3RD SEM MTMH GROUP THEORY UNIT-1

LECTURE NOTE #3

10/9/2020
S. Chakraborty.

Finite Groups:

A group $(G, \circ)$ is said to be a finite group if G contains a finite number of elements; i.e., if $O(G)$ is finite, OR, $|G|$ is finite.

Examples:

① Let $S = \{z \in \mathbb{C} : z^3 = 1\}$. So, $S = \{1, \omega, \omega^2\}$, where $\omega^3 = 1$. $(S, \cdot)$ forms an abelian group.

② Let $S = \{z \in \mathbb{C} : z^4 = 1\}$. So, $S = \{1, i, -1, -i\}$; $i^4 = 1$. $(S, \cdot)$ forms an abelian group.

③ Let $S = \{z \in \mathbb{C} : z^n = 1\}$, the set of n distinct nth roots of Unity. $(S, \cdot)$ forms an abelian group $\longrightarrow$ show it.

(i) Let $z_1, z_2 \in S$. Then $z_1^n = 1 = z_2^n \Rightarrow (z_1 \cdot z_2)^n = z_1^n \cdot z_2^n = 1$.
$\Rightarrow S$ is closed w.r.t. multiplication $(\cdot)$.

(ii) Multiplication is associative on the set $\mathbb{C}$, and $S \subseteq \mathbb{C}$, it is so on S also.

(iii) $1 \in S$, as in S, $z^n = 1 \Rightarrow z^n = \cos 2k\pi + i \sin 2k\pi$
$\Rightarrow z = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}$; $k = 1, 2, \cdots, n$.
So, for $k = n$, we have $z = 1 \in S$.
1 is the identity element, since $1 \cdot z = z \cdot 1 = z, \forall z \in S$.

(iv) Let $\alpha = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, for $k = 1$. Then $S = \{\alpha, \alpha^2, \cdots, \alpha^{n-1}, (\alpha^n = 1)\}$. $O(S) = n$, (finite).
Let us take $\alpha^p \in S$, for $p \in \{1, 2, \cdots, n\}$
$\therefore \alpha^p = \cos\frac{2\pi p}{n} + i \sin\frac{2\pi p}{n}$.
Inverse of α^p is given by $\frac{1}{\alpha^p} = \alpha^{-p} = \cos\frac{2\pi p}{n} - i \sin\frac{2\pi p}{n}$

$\alpha^{-p} = \cos\frac{2\pi p}{n} - i \sin\frac{2\pi p}{n} = \cos\left[\frac{2\pi(n-p)}{n}\right] + i \sin\left[\frac{2\pi(n-p)}{n}\right]$.

$\Rightarrow \alpha^{-p} = \alpha^{n-p}$; because $\alpha^{n-p} \in S$. $\forall p \in \{1, 2, \cdots, n\}$.

$\alpha^{n-p} = \cos\left(2\pi - \frac{2\pi p}{n}\right) + i \sin\left(2\pi - \frac{2\pi p}{n}\right)$
$= \cos\frac{2\pi p}{n} - i \sin\frac{2\pi p}{n}$
$= \alpha^{-p}$

$\therefore$ Inverses of all elements of S exist.
$\therefore (S, \cdot)$ forms a group. And it is an abelian group, as commutative property holds.

④ Z_n is the set of the classes of residues of integers modulo n ($n \in Z^+$).

(i) Z_n forms an abelian group w.r.t. the binary composition 'addition modulo n' $\oplus_n$.
i.e; $(Z_n, \oplus_n)$ is an abelian group; where $Z_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$, $o(Z_n) = n$, finite.

(ii) BUT, Z_n does not form a group w.r.t. the binary composition 'multiplication modulo n' $\odot_n$. Because $\bar{0} (\in Z_n)$ has no inverse.

(iii) Let us take the set as $Z_n - \{\bar{0}\}$ and the b.c. defined on it as $\odot_n$.
Then, $(Z_n - \{\bar{0}\}, \odot_n)$ forms a group when n is prime.
But " does not form " " n is composite.
Beause, when n is composite, let us take $p, q \in Z^+$ s.t. $p.q = n$. Then $\bar{p}, \bar{q} \in Z_n - \{\bar{0}\}$, and $\bar{p} \odot_n \bar{q} = \overline{pq} = \bar{0} \notin Z_n - \{\bar{0}\}$. $\Rightarrow Z_n - \{\bar{0}\}$ is not closed w.r.t. the b.c. $\odot_n$.

