Progressive Education Society's
Modern College of Arts, Science and Commerce(Autonomuous), Shivajinagar, Pune-5
M.Sc.(Mathematics) Part-I
Subject: Group Theory

Intrduction Symmetries of a square
Consider a square $PWGB$.
Consider all possible rotations of a square say
R_0 - Rotation of a square by zero degree
R_{90} - Rotation of a square by 90 degree
R_{180} - Rotation of a square by 180 degree
R_{270} - Rotation of a square by 270 degree
H- Rotation of 180 degree about horizontal axis
V- Rotation of 180 degree about vertical axis
D - Rotation of 180 degree about main diagonal
D'-Rotation of 180 degree about the other diagonal
Consider a set contains all this elements say $S = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$
If we apply an operation that is composition so we can see that
composition of two elements in the set S is again in S.
If we take composition of any element with R_0 we get same element.
Also R_0 exist in each of the row
and associativity of elements with respect to composition holds for every element in the set.
So we can see that S forms a group with respect to composition. This set is called dihedral group of order 8. and it is denoted by D_4.

Definition and examples

Definition: Binary operation:
Let G be a set. A binary opration on G is a function that assigns each ordered pair of elements of G an element of G.
For example: 1. Addition on set of Integers
2.Multiplication on set of real numbers.

Definition: Group Let G be a nonempty set together with a binary operation (Say multiplication) is called a group if it satisfies following properties:
1. Closure: For $a, b \in G \Rightarrow ab \in G$
2. Associativity: $(ab)c = a(bc)$ for all $a, b, c \in G$
3. Identity: There is an element e in G such that $ae = ea = a$.
4. Inverses: For each element a in G, there is an element $b \in G$ such that $ab = ba = e$

Examples:
1. Z- Set of integers with respect to addition
For Closure: let $a, b \in Z$ then $a + b \in Z$ as addition of two integers is again an integer. So Z is closed with respect to addition.
For Associative: Since $(ab)c = a(bc)$ for all $a, b, c \in Z$. So associativity exists
For Identity: Since $a + 0 = a$ for all $a \in G$ so 0 is the identity element of Z.
For Inverse: For $a \in Z$ there exists $-a \in Z$ such that $a + (-a) = 0$.
All the properties of group satisfied by Z so Z is a group with respect to addition.

2.Set of integers with respect to multiplication?
3.Set of real numbers with respect to addition?
4.Set of positive real numbers with respect to multiplication?
5.Set of postive rationals with resect to multiplication?
6.Set of positive irrationals with resect to multiplication?
7.Set of $n \times n$ Matrices with real entries with respect to addition.

Elementary properties of Groups

Uniqueness of the identity:
In the group G there is only one identity element.
Proof: Let G be a group. By contrary suppose there exists two identities e and e' in G.
Then $ae = ea = a$ for all $a \in G$ ...1
and $ae' = e'a = a$ for all $a \in G$ ...2
Put $a = e'$ in 1 and $a = e$ in 2
we get $e'e = e'$ and $e'e = e$ so $e' = e$
Therefore there exists unique identity element.

Cancellation law:
In a group G, the right and left cancellation laws hold;
That is $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.
Proof: Suppose $ba = ca$. Let a' be an inverse of a then multiplying by a' on both side we get $(ba)a' = (ca)a'$ by associativity $b(aa') = c(aa')$
so we have $be = ce$ therefore $b = c$.
Similarly we can prove $ab = ac \Rightarrow b = c$

Uniqueness of Inverses
For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.
Proof: Suppose b and c are both inverses of a.
Then $ab = e$ and $ac = e$ so we have $ab = ac$
by cancellation law we can cancel a so we get $b = c$
There exists an unique inverse for every element in a group G.

Socks- Shoes Property:
For a, b in a group G, $(ab)^{-1} = b^{-1}a^{-1}$
Proof: Since $(ab)(ab)^{-1} = e$ and
$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a = aea^{-1} = aa^{-1} = e$
we have $(ab)(ab)^{-1} = (ab)(b^{-1}a^{-1}) \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$

Definition: Order of a group
The number of elements of a group (finite or infinite) is called its order. **Notation:** $|G|$

For example
1. Order of the group of real numbers is infinite.
2. Order of the group $\{1, -1, i, -i\}$ is of order 4.

