

→ If  $S \leq G$  then  $S$  is a group in its own.

→ A subset  $S$  of a group  $G$  is a subgroup if and only if  
 $1 \in S$  and  $s, t \in S \Rightarrow st^{-1} \in S$

→ Def:- If  $G$  is a group and  $a \in G$  and the cyclic group generated by  $a$  is denoted as  $\langle a \rangle$  is set of all powers of  $a$   
 $G$  is called cyclic if  $\exists a \in G$  such that  $G = \langle a \rangle$

Order of  $a \in G$ , denoted by  $\text{Ord}(a)$  is  $|\langle a \rangle| = \text{number of elements of } \langle a \rangle$   
 $= \min(m)$  such that  $a^m = 1$  and  $m \in \mathbb{Z}^+$

→  $G$  is a finite group and  $S$  is a non-empty subset of  $G$ . Then  $S$  is a subgroup if and only if  $s, t \in S \Rightarrow st \in S$

→ Definition:-  $f: G \rightarrow H$  is a homomorphism  
 $\text{kernel}(f) = \{a \in G, f(a) = 1\}$   
 $\text{image}(f) = \{h \in H, h = f(a) \text{ for some } a \in G\}$

→  $\text{ker}(f)$  is a subgroup of  $G$  and  $\text{img}(f)$  is a subgroup of  $H$

Theorem:- Intersection of any family of subgroups  $\{H_i\}$  of  $G$  is a subgroup of  $G$ .

Proof:-  $\mathcal{F} = \{H_i : H_i \leq G\} \Rightarrow \bigcap_i H_i$  contains  $1$   
 $a, b \in \bigcap_i H_i \Rightarrow a, b \in H_i \forall i \Rightarrow ab^{-1} \in H_i \forall i \Rightarrow ab^{-1} \in \bigcap_i H_i$   
 So,  $\bigcap_i H_i \leq G$

Corollary:- If  $X$  is a subset of a group  $G$ , then there is a

Corollary:- If  $X$  is a subset of a group  $G$ , then there is a smallest subgroup  $H$  of  $G$  containing  $X$ , i.e., if  $X \subset S$  and  $S \leq G$  then  $H \leq S$

Definition:-  $X$  is non-empty subset of a group  $G$ , then a word on  $X$  is an element  $w \in G$  of the form

$$w = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$$

where  $x_i \in X$  and  $e_i = \pm 1$  and  $n \geq 1$ .  
( $x_i, x_j$  may be same)

Theorem:-  $X$  be a subset of a group  $G$ . If  $X = \emptyset$  then  $\langle X \rangle = 1$  if  $X$  is non-empty, then  $\langle X \rangle$  is set of all words on  $X$

Proof:- If  $X = \emptyset$ ,  
 $X$  generates  $\langle X \rangle \Rightarrow \langle X \rangle = 1$ .

If  $X \neq \emptyset$ ,  
 $W$  be the word of  $X$   
 $1 \in W$  as  $x_i^{-1} x_i \in W$ ,  $x_i^{-1} \in W$ ,  $x_i \in X$   
 $x_i \in W$   $\forall x_i \in X$   
 $\langle X \rangle \subset W$  as  $\langle X \rangle$  is the smallest subgroup.

arbitrarily,  
 $a \in W \Rightarrow a = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$   
 $\Rightarrow x_1^{e_1} \in \langle X \rangle, x_2^{e_2} \in \langle X \rangle, \dots, x_n^{e_n} \in \langle X \rangle$   
 $\Rightarrow a \in \langle X \rangle \Rightarrow W \subset \langle X \rangle$

$$W \subset \langle X \rangle \text{ and } \langle X \rangle \subset W \Rightarrow W = \langle X \rangle$$

Q)  $S$  be a proper subgroup of  $G$ . If  $G-S$  is the complement of  $S$  in  $G$ , then prove that  $\langle G-S \rangle = G$

Ans:-  $x \in \langle G-S \rangle$   $x = g_1^{e_1} g_2^{e_2} \dots g_r^{e_r}$   $g_i \in G$   
 $x \in G$

Ans:-  $x \in \langle G-S \rangle$   $x = \gamma_1 \gamma_2 \dots \gamma_r$   $v$   
 $x \in G$

$x \in (G-S)$  then  $x \in \langle G-S \rangle$

$x \in S$ ,  $\exists \gamma \in (G-S)$  such that  $x\gamma \notin S$ ,  $x\gamma \in (G-S)$   
 $x\gamma \in \langle G-S \rangle$

$\gamma^{-1} \in (G-S)$   $x\gamma\gamma^{-1} \in \langle G-S \rangle \Rightarrow x \in \langle G-S \rangle$

$\langle G-S \rangle \supset S$   $\langle G-S \rangle \supset (G-S)$   
 $\Rightarrow \langle G-S \rangle = G$

Q) Generators of  $S_n$  are what?

Ans:-  $(1,2), (1,3), \dots, (1,n)$   $(r_1, r_2, r_3, \dots, r_n)$   
 $= (r_1, r_n)(r_1, r_{n-1}) \dots (r_1, r_2)$   
 $= (1, r_1)(1, r_n)(1, r_{n-1}) \dots$

Q) Prove that  $S_4$  cannot be generated by  $(1,3)$  and  $(1,2,3,4)$

Ans:-  $(1,2,3,4) = (1,4)(1,3)(1,2); (1,3)$

$(1,2,3,4)^4 = e, (1,3)^2 = e$

$(1,2,3,4)(1,3) = (1,4)(2,3) = (1,3)(4,3,2,1)$   
 $= (1,3)(1,2,3,4)^{-1}$

$\langle (1,3), (1,2,3,4) \rangle = D_4$   $|D_4| = 2 \times 4 = 8$

$|S_4| = 24 = 4!$   $\text{So } \langle (1,3), (1,2,3,4) \rangle \neq S_4$

Q) Let  $G$  be finite group. Prove that the number of elements of  $x$  of  $G$  such that  $x^7 = e$  is odd

Ans:- if  $x \neq e$ ,  $\text{Ord}(x) = 7$  as 7 is a prime

$(x^i)^7 = e \quad \forall 1 \leq i \leq 6$   
 $\dots$  is multiple of 6

11-1

$$(a^i)^7 = e \quad \forall 1 \leq i \leq 6$$

No. of elements of this form is multiple of 6

And we have  $e^7 = e$

So total no. of elements =  $6n+1$  which is odd.