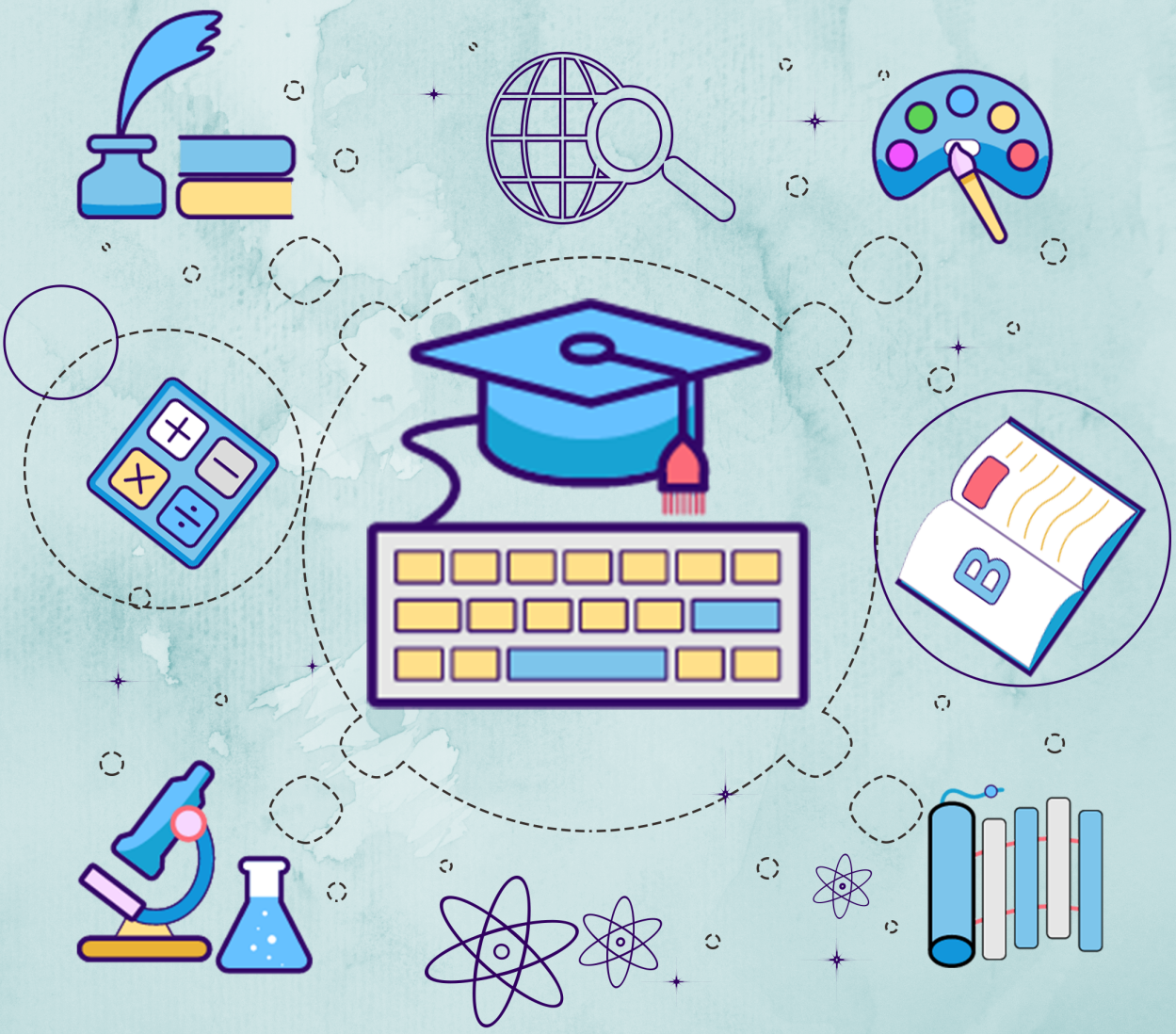
APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

KeralaNotes



SYLLABUS | STUDY MATERIALS | TEXTBOOK

PDF | SOLVED QUESTION PAPERS

www.keralanotes.com

KeralaNotes

KTU STUDY MATERIALS

DISCRETE MATHEMATICAL STRUCTURES

MAT 203

Module 5

Related Link :

- KTU S3 STUDY MATERIALS
- KTU S3 NOTES
- KTU S3 SYLLABUS
- KTU S3 TEXTBOOK PDF
- KTU S3 PREVIOUS YEAR SOLVED QUESTION PAPER

Module -5

Algebraic Structures

Syllabus

Algebraic system - properties - Homomorphism and Isomorphism. Semi group and monoid - cyclic monoid, sub semi group and sub monoid, Homomorphism and isomorphism of semi group and monoid group - Elementary properties - sub groups, symmetric group of three symbol, The direct product of two group, Group Homomorphism, Isomorphism of groups, cyclic group, Right cosets - Left Cosets, Lagrange's Theorem

Definition (*Group*)

If G is a nonempty set and $*$ is a binary operation on G, then $(G,*)$ is called a group if the following condition are satisfied

1) For all $a, b \in G$, $a * b \in G$. That is G is closed under the operation $*$
2) For all a, b and $c \in G$, $(a * b) * c = a * (b * c)$. (Associative property)
3) There exist $e \in G$ with $a * e = e * a = a$ for all $a \in G$.(existence of identity)
4) For each element $a \in G$ there is an element $b \in G$ such that $a * b = b * a = e$ (existence of inverse)
5) Furthermore if $a * b = b * a$ for all$a, b \in G$. Then $(G,*)$ is called a commutative or abelian group

Eg. $G = \mathbb{Z}$ $+$ $\mathbb{Z}$ → Integers

$(\mathbb{Z}, +)$

1) when we add two integers result will be also integers ∴ $\mathbb{Z}$ is closed under operator $+$

$x, y \in \mathbb{Z} \quad x+y \in \mathbb{Z}$

2) $(x+y)+z = x+(y+z)$

$\forall\ x, y, z \in \mathbb{Z}$

3) $0 \in \mathbb{Z}$ $\quad 0+x = x+0 = x$ $\quad$ e → Identity element

4) $\forall\ x \in \mathbb{Z}\ \exists\ -x \in \mathbb{Z}$

$x + (-x) = 0$

∴ $\mathbb{Z}$ is a Groupoid under operation

5) $a, b \in \mathbb{Z}$

$\forall\ x, y \in \mathbb{Z}$

$x+y = y+x$

∴ $\mathbb{Z}$ is a abelian group

Eg | $G = \{-1, 1, 0\}$ +

$(G, +)$.

