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

1. $\forall$ a,b$\in$G, a+b$\in$G - Closure
2. $\forall$ a,b,c$\in$G, (a+b)+c=a+(b+c) - Associative
3. $\exists$ 0$\in$G, $\forall$ a$\in$G, a+0=a - Existance identity
4. $\forall$ a$\in$G, $\exists$ -a$\in$G, a+(-a)=0 - Existance of inverse
5. $\forall$ a,b$\in$G, a+b=b+a

$(\mathbb{Z}, +)$ - is a group.
Commutative
abelian

Ex: $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
$a, b \in \mathbb{Z}$
$a+b \in \mathbb{Z}$.
$0+a=a$
$a, \exists -a \in \mathbb{Z}$
$+1 \quad -1$

$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$
$+_6$ - Binary oper.
$\forall a, b \in \mathbb{Z}_6,$
$a +_6 b \in \mathbb{Z}_6.$
$4 +_6 5 = 9 \bmod 6$
$= 3$

$N = \{1, 2, 3, \ldots\}$
$+ \quad (-a) \notin N$
$0 \notin N.$

Set of permutation S_n - Symmetric group.

S_3, $\{1, 2, 3\}$, $n!$

$3! = 3 \times 2 \times 1 = 6.$

$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3$

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

Binary operator composition of mappings.

$g \circ f \neq$

$(2\ 3\ 1)$

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

$f(g(1))$

$f(1)$

$(f \circ g)(x) = f(g(x))$

$= (3\ 1\ 2)$

$(S_3, \circ)$ - group

$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ - identity permutation

But, not commutative.

Sub-groups

Let $(G, +)$ be a group, $(H,+)$ is a sub-group of $(G,+)$ if it is a group, and $H \subseteq G$.

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|

$O(G) = |G|$

$\mathbb{Z}_m$ - abelian group under $+_m$

$G = \mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}, +_{10}$

$H \subseteq G,$

$O(H) \mid O(G)$

$\{0, 1, 3, 4\}$ $1 +_{10} 4 = 5$ Not closed

$H = \{0, 2, 4, 6, 8\}$ - closure wrt $+_{10}$.

Order of Elements

$(\mathbb{Z}_m, +_m)$, $o(\mathbb{Z}_m) = m$

$(\mathbb{Z}_m \setminus \{0\}, \times_m)$, $o(\mathbb{Z}_m) = ??$,

Let a^n denote $a+\ldots+a$ (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 $\phi(m)$.

$o(5) = ?$

$5^1 = 5$

$5^2 = 5 +_{10} 5 = 10 = 0$

$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}, +_{10}$

$n = 1, 2, \ldots$

$2,\ 2^2 = 2 +_{10} 2 = 4$

$2^3 = 2 +_{10} 2 +_{10} 2 = 6$

$2^4 = 2 +_{10} 2 +_{10} 2 +_{10} 2 = 8$

$2^5 = 2 +_{10} 2 +_{10} 2 +_{10} 2 +_{10} 2 = 10 = 0$

$\boxed{o(2) = 5}$

Cyclic Groups

G - group

$\exists\, a \in G$, $\exists$

generator

$G = \{a^n \mid n \in N\}$

Claim: let G be a group and a be an element of order n. The set <a>={1, a,…,a^{n-1}} is a sub-group of G.

$(Z_{10}, +_{10})$, $o(2)=5$

a is called the *generator* of <a>

$o(a)=n \Rightarrow a^n = 1$

$\{2^n \mid n \in N\}$

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

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

$\{2^1, 2^2, 2^3, 2^4, 2^5 =$

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

Thank you