Definition: Order of an element:
The order of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive group we have $ng = 0$) . If no such integer exists, we say that g has infinite order
Notetion: $|g|$

For example:
1. Consider the group $U(10) = \{1, 3, 7, 9\}$
Here $|1| = 1, |3| = 4, |7| = 4, |9| = 2$

2. $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
Here $|0| = 1, |1| = 9, |2| = 9, |3| = 3, |4| = 9, |5| = 9, |6| = 3, |7| = 9, |8| = 9$

Definition: Subgroup
A subset H of a group G is itself a group under the operation of G is called subgroup of G.
Notation: $H \leq G$
For example 1. $\{e\}$ and G are the trivial subgroups of the group G. 2. Z, Q is a subgroup of R with respect to addition.

One step subgroup test:
Let G be a group and H be a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G.
Proof: Let G be a group and H be a nonempty subset of G
To prove: H is a subgroup of G that is to prove H is itself a group.
Since opertaion of H is same as G so associativity holds.
Now as H is nonempty take any element say x in H
as ab^{-1} is in H take $a = x$ and $b = x$ so we have $xx^{-1} \in H$
But $xx^{-1} = e$ so $e \in H$.
Therefore H contains an identity element.
Now to check whether $x^{-1} \in H$ for $x \in H$
Choose $a = e$ and $b = x$ then we have $ab^{-1} \in H$ so $ex^{-1} \in H$
$x^{-1} \in H$. Inverse exists for every element in H.
Now to H is closed
Let $x, y \in H$ we need to show that $xy \in H$
Since $y^{-1} \in H$ so take $a = x$ and $b = y^{-1}$ so we have $ab^{-1} = x(y^{-1})^{-1} = xy \in H$
Therefore H is a group itself and hence it is a subgroup of G.

Two step subgroup test:
Let G be a group and let H be any nonempty subset of G. If $ab \in H$ whenever $a, b \in H$ and $a^{-1} \in H$ whenever $a \in H$, then H is a subgroup of G.
Proof: Let G be a group and H be a nonempty subset of G
To show that H is subgroup of G.
By one step subgroup test it is sufficient to prove that $a, b \in H \Rightarrow ab^{-1} \in H$.
Let $a, b \in H$ by assumtion $a^{-1}, b^{-1} \in H$ also H is closed so $ab^{-1} \in H$
Hnece H is a subgroup of G.

Finite subgroup test:
Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.
Proof: Let G be a group and H be a nonempty subset of G
To show that H is subgroup of G.
By two step subgroup test it is sufficient to prove that $a^{-1} \in H$ whenever $a \in H$
If $a = e$ then $a^{-1} = e^{-1} = e = a$ then we are done.
If $a \neq e$, cosider the sequence $a, a^2, ...$
By closureness all these elements are in H.
As H is finite so all of these elements are not distinct say $a^i = a^j$ and $i > j$
then $a^i(a^j)^{-1} = a^j(a^j)^{-1} \Rightarrow a^i a^{-j} = e \Rightarrow a^{i-j} = e$
Since $a \neq e$ so $i - j > 1$ so $aa^{i-j-1} = a^{i-j} = e$
therefore $a^{-1} = a^{i-j-1}$ and $j - j - 1 \geq 1$ so $a^{i-j-1} \in H$

So $a^{-1} \in H$ for all $a \in H$
By two step subgroup test H is a subgroup of G.

Examples
1. Let G be an abelian group with identity e.
Consider $H = \{x \in G | x^2 = e\}$
Since $e^2 = e$ so $e \in H$, H is non-empty. Let $a, b \in H$, then $a^2 = e, b^2 = e$
Consider $(ab^{-1})^2 = ab^{-1}ab^{-1} = aab^{-1}b^{-1} = a^2(b^2)^{-1} = ee^{-1} = e$
Therefore by one step subgroup test $ab^{-1} \in H$

