$$= a * a^{-1} \qquad [\because a * e = a]$$

$$= e \qquad \ldots (1)$$

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

$$= b^{-1} * e * b$$

$$= b^{-1} * b \qquad [\because e * b = b]$$

$$= e \qquad \ldots (2)$$

By (1) and (2), we get

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

$$\Rightarrow \quad (a * b)^{-1} = b^{-1} * a^{-1}$$

Example 7. Every group of order 4 is abelian.

Solution : Let $(G, *)$ be a group of order 4 where $G = \{e, a, b, c\}$. Since G is of even order, there exists at least one element (say) a such that $a^{-1} = a$.

Then two cases arise

(i) $b^{-1} = b$, $c^{-1} = c$, (ii) $b^{-1} = c$, $c^{-1} = b$.

Case (i) : $e^{-1} = e$, $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$

Every element as its own inverse.

The $(G, *)$ is abelian.

Case (ii) : $a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$

$\therefore$ $a^2 = e$, $b * c = e$, $c * b = e$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Since $(G, *)$ is a group, its elements will appear in a row (column) only once.

Since, a, e appears in the second row and b appears in the third column, c will appear as (2, 3)th element.

$\therefore$ (2, 4)th element is b

(3, 3)th element is a

(3, 2)th element is c

(4, 2)th element is b

(4, 4)th element is a

Example 8. Show that G $= \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \neq 0 \in R \right\}$ is an abelian group under matrix multiplication.

Solution :

(i) **Closure law**

$$\text{Let } A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G.$$

$$\text{Then } AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in G.$$

(ii) **Commutative Law :** $AB = BA$ is true $\forall\ A, B \in G$, since

$$AB = BA = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \qquad [\because ab = ba \text{ is true in } R]$$

(iii) Matrix multiplication is associative.

(iv) **Identity :** $I = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G$ is the identity in G, since

$$A\,I = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = A \ \forall\ A \in G.$$

(iv) **Inverse :** If

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G. \text{ Then } A^{-1} = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \in G.$$

is the inverse of A, since

$$AA^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = 1 \qquad (\because a \neq 0 \in R \Rightarrow 1/a \neq 0 \in R)$$

Hence G is an abelian group under matrix multiplication.

Example 9. Show that the set S = {1, 5, 7, 11} is a group w.r.t multiplication modulo 12.

Solution : The composition tables of S w.r.t $\odot_{12}$ of as follows :

$\odot_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Here $5 \odot_{12} 7 = 35$, which on division by 12 gives the remainder 11, $11 \odot_{12} 7 = 77$, which on division by 12 gives the remainder 5 etc.

Hence S is a group, in which 1 is the identity and each element of S is its own inverse.

Example 10. Show that the set of matrices

$$\mathbf{G} = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}, \ a \in \mathbf{R} \right\}$$ **forms a group under matrix multiplication.**

Solution : (i) Closure law

Let $A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \in G$ and $A_\beta = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \in G$.

Then $A_\alpha A_\beta = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$

$$A_\alpha A_\beta = \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -(\cos\alpha\sin\beta + \sin\alpha\cos\beta) \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta} \in G.$$

Note that $A_\alpha A_\beta = A_{\alpha+\beta}$ ... (1)

(ii) We know that the matrix multiplication is associative.

(iii) **Identity :** $I_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity in G.

Since $A_\alpha I_0 = I_0 A_\alpha = A_\alpha$ for $A_\alpha \in G$.