1) $1 + -1 = 0$

$1 + 0 = 1$

$-1 + 0 = 1$) not in the set

$1 + 1 = 2$

∴ No group

Eg:

1) $G = \{-1, 1\}$ • - multiplication

$-1 \times 1 = -1$ ∴ The $A = \{-1, 1\}$

$1 \times -1 = -1$

$-1 \times -1 = 1$ $(A, \cdot)$

$1 \times 1 = 1$

2) Satisfy associative property

3) $e = 1$ $1 \cdot 1 = 1$

$a * e = e * a = a$

4) $-1 \cdot 1 =$ (* satisfy

condition

1. $(\mathbb{Z}, +)$ → Group, Abelian group

2. $(\mathbb{R}, +)$

1) $\mathbb{R}$ is closed under the operation +

let $x, y \in \mathbb{R}$

$x + y \in \mathbb{R}$

2) Let $x, y, z \in \mathbb{R}$

$(x + y) + z = x + (y + z)$

3) Since $0 \in \mathbb{R}$, such that

$x + 0 = 0 + x = x \quad \forall x \in \mathbb{R}$

$\therefore$ 0 act as identity element in $\mathbb{R}$

There exist

4) $x \in \mathbb{R} \quad \exists \; -x \in \mathbb{R}$

$x + (-x) = 0$ [identity element]

5) $x + y = y + x \quad \forall x, y \in \mathbb{R}$

$(\mathbb{R}, +)$ → Group, Abelian Group

rational numbers

3. $(\mathbb{Q}, +)$

1) $x, y \in \mathbb{Q}$

$x + y \in \mathbb{Q}$

$\mathbb{Q}$ is closed under the operation +

2) $(x * y)$

$x, y, z \in Q$

$(x+y)+z = x+(x+y)$

3) $x * 0 = 0 + x = x$

0 act as a identity element in Q $x \in Q$

4) $x \in Q \;\;] \;\; -x \in Q$

$x + (-x) = 0$

5) $x, y \in Q$

$x + y = y + x$

$\therefore (Q, +) \rightarrow$ Group. Abelian group

4. $\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ $a_{ij} \in z$

generally

$M_{2\times 2}(z)$

$\begin{bmatrix} 1 & -1 \\ 2 & 2 \end{bmatrix}$ $\begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$ $n \times n$ matrix element should be a real number

$M_{2\times 2}(z)$ $M_{3\times 3}[z]$

$M_{n\times n}(\mathbb{R})$

4. $\left(M_{2\times 2}(\mathbb{Z}) \quad + \right)$

(i) Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$.

$$A + B = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix}$$

($a_{11} + b_{11}$: integer, integer)

$$A + B \in M_{2\times 2}(\mathbb{Z})$$

$M_{2\times 2}(\mathbb{Z})$ is closed under the operator $+$.

(ii) Let $a, b, A, B, C \in M_{2\times 2}(\mathbb{Z})$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \quad C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

$$(A + B) + C = A + (B + C)$$

$$\begin{bmatrix} a_{11} + b_{11} + c_{11} & a_{12} + b_{12} + c_{12} \\ a_{21} + b_{21} + c_{21} & a_{22} + b_{22} + c_{22} \end{bmatrix} =$$

$$\begin{bmatrix} a_{11} + b_{11} + c_{11} & a_{12} + b_{21} + c_{12} \\ a_{21} + b_{21} + c_{21} & a_{22} + b_{22} + c_{22} \end{bmatrix}$$

(iii) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M_{2\times 2}(\mathbb{Z})$

Let $A \in M_{2\times 2}(\mathbb{Z})$ $\quad A \neq 0$

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$0 + A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

identity element

$$A + e = \underline{e} + A = A$$

$$\forall\ A \in M_{2\times 2}(\mathbb{Z})$$

(iv) $\forall\ A \in M_{2\times 2}(\mathbb{Z})\ \exists\ B \in M_{2\times 2}(\mathbb{Z})$

$$\exists\ A + B = 0$$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \qquad B = \begin{bmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{bmatrix}$$

$B \in M_{2\times 2}(\mathbb{Z})$ $\qquad A + B = 0$

$$B + A = 0$$

$\therefore (M_{2\times 2}(\mathbb{Z}), +)$ Form a group

(v) Let $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \qquad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$

$$A + B = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

$$\begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{bmatrix} =$$

$$\begin{bmatrix} b_{11}+a_{11} & b_{12}+a_{12} \\ b_{21}+a_{21} & b_{22}+a_{22} \end{bmatrix}$$

$$= \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

$$= B + A$$

$$A + B = B + A$$

$$\forall\ A, B \in M_{2\times 2}(\mathbb{Z}) \quad A + B = B + A$$

$(M_{2\times 2}(\mathbb{Z}),\ +)$ → Group

→ Abelian group

5. $G = (\{1, -1\}, \cdot)$

$i = \sqrt{-1}$

$i^2 = -1$

6. $G = (\{1, -1, i, -i\}, \cdot)$

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

$i \times -i$

$= 1$

$i \times i = -1$

(i) closed

(ii) $x, y, z \in \{1, -1, -i, i\}$

$(x+y)+z = x+(y+z)$

(iii) ~~$x+0 = 0+x$~~ $x \cdot 1 = 1 \cdot x = x$

⇓

Here identity element = 1

$\because 1+0 = 0+1 = 1$

(iv) when we add any number with x we should get 1 so we can say its inverse

$1 + x = 1$

$x = 1$

inverse

$-1 + x = 1$

$x = -1$

$i \cdot x = 1$

$x = -i$

$-i \cdot x = 1$

$x = i$

$(i)^{-1} = -i$

$(-i)^{-1} = i$

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

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

(v) $a+b = b+a$ transpose

$\Rightarrow A^T = A$

Addition modulo 2

$Z_2 = \{0, 1\}$ $+_2$

$Z_3 = \{0, 1, 2\}$ $+_3$

$Z_4 = \{0, 1, 2, 3\}$ $+_4$

$Z_5 = \{0, 1, 2, 3, 4\}$ $+_5$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ $+_6$

$Z_n = \{0, 1, 2, 3, 4, 5 \ldots (n-1)\}$ $+_n$

Group, Abelian group

$+_2 \Rightarrow$ $0+0=0$

$0+1=1$

$1+1=0$

$1+1+1=1$

$1+1+1+1=0$

$+_2$	0	1
0	0	1
1	1	0

$1+2=3=0$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$2+2=4-3=1$

$0+x=0$ when we add 0 with any number we must get 0 so we can say as it inverse

0 => Identity element

$a^{-1}=b$

$b^{-1}=a$

$0^{-1}=0$

$1^{-1}=2$ (when taking inverse, where zero exist it will be its)

Semi Group $(G, *)$

conditions:

→ G is closed under the operation *

→ Let $a, b, c \in G$

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

Natural Numbers

Eg: $(\mathbb{N}, +)$

1. $\mathbb{N}$ is closed under operation +

2. Let $a, b, c \in \mathbb{N}$

$$(a+b)+c = a+(b+c)$$

3. $A + e = e + A = A$
   $0 + x = x + 0 = 0$

but 0 is not Natural Numbers

∴ It is Not a group

It is Semi-Group

inverse $a + 0 = a$

since it has no idententity element NO inverse

Monoid $(G, *)$

conditions

→ G is closed under the operation $*$

→ Let $a, b, c \in G$ [Associativity]