2. Let G be an abelian group and consider $H = \{x^2 | x \in G\}$
for $e \in G$, $e^2 = e \in H$ so H is non-empty
let $a^2, b^2 \in H$ so $a, b \in G$ since G is a group so $ab \in G$ and $(ab)^2 = a^2b^2$
as $ab \in G$ so $(ab)^2 \in H$ then $a^2b^2 \in H$
Now let $a^2 \in H$ so $a \in G$ and $a^{-1} \in G$ so $(a^2)^{-1} = (a^{-1})^2$
So $(a^2)^{-1} \in H$
By two step subgroup test H is a subgroup of G

3. Let $Z_6 = \{0, 1, 2, 3, 4, 5\}$ and $H = \{0, 1, 5\}$
Since H is non empty and $0 + 1, 1 + 5, 0 + 5 \in H$
so H is closed with respect to same operation of Z_6
so by finite subgroup test H is a subgroup of G.

Generator of an element in a group G:
Let G be a group and $a \in G$ then generator of a is denoted by $< a >$ and is defined as
$< a >= \{a^n | n \in Z\}$

For example:
1. $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$
and $< 2 >= \{2, 4, 6, 0\}$, $< 3 >= \{3, 6, 1, 4, 7, 2, 5, 0\}$
2. $U(12) = \{1, 5, 7, 11\}$
$< 5 >= \{5, 1\}$, $< 7 >= \{7, 1\}$

Theorem: Let G be a group and let a be any element of G. Then $< a >$ is a subgroup of G.
Proof: Let G be a group and $< a >= \{a^n | n \in Z\}$
Since $a \in < a >$ so $< a >$ is nonempty
Let $a^k, a^m \in < a >$, Consider $a^k(a^m)^{-1} = a^{k-m} \in < a >$
As $k, m \in Z \Rightarrow k - m \in Z$
So by one step suubgroup test $< a >$ is a subgroup of G.

Center of a group
The center of a group G is the subset of elements of G that commute with every element of G.
It is denoted by $Z(G)$.
That is $Z(G) = \{a \in G | ax = xa \ \forall x \in G\}$

for example
1.$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
then $Z(Z_{10}) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = Z_{10}$
2.$K_4 = \{e, a, b, c\}$
then $Z(K_4) = \{e, a, b, c\} = K_4$

Theorem: The center of a group G is a subgroup of G.
Proof: Let G be a group and $Z(G) = \{a \in G | ax = xa \ \forall x \in G\}$
To prove: $Z(G)$ is a subgroup of G
Since $ex = xe$ for all $x \in G$ therefore $e \in Z(G)$ so $Z(G)$ is non-empty
Now let $a, b \in Z(G)$ so $ax = xa$ and $bx = xb$ for all $x \in G$
Consider $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$ for all $x \in G$
so $ab \in Z(G)$
Let $a \in Z(G)$ so $ax = xa$ for all $x \in G$
we need to show that $a^{-1} \in Z(G)$
Consider $ax = xa$, multiply a^{-1} from left and right we get
$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$
$a^{-1}a(xa^{-1}) = a^{-1}x(aa^{-1})$
$exa^{-1} = a^{-1}xe$
$xa^{-1} = a^{-1}x$, for all $x \in G$
So $a^{-1} \in Z(G)$
Hence by two step subgroup test center of G is a subgroup of G.

Centralizer of a in G
Let a be an element of a group G.
The centralizer of a in G is the set of all elements in G that commute with a.
It is denoted by $C(a)$ and $C(a) = \{g \in G | ga = ag\}$
For example:
Let $U(5) = \{1, 2, 3, 4\}$
$C(2) = \{1, 2, 3, 4\}$

Theorem: For each a in a group G, the centralizer of a is a subgroup of G.
Proof: Let G be a group and $C(a)$ and $C(a) = \{g \in G | ga = ag\}$ be the centralizer of a in G
Let $g, h \in C(a)$ then $ga = ag$ and $ha = ah$
Consider $(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$ so $gh \in C(a)$
Let $g \in C(a)$ so $ga = ag$
we neeed to show that $g^{-1} \in C(a)$
As $ga = ag$ multiply by g^{-1} from left and right
So $g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1}$
$(g^{-1}g)ag^{-1} = g^{-1}a(gg^{-1})$
$eag^{-1} = g^{-1}ae$
$ag^{-1} = g^{-1}a$
So $g^{-1} \in C(a)$
Therefore by two step subgroup test $C(a)$ is a subgroup of G