(iv) **Inverse :** $A_{-\alpha}$ is the inverse of A_α for each $A_\alpha \in G$, since

$A_\alpha A_{-\alpha} = A_{\alpha+(-\alpha)} = A_0 = I_0$, using (1)

Example 11. Find the left cosets of {[0], [3]} in the addition modular group (Z_6, $+_6$). **[MCA, N/D. 2002] [A.U N/D 2010]**

Solution : Let Z_6 = {[0], [1], [2], [3], [4], [5], [6]} be a group and H = {[0], [3]} be a sub-group of Z_6 under $+_6$ (addition mod 6)

The left cosets of H are

$$[0] + H = \{[0], [3]\} = H$$
$$[1] + H = \{[1], [4]\}$$
$$[2] + H = \{[2], [5]\}$$
$$[3] + H = \{[3], [6]\} = \{[3], [0]\} = \{[0], [3]\} = H$$
$$[4] + H = \{[4], [7]\} = \{[4], [1]\} = [1] + H$$
$$[5] + H = \{[5], [8]\} = \{[5], [2]\} = [2] + H$$
$$\therefore \quad [0] + H = [3] + H = H$$

and $\quad [1] + H = [4] + H, [2] + H = [5] + H$

are the distinct left cosets of H in Z_6

Example 12. If $f: G \to G'$ is a group homomorphism from {G, *} to {G′, Δ} then prove that for any $a \in G$, $f(a^{-1}) = [f(a)]^{-1}$ **[A.U N/D 2012]**

Solution : $\forall\ a \in G$ and $\forall\ a^{-1} \in G$

$$\therefore \quad f(a * a^{-1}) = f(a) \Delta f(a^{-1})$$

i.e., $$f(e) = f(a) \Delta f(a^{-1})$$

i.e., $\quad e' = f(a) \Delta f(a^{-1}) \quad \ldots (1)$

$|||^{ly}$, $\quad f(a^{-1} * a) = f(a^{-1}) \Delta f(a)$

i.e., $\quad f(e) = f(a^{-1}) \Delta f(a)$

$$e' = f(a^{-1}) \Delta f(a) \quad \ldots (2)$$

From (1) & (2), we get

$$f(a) \Delta f(a^{-1}) = f(a^{-1}) \Delta f(a)$$

$\Rightarrow f(a^{-1})$ is the inverse of $f(a)$

i.e., $f(a^{-1}) = [f(a)]^{-1}$

Example 13. Let G be a group and a $\in$ G. Let f : G $\to$ G be given by f(x) $=$ a x a^{-1} for all $x \in$ G. Prove that f is an isomorphism of G on to G. **[A.U. A/M. 2005, N/D 2010]**

Solution : The map f is a homomorphism if $x, y \in$ G, then

$$f(x)\, f(y) = (axa^{-1})\,(aya^{-1})$$
$$= ax\,(a^{-1}a)\, ya^{-1}$$
$$= axya^{-1}$$
$$= a\,(xy)\, a^{-1} = f(xy).$$

So f is a homomorphism.

f is one-to-one : If $f(x) = f(y)$, then $axa^{-1} = aya^{-1}$, so by left cancellation, we have $xa^{-1} = ya^{-1}$, again by right cancellation we get $x = y$.

f is onto : Let $y \in$ G, then $a^{-1}ya \in$ G and $f(a^{-1}ya)$

$$= a\,(a^{-1}ya)\,a^{-1}$$
$$= (aa^{-1})\,y\,(aa^{-1})$$
$$= y. \quad \text{So } f(x) = y \text{ for some } x \in G.$$

Thus f is an isomorphism.

PERMUTATION FUNCTIONS

Definition :

A bijection from a set A to itself is called a **permutation** of A.

Example 14 : Let A=R and let $f : A \to A$ be defined by $f(a) = 2a + 1$. Since f is one to one and onto, it follows that f is a permutation of A.