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

→ $a * e = e * a = a$ [identity element]

whole numbers [Natural + {0}]

Eg: $(W, +)$

1. W is closed under operation +

2. Let $a, b, c \in N$

$(a + b) + c = a + (b + c)$

3. $A + e = e + A = A$

~~$0 + x = x + 0 = 0$~~

$a + e = e + a = a$ 0 identity element

$1 + 0 = 0 + 1 = a = 1$

4. 1 exist but -1 not exist

Not inverse

∴ It is Not a group

∴ It is a monoid

Sub group

$H \subseteq G$

$(H *)$ $(G *)$

→ closed ✓
→ Associativity ✓
→ Identity ✓
→ inverse ✓

Eg: $Z_4 = (\{0,1,2,3\} +_4)$

$(Z_4, +_4)$

$H = \{0, 2\}$

$(H, +_4)$

$+_4$	0	2
0	0	2
2	2	0

↓

Group

∴ H is form a subgroup for $(Z_4, +_4)$

Eg: $Z_6 = (\{0,1,2,3,4,5\} +_6)$

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

→ closed ✓
→ Associativity ✓
→ Identity ✓
→ inverse ✓

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$4+4 = 8 - 6 = 2$

Sub Semigroup

Let $(S, *)$ be a semigroup and $T \subseteq S$ then $(T, *)$ is said to be a subgroup of $(S, *)$ if T is closed under the operation $*$

$T \subseteq S$

→ closed
→ Associativity

Eg: $(z^+, +)$ — set of +ve integers

$(N, +)$ — $(N, +)$ is a sub semi group of $(z^+, +)$

$(0, +)$ — Not sub semi group

$0 \subseteq z^+$ — subset of odd integers

$0 = \{1, 3, 5, \ldots\}$

$1 + 3 = 4 \notin 0$

Sub monoid

Let $(M, *, e)$ be a monoid and $T \subseteq M$. Then $(T, *, e)$ is known as submonoid of $(M, *, e)$ if T is closed under the operation $*$ & add the identity $e \in T$

monoid → closed
→ Assoc..
→ Identity element

Eg: $(Z^+ + 0)$ → monoid $M = Z^+ \cup \{0\}$

$(M + 0)$ sub monoid

$(N +)$ 0 Not submonoid

since 0 is not Natural number

Theorem

imp

prove that the set of idopotent element of M for any abelian monoid $(M *)$ form a submonoid

commutative statisfies

$\forall\ a, b \in G \quad a * b = b * a$

$(M, *, e) \quad \forall\ a, b \in M$

$a * b = b * a$

$a \in M$ is called idopotent element if

$a * a = a$

we have to prove

$(T * e)$

$e \in T$

$(M * e)$

$(M * e)$ $T \subseteq M$

$(T * e)$ → closed
→ Asso
→ ident

$T = \{a, b, c \cdots\}$

$a * a = a$
$b * b = b$ } idopotent
$c * c = c$

$a, b, c \ldots$

$e * e = e \quad \therefore e \subseteq T$

we have to check is it closed

$a, b \in T \quad a * b \in T$

$a * a = a$

$b * b = b$

to prove $a, b \in T$

we have to prove this $\boxed{(a * b) * (a * b) = a * b}$

$(a * b) * (a * b) = (a * b) * (b * a)$ [M is abelian]

$= a * (b * b) * a$ [M is Associative]

$= a * b * a$ [b idopotent element $b * b = b$]

$= a * b$ a " $a * a = a$

$(a * b) * (a * b) = a * b$

$\Rightarrow a * b$ is idopotent element

$\therefore a * b \in T$ ie if $a, b \subseteq T$

$a * b \subseteq T$

$\Rightarrow T$ is closed

$\Rightarrow e \in T$

Cyclic group

$$Z_3 = (\{0,1,2\}, +_3)$$

$1 \Rightarrow 1+1 = 2$

$1+1+1 = 3 = 0 \quad [3-3=0]$

$1+1+1+1 = 4 = 1 \quad [4-3=1]$

$\{0,1,2\}$

In this case we can generate all elemen of that set with a single element

→ Generator → (1), Here 1 is generator

[an element which can generate remaing element]

Then it is known as cyclic group if generator exist

0

$0+0=0$

$0+0+0=0$

0 is not generator

2

$2+2 = 1 \quad [4-3]$

$2+2+2 = 0 \quad [6-3-3-3=0]$

2 is a generator

IMP Q

Page 219

prove that every cyclic monoid is an abelian monoid

let us assume $(M * e)$ is a cyclic monoid

we need to prove $(M * e)$ is a abelian monoid

$$x * y = y * x \quad \forall x, y \in M$$

LHS

$x * y = a^n * a^m$ for some a, n

let take 'a' as generating element

$a^n = x$

$a^m = y$

$= \underbrace{a * a * a * \cdots}_{n} \; \underbrace{a * a * a * \cdots}_{m}$

$= a^{n+m}$

$= a^{m+n}$

$= a^m . a^n = y * x = RHS$

$\forall x, y \in M$

∴ This forms a abelian monoid

Theorem

For every Group G,

a) The identity elements of G is unique

b) The inverse of each element of a is unique

c) If $a, b, c \in G$ and $ab = ac$, then $b = c$ [left cancellation property]

d) If $a, b, c \in G$ and $ba = ca$ then $b = c$ [right cancellation property]

G e_1, e_2 $e_1 = e_2$

---

a) **case I** e_1 is an identity element in G

$$e_1 * e_2 = e_2 = e_2 * e_1$$

$a * e = e * a = a$

case II

e_2 is an identity element in G

$$e_2 * e_1 = e_1 = e_1 * e_2 = e_2$$

$$e_1 = e_2$$

$\therefore$ Identity element unique

b) $a \in G$ b, c are inverse of a

$a * b = e = b * a$

$a * c = e = c * a$

b inverse of a

c "

$a * b = e = b * a$

$a * c = e = c * a$

$(a * c = e)$

$b = b * e$

$= b * a * c$

$b * a = e$

$= b * a * c$

$= a e * c$

$= a c$ since e is an idententy element

∴ Inverse element of G is unique

c) $a, b, c \in G$ $ab = ac$ $\boxed{b = c}$

$a * b = a * c$ $a^{-1} \in G$

$\times a^{-1}$

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

[Associative]

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

$e * b = e * c$

$b = c$

d) $a, b, c \in G$ $ba = ca$ $\boxed{b = c}$

$b * a = c * a$ $a^{-1} \in G$

$\times a^{-1}$

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

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

$b * (a \times a^{-1}) = c * (a \times a^{-1})$

$b * e = c * e$

$b = c$ //

P 234

IMP Q show that any group G is abelian if and only if $(ab)^2 = a^2b^2 \quad \forall\ a, b \in G$