Composition Table:

When G is a non-empty finite set, a b.c. o on the set G can be defined by the composition table: if the order of G is n, the table has n rows and n columns, one for each element of G. The table has n^2 entries which are all elements of G. If $G = \{a_1, a_2, \cdots, a_n\}$, then $a_i \circ a_j$ appears on the table in the ith row & jth column where the elements of G are listed on the topmost row and the leftmost column in the same order.

NOTE: In every row/column of the composition table, each element of G appears exactly once.
Let us consider the ith row and its entries are: $a_i \circ a_1, a_i \circ a_2, \cdots, a_i \circ a_n$, all $\in G$. No two of these are equal. Because, if so, then $a_i \circ a_r = a_i \circ a_s \Rightarrow a_r = a_s$ (Cancellation law) which is not possible. Similar arguments for columns hold. $(r, s = 1, 2, \cdots, n)$

Application of the Composition Table:

We can use the composition table in order to prove whether a given non-empty set and a b.c. defined on it constitutes a group and an abelian group.

Examples:

① Let $S = \{1, i, -1, -i\}$. The composition table for the b.c. 'multiplication, $\cdot$' on S is:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

(i) All the entries of the table $\in S$. So S is closed w.r.t. '$\cdot$'.

(ii) Multiplication is associative on $\mathbb{C}$ and $S \subseteq \mathbb{C}$, so is on S also.

(iii) The 1st row and the 1st column contain the elements of S in the same order as the topmost row & leftmost column. And the intersection element is 1, which determines the identity element.

(iv) To find out the inverses of all elements, first locate the identity element in each row. Then find out the rule of its composed elements.

eg, inverse of 1 is 1
" " i is $-i$
" " -1 " -1
" " $-i$ " i .

(v) Mark the principal diagonal in order to examine the commutative property. If the table be symmetric about the principal diagonal i.e., if $a_i \circ a_j = a_j \circ a_i$, then the group is abelian.

Here $(S, \cdot)$ forms an abelian group.

② $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\oplus_5$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Use similar arguments as in ① you see that $(Z_5, \oplus_5)$ forms an abelian group.

REMARKS: See here in every row/column each element appears exactly once.

Exercises-9 (S.K. Mapa).

(8) The following table defines a b.c. $*$ on the set $S = \{a, b, c\}$. Examine if $(S, *)$ is a group.

$*$	a	b	c
a	a	b	c
b	b	a	c
c	c	a	b

(3rd column)

No, $(S, *)$ is not a group.
Because, $O(S)$ is finite and in the composition table (given) the 3rd column contains the element c twice, which is not possible for a finite group.

(9) A b.c. $*$ is defined on the set $S = \{a, b, c\}$ s.t. $a*a = b*b = c*c = c$. Can you complete the composition table in order that $(S, *)$ may be a group?

$*$	a	b	c
a	c	b	a
b	a	c	b
c	a	b	c

So, $(S, *)$ does not form a group.

Since $c*c = c \Rightarrow c$ is the identity.
$\therefore a*c = c*a = a$, $b*c = c*b = b$.
For a finite group, since in every row/column of the composition table, each element appears exactly once, we ~~take~~ consider first row and we write $a*b = b$
& then 2nd row, " $b*a = a$.
Then we consider the first column where 'a' appears twice & in the 2nd column, 'b' " " .
which is not possible for a finite group.

(10) Complete the following composition table for the set $S = \{a, b, c\}$ so that $(S, *)$ may be a group.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

a is the identity element.
$b*b$ = either a or c
if $b*b = a$, then $c*b = b$, not possible because then b is an identity.
So, $b*b = c$, then $c*b = a$,
and $b*c = a$, and $c*c = b$.

$\therefore (S, *)$ forms a group.

B. Sc. MTMH 3RD SEM ** GROUP THEORY UNIT-1.

Lecture Note # 4. 24/09/2020

GROUP U_n: The set of all units in the monoid $(Z_n, \odot_n)$ forms an abelian group w.r.t. multiplication (mod n), $\odot_n$. This is known as group U_n.