Example 15 : Let A = {1, 2, 3}. Then all the permutations of A are

$$1_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Using the permutations of compute

(a) p_4^{-1} ; (b) $p_3 \circ p_2$

Solution : (a) Viewing p_4 as a function, we have

$$p_4 = \{(1, 3), (2, 1), (3, 2)\}$$

Then $$p_4^{-1} = \{(3, 1), (1, 2), (2, 3)\}$$

or, when written in increasing order of the first component of each ordered pair, we have

$$p_4^{-1} = \{(1, 2), (2, 3), (3, 1)\}$$

Thus $$p_4^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = p_3$$

(b) The function p_2 takes 1 to 2 and p_3 takes 2 to 3, so $p_3 \circ p_2$ takes 1 to 3. Also, p_2 takes 2 to 1 and p_3 takes 1 to 2, so $p_3 \circ p_2$ takes 2 to 2. Finally, p_2 takes 3 to 3 and p_3 takes 3 to 1, so $p_3 \circ p_2$ takes 3 to 1. Thus

$$p_3 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

We may view the process of forming $p_3 \circ p_2$ as shown in fig. Observe that $p_3 \circ p_2 = p_5$.

$$p_3 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = p_5$$

Theorem : If $A = \{a_1, a_2, \ldots a_n\}$ is a set containing n elements, then there are

$n! = n \cdot (n-1) \ldots 2.1$ permutations of A

Definition : Cyclic permutation

Let $b_1, b_2, \ldots b_r$ be r distinct elements of the set $A = \{a_1, a_2, \ldots a_n\}$. The permutation $p : A \to A$ defined by

$$p(b_1) = b_2$$
$$p(b_2) = b_3$$
$$\vdots$$
$$p(b_{r-1}) = b_r$$
$$p(b_r) = b_1$$

$p(x) = x$, if $x \in A$, $x \notin \{b_1, b_2, \ldots b_r\}$ is called a **cyclic permutation** of length r, or simply a **cycle** of length r, and will be denoted by $(b_1, b_2, \ldots b_r)$.

Example 16: Let $A = \{1, 2, 3, 4, 5\}$. The cycle $(1, 3, 5)$ denotes the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

Example 17: Let $A = \{1, 2, 3, 4, 5, 6\}$. Compute $(4, 1, 3, 5) \circ (5, 6, 3)$ and $(5, 6, 3) \circ (4, 1, 3, 5)$.

Solution : We have

$$(4, 1, 3, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix}$$

$$(5, 6, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}$$

Then $(4, 1, 3, 5) \circ (5, 6, 3)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$$

and $(5, 6, 3) \circ (4, 1, 3, 5)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 6 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 1 & 4 & 3 \end{pmatrix}$$

Observe that

$$(4, 1, 3, 5) \circ (5, 6, 3) \neq (5, 6, 3) \circ (4, 1, 3, 5)$$

and that neither product is a cycle.

Definition :

Two cycles of a set A are said to be **disjoint** if no element of A appears in both cycles.

Example 18 : Let $A = \{1, 2, 3, 4, 5, 6\}$. Then the cycles $(1, 2, 5)$ and $(3, 4, 6)$ are disjoint, whereas the cycles $(1, 2, 5)$ and $(2, 4, 6)$ are not.

Theorem : A permutation of a finite set that is not the identity or a cycle can be written as a product of disjoint cycles of length ≥ 2.

Example 19: Write the permutation $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 5 & 2 & 1 & 8 & 7 \end{pmatrix}$ of the set $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ as a product of disjoint cycles.

Solution : We start with 1 and find that $p(1) = 3$, $p(3) = 6$, and $p(6) = 1$, so we have the cycle (1, 3, 6). Next we choose the first element of A that has not appeared in a previous cycle. We choose 2, and we have $p(2) = 4$, $p(4) = 5$ and $p(5) = 2$, so we obtain the cycle (2, 4, 5). We now choose 7, the first element of A that has not appeared in a previous cycle. Since $p(7) = 8$ and $p(8) = 7$, we obtain the cycle (7, 8). We can then write p as product of disjoint cycles as

$$p = (7, 8) \circ (2, 4, 5) \circ (1, 3, 6).$$

Definition : Even and Odd Permutations

A cycle of length 2 is called a **transposition**. That is, a transposition is a cycle $p = (a_i, a_j)$, where $p(a_i) = a_j$ and $p(a_j) = a_i$.

Observe that if $p = (a_i, a_j)$ is a transposition of A, then $p \circ p = 1_A$, the identity permutation of A.