Assume G is abelian

we need to prove $\boxed{(ab)^2 = a^2b^2 \quad \forall\ a, b \in G}$

$ab = a * b$

LHS : $(ab)^2 = (a*b)^2$

$= (a*b)*(a*b)$ since G is abelian

$= \cancel{(a*b)*(b*a)}$

$= a*(b*a)*b$ Associative

$b*a = a*b$ commute

$= a*(a*b)*b$

$= (a*a)*(b*b)$ Associative

$= a^2 * b^2$

$= a^2b^2$

-> closed
-> associ
-> inver
-> Ident
-> comm

Suppose that $(ab)^2 = a^2b^2 \quad \forall\ a, b \in G$

we have to prove that G is abelian

$a*b = b*a \quad \forall\ a, b \in G$

$(ab)^2 = a^2b^2$

$(a*b)*(a*b) = (a*a)*(b*b)$

it is inverse so there exist a^{-1} and b^{-1}

~~LHS × a^{-1}, RHS × b^{-1}~~ × - left side, side b^{-1}
LHS & RHS

$a^{-1} * (a * b) * (a * b) \times b^{-1}$

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

$e * b * a * e = e * a * a * b * e$

↓

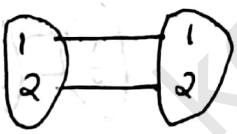
- e identity element
so when we multiply with any element we get same element

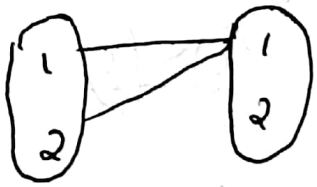
$b * a = a * b \quad \forall\, a, b \in G$

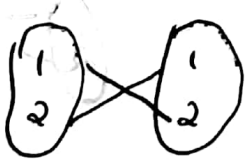
∴ Group G is abelian if and only if

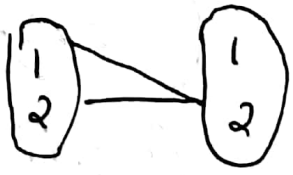
$(ab)^2 = a^2 b^2$ for all $a, b \in G$ P=237

Q $A = \{1, 2\}$

$f_1 =$ 

$f_3 =$ 

$f_2 =$ 

$f_4 =$ 

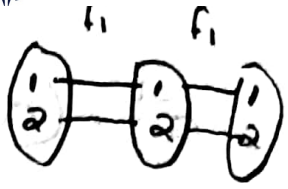
$G = (\{f_1, f_2, f_3, f_4\}, \circ)$ composition

$f: A \to B \quad g: B \to C$ $(G, \circ)$

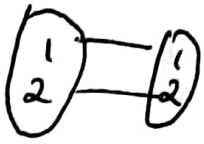
$g \circ f = A \to C$

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_3	f_3	f_3
f_4	f_4	f_4	f_4	f_4

$f_1 \circ f_1$

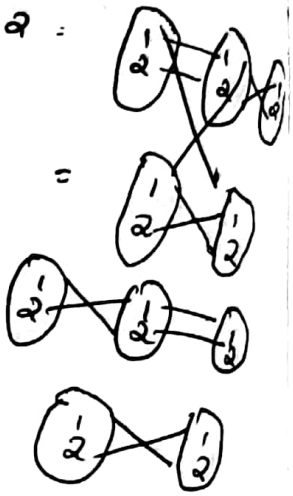


$=$

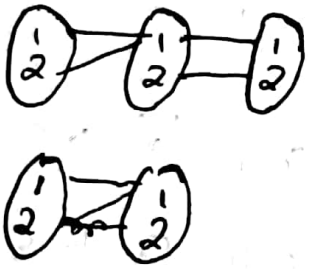


$= f_1$

$f_1 \circ f_2$:

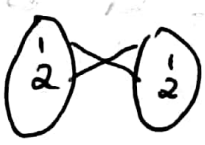


$f_1 \circ f_3 =$



$f_2 \circ f_1$

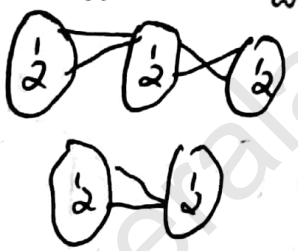
$=$



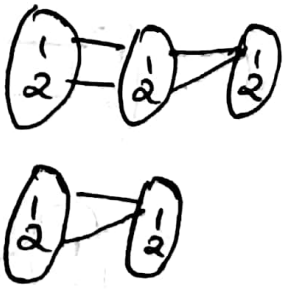
f_2

$f_2 \circ f_3$

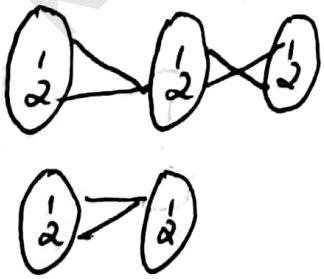
First we have to work f_3



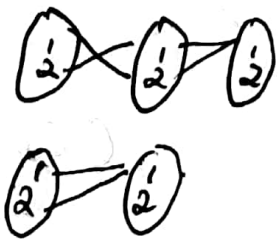
$f_3 \circ f_1$



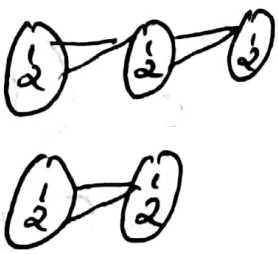
$f_2 \circ f_4$



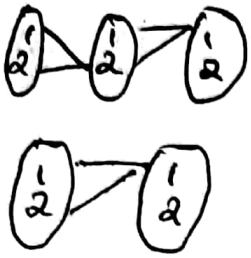
$f_3 \circ f_2$



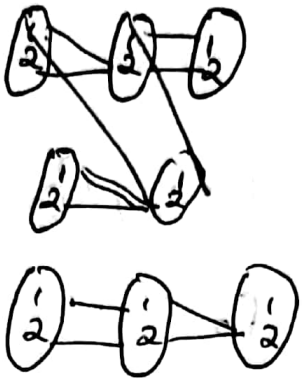
$f_3 \circ f_3$



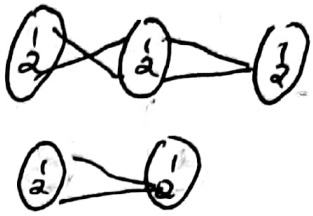
$f_3 \circ f_4$



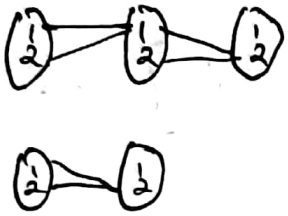
$f_4 \circ f_1$



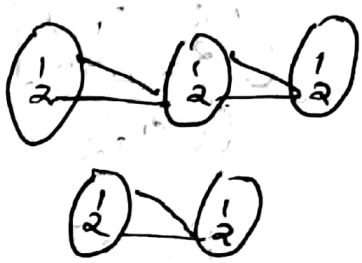
$f_4 \circ f_2$



$F_4 \circ f_3$

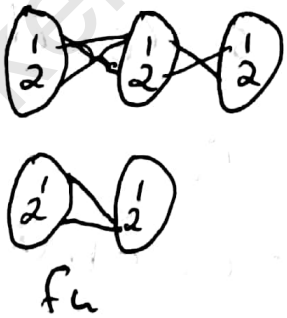


$F_4 \circ f_4$

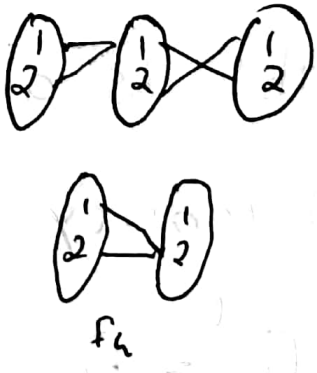


→ It is not a group since 3rd and 4th row are not distinct

→ $f_1 \circ (f_2 \circ f_3) = f_1 \circ (f_2 \circ f_3)$



f_4



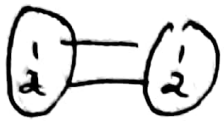
f_4

$f_1 \circ f_4 = f_1 \circ f_4$ ∴ Associativity

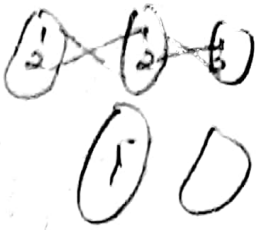
P: 218.

2 let S_2 be the set of all permutation on

$A = \{1, 2\}$

$f_1 =$ 

$F_2 =$ 



By using matrix method

o	f_1	f_2
f_1	f_1	f_2
f_2	F_2	$F_2 f_1$

$f_1 \circ f_2$

$\begin{bmatrix}1&2\\2&1\end{bmatrix}\begin{bmatrix}1&2\\1&2\end{bmatrix}$

$= \begin{bmatrix}1&2\\1&2\end{bmatrix}$

$f_1 \circ f_2$

$\begin{bmatrix}1&2\\2&1\end{bmatrix}\begin{bmatrix}1&2\\1&2\end{bmatrix}$

$\begin{bmatrix}1&2\\2&1\end{bmatrix} = f_2$

$f_2 \circ f_1$

$\begin{bmatrix}1&2\\2&1\end{bmatrix}\begin{bmatrix}1&2\\1&2\end{bmatrix}$

$\begin{bmatrix}1&2\\2&1\end{bmatrix}$

$f_2 \circ f_1$

$\begin{bmatrix}1&2\\2&1\end{bmatrix}\begin{bmatrix}1&2\\2&1\end{bmatrix}$

$\begin{bmatrix}1&2\\2&1\end{bmatrix}\begin{bmatrix}1&2\\1&2\end{bmatrix}$

→ This is a group since it an distinct

→ Identity element f_1

→ $f_1^{-1} = f_1$

$F_2^{-1} = F_2$

→ Associativity

→ Abelian group

∴ S_2 is set of all permutation is abelian group

$S_2 = \{1, 2\}$

$S_3 = \{1, 2, 3\}$ → permutation

Homomorphism and Isomorphism of a Groups

If (G, o) and $(H, *)$ are groups and $f: G \to H$, then f is called a group homomorphism. if for all $a, b \in G$

$$f(a \circ b) = f(a) * f(b)$$

or

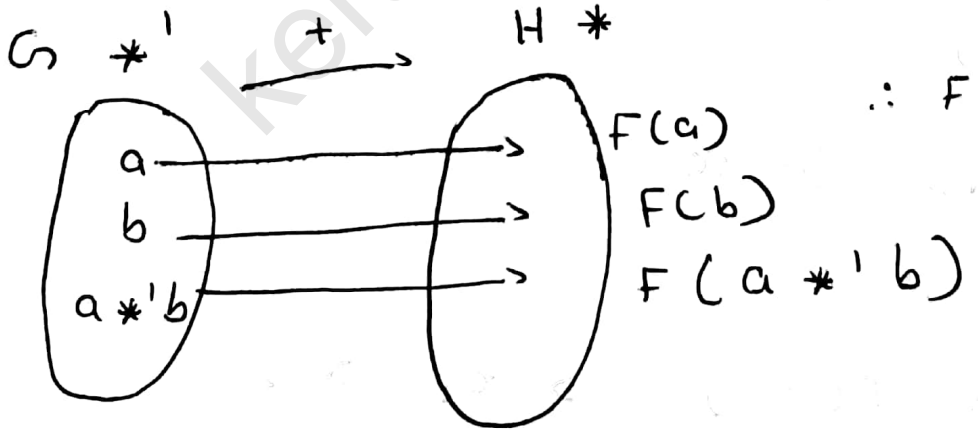
$$f(a *' b) = f(a) * f(b)$$

$(G, *')$ $(H, *)$

$f: G \to H$

$a, b \in G \Rightarrow a *' b$ also $\in G$

$$f(a *' b) = f(a) * f(b)$$



$\therefore F(a) * F(b)$ exist in $H *$

~~if f(x)~~

if $\boxed{F(a) * f(b) = f(a *' b)}$

↓

Homomorphism

Bijection (one-one, onto)

↓

Isomorphism denoted by $\cong$

Q prove that $(R^+, \cdot)$ (+ve real no) isomorphic to $(R, +)$

$(R^+, \cdot)$ $(R, +)$

both are groups.

$f: R^+ \longrightarrow R$

$\rightarrow f(a \cdot b) = f(a) + f(b)$ $\forall a, b \in R^+$

$\rightarrow$ one-one

$\rightarrow$ onto

If we can prove this then we can say that $(R^+, \cdot)$ isomorphic to $(R, +)$

$f(x) = \ln x$

<u>one-one</u>

$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\ln x_1 = \ln x_2$

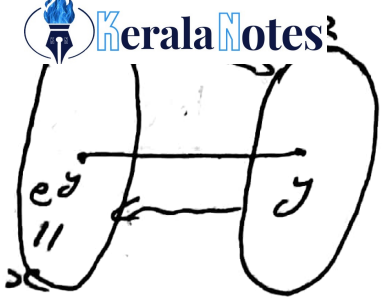
$e^{\ln x_1} = e^{\ln x_2}$

$x_1 = x_2$ $\therefore f(x)$ is one-one

onto

let $y \in \mathbb{R}$

$e^y > 0$



$e^0 = 1 > 0$

$e^1 = e > 0$

$e^{-1} = \frac{1}{2} > 0$

$f(x) = \ln x$

$f(x) = f(e^y)$

$= \ln e^y$

$= y$

$f(x_1) = x_2$

$f(xy) = f(x)f(y)$

$= \ln(xy)$

$= \ln x + \ln y$

$= f(x) + f(y)$

$\therefore$ f is homomorphic and one-one, onto

$\therefore$ It is isomorphic

$\therefore (\mathbb{R}^+, \cdot)$, $(\mathbb{R}, +)$ are isomorphic

Q Ex 5.39 ($p = 247$)

