4th. sem (General)

course name → Algebra.
code → BMG4CC1D

Finite Groups:- A group (G, o) is said to be a finite group if G contains a finite number of elements.

The order of a finite group (G, o) is the number of elements of G. The order of the group G is denoted by $o(G)$ or by $|G|$.

Some examples of groups:-

(1) Let $S = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$. Then S is an abelian group with respect to multiplication.

The composition table for the set is

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(i) It appears from the table that the set S is closed under multiplication.

(ii) multiplication is associative on $\mathbb{C}$ and S is a subset of $\mathbb{C}$, therefore multiplication is associative on S.

(iii) It appears from the row of 1 in the table that 1 is the left identity. Also from the column of 1 in the table that 1 is the left

Scanned with CamScanner

identity element. Therefore 1 is the identity element.

(iv) The inverse of 1 is 1, inverse of ω is ω^2, the inverse of ω^2 is ω.

∴ inverse of each element of S exists in S.

(v) The table is symmetric about the principal diagonal. Therefore multiplication is commutative on S.

Hence $(S, \cdot)$ is an abelian group.

HW Let $S = \{1, i, -1, -i\}$ where $i^4 = 1$. check wheather $(S, \cdot)$ is abelian group or not.

(2) Let $S = \{z \in \mathbb{C} : z^n = 1\}$. S is the set of n distinct nth roots of unity. Then $(S, \cdot)$ is an abelian group.

($\mathbb{C}$ being the set of complex numbers)

proof: (i) Let $z_1, z_2 \in S$. Then $z_1^n = 1$ and $z_2^n = 1$ clearly $(z_1 \cdot z_2)^n = z_1^n \cdot z_2^n = 1$ and this implies that $z_1 \cdot z_2 \in S$. So, S is closed under multiplication.

(ii) multiplication is associative on the set $\mathbb{C}$ and S is a subset of $\mathbb{C}$. So, multiplication is associative on the set S.

iii) clearly $1 \in S$ and $1 \cdot z = z \cdot 1 = z \quad \forall z \in S$.

Scanned with CamScanner

Therefore 1 is the identity element of S.

iv) Let $z \in S$, then $z^n = 1$

now $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$, so $\frac{1}{z} \in S$. and

$z \cdot \frac{1}{z} = \frac{1}{z} \cdot z = 1 \quad \forall\ z \in S$.

so, $\frac{1}{z}$ is the inverse of z in S.

v) clearly multiplication is commutative on the set $\mathbb{C}$ and S is a subset of $\mathbb{C}$. Therefore multiplication is commutative on S.

Hence $(S, \cdot)$ is an abelian group.

(3) The set Z_3, the classes of residues of integers modulo 3, forms an abelian group with respect to $+$, addition.

The elements of Z_3 are $\bar{0}, \bar{1}, \bar{2}$. The composition table is

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

(i) It appears from the table that the set is closed under '+'.

(ii) '+' is associative.

(iii) It appears from the table that $\bar{0}$ is a

Scanned with CamScanner

left identity element as well as right identity. Therefore $\bar{0}$ is the identity element.

iv) The inverse of $\bar{0}$ is $\bar{0}$, inverse of $\bar{1}$ is $\bar{2}$, the inverse $\bar{2}$ is $\bar{1}$. Therefore the inverse of each element belongs to the set.

v) The table is symmetric about the principal diagonal. Therefore '+' is commutative.

Hence $(Z_3, +)$ is an abelian group.

** Group U_n

Let us consider the S of all units (i.e, elements $\bar{u}$ satisfying $\gcd(u,n)=1$) in the monoid $(Z_n, \cdot)$ (where $n>1$). We prove that the set S forms a commutative group under multiplication (mod n).

Proof: i) Let $\bar{u}, \bar{v} \in S$, then u is prime to n and v is prime to n. This implies uv is prime to n and therefore $\bar{u}\cdot\bar{v} \in S$. This shows that the set S is closed under multiplication (mod n).

ii) multiplication (mod n) is associative on the set Z_n. S being a subset of Z_n, multiplication (mod n) is associative on the set S.

iii) $\bar{1} \in S$ and $\bar{1}\cdot\bar{u} = \bar{u}\cdot\bar{1} = \bar{u}$ for all $\bar{u} \in S$. So, 1 is the identity element.

Scanned with CamScanner

iv) Let $\bar{u} \in S$. Then $\bar{u}$ is a unit of the monoid $(Z_n, \cdot)$. So there exists an element $\bar{v} \in Z_n$ such that $\bar{u} \cdot \bar{v} = \bar{v} \cdot \bar{u} = \bar{1}$. This shows that $\bar{v}$ is a unit of Z_n. So, $\bar{v} \in S$ and $\bar{v}$ is the inverse of $\bar{u}$.

v) multiplication (mod n) is commutative on the set Z_n. S being a subset of Z_n, multiplication (mod n) is commutative on the set S.

Therefore the set S forms a commutative group under multiplication (mod n). This group is denoted by U_n. $U_n = \{ \bar{u} : g.c.d(u, n) = 1 \}$.

For example:- $U_4 = \{ \bar{1}, \bar{3} \}$; $U_{10} = \{ \bar{1}, \bar{3}, \bar{7}, \bar{9} \}$ etc.

Now check yourself $(U_{10}, \cdot)$ is a commutative group.

** Klein's 4-group

Let $S = \{e, a, b, c\}$ and let '$\circ$' be the binary composition defined on S by $e \circ a = a \circ e = a$; $e \circ b = b \circ e = b$; $e \circ c = c \circ e = c$; $e \circ e = a \circ a = b \circ b = c \circ c = e$ $a \circ b = b \circ a = c$; $a \circ c = c \circ a = b$; $b \circ c = c \circ b = a$.

Now the composition table is given below —

Scanned with CamScanner

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

principal diagonal

~~clearly $(S, \circ)$ is an abelian group~~

(i) clearly it appears from the table that S is closed under the composition '$\circ$'.

(ii) clearly '$\circ$' is associative since

$(a \circ b) \circ c = c \circ c = e$

and $a \circ (b \circ c) = a \circ a = e$. $\therefore (a \circ b) \circ c = a \circ (b \circ c)$

$\forall a, b, c \in S$.

~~similarly for~~

(iii) clearly e being identity element here.

(iv) each element being its own inverse here.

(v) The composition table is symmetric about the ~~prin~~ principal diagonal, therefore '$\circ$' is abelian.

So, $(S, \circ)$ is an abelian group (of order 4)

It is called Klein's 4-group and denoted by V.

Note:- An important property of the group is that every element of the group V is its own inverse.

Scanned with CamScanner