Every cycle can be written as a product of transpositions. In fact,

$$(b_1, b_2, \ldots b_r) = (b_1, b_r) \circ (b_1, b_{r-1}) \circ \ldots \circ (b_1, b_3) \circ (b_1, b_2)$$

This case can be verified by induction on r, as follows :

Basis Step

If $r = 2$, then the cycle is just (b_1, b_2), which already has the proper form.

Induction Step

We use P (k) to show P $(k+1)$. Let $(b_1, b_2, \ldots b_k, b_{k+1})$ be a cycle of length $k+1$. Then $(b_1, b_2, \ldots b_k, b_{k+1}) = (b_1, b_{k+1}) \circ (b_1, b_2, \ldots b_k)$ as may be verified by computing the composition. Using P(k), $(b_1, b_2, \ldots b_k) = (b_1, b_k) \circ (b_1, b_{k-1}) \circ \ldots \circ (b_1, b_2)$. Thus, by substitution,

$$(b_1, b_2, \ldots b_{k+1}) = (b_1, b_{k+1}) \circ (b_1, b_k) \circ \ldots \circ (b_1, b_3)\ (b_1, b_2).$$

This completes the induction step. Thus, by the principle of mathematical induction, the result holds for every cycle. For example,

$$(1, 2, 3, 4, 5) = (1, 5) \circ (1, 4) \circ (1, 3) \circ (1, 2)$$

Corollary 1 : Every permutation of a finite set with atleast two elements can be written as a product of transpositions.

Theorem : If a permutation of a finite set can be written as a product of an even number of transpositions, then it can never be written as a product of an odd number of transpositions, and conversely.

A permutation of a finite set is called **even** if it can be written as a product of an even number of transpositions, and it is called **odd** if it can be written as a product of an odd number of transpositions.

Example 20 : Is the permutation

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

even or odd ?

Solution : We first write p as a product of disjoint cycles, obtaining

$$p = (3, 5, 6) \circ (1, 2, 4, 7).$$

Next we write each of the cycles as a product of transpositions :

$$(1, 2, 4, 7) = (1, 7) \circ (1, 4) \circ (1, 2)$$

$$(3, 5, 6) = (3, 6) \circ (3, 5)$$

Then $p = (3, 6) \circ (3, 5) \circ (1, 7) \circ (1, 4) \circ (1, 2)$. Since p is a product of an odd number of transpositions, it is an odd permutation.

Note : From the definition of even and odd permutations, it follows.

(a) The product of two even permutation is even.

(b) The product of two odd permutations is even.

(c) The product of an even and an odd permutation is odd.

Example 21 : Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$ **is odd, while the permutation** $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ **is even.**

Solution :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 5)\ (2\ 6\ 3)$$

$$= (1\ 5)\ (2\ 6)\ (2\ 3)$$

The given permutation can be expressed as the product of an odd number of transpositions and hence the permutation is odd. Again

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\ 6)\ (2\ 3\ 4\ 5)$$

$$= (1\ 6)\ (2\ 3)\ (2\ 4)\ (2\ 5)$$

Since it is a product of even number of transposition, the permutation is an even permutation.

Example 22 : Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ **as a product of transposition.**

Solution :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 6)\ (2\ 5\ 3) = (1\ 6)\ (2\ 5)\ (2\ 3)$$

Example 23 : Find the inverse of the permutation.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Solution : Given $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

Let the inverse of the permutation be $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix}$

Then $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ x & y & z & u & v\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}$

$\Rightarrow \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ y & z & x & v & u\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}$

$\Rightarrow y = 1, z = 2, x = 3, v = 4, u = 5.$

Hence the inverse permutation is $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 1 & 2 & 5 & 4\end{pmatrix}$.

Example 24 : If A = (1 2 3 4 5), B = (2 3) (4 5). Find AB.

