Notes on Group Theory - I (Core Course IV) by SB (Subhasundar Bandyopadhyay)

Books followed: 1. Higher Algebra (Abstract and Linear) - S.K. Mapa
2. Contemporary Abstract Algebra - Joseph
3. Fundamentals of Abstract Algebra - D.S. Malik, John M. Mordeson and M.K. Sen

Symmetries of a square: Let S be the set of all points in a Euclidean space (line, plane, 3-dimensional space etc.). An isometry is a bijection of S onto S that preserves distance between two points in S.
A symmetry of a geometrical figure in a Euclidean space is an isometry that keeps the figure as a whole unchanged.

Let us consider a square ABCD with centre at O, the origin and sides parallel to the axes of a Co-ordinate system (Fig 1).

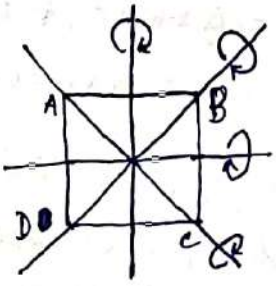


Fig 1

The following rigid motions (i.e rotation and translation) of the square ABCD are all the symmetries of the square: clockwise rotations of the square about the centre and through angles 90°, 180°, 270° and 360°, denoted by r_1, r_2, r_3 and i respectively; reflections h and v about the horizontal and vertical axes, denoted by h and v respectively; reflections d, d' about the diagonals. The following figures should be helpful

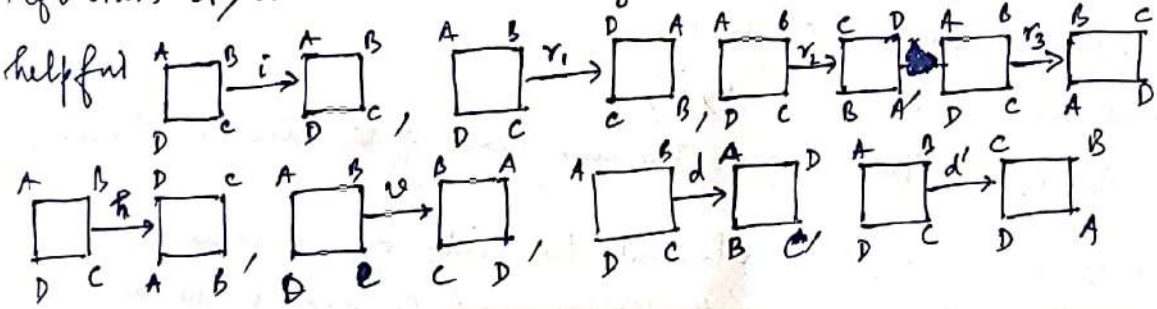


Fig 2

A multiplication * on two rigid motions can be defined by performing two such motions in succession. For example, $r_1 * h$ is determined by first performing motion h and then motion r_1. We see $r_1 * h = d$

The complete multiplication table for the operation $*$ is as follows:

$*$	i	r_1	r_2	r_3	h	v	d	d'
i	i	r_1	r_2	r_3	h	v	d	d'
r_1	r_1	r_2	r_3	i	d	d'	v	h
r_2	r_2	r_3	i	r_1	v	h	d'	d
r_3	r_3	i	r_1	r_2	d'	d	h	v
h	h	d'	v	d	i	r_2	r_3	r_1
v	v	d	h	d'	r_2	i	r_1	r_3
d	d	h	d'	v	r_1	r_3	i	r_2
d'	d'	v	d	h	r_3	r_1	r_2	i

Fig 3

We will see later that the set of these symmetries of a square under the operation $*$ forms a group, called the group of symmetries of the square. It is also called the dihedral group D_4.

Definition of Group: A non-empty set G is said to form a group with respect to a binary operation $*$ on G if the following properties hold:

(i) $a*(b*c) = (a*b)*c$, $\forall a, b, c \in G$ (associative property)

(ii) $\exists\ e \in G$ such that $a*e = e*a = a$, $\forall a \in G$ (existence of an identity)

(iii) For each $a \in G$, $\exists$ a $b \in G$ such that $a*b = b*a = e$ (existence of an inverse in (ii))

Thus a group is a system $(G, *)$ satisfying axioms (i), (ii) and (iii). e is said to be an identity in the group, b in (iii) is said to be an inverse of the element a.

Theorem 1.1 A group $(G, *)$ contains only one identity element.

Proof: Let e_1, e_2 be two identity elements in $(G, *)$.

Then $a*e_1 = e_1*a = a$, $\forall a \in G$, —(i)

$a*e_2 = e_2*a = a$, $\forall a \in G$ —(ii)

Now, we have $e_1*e_2 = e_2$ by (i)

and also $e_1*e_2 = e_1$ by (ii)

$\therefore e_1 = e_2$. This proves the uniqueness of the identity element.

Theorem 1.2 In a group $(G, *)$, each element has only one inverse.