$G = (\{1, -1, i, -i\}, *)$

$Z_4 = (0, 1, 2, 3)\ +_4$

prove isomorphism

$(G, *) \cong (Z_4, +_4)$

$\cong$ isomorphism

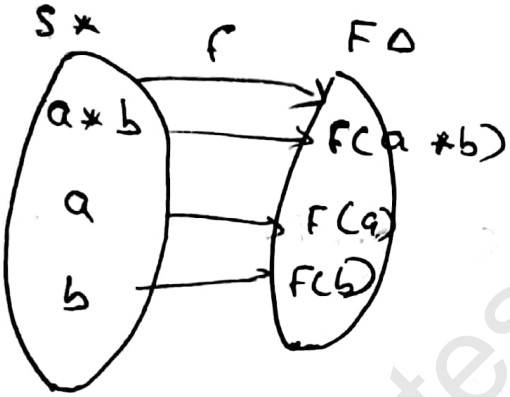
Homomorphism and Isomorphism of Semi group

P = 224

$(S, *)$ (T, Δ)

$f : S \to T$

$\forall (a, b) \in S \quad f(a * b) = f(a) \Delta f(b)$



$F(a) \Delta F(b) = f(a * b)$

f- homomorphism + one-one

↓

f is homomorphism + "

monomorphism

f homomorphism + onto

↓

epimorphism

f homomorphism + one-one + onto

↓

Isomorphism

consider two semigroup $(Z^+, +)$ and $(Z^+, \cdot)$

Ex: 5.17

$f: Z^+ \longrightarrow Z^+$

$F(a,b) = F(a) \cdot F(b)$ -> If it satisfy it is homomorphism

$f(x) = 2^x$

$F(a+b) = 2^{a+b}$

$= 2^a \cdot 2^b$

$= F(a) \cdot F(b)$

$\therefore F(a+b) = F(a) \cdot F(b) \quad \forall \; a, b \in Z^+$

$\therefore$ F is homomorphism

Eg: Define two monoid sel $(N, +, 0)$ $(N, \cdot, 1)$

P = 227
Ex: 5.1

$F(x) = 3^x$

Theorem

IMP

Every subgroup of a cyclic group is cyclic

$(Z_3, +_3)$

$Z_3 = \{0, 1, 2\}$

$\langle 1 \rangle = \{1, 1^2, 1^3, 1^4 \ldots\}$

Generators of $\langle 2 \rangle$

1	2
$1+1=2$	$2+2=1$
$1+1+1=0$	$2+2+2=0$
$1+1+1+1=1$	

1 is generator 2 is also generator

$\langle 1 \rangle = \langle 2 \rangle = Z_3$

$\therefore Z_3$ is a cyclic group

$(G, *)$ a cyclic group $H \subseteq G$

$(H, *)$ - sub group

-> we need to prove this subgroup is also cyclic

let $(G, *)$ be a cyclic group

let $a \in G$ be a generator of G

$\langle a \rangle = G$

let $(H, *)$ be the subgroup of $(G, *)$

$H \subseteq G$ — subset

If $H = \{e\}$ — trivial group

identity element

It is also a group

$(H, *)$ is a subgroup

if $H \neq \{e\}$

$H = \{x_1, x_2, x_3 \cdots\}$

$H \subseteq G \Rightarrow x_1, x_2, x_3 \cdots \in G$ — Also

Since G is a cyclic we can generate elements

$x_1 = a^{n_1}$

$x_2 = a^{n_2}$

$\vdots$

$x_n = a^{n_n}$

$a^b \in H$

$b = \min\{n_1, n_2, n_3 \cdots\}$

$= a^b$

$\subseteq \boxed{\langle a^b \rangle = H}$ we need to prove

$\langle a^b \rangle \subseteq H$ - (1)

$H \subseteq \langle a^b \rangle$ - (2)

$A = B$

$A \subseteq B$

$B \subseteq A$

$a^b \in H$

Also

$a^b * a^b \in H$

$a^t * a^t * a^t \in H$ $\quad t=3 \quad s=7$

$7 = 2\times 3 + 1$

$b \in H \subseteq G$

$b = a^s$ $\quad a^t$ ↗

$s = 10 \quad t = 4$

$10 = 2\times 4 + 2$

$\boxed{s = qt + r}$

remainder $\quad s/t$ = remainder

$0 \le r < t$

$a^s = a^{qt+r}$

$a^s = a^{qt} \cdot a^r$

$a^r = a^{s-qt}$ $\quad a^r = a^s a^{-qt}$

$= a^s (a^t)^{-q} = b(a^t)^{-q}$

$b \in H$

$(a^t)^{-q} \in H$

$b \cdot (a^t)^{-q} \in H$

<u>To</u>

$\Rightarrow a^r \in H$ $\quad 0 \le r < t$

a^{n_1}

a^{n_2}

a^{n_3}

$\vdots$

a^{n_n}

$\Rightarrow \therefore r = 0$ otherwise it will contradict

$a^s = a^{tq}$

$= (a^t)^q$

$b = a^s \in \langle a^t \rangle$

$b \in \langle a^t \rangle \rightarrow b \in H \Rightarrow b \in \langle a^t \rangle$

$\langle a^t \rangle \subseteq H$ —(1)

$H \subseteq \langle a^t \rangle$ $\quad \langle a^t \rangle = H$

∴ Every subgroup of cyclic is cyclic

X ═══════ X

Or

$\langle G, * \rangle = \langle a \rangle$ $\quad a * a * \underbrace{\cdots a}_{n \text{ times}} = a^n$ $\quad a^0 = e$

$a^m = \underbrace{(a^{-1}) * (a^{-1}) * \cdots * (a^{-1})}_{m \text{ times}}$

Proof

Let $\langle G, * \rangle$ be a cyclic group

$G = \langle a \rangle = \{ a^n \mid n \in Z \}$

Let H be a subgroup of G

$H \subseteq G \rightarrow H$ subgroup of G

we need to Show H is cyclic

If $H = \{e\} = \langle e \rangle$

Assume $H \neq \{e\}$

$x \in H$

$x \in a^n$ for some $n \in Z$

Let m be the smallest positive integer such that $a^m \in H$

Let $b = a^m$. $\quad H = \langle a^m \rangle = \langle b \rangle$

Let $c = a^x \in H$. $c = a^x$ for some integer x

Given $x, y \in \mathbb{Z}$ $\exists$ unique $q, r \in \mathbb{Z}$ such that $x = mq + r$ where $0 \leq r \leq y$

$\rightarrow$ $\exists$ $q, r \in \mathbb{Z}$ such that $x = mq + r$ $0 \leq r < m$

$$c = a^x = a^{mq+r} = (a^{mq}) \cdot a^r$$

$$(a^m)^{-q} (a^x) = a^r$$

$$(a^m)^{-q}, (a^x) \in H \rightarrow a^r \in H$$

since m is the smallest positive integer where $a^m \in H$, and $a^r \in H$ with $0 \leq r < m$