Solution : Given A = (1 2 3 4 5), B = (2 3) (4 5)

$$AB = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 4 & 5 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 2 & 5 & 4\end{pmatrix}$$

$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 5 & 4 & 1\end{pmatrix}$$

$$= (1\ 3\ 5)$$

Example 25 : If A = {1, 2, 3, 4, 5, 6, 7, 8} then express the following permutations as a product of disjoint cycles.

(a) $p = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 6 & 5 & 7 & 8 & 4 & 3 & 2 & 1\end{pmatrix}$

(b) $p = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 2 & 3 & 1 & 4 & 6 & 7 & 8 & 5\end{pmatrix}$

Solution :

(a) $p(1) = 6, p(6) = 3, p(3) = 7, p(7) = 2, p(2) = 5, p(5) = 4, p(4) = 8, p(8) = 1.$

$\therefore p = (1, 6, 3, 7, 2, 5, 4, 8\}$

(b) $p(1) = 2, p(2) = 3, p(3) = 1 \Rightarrow (1, 2, 3)$

$p(5) = 6, p(6) = 7, p(7) = 8, p(8) = 5 \Rightarrow (5, 6, 7, 8)$

$p = (5, 6, 7, 8) \circ (1, 2, 3)$

Example 26 : Let A = $\{1, 2, 3, 4, 5, 6\}$ and

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$$ be a

permutation of A.

(a) Write p as a product of disjoint cycles.

(b) Compute p^{-1}

(c) Compute p^2

(d) Find the period of p, that is, the smallest positive integer k such that $p^k = 1_A$.

Solution :

(a) Given $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

Since $p(1) = 2$, $p(2) = 4$ and $p(4) = 1$, we write $p = (1, 2, 4)$ as the other elements are fixed.

(b) $p^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$

(c) $p^2 = p \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$

(d) $p^3 = p^2 \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = 1_A.$

$p^4 = p$, $p^5 = p^2$ etc.

$\therefore$ The period of $p = 3$.

$$(p_2 \circ p_1)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$\therefore \quad (p_2 \circ p_1)^{-1} = p_1^{-1} \circ p_2^{-1}$

Example 27 : If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ and

$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ are permutations,

prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Solution : $f^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ and

$$g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$f^{-1} \circ g^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$(g \circ f)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Hence $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Example 28 : Let $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}$ and

$p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 4 & 7 \end{pmatrix}$

(a) Compute $p_1 \circ p_2$

(b) Compute p_1^{-1}

(c) Is p_1 an even or odd permutation ? Explain.

Solution :

(a) $p_1 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 2 & 1 & 5 & 4 & 7 \end{pmatrix}$

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

(b) $p_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 2 & 5 & 6 & 7 & 1 \end{pmatrix}$

(c) $p_1 = (1, 7, 6, 5, 4) \circ (2, 3)$

(i) **Closure :** Let $b \in H \Rightarrow b^{-1} \in H$

$\therefore$ For $a, b \in H \quad \Rightarrow a, b^{-1} \in H$

$$\Rightarrow a * (b^{-1})^{-1} \in H$$

$$\Rightarrow a * b \in H$$

$\therefore$ H is closed under the operation "$*$"

(ii) **Associative :** Since $H \subseteq G$, the elements of H are also the elements of G.

Since $*$ is associative in G, it must also be associative in H.

(iii) **Identity :** Let $a \in H, \quad \Rightarrow a * a^{-1} \in H$

$$\Rightarrow e \in H$$

$\therefore$ e is the identity element of H.

(iv) **Existence of inverse :** Let $e \in H$, $a \in H$

$$\Rightarrow e * a^{-1} \in H$$

$$\Rightarrow a^{-1} \in H$$

$\therefore$ Every element of H has an inverse in H.

$\therefore$ H itself is a group under the operation $*$ in G.

Theorem 2 :

Let $(G, *)$ be a finite group, and H is non-empty subset of G and H is closed under $*$. Then H is a subgroup of G.

Proof : $(G, *)$ is a finite group and H is a subset of G which is closed under $*$.

i.e., $a, b \in H \Rightarrow a * b \in H$.

