1500 series

CS & IT ENGINEERING

Discrete Mathematics

Lecture No.- 06

By- Satish Yadav Sir

Recap of Previous Lecture

Topic: Recurrence Relation

Topics to be Covered

Topic

Group Theory

[redacted]

Q

s1. $\{10n \mid n \in Z\}$ under addition

s2. $\{a/2^n. \mid a, n \in Z, n \geq 0\}$ under addition

Group:

closed.

Associative

identity.

Inverse.

$\boxed{\text{commutative.}}$

(N. Abel)

(1802 – 1829)

(a) only S1 is Group

(b) only S2 is Group

(c) Both S1 and S2 are Group

(d) Both S1 and S2 are not Group

$\frac{a}{2^n}$ $a, n \in \mathbb{Z}$

1) $\frac{a}{2^x} \in G$ $\frac{b}{2^y} \in G$ $\frac{a}{2^x} + \frac{b}{2^y} \in G$

$a, x \in \mathbb{Z}$ $b, y \in \mathbb{Z}$

2) $\frac{a}{2^x} + \left(\frac{b}{2^y} + \frac{c}{2^z}\right) = \left(\frac{a}{2^x} + \frac{b}{2^y}\right) + \frac{c}{2^z}$

$\left(\frac{3}{2^2} + \frac{4}{2^3}\right) + \frac{5}{2^4} = \frac{3}{2^2} + \left(\frac{4}{2^3} + \frac{5}{2^4}\right)$

$\frac{25}{2^4}$ $\frac{25}{2^4}$

$\frac{3}{2^2}$ $\frac{4}{2^3}$

$\frac{2\times}{2\times}\frac{3}{2^2} + \frac{4}{2^3}$

$\frac{6}{2^3} + \frac{4}{2^3}$

$\frac{10}{2^3} \in G$ $10 \in \mathbb{Z}$ $3 \in \mathbb{Z}$

3) $\frac{a}{2^n} + 0 = \frac{a}{2^n}$ (0 is identity)

4) $\frac{a}{2^n} + \left(\frac{-a}{2^n}\right) = 0$

$\frac{a}{2^b} + \frac{c}{2^d} = \frac{c}{2^d} + \frac{a}{2^b}$

$\underbrace{\frac{3}{2^2} + \frac{4}{2^3}} = \underbrace{\frac{4}{2^3} + \frac{3}{2^2}}$

$\frac{10}{2^3} = \frac{10}{2^3}$

S_1. $\left(\{ 2^n \mid n \in \mathbb{Z} \}, \times \right)$

abelian Group?

Yes ✓

$a \in \mathbb{Z}$.

$2^a \in G$

$2^b \in G$.

$b \in \mathbb{Z}$.

$2^a \times 2^b$

$2^{a+b} \in G$.

$a+b \in \mathbb{Z}$.

Symmetric diff. $(\Delta / \oplus)$

S_2. $(P(A), \Delta)$

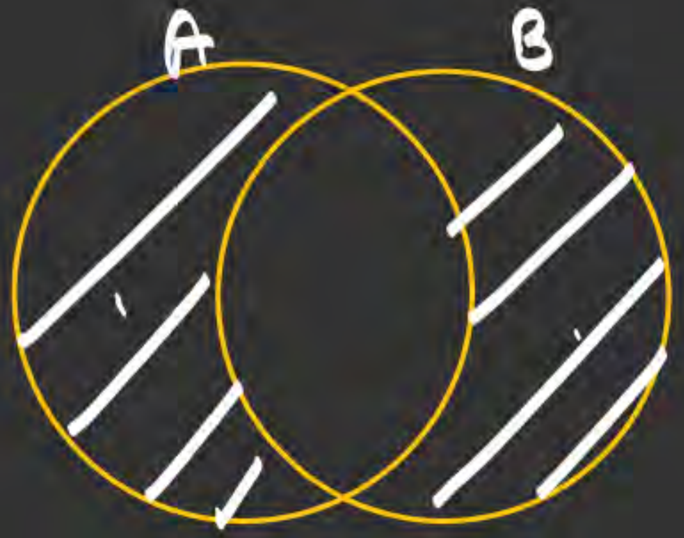
$A = \{a, b, c\}$

→ abelian Group?

$A = \{1, 2, 3\}$.

