GROUPS :—

A non-empty subset G is called group s.t satisfy 4 axioms.

a) closer axiom.

b) Associative axiom.

c) Identity axiom

d) Inverse axiom.

a) closer axiom :—

If $\forall a, b \in G \Rightarrow ab \in G$.

b) Associative axiom :—

If $\forall a, b, c \in G \Rightarrow (ab)c = a(bc)$

c) Identity axiom :—

There exists an element $e \in G$ such that $ea = ae = a \ \forall a \in G$. where e is the identity elements

d) Inverse axiom :—

For every element $a \in G$, there exist an element $b \in G$ such that $ab = ba = e$.

Then the element b is called inverse of a.

Properties of cyclic group :—

Theorem-1

Every subgroup of a cyclic group is cyclic,

Proof: Suppose G is a cyclic group generated by a.

∴ we can write it as $G = \{a^3\}$.

Let H be a subgroup of G.

i) If $H = G$ there is no need to prove.

(iii) Let H be a proper subgroup of G.

⇒ All the elements of H are integral powers of a

If $a^s \in H \Rightarrow a^{-s} \in H$.

∴ H contains positive as well as negative integral powers of a

Consider a least positive integer n.

Such that $a^k \in H$.

Then our aim is to prove that H is a cyclic group taking a^k as its generator,

Let $a^k \in H$ ------ (1)

(where a^k is the arbitary element)

By division algorithm, there exist integers q and r such that $k = nq + r$ ------ (2)

$0 \leq r < n$.

Groups

$\therefore a^k \in H$.

$\Rightarrow (a^k)^q = a^{kq} \in H$ (By closure axiom).

$\Rightarrow (a^{ab})^{-1} = (a^{-kq} \in H$ ---- 3) (since H is sub group)

From (1) and (2) we get.

$a^k \cdot a^{-aq} \in H$.

(Since H is a sub group)

$\Rightarrow a^{k-aq} \in H$.

⇒ Now n is the least positive integer such that $a^k \in H$.

$\Rightarrow r = 0$

So $k = nq + r = nq + 0 = nq$

$\therefore a^k = a^{kq} = (a^k)^q$

Thus each element are of H are in the form of $(a^m)^q$.

Hence H is a cyclic group and a^k is its generator i.e $H = (a^k)$.

Therefore every subgroup of a cyclic group is cyclic. (Proved)

Theorem-2 :—

Every cyclic group is an abelian group under multiplication.

Proof Let G is a cyclic group generated by the element a of G.

Let x and y are any two elements in G.

Then there exist integers p and r such that $x = a^p$ and $y = a^r$.

For G is to be abelian group we have to show $xy = yx$

$\therefore xy = a^p \cdot a^r = a^{p+r} = a^{r+p} = a^r a^p = yx$.

Since it satisfy commutative property then G is abelian group.

Classification of Subgroups of Cyclic group :—

1) Abelian or Commutative group :—

A non empty set G is said to be an abelian or commutative group if it satisfy all the four axioms of the group and also commutative property.

In other words a group G is said to be abelian or Commutative if is satisfy commutative property.

i.e for any $a, b \in G \Rightarrow ab = ba$ where G is a group.

2) Non-abelian group :—

A group G is said to be non-abelian (or non-commutative) if it does not satisfy commutative property.

For example :—

If G is a group under multiplication and for any a, b ∈ G.

⇒ ab ≠ ba.

3) Order of the group :—

Total number of elements present in a group G is said to be order of a group and denoted by O(G).

For example :—

If G = {a, b, c, d}

Then O(G) = 4, where all the elements of G are not unique.

4) Semi Group :—

A non-empty set G is called a semi group if the binary operation "o" is associative in G.

For example :—

Set of all natural numbers N is a semi group under addition.

5) Symmetric group :—

A group is said to be a symmetric group of degree n if it is a non-abelian group of order n! and denoted by S_n.

6) Finite group :—

If the number of elements in a group G is countable then it is called finite group wise it is infinite group.

Example :—

If G = {$a_1, a_2, a_3, \ldots, a_n$}

then O(G) = n.

Since n is countable then G is called finite group

*) cyclic groups :—

A group G is said to be a cyclic group if for some $a \in G$ every element of the group G is of the form a^n, where n is some integer.

The element a is called a generator of G and denoted by $\langle a \rangle$ or $G(a)$

i.e. $G = \{x \mid x = a^n\}$ The elements of G would be of the form.

$\{ \ldots\ldots a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3 \ldots\ldots \}$

Example :—

The set of all integers is a cyclic group under addition with generator (1) and it is a cyclic group under multiplication having (-1) as its generator.

Permutations :—

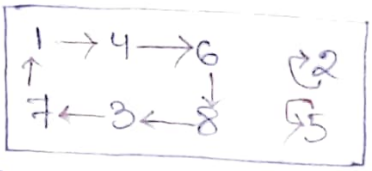


Diagram of a cyclic permutation with two fixed points; a 6-cycle and two 1-cycles.

A permutation is called a cyclic permutation if and only if it has a single non-trivial cycle. (a cycle of length > 1).

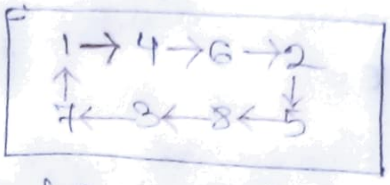
For example, the permutation, written in two-line notation (in two ways) and also cycle notations,

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

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

is a six-cycle; its cycle diagram is shown at right.

Some authors restrict the definition to only those permutations which consist of one non-trivial cycle (that is, one fixed points allowed).



A cyclic permutation with no trivial cycles; an 8 cycle

For example, the permutation :—

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

$$(1\ 4\ 6\ 2\ 5\ 8\ 3\ 7)$$

is a cyclic permutation under this more restrictive definition

Basic properties of permutation :—

One of the basic results on symmetric groups is that any permutation can be expressed as the product of disjoint cycles (more precisely: cycles with disjoint orbits); such cycles commute with each other; and the expression of the permutation is unique up to the order of the cycles. The multi-set of lengths of the cycles in this expression (the cycle type) is therefore uniquely determined by the permutation, and both the signature and the conjugacy class of the permutation in the Symmetric group are determined by it.

The number of k-cycles in the symmetric group S_n is given, for $1 \le k \le n$ by the following equivalent formulas

$$\binom{n}{k}(k-1)! = \frac{n(n-1)\cdots(n-k+1)}{k} = \frac{n!}{(n-k)!\,k}.$$

A k-cycle has signature $(-1)^{k-1}$

The inverse of a cycle $\sigma = (s_0 s_1 \cdots s_{k-1})$ is given by reversing the order of the entries: $\sigma^{-1} = s_{k-1} \cdots s_1 s_0)$ In particular, since $(ab) = (ba)$, every two-cycle is its own inverse. Since disjoint cycles commute, the inverse of a product of disjoint cycles is the result of reversing each of the cycles separately

Even permutation :—

Even permutation is a set of permutations obtained from even number of two element swaps in a set. It is denoted by a permutation symbol of $+1$ .... For Example, for $n = 1, 2, 3, 4, 5, \ldots$, the even permutations possible are 0, 1, 3, 12, 60 and so on ....

Odd permutation :—

It is denoted by a permutation symbol of -1. For a set of n numbers where $n > 2$, there are $n!$ 2 permutation possible. For example, for $n = 1, 2, 3, 4, 5, \ldots$, the odd permutation possible are 0, 1, 3, 12, 60 and so on ...