Let $O(G) = n$

Now $a, a \in H$

Then $\quad a * a = a^2 \in H$

$a^2, a \in H$. Then $a^2 * a = a^3 \in H$ and so on.

Since G is finite there exists a 'm' with $1 \leq m \leq n$ such that

$$a^m = e \in H$$

That is $e \in H$

Hence identity exists.

Let $a \in H$, then $a^{m-1} \in H$.

i.e., $a^{m-1} = a^m * a^{-1} \in H$

i.e., $e * a^{-1} \in H$

i.e., $a^{-1} \in H$.

$\Rightarrow$ inverse exists.

Since every element of H is G, associative property is true in H.

Hence $(H, *)$ is a group and so H is a subgroup of G.

Theorem 3.

The kernal of a homomorphism g from a group $<G, *>$ to $<H, \Delta>$ is a subgroup of $<G, *>$.

Proof : Since $g(e_G) = e_H, e_G \in ker(g)$

Also , if $a, b \in ker(g)$,

i.e., $g(a) = g(b) = e_H$, then

$$g(a * b) = g(a) \Delta g(b) = e_H \Delta e_H = e_H$$

so that $a * b \in ker(g)$.

Finally, if $a \in ker(g)$, then $g(a^{-1}) = [g(a)]^{-1} = e_H^{-1} = e_H$.

Hence $a^{-1} \in ker(g)$ and $ker(g)$ is a subgroup of $<G, *>$.

Theorem 4.

Every cyclic group is abelian. **[A.U. M/J 2013, N/D 2013]**

Solution: Let $(G, *)$ be a cyclic group generated by an element $a \in G$.

(i.e.,) $G = (a)$

Then for any two elements $x, y \in G$

We have $x = a^n$, $y = a^m$, where m, n are integer.

$$\begin{aligned} \text{Therefore} \quad x * y &= a^n * a^m = a^{n+m} \\ &= a^{m+n} = a^m * a^n \\ &= y * x \end{aligned}$$

Thus, $(G, *)$ is abelian.

Problems based on sub group

Example 1. Is the union of two subgroups of a group, a subgroup of G? Justify your answer.

Solution : The union of two subgroups of a group need not be a subgroup of G.

Let the group $(Z, +)$

Let $H = 3Z = \{0, \pm 3, \pm 6, ...\}$

Let $K = 2Z = \{0, \pm 2, \pm 4, ...\}$

$\Rightarrow$ H and K are subgroups of $(Z, +)$.

$\Rightarrow \quad 3 \in 3Z \in 3Z \cup 2Z = H \cup K$

$\Rightarrow \quad 2 \in 2Z \in 2Z \cup 3Z = H \cup K$

But $\quad 3 + 2 = 5 \notin 2Z \cup 3Z$

$\therefore$ $H \cup K$ is not a subgroup of $(Z, +)$

Example 2. The identity element of a subgroup is same as that of the group. **[A.U N/D 2012]**

Solution : Let H be the subgroup of the group G and e and e' be the identity elements of G and H respectively.

Now if $a \in H$, then $a \in G$ and $ae = a$, because e is the identity element of G.

Again $a \in H$, then $ae' = a$ since e' is the identity element of H.

Thus $ae = ae'$ which gives $e = e'$

Example 3. If H and K are subgroup of G, prove that $H \cup K$ is a subgroup of G if and only if either $H \subseteq K$ or $K \subseteq H$.

[A.U N/D 2014]

Solution : Given H and K are two subgroups of G and $H \subseteq K$ or $K \subseteq H$.

If $H \subseteq K$ then $H \cup K = K$ which is a subgroup of G.

If $K \subseteq H$ then $H \cup K = H$ which is a subgroup of G.

Conversely suppose $K \not\subset H$ and $H \not\subset K$.

Then there exists $a \in H$ and $a \notin K$ and there exists a $b \in K$ and $b \notin H$.