We have the set Z_n forms a commutative monoid w.r.t. $\odot_n$.

But $(Z_n, \odot_n)$ does not form a group since $\bar{0}$ has no inverse [$\nexists\, \bar{a} \in Z_n$ s.t. $\bar{a}.\bar{0} = \bar{1}$ (identity)].

To find the necessary and sufficient condition for the existence of a unit in the monoid $(Z_n, \odot_n)$.

Let $\bar{u} \in Z_n$ be a unit. Then $\exists\, \bar{v} \in Z_n$ s.t.

$\bar{u} \odot_n \bar{v} = \bar{1} \Rightarrow uv - 1 = kn \Rightarrow uv - kn = 1$

$\Rightarrow \gcd(u, n) = 1$, for $v, k \in \mathbb{Z}$.

↑ necessary condition.

For sufficient condition, let $\gcd(u,n) = 1$, $(u < n)$.

Then $\exists\, p, q \in \mathbb{Z}$ s.t. $up + nq = 1$

$\Rightarrow up - 1 = -nq$

$\Rightarrow up \equiv 1 \pmod n \longrightarrow$ (i)

$\Rightarrow p$ is not multiple of n. Therefore,

let us take $p \equiv r \pmod n$, $0 < r < n$ so that $\bar{r} \in Z_n$

$\Rightarrow up \equiv ur \pmod n \longrightarrow$ (ii)

(i) & (ii) $\Rightarrow ur \equiv 1 \pmod n \Rightarrow \bar{u} \odot_n \bar{r} = \bar{1}$

So, we get $\bar{u} \odot_n \bar{r} = \bar{r} \odot_n \bar{u} = \bar{1}$ [$\because (Z_n, \odot_n)$ is a commutative monoid]

$\Rightarrow \bar{u}$ is a unit.

Therefore,

$\bar{u} \in Z_n$ is a unit in the monoid $(Z_n, \odot_n)$ if and only if $u < n$ and $\gcd(u, n) = 1$.

We define: $U_n = \{\bar{u} \in Z_n : \gcd(u,n) = 1\}$.

To prove: $(U_n, \odot_n)$ forms an abelian group.

(i) Let $\bar{u}, \bar{v} \in U_n$. Then $\gcd(u,n)=1$, $\gcd(v,n)=1$
$\Rightarrow \gcd(uv, n) = 1$
$\Rightarrow \bar{u} \odot \bar{v}$ is a unit.
$\Rightarrow \bar{u} \odot \bar{v} \in U_n$. [closure Prop.].

(ii) $\odot$ is associative on Z_n and $U_n \subseteq Z_n$, so $\odot$ " " on U_n.

(iii) $\bar{1} \in U_n$ and $\bar{1} \odot \bar{u} = \bar{u} \odot \bar{1} = \bar{u}$, $\forall\, \bar{u} \in U_n$.
$\Rightarrow \bar{1}$ is the identity element in $(U_n, \odot)$.

(iv) For each $\bar{u} \in U_n$, $\exists\, \bar{v} \in U_n$ s.t.
$\bar{u} \odot \bar{v} = \bar{v} \odot \bar{u} = \bar{1}$ [$\because \odot$ is commutative on Z_n].
$\Rightarrow \bar{v}$ is the inverse of $\bar{u}$.

(v) Also $\odot$ is commutative on U_n, hence $(U_n, \odot)$ forms an abelian group.

To find: Order of the group U_n.

Let us denote $\phi(n)$ = {the number of integers less than n and prime to n.
Euler-Phi function

Then $O(U_n) = \phi(n)$, where $n \geq 2$, and $\phi(1) = 1$.

eg:

$$O(U_8) = \phi(8) = 4 \;;\; O(U_{10}) = \phi(10) = 4 \;;$$
$$O(U_{11}) = \phi(11) = 10 \;;\; O(U_7) = \phi(7) = 6.$$

$U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$; $U_{10} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

$U_{11} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}\}$; $U_7 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.

Note: If n be prime, $U_n = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{n-1}\}$;
$\therefore O(U_n) = \phi(n) = n-1$, if n be prime.