(set, operation)

$(P(A), \Delta)$



$B \Delta A = A \Delta B = \underline{\underline{(A \cup B) - (A \cap B)}}$

$= (A - B) \cup (B - A)$

1) **closed**:

$A \in P(A)$ $\quad$ $A \Delta B \in P(A)$

$B \in P(B)$

2) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

3) $A \Delta \phi = A$.

4) $A \Delta A = \phi$

1) Closed $a \in G,\ b \in G \quad a * b \in G.$

2) Associative

$$a*(b*c) = (a*b)*c.$$

3) identity: $a * e = a = e * a.$

4) Inverse. $a * a^{-1} = e = a^{-1} * a.$

(Set, operation)

$\downarrow$

G

$\{10n \mid n \in \mathbb{Z}\}$

$(10(-2),\ 10(-3),\ \ldots\ 10(0)\ \ldots\ 10(1),$

1) $10a \in G$. $10b \in G$.

$a \in \mathbb{Z}$ $b \in \mathbb{Z}$

$10a + 10b \in G$.

$10(a+b) \in G$.

$a+b \in \mathbb{Z}$.

$e = 0$

4) $10(a) + 10(-a) = 0$

$a \in \mathbb{Z}$. $-a \in \mathbb{Z}$.

3) $10(a) + 0 = 10(a)$

$10(a) + 10(0) = 10(a)$

Q

S1 :the binary operation (o) on Z by $x \circ y = x + y + 1$. that $(Z, \circ)$ is an abelian group.

S2: Let $G = \{q \in Q \mid q \neq -1\}$. Define the binary operation o on G by $x \circ y = x + y + xy$. $(G, \circ)$ is an abelian group.

(a) only S1 is valid
(b) only S2 is valid
(c) Both S1 and S2 are valid
(d) Both S1 and S2 are invalid

$x \circ y = x + y + 1$

1) Closed.

2) Asso

3) identity.

$a * e = a$

$a + e + 1 = a.$

$e = -1.$

4) Inverse.

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

$a + a^{-1} + 1 = -1$

$a^{-1} = -2 - a.$

$x \circ y = x + y + xy.$

1) C

2) A

3) Identity.

$a * e = a.$

$\cancel{a} + e + ae = \cancel{a}.$

$e(1+a) = 0$

$e = 0$

4) Inverse.

$a * a^{-1} = e.$

$a + a^{-1} + a \cdot a^{-1} = 0$

$a^{-1} + a \cdot a^{-1} = -a.$

$a^{-1}(1+a) = -a.$

$a^{-1} = \dfrac{-a}{1+a}$

$(a \neq -1)$

$a * e = a$ $a * a^{-1} = e.$

Q

S1: G is abelian if and only if $(ab)^2 = a^2b^2$ for all a, b €

S2: If G is a group, for all a, b € G,

a) $(a^{-1})^{-1} = a$ (True)

b) $(ab)^{-1} = b^{-1} \cdot a^{-1}$ (T)

S3: group G is abelian if and only if for all a, b ∈ G, $(ab)^{-1} = a^{-1}\, b^{-1}$ ✓

$(ab)^2$

$(ab)(ab)$

$a\,b\,a\,b$

$a\,a\,b\,b$

$a^2 b^2$

$ba = ab$

abelian Group

$(ab)^{-1} = b^{-1} \cdot a^{-1}$

$= a^{-1} \cdot b^{-1}$

Group:

$(ab)^{-1} = \boxed{b^{-1} \cdot a^{-1}}$ ✓

y

$(ab) \cdot y = e$

$(ab) \cdot (b^{-1} \cdot a^{-1}) = e$

$a \cdot b \cdot b^{-1} \cdot a^{-1}$

$\downarrow$

$a \cdot e \cdot a^{-1}$

$\downarrow$

$a \cdot a^{-1} = e$

$a^{-1} = x$

$a \cdot a^{-1} = e$

$a \cdot x = e$

Group.

$(ab)^{-1} = a^{-1} \cdot b^{-1}$

$(G, \circ)$ Group.

where.

$$x \circ a \circ y = b \circ a \circ c \rightarrow x \circ y = b \circ c$$

Check $(G, \circ)$ is abelian Group.

Q

(T)

S1: If H, K are subgroups of a group G, that $H \cap K$ is also a subgroup of G.

S2: If H, K are subgroups of a group G, that $H \cup K$ is also a subgroup of G.