$r = 0$

$a^x = (a^m)^q = b^q$ $\qquad H = \langle b \rangle$

Coset

If H is a subgroup of G then for each $a \in G$, the set $aH = \{ab^h / b^h \in H\}$ is called a left coset of H in G, the set $Ha = \{ha / b \in H\}$ is a right coset of H in Q

$(H, *) \leq (G, *)$

$aH = \{ab / b \in H\}$ -> left coset of H in Q

$Ha = \{ha / b \in H\}$ -> Right coset "

Eg: $Z_4 = \{0, 1, 2, 3\}$

$\langle 1 \rangle = \{1, 2, 3, 0\}$

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

$\langle 3 \rangle = \{3, 2, 1, 0\}$

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

$3+3 = 6 - 3 = 3$

$-3 = 0$

$3+3+3 = 9 - 3 = 6 - 3$

$3 - 3 = 0$

3

$3+3 = 6 - 4 = 2$

$3+3+3 = 9 - 4 = 5 - 4$

$= 1$

$3+3+3+3 = 12 - 4 = 8 - 4$

$4 - 4 = 0$

$(Z_4, +_4)$

$\langle 1 \rangle = \{1, 2, 3, 0\}$
$\langle 3 \rangle = \{1, 2, 3, 0\}$
} Z_4 [proper subgroup]

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

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

group other than identity and all group

$Z_4 = \{0, 2\}, \{0\}$

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

take any element

1 a H

$0 +_4 H = \{0, 2\}$

$1 +_4 H = \{0, 1, 3\}$ — same set

$2 +_4 H = \{2 + 0\}$

$3 +_4 H = \{3, 1\}$ — same set

$\therefore$ 2 coset

coset

left coset

$2 \to$ coset

$H \quad a$

$H \quad 0 +_4 0 = \{0, 2\}$

$H \quad +_4 1 = \{1, 3\}$

$H \quad +_4 2 = \{2, 0\}$

$H \quad +_4 3 = \{3, 1\}$

right coset

left coset = Right lose

left coset and right coset will be equal if given group is cyclic or abelian

Theorem

If H is a subgroup of the finite group G, then for all $a, b \in G$

a) $|aH| = |H|$ — cardinality: No of element in aH = H

b) Either $aH = bH$ or $aH \cap bH = \phi$

Proof

1. $|aH| = |H|$

$x \leq y \quad y = x$

$y \leq x$

$|aH| \leq |H| \quad -c_1)$

$|H| \leq |aH| \quad -c_2)$

$\boxed{|aH| = |H|}$

$H \subseteq G \quad a \in G$

$H = \{a_1, b_1, c_1\}$

since G is finite its subset element also will be finite

~~$aH = \{aa_1, bb_1$~~

$aH = \{a a_1, a b_1, a c_1\}$

$|aH| \leq |H|$

$\boxed{a a_1 = a c_1}$ when the element equal there we be lesser no of element so

eg. 2, 3, 4, 8, 2 → 4 element

2 = 2

3, 4, 2 → 3 element

left cancellation

$a a_1 = a c_1$

$\times a^{-1}$

$a^{-1} a a_1 = a^{-1} a c_1$

$e a_1 = e c_1$

$\rightarrow a_1 = c_1$ if this happens then we not get

$\therefore a a_1 \neq a c_1$

ie $a a_1 = b b_1 = a c_1$

$|aH| = |H|$

2. $aH = bH$ or $aH \cap bH = \phi$

$a, b \in HG$

Assume

$aH \cap bH \neq \phi$

$\exists\ c \in aH \cap bH$

there exist atleast 1 element c which is belong to $aH \cap bH$

$c \in aH$ and $c \in bH$

we have to prove $aH = bH$

$aH \subseteq bH$

$bH \subseteq aH$

$aH \subseteq bH$

if $x \in aH \Rightarrow x = ah$ for some $h \in H$

$c = ah_1 \quad c = bh_2$

$a b_1 \overset{xh^{-1}}{=} b h_2$

$a = b h_2 h_1^{-1}$

$x = ah$

$x = a b h_2 h_1^{-1} h$

$= b h_3$

$x \in bH \qquad aH = bH$

P = 251

5.5 Theorem

Lagrange's theorem

If G is a finite group of order n with H a subgroup of order m, then m divides n

Proof

If $H = G$ then proof is completed. Otherwise $m < n$ and there exist an element $a \in G - H$. Since $a \notin H$, it follows that $aH \neq H$, so $aH \cap H = \emptyset$.

$$\text{If } G = aH \cup H, \text{ then } |G| = |aH| + |H|$$

$$= 2|H|$$

Then $O(G)$ divides $O(H)$. If not

There is an element $b \in G - (aH \cup H)$ with $bH \cap H = \emptyset = bH \cap aH$ and $|bH| = |H|$

$$\text{If } G = bH \cup aH \cup H \text{ then } |G| = |aH| + |bH| + |H|$$

$$= |H| + |H| + |H|$$

$$= 3|H|$$

Then $O(G)$ divides $O(H)$. If not there is an element $c \in G - (bH \cup aH \cup H)$
So this process terminates and find that $G = a_1H \cup a_2H \cup a_3H \cup \ldots \cup a_kH$.
therefore

$$|G| = |a_1H| + |a_2H| + |a_3H| + \cdots + |a_kH|$$
$$= |H| + |H| + |H| + \cdots + |H|$$
$$= k|H|$$

Then $O(G)$ divides $O(H)$.

Corollary

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

Proof

Since Order of an element is the order of the subgroup generated by that element. Every elements$a \in G$, $O(a)$ divides $|G|$

Corollary

Every group of prime order is cyclic.

Proof

Suppose that G has prime order. Let $a \in G$ and $a \neq e$, then,$|\langle a\rangle|$divides $|G|$ and $|\langle a\rangle| \neq 1$. Thus $|\langle a\rangle| = |G|$

5.36 ***Example***

a) For $\beta = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$, find the subgroup $K = \langle\beta\rangle$

b) Determine the left cosets of K in $G = S_4$

Solution

a) $\beta = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$ has order 4 and generates the cyclic subgroup $K = \langle\beta\rangle =$

$$\left\{\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}\right\} \text{ of } S_4$$

b) **Left cosets of K in $G = S_4$**

1. $\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix} K =$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}\left\{\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 3 & 2\end{pmatrix}\right\}$$

2. $\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix} K =$

$$\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\left\{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix}\right\}$$

3. $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix} K =$

$$\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\left\{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\right\}$$

4. $\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} K =$

$$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\left\{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\right\}$$

5. $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} K =$

$$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\left\{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$$

$$= \left\{\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$$

6. $\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}K =$

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\left\{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$$

$$=\left\{\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\right\}$$

7. $\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}K =$

$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\left\{\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}$$

$$=\left\{\begin{pmatrix}1&2&3&4\\4&3&2&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\right\}$$

8. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}K = K$

Exercises

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

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

3. Let $S = \mathbb{R}^* \times \mathbb{R}$. define the binay operation $\circ$ on $S$by $(u, v) \circ (x,\ y) = (ux, vx + y)$.prove that $(S,\circ)$ is a non abelian group

