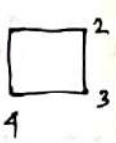
Revision

Symmetries of square can also be written as a subset of S_4.

$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$ and $\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$ gives the clockwise rotation of the square about the centre and through the angles $0°$, $90°$, $180°$ and $270°$.



$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$ and $\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$ are two reflections about the diagonals,

$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$ and $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ are two reflections about horizontal and vertical axes respectively. This eight permutations of 4 symbols 1,2,3 & 4 forms a subgroup S_4. This also can be treated as D_4 (the dihedral group)

If we denote $\rho_0 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, $\rho_1 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = (1234)$ $\rho_2 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = (13)(24)$

$\rho_3 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} = (1432)$, $\rho_4 = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix} = (24)$ $\rho_5 = \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} = (13)$

$\rho_6 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = (14)(23)$ $\rho_7 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = (12)(34)$. Then the Composition Table is

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6	ρ_7
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6	ρ_7
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	ρ_7	ρ_6	ρ_4	ρ_5
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	ρ_5	ρ_4	ρ_7	ρ_6
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	ρ_6	ρ_7	ρ_5	ρ_4
ρ_4	ρ_4	ρ_6	ρ_5	ρ_7	ρ_0	ρ_2	ρ_1	ρ_3
ρ_5	ρ_5	ρ_7	ρ_4	ρ_6	ρ_2	ρ_0	ρ_3	ρ_1
ρ_6	ρ_6	ρ_5	ρ_7	ρ_4	ρ_3	ρ_1	ρ_0	ρ_2
ρ_7	ρ_7	ρ_4	ρ_6	ρ_5	ρ_1	ρ_3	ρ_2	ρ_0

ρ_0 is the identity

$\rho_1^{-1} = \rho_3$ $\rho_3^{-1} = \rho_1$

$\rho_2^{-1} = \rho_2$ $\rho_4^{-1} = \rho_4$

$\rho_5^{-1} = \rho_5$ $\rho_6^{-1} = \rho_6$

$\rho_7^{-1} = \rho_7$

Definition of a group: G is a non-empty set. '$\circ$' is a binary operation on G. Then G is said to be a group with respect to the binary operation $\circ$ (or $(G, \circ)$ is said to a group) if the following conditions hold: (i) $a \circ (b \circ c) = (a \circ b) \circ c$, $\forall a, b, c \in G$. (Associative property)

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

(iii) for each $a \in G$, $\exists\ b \in G$ such that $a \circ b = b \circ a = e$ (existence of inverse)

Note: Sometimes this condition is added: $a \circ b \in G$, $\forall a, b \in G$. But this equivalent with "$\circ$ is a binary operation on G". So, we need not add it.

Theorem 1.1 Identity element in a group is unique.

Theorem 1.2 Each element in a group has only one inverse

A group $(G, \circ)$ is said to be commutative or abelian if $a \circ b \in G$, $\forall a, b \in G$.

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

S_3 is an example of a non-commutative group -

Let $S = \{A : A \text{ is real } n \times n \text{ non-singular matrices}\}$

Then $(S, \cdot)$ is a non-abelian group.

Example1 what is the inverse of $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 6 & 7 & 5 & 8 \end{pmatrix}$ in S_8?

We need α in S_8 s.t

$$\alpha \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 6 & 7 & 5 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

So, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 3 & 7 & 5 & 6 & 8 \end{pmatrix}$

As 1 goes to 1 in the resultant map and in the right 1 goes to 3, so, in α 3 should go to 1 and so on.

Theorem 1.3 Let G be a group. Then

(i) $(a^{-1})^{-1} = a$, $\forall a \in G$

(ii) $(ab)^{-1} = b^{-1}a^{-1}$ $\forall a, b \in G$

(iii) $ab = ac \Rightarrow b = c$ (Left Cancellation Law)

and $ba = ca \Rightarrow b = c$ (Right " ")

2. Prove that $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$ for n elements $a_1, a_2, \cdots a_n$ in a group G, $n \geq 2$.

Proof: $(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$. So, the result is true for $n = 2$

Let the result is true for $n = m$ (≥ 2)

So, $(a_1 a_2 \cdots a_m)^{-1} = a_m^{-1} a_{m-1}^{-1} \cdots a_1^{-1}$ ——— (1)

now $(a_1 a_2 \cdots a_m a_{m+1})^{-1} = \{(a_1 a_2 \cdots a_m) a_{m+1}\}^{-1} = a_{m+1}^{-1} (a_1 a_2 \cdots a_m)^{-1}$ $[\because (ab)^{-1} = b^{-1} a^{-1}]$

$= a_{m+1}^{-1} a_m^{-1} a_{m-1}^{-1} \cdots a_1^{-1}$ [From (1)]

So the result is true for $n = m+1$

So, by principle of Mathematical induction,

$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$ for $n \geq 1$ ———

Corollary 1.3.1 In a composition table for a group G, each element appears exactly once in each row and exactly once in each column.

3. Complete the following composition table such that the set $S = \{a, b, c\}$ forms a group with respect to '$*$'

$*$	a	b	c
a	a	b	c
b	b		
c	c		

Ans: $b * b$ = [illegible] either a or c but if $b * b = a$

then $b * c$ should be c which is not possible

from the corollary 1.3.1 . So $b * b = c$ So, $b * c = a$

So, $c * b = a$, and $c * c = b$. So the full composition table is

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Theorem 1.4 A semigroup S is a group if and only if
(i) $\exists\ e \in S$ such that $ea = a$, $\forall a \in S$ (e is called a left identity)
(ii) For each $a \in S$, $\exists\ b \in S$ such that $ba = e$ (b is called a left inverse)

(i.e A semigroup S is a group if it has a left identity element and each element of S has a left inverse in S.)

Similarly,
Theorem 1.5 A semigroup S is a group if and only if
(i) $\exists\ e \in S$ such that $ae = a$, $\forall a \in S$ (e is called a right identity)
(ii) For each $a \in S$, $\exists\ b \in S$ such that $ab = e$ (b is called a right inverse)

(i.e A semigroup S is a group if it has a right identity element and each element of S has a right inverse in S.)

Note: Consider a non-empty set $\mathbb{Z}$ and define a binary operation '$\circ$' on $\mathbb{Z}$ by $a \circ b = b$, $\forall a, b \in \mathbb{Z}$.

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

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

So, $(a \circ b) \circ c = a \circ (b \circ c)$ $\forall a, b, c \in \mathbb{Z}$

So, $(\mathbb{Z}, \circ)$ is a semi-group

Now take $0 \in \mathbb{Z}$

Now $0 \circ a = a$, $\forall a \in \mathbb{Z}$. So, 0 is a left identity. Also $a \circ 0 = 0$, $\forall a \in \mathbb{Z}$. So 0 is a right inverse of each element $a \in \mathbb{Z}$. But $(\mathbb{Z}, \circ)$ is not a group as there is no identity element in $(\mathbb{Z}, \circ)$.

Note: left identity and right inverse existence in a semigroup does not imply that it is a group.