(a) only S1 is valid ✓

(b) only S2 is valid

(c) Both S1 and S2 are valid

(d) Both S1 and S2 are invalid

$$\begin{array}{c|ccc} \oplus_6 & 0 & \cdots & 5 \\ \hline 0 & & & \\ \vdots & & & \\ 5 & & & \end{array}$$

$H = \{0, 3\}$ $K = \{0, 2, 4\}$.

$H \cup K = \{0, 2, 3, 4\}$

which is not closed.

not a Group

not a subgroup.

$H \cap K = \{0\}$

Q

S1: If G is a finite group and $a \in G$, then $O(a)$ divides $|G|$.

$|G| = p$

S2: Every group of prime order is cyclic..

Generator.

$O(x) = p$

...r of Group: no. of elements in the group.

Order of a = $O(a)$

= no. of elements generated by a during exponent.

(a) only S1 is valid

(b) only S2 is valid

(c) Both S1 and S2 are valid

(d) Both S1 and S2 are invalid

	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

$2^1 = 2$

$2^2 = 4$

$2^3 = 0$

$\langle 2 \rangle = \{0, 2, 4\}$ H

$\frac{|G|}{|H|}$

$O(2) = 3.$

$3^1 = 3$

$3^2 = 0$

$\langle 3 \rangle = \{0, 3\}$

Q

(H/W)

S1: Let p be a prime. If G has order 2p, then every proper subgroup of G is cyclic

S2:Let H and K be subgroups of a group G, where e is the identity of G. if $|H| = 10$ and $|K| = 21$, then $H \cap K = \{e\}$.

(a) only S1 is valid
(b) only S2 is valid
(c) Both S1 and S2 are valid
(d) Both S1 and S2 are invalid

practice:

Question → ✓
↳ X. → new concept ✓
old concept (Revision)

practice.
(180°)

$\boxed{\text{3 hrs.}}$
↓
patience.

a) $\{-1, 1\}$ under multiplication

b) $\{-1, 1\}$ under addition

c) $\{-1, 0, 1\}$ under addition

d) $\{10n | n \in \mathbf{Z}\}$ under addition

e) The set of all one-to-one functions $g: A \to A$, where $A = \{1, 2, 3, 4\}$, under function composition

f) $\{a/2^n | a, n \in \mathbf{Z}, n \geq 0\}$ under addition

(a) Yes. The identity is 1 and each element is its own inverse.
(b) No. The set is not closed under addition and there is no identity.
(c) No. The set is not closed under addition.
(d) Yes. The identity is 0; the inverse of $10n$ is $10(-n)$ or $-10n$.
(e) Yes. The identity is 1_A and the inverse of $g : A \to A$ is $g^{-1} : A \to A$.
(f) Yes. The identity is 0; the inverse of $a/(2^n)$ is $(-a)/(2^n)$.

4. Let $G = \{q \in \mathbf{Q} | q \neq -1\}$. Define the binary operation $\circ$ on G by $x \circ y = x + y + xy$. Prove that $(G, \circ)$ is an abelian group.

5. Define the binary operation $\circ$ on $\mathbf{Z}$ by $x \circ y = x + y + 1$. Verify that $(\mathbf{Z}, \circ)$ is an abelian group.

(i) For all $a, b, c \in G$,
$(a \circ b) \circ c = (a + b + ab) \circ c = a + b + ab + c + (a + b + ab)c = a + b + ab + c + ac + bc + abc$
$a \circ (b \circ c) = a \circ (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + bc + ab + ac + abc.$
Since $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in G$ it follows that the (closed) binary operation is associative.
(ii) If $x, y \in G$, then $x \circ y = x + y + xy = y + x + yx = y \circ x$, so the (closed) binary operation is also commutative.
(iii) Can we find $a \in G$ so that $x = x \circ a$ for all $x \in G$?
$x = x \circ a \Longrightarrow x = x + a + xa \Longrightarrow 0 = a(1 + x) \Longrightarrow a = 0$, because x is arbitrary, so 0 is the identity for this (closed) binary operation.
(iv) For $x \in G$, can we find $y \in G$ with $x \circ y = 0$? Here $0 = x \circ y = x + y + xy \Longrightarrow -x = y(1 + x) \Longrightarrow y = -x(1 + x)^{-1}$, so the inverse of x is $-x(1 + x)^{-1}$.
It follows from (i) - (iv) that $(G, \circ)$ is an abelian group.

