#### Groups-Rings-Fields

#### DR. ODELU VANGA

COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY
CHITTOOR, INDIA

# Groups

Definition: A set G with a binary operation + (addition) is called a commutative group if

```
2,={0,1,2,3,4,5}
(1 \forall a,b \in G, a+b \in G - Chsure)
\begin{array}{c} 2 \ \forall \ a,b,c \in G, \ \underline{(a+b)+c=a+(b+c)}-\text{Associative} \\ 3 \ \exists \ 0 \in G, \ \forall \ \underline{a \in G}, \ \underline{a+0=a}-\text{ Distance for the first } \end{array}
                                                                              +6 - Binary ofer.
                                                                         Ya, & E 26,
 4 \forall a∈G, \exists -a∈G, a+(-a)=0 - Existance of
                                      Ex: Z={0,±1,±2,-} a+6 626.
                                                       inverse
  5. \forall a,b \in G, \underline{a+b=b+a}
        (2,+)-is a group.

L'ammulative

abelieur
                                                                               4 +6 5 = 9 mod 6
                                                 a, 6 EZ
                                                   a+8 EZ
                                                                         N= {1,2,3,---}
                                                70+0=9
                                                    a, 3-a \ 2
                                                                              + (a) \neq N
```

Set of permutation  $S_n$  - Symmetric group.  $S_3, \qquad \{1, 2, 3\},$  $3! = 3 \times 2 \times 1 = 6.$  $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2^{d} \end{pmatrix}$  $\in S_3$ Binary operator  $f\circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ Camposition of megpings.  $(f \circ g)(a) = f(g(x))$ = (3 1 2)  $(5_3,0)$ -group  $T = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} - identity$ permuldon But, not commente

#### **Sub-groups** a group, and $H \subseteq G$ .

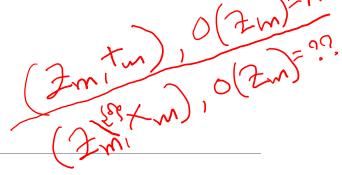
Let (G, +) be a group, (H, +)is a sub-group of (G, +) if it is

**Claim:** Let (G, +) be a finite group, and  $H \subseteq G$ . If H is closed under +, then (H, +) is a sub-group of (G, +).

**Lagrange theorem:** if G is finite and (H, +) is a sub-

group of (G, +) then |H| divides |G|

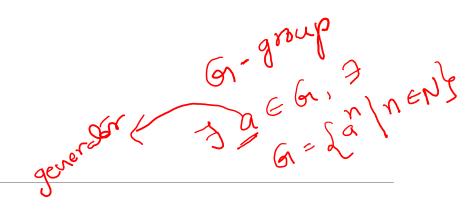
# **Order of Elements**



Let  $a^n$  denote a+...+a (n times). We say that a is of order n if  $a^n = 0$ , and for any m<n,  $a^m \neq 0$ 

Euler theorem: In the multiplicative group of  $Z_m$ , every element is of order at most  $\phi(m)$ .

### Cyclic Groups



Claim: let G be a group and a be an element of order n. The set  $\langle a \rangle = \{1, a, ..., a^{n-1}\}$  is a sub-group of G.

**a** is called the *generator* of <a>

 $O(q)=N \Rightarrow q''=1$ 

If G is generated by a, then G is called cyclic, and a is called a primitive element of G.

**Theorem:** for any prime p, the multiplicative group of  $Z_p$  is cyclic

# Thank you