Proof: Let $a \in G$ and a', a'' be two inverses of a and e be the identity element. Then $a*a' = a'*a = e$ —(i)

$a*a'' = a''*a = e$ —(ii)

we have, $a'*(a*a'') = (a'*a)*a''$, since $*$ is associative.

but $a'*(a*a'') = a'*e$ (from (ii)) and $(a'*a)*a'' = e*a''$ (from (i))

$= a'$ $= a''$

$\therefore a' = a''$ and this proves that inverse of a is unique

Note: A group $(G, *)$ is said to be commutative or abelian if $a*b = b*a, \forall a, b \in G$

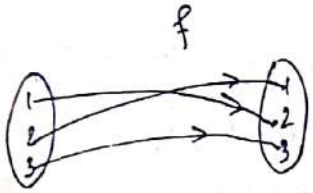
Examples of groups including permutation groups, dihedral groups, and quaternion groups (through matrices):

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are all examples of commutative groups

$\mathbb{Z}$ = the set of all integers, $\mathbb{Q}$ = the set of all rational numbers, $\mathbb{R}$ = the set of all real numbers and $\mathbb{C}$ = the set of all complex numbers, and '+' is the usual addition. Here 0 is the identity and $-a$ is the inverse of a.

Also $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$, $(\mathbb{C}\setminus\{0\}, \cdot)$ are examples of commutative group. ~~Here the identity~~ Here '$\cdot$' is usual multiplication. Here the identity element is 1. If $a \neq 0$, then $\frac{1}{a}$ is the inverse of a.

2. Let $S = \{1, 2, 3\}$. A bijective mapping $f: S \to S$ is said to be a permutation on S. For example, f given by



, that is, $f(1) = 2$, $f(2) = 1$, $f(3) = 2$, is a permutation on S. This permutation is denoted by

$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. There are six permutations on S. They are the set

$S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$ where $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

If f, g are two permutations on S, then multiplication $\circ$ between f and g is ~~defined~~ defined as the composite mapping $f \circ g: S \to S$ where $f \circ g(x) = f(g(x))$ i.e, $\rho_1 \circ \rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \rho_5$

The multiplication table for S_3 is given by

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5
ρ_1	ρ_1	ρ_2	ρ_0	ρ_5	ρ_3	ρ_4
ρ_2	ρ_2	ρ_0	ρ_1	ρ_4	ρ_5	ρ_3
ρ_3	ρ_3	ρ_4	ρ_5	ρ_0	ρ_1	ρ_2
ρ_4	ρ_4	ρ_5	ρ_3	ρ_2	ρ_0	ρ_1
ρ_5	ρ_5	ρ_3	ρ_4	ρ_1	ρ_2	ρ_0

$(S_3, \circ)$ is a group. It is also non-commutative

as $\rho_2 \circ \rho_3 = \rho_4$ but $\rho_3 \circ \rho_2 = \rho_5$ $\therefore \rho_2 \circ \rho_3 \neq \rho_3 \circ \rho_2$.

$(S_3, \circ)$ is called symmetric group of degree 3. It has $3! = 6$ elements

Similarly $(S_n, \circ)$ is called symmetric group of degree n. It has $n!$ elements.

Let $S = \{1, 2, \ldots, n\}$. A permutation $f: S \to S$ is said to be a cycle of length r, or an r-cycle if there are r elements $i_1, i_2, \ldots, i_r \in S$ such that $f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{r-1}) = f(i_r), f(i_r) = f(i_1)$ and $f(j) = j$, for $j \neq i_1, i_2, \ldots, i_r$ and $j \in S$. For example

Let $S = \{1, 2, 3, 4\}$, $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

Here f is a 3-cycle as $f(2) = 3, f(3) = 4, f(4) = 2$ and $f(1) = 1$

and g is a 2-cycle as $f(2) = 4$ and $f(4) = 2$ and $f(1) = 1, f(3) = 3$

Note: An ~~r-cycle~~ r-cycle is denoted by $(i_1, i_2, \ldots, i_r)$. So,

$f = (2, 3, 4)$, $g = (2, 4)$

For the time being, we state a theorem on permutation which says that every permutation on a finite set is either a cycle or it can be expressed as a product of disjoint cycles.

Note: The identity permutation $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ is the product of n disjoint cycles $(1), (2), \ldots, (n)$, each of length 1.

A 2-cycle is called a transposition.

A 1-cycle is the identity permutation and it can be expressed as the product of the transpositions (r, s) and (s, r)

Any r-cycle can be expressed as the product of $r-1$ cycles.

Let $(i_1, i_2, \ldots, i_r)$ be an r-cycle

Then $(i_1, i_2, \ldots, i_r) = (i_1, i_r)(i_1, i_{r-1}), \ldots, (i_1, i_2)$

A permutation is said to be even if it can be expressed as the product of an even number of transpositions, and odd if if it can be expressed as the product of an odd number of transpositions.

Since r-cycle $(i_1, i_2, \ldots, i_r)$ is the product of $r-1$ cycles, so, an r-cycle is an odd or even permutation according r is even or odd.

The identity permutation i can be expressed as the product of two transpositions (r, s) and (s, r). So i is even.

The product of two even permutations is even; the product of two odd permutations is even; the product of an even permutation and an odd permutation is odd.

The inverse of an odd permutation is odd and the inverse of an even permutation is even.

We state another theorem That the number of even permutations on a finite set (containing at least 2 elements) is equal to the number of odd permutations.

Consider the set S_3 now. ρ_0 is the identity permutation, so it is even.

$\rho_1 = (1,2,3) = (1,3)(1,2)$ is even $\rho_3 = (2,3)$ is odd,

$\rho_2 = (1,3,2) = (1,2)(1,3)$ is even $\rho_4 = (1,3)$ is odd, $\rho_5 = (1,2)$ is odd.

The set of all even permutations on the set $\{1, 2, \ldots, n\}$ forms a group with respect to multiplication of permutations. This group is called the alternating group of degree n and is denoted by A_n. A_n contains $\frac{n!}{2}$ elements. A_n is a non-commutative group for $n \geq 4$.