Since $x, y \in \mathbf{Z} \Longrightarrow x + y + 1 \in \mathbf{Z}$, the operation is a (closed) binary operation (or $\mathbf{Z}$ is closed under $\circ$). For all $w, x, y \in \mathbf{Z}$, $w \circ (x \circ y) = w \circ (x + y + 1) = w + (x + y + 1) + 1 = (w + x + 1) + y + 1 = (w \circ x) \circ y$, so the (closed) binary operation is associative. Furthermore, $x \circ y = x + y + 1 = y + x + 1 = y \circ x$, for all $x, y \in \mathbf{Z}$, so $\circ$ is also commutative. If $x \in \mathbf{Z}$ then $x \circ (-1) = x + (-1) + 1 = x [= (-1) \circ x]$, so -1 is the identity element for $\circ$. And finally, for each $x \in \mathbf{Z}$, we have $-x-2 \in \mathbf{Z}$ and $x \circ (-x-2) = x + (-x-2) + 1 = -1 [= (-x-2) + x]$, so $-x-2$ is the inverse for x under $\circ$. Consequently, $(\mathbf{Z}, \circ)$ is an abelian group.

8. For any group G prove that G is abelian if and only if $(ab)^2 = a^2b^2$ for all $a, b \in G$.

9. If G is a group, prove that for all $a, b \in G$,

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

10. Prove that a group G is abelian if and only if for all $a, b \in G$, $(ab)^{-1} = a^{-1}b^{-1}$.

8. Proof: Suppose that G is abelian and that $a, b \in G$. Then $(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2$, by using the associative property for a group and the fact that this group is abelian.
Conversely, suppose that G is a group where $(ab)^2 = a^2b^2$ for all $a, b \in G$. If $x, y \in G$, then $(xy)^2 = x^2y^2 \Rightarrow (xy)(xy) = x^2y^2 \Rightarrow x(yx)y = x(xy^2) \Rightarrow (yx)y = xy^2$ (by Theorem 16.1 (c)) $\Rightarrow (yx)y = (xy)y \Rightarrow yx = xy$ (by Theorem 16.1 (d)). Therefore, the group G is abelian.

9. (a) The result follows from Theorem 16.1(b) since both $(a^{-1})^{-1}$ and a are inverses of a^{-1}.
(b) $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(e)b = b^{-1}b = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(e)a^{-1} = aa^{-1} = e$. So $b^{-1}a^{-1}$ is an inverse of ab, and by Theorem 16.1(b), $(ab)^{-1} = b^{-1}a^{-1}$.

10. G abelian $\Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$. By Exercise 9(b), $b^{-1}a^{-1} = (ab)^{-1}$, so G abelian $\Longrightarrow a^{-1}b^{-1} = (ab)^{-1}$. Conversely, if $a, b \in G$, then $a^{-1}b^{-1} = (ab)^{-1} \Longrightarrow a^{-1}b^{-1} = b^{-1}a^{-1} \Longrightarrow ba^{-1}b^{-1} = a^{-1} \Longrightarrow ba^{-1} = a^{-1}b \Longrightarrow b = a^{-1}ba \Longrightarrow ab = ba \Longrightarrow G$ is abelian.

5. Let G be a group with subgroups H and K. If $|G| = 660$, $|K| = 66$, and $K \subset H \subset G$, what are the possible values for $|H|$?

From Lagrange's Theorem we know that $|K| = 66 (= 2 \cdot 3 \cdot 11)$ divides $|H|$ and that $|H|$ divides $|G| = 660 (= 2^2 \cdot 3 \cdot 5 \cdot 11)$. Consequently, since $K \neq H$ and $H \neq G$, it follows that $|H|$ is $2(2 \cdot 3 \cdot 11) = 132$ or $5(2 \cdot 3 \cdot 11) = 330$.

11. Let H and K be subgroups of a group G, where e is the identity of G.

a) Prove that if $|H| = 10$ and $|K| = 21$, then $H \cap K = \{e\}$.

(a) Let $x \in H \cap K$. $x \in H \Longrightarrow o(x) | 10 \Longrightarrow o(x) = 1, 2, 5$, or 10. $x \in K \Longrightarrow o(x) | 21 \Longrightarrow o(x) = 1, 3, 7$, or 21. Hence $o(x) = 1$ and $x = e$.

THANK YOU