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

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

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

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

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

7. find all subgroups in each of the following groups

   a. $(\mathbb{Z}_{12}, +)$

   b. $(\mathbb{Z}_{11}^{*}, \cdot)$

   c. S_3

Answer

1. (i) for all $a, b, c \in G, (a \circ b) \circ c = (a + b + ab) \circ c$

$$= a + b + ab + c + (a + b + ab)c$$

$$= a + b + ab + c + ac + bc + abc$$

$$= a + b + c + ab + ac + bc + abc - - - (1)$$

$$a \circ (b \circ c) = a \circ (b + c + bc)$$

$$= a + b + c + bc + a(b + c + bc) + abc$$

$$= a + b + c + ab + ac + bc + abc - - - (2)$$

Since $(1) = (2) \Longrightarrow (a \circ b) \circ c = a \circ (b \circ c)$

It follows that the closed binary operation is associative

(ii) if $x, y \in G$ then $x \circ y = x + y + xy - - - (1)$

$$y \circ x = y + x + yx$$

$$= x + y + xy - - - (2)$$

There for $x \circ y = y \circ x$. So the binary operation is also commutative

(iii) Can we find $a \in G$ so that $x = x \circ a$ for all $x \in G$?

$$x = x \circ a \Longrightarrow x = x + a + ax$$

$$\Rightarrow a + ax = 0$$

$$\Rightarrow a(1 + x) = 0$$

$$\Rightarrow a = 0$$

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 $0 = x \circ y$

$$\Rightarrow 0 = x + y + xy$$

$$\Rightarrow y + xy = -x$$

$$\Rightarrow y(1 + x) = -x$$

$$\Rightarrow y = -\frac{x}{1+x}$$

That is $x \circ \left(-\frac{x}{1+x}\right) = x + \left(-\frac{x}{1+x}\right) + x\left(-\frac{x}{1+x}\right)$

$$= x - \frac{x}{1+x} - \frac{x^2}{1+x}$$

$$= x - \frac{x+x^2}{1+x}$$

$$= x - \frac{x(1+x)}{1+x}$$

$$= x - x$$

$$= 0$$

So inverse of x is $-\frac{x}{1+x}$. Therefore G is abelian group.

2. Since $x, y \in \mathbb{Z} \Rightarrow x + y + 1 \in \mathbb{Z}$, the operation is closed binary operation.

   (i)For all $w, x, y \in \mathbb{Z}$

$$w \circ (x \circ y) = w \circ (x + y + 1)$$

$$= w + x + y + 1 + 1$$

$$= w + x + y + 2$$

$$(w \circ x) \circ y = (w + x + 1) \circ y$$

$$= w + x + 1 + y + 1$$

$$= w + x + y + 2$$

(ii)Therefore $w \circ (x \circ y) = (w \circ x) \circ y$. Closed binary operation is associative

(iii)Further more $x \circ y = x + y + 1 = y + x + 1 = y \circ x$. That is binary operation is commutative

(iv)if $x \in \mathbb{Z}$, then $x \circ (-1) = x + (-1) + 1 = x$. So -1 is the identity element for $\circ$

(v) for each $x \in \mathbb{Z}$, we have $-x - 2 \in \mathbb{Z}$ and ,

$$x \circ (-x - 2) = x - x - 2 + 1$$

$$= -1$$

$$(-x - 2) \circ x = -x - 2 + x + 1$$

$$= -1$$

Therefore $-x - 2$ is the inverse for x under the $\circ$. Consequently $(\mathbb{Z}, \circ)$ is an abelian group

3. $(i)$for all $(a, b), (u, v), (x, y) \in S$, where

$$(a, b) \circ [(u, v) \circ (x, y)] = (a, b) \circ (ux, vx + y)$$

$$= (aux, bux + vx + y) - - - (1)$$

$$[(a,b)\circ(u,v)]\circ(x,y) = [au, bu+v]\circ(x,y)$$

$$= (aux, bux + vx + y) - - - (2)$$

So given closed binary operation is associative

(*ii*) To find the identity element we need $(a,b) \in S$ such that $(a,b)\circ(u,v) = (u,v)$and $(u,v)\circ(a,b) = (u,v)$ for all $(u,v) \in S$

$$(u,v) = (u,v)\circ(a,b)$$

$$= (ua, va + b)$$

$$\Rightarrow u = ua \text{ and } v = va + b$$

$$\Rightarrow a = 1 \text{ and } b = 0$$

Therefore $(1,0)$ is the identity element for this binary operation

(*iii*)Given $(a,b) \in S$ can we find $(c,d) \in S$, so that $(a,b)\circ(c,d) = (c,d)\circ(a,b) = (1,0)$

That is $(1,0) = (a,b)\circ(c,d)$

$$= (a,b)\circ(c,d) = (ac, bc + d)$$

$$\Rightarrow ac = 1 \text{ and } bc + d = 0$$

$$\Rightarrow c = a^{-1} \text{ and } d = -ba^{-1}$$

Therefore $(a^{-1}, -ba^{-1})$ is the inverse of (a,b)

There fore $(S, \circ)$ form group under this binary operation

Since $(1,2),(2,3) \in S$ and $(1,2)\circ(2,3) = (2,7)$ while$(2,3)\circ(1,2) = (2,5)$, this group is non abelian

4. Suppose G is abelian and $a, b \in G$. Then $(ab)^2 = (ab)(ab)$

$$= a(ba)b$$

$$= a(ab)b$$

$$= a^2b^2$$

By using associative property for a group and the fact that this group is abelian

Conversly suppose that G is a group where $(ab)^2 = a^2b^2$ for all $a, b \in G$

Let $x, y \in G$

$$(xy)^2 = x^2y^2$$

$$\Rightarrow (xy)(xy) = xxyy$$

$$\Rightarrow (xy)(xy) = xxyy$$

$$\Rightarrow xyxy = xxyy$$

$$\Rightarrow yx = xy$$

therefore the group G is abelian

5.

a. Consider the element $a \in G$.since both $(a^{-1})^{-1}$ and $a$are the inverse of a^{-1}. But inverse of an elemnt in group $G(a^{-1})^{-1}$is unique . therefore $(a^{-1})^{-1} = a$

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

$$= b^{-1}(e)b$$

$$= b^{-1}b$$

$$= e$$

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

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

$$= aa^{-1}b$$

$$= e$$

So $b^{-1}a^{-1}$ ia an inverse of ab and $(ab)^{-1} = b^{-1}a^{-1}$

6. G abelian $\Rightarrow a^{-1}b^{-1} = b^{-1}a^{-1}$

$$= (ab)^{-1}$$

Conversly if $a, b \in G$ then $a^{-1}b^{-1} = (ab)^{-1}$

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

$\Rightarrow ba^{-1}b^{-1} = bb^{-1}a^{-1}$

$\Rightarrow ba^{-1}b^{