' = e \Rightarrow a = (a')^{-1} = (a^{-1})^{-1}$

iv) $(a*b)*(b^{-1}*a^{-1}) = ((a*b)*b^{-1})*a^{-1} = (a*(b*b^{-1})*a^{-1}) = (a*e)*a^{-1} = a*a^{-1} = e$.
Similarly we can show that $(b^{-1}*a^{-1})*(a*b) = e$
Therefore $(a*b)*(b^{-1}*a^{-1}) = (b^{-1}*a^{-1})*(a*b) = e$ and

Hence $(a*b)^{-1} = b^{-1}*a^{-1}$.

v) Left as an exercise.

Definition: Let $(G, *)$ be a group and a be a member of G. Let e be the identity element of G. We write $a*a*$ ……$*a$, (n times) as a^n. When n is a negative integer we mean a^n as $a^{-1}*a^{-1}*$ ……$*a^1$, (-n times) .a is said to be of finite order if there exists a natural number n such that $a^n = e$. Otherwise a is said to be of infinite order. When a is of finite order the smallest positive integer n for which $a^n = e$ is called the order of a.
Some properties: Let G be a group and a be an element of G, then

$(a^m)^n = (a^n)^m = a^{mn}$ for any integers

Some problems:

1) Let $(G, *)$ be a group with the property that each non-identity element is of order 2. Show that the group is commutative.
   Solution:
   Since any element $a \in G$ is of order 2, so $a^2 = e$ and hence $a^{-1} = a$. For any two elements $a,b \in G$, $(a*b)^{-1} = a*b \Rightarrow b^{-1}*a^{-1} = a*b \Rightarrow b*a = a*b$
   Hence the group is commutative.
2) Let $S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a,b \in \square \right\}$. Show that S with general matrix multiplication forms a group.
   Solution is left to the readers as a simple exercise

3) Let G be a finite group and H be a proper subset of G. When is H a subgroup of G? Apply this to find

whether {1,ω} is a subgroup of the group of cube roots of unity. If G is any group and H be finite subset of G , is the condition remain same ?

4) Let G be a finite abelian group containing the elements $e,a_1,a_2,\ldots\ldots\ldots\ldots,a_n$. Let $x = a_1a_2\ldots\ldots\ldots\ldots\ldots\ldots a_n$. Show that $x^2 = e$, where e is the identity element of G.

   Solution:

   $G = \{a_1, a_2, \ldots\ldots\ldots\ldots\ldots,a_n\}$. $x = a_1.a_2\ldots\ldots\ldots\ldots a_n$.

   One of $a_1, a_2, \ldots\ldots\ldots\ldots\ldots,a_n$ is the identity element e. $x.x = (a_1a_2\ldots\ldots\ldots\ldots\ldots a_n)(a_1\ a_2\ldots\ldots\ldots\ldots\ldots a_n)$

   Now for each $a_i \in G$, $a_i^{-1} \in G$ and $a_i.a_i^{-1} = e$. Also G is commutative. So $x.x = e.e.e\ldots\ldots\ldots e$, (n times)

   i.e $x.x = e$

5) Let G be a group containing an even number of elements. Show that G containing an element x other than the identity element e, such that $x.x = e$.

SOLUTION:

Let us consider a set $S = \{ x \in G: x \neq x^{-1}\}$ and a set $T = \{ x \in G: x = x^{-1}\}$. Obviously $S \cup T = G$ and $e \in T$. It is also obvious that $x \in S \Rightarrow x^{-1} \in S$ as $x \neq x^{-1} \Rightarrow (x^{-1}) \neq (x^{-1})^{-1}$. Therefore S contains an even number of elements. Also $e \in T$. Since G contains an even number of elements and $S \cup T = G$ so T must contain an even number of elements i.e there exists at least one element x other than e which belongs to T. Now $x \in T \Rightarrow x = x^{-1} \Rightarrow x.x = x^{-1}.x \Rightarrow x.x = e$.