Now $a, b \in H \cup K$. Because $H \cup K$ is a subgroup, it follows that $a * b \in H \cup K$. Hence $a * b \in H$ or $a * b \in K$.

Case (i) : If $a * b \in H$

Then $a^{-1} * (a * b) \in H$

That is $b \in H$ which is a contradiction.

Case (ii) : If $a * b \in K$

Then $a * b * b^{-1} \in K$

i.e., $a \in K$ which is a contradiction.

Thus either $H \subseteq K$ or $K \subseteq H$

Example 4. Prove that the intersection of two subgroups of a group is a subgroup of G. **[A.U M/J 2013, N/D 2013, N/D 2014]**

Solution : Given H and K are subgroups of G.

Let $a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow$ $a * b^{-1} \in H$ and $a * b^{-1} \in K$ (as H and K are subgroups)

$\Rightarrow$ $a * b^{-1} \in H \cap K$.

Thus $H \cap K$ is a subgroup of G.

Example 5. Show that the set of all elements a of a group (G, $*$) such that $a * x = x * a$ for every $x \in G$ is a subgroup of G. **[A.U N/D 2010]**

Solution : Let $H = \{a \in G \mid ax = xa, \forall x \in G\}$

As $ey = ye = y, \forall y \in G, e \in G$, H is non empty.

Let x and z in H

Then $xy = yx$ and $zy = yz$ for all $y \in G$

$$(xz)y = x(yz) \Rightarrow (yx)z = y(xz), \forall y \in G$$

$$\therefore \quad xz \in H, \quad \forall x, z \in H$$

$$x \in H \Leftrightarrow xy = yx, \quad \forall y \in G$$

$$\Leftrightarrow x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1}, \quad \forall y \in G$$

$$\Leftrightarrow (x^{-1}x)(yx^{-1}) = (x^{-1}y)(xx^{-1})$$

$$\Leftrightarrow yx^{-1} = x^{-1}y$$

$$\Leftrightarrow x^{-1} \in H$$

$\therefore$ H is a subgroup.

Example 6. If 'a' is a generator of a cyclic group G, then show that 'a^{-1}' is also a generator of G. **[A.U M/J 2012]**

Solution : Let $G = (a)$ be a cyclic generated by 'a'

If $x \in G$, then $x = a^n$ for some $n \in Z$

$\therefore$ $x = a^n = (a^{-1})^{-n}$, $(-n \in Z)$

$\therefore$ 'a^{-1}' is also a generator of G.

Example 7. Find all the subgroups of (z_9, $+_9$) **[A.U M/J 2014]**

Solution : $Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

The operation is addition modulo 9.

Consider the subsets

$H_1 = \{0, 2, 4, 6, 8\}$

$$H_2 = \{0, 3, 6\}$$
$$H_3 = \{0, 4, 8\}$$
$$H_4 = \{0, 5\}$$

The improper subgroups of $(Z_9, +_9)$ are $[\{0\}, +_9]$ and $[Z_9, +_9]$

$+_9$	0	5
0	0	5
5	5	1

[H_4 is closed]

$+_9$	0	4	8
0	0	4	8
4	4	8	3
8	8	3	7

[H_3 is closed]

$+_9$	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

[H_2 is closed]

$+_9$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	1
4	4	6	8	1	3
6	6	8	1	3	5
8	8	1	3	5	7

[H_1 is closed]

The operation tables shows that
H_1, H_2, H_3 and H_4 are closed for $+_9$

$\therefore$ The possible proper subgroups of $(Z_9, +_9)$ are $(H_1, +_9)$, $(H_2, +_9)$, $(H_3, +_9)$ and $(H_4, +_9)$

Example 8. Any cyclic group of order n is isomorphic to the additive group of residue classes of integers modulo n.

Proof :

Let $G = \{a, a^2, ..., a^n = e\}$ be a cyclic group of order n generated by a.

We know that $(Z_n, +_n)$ is the additive group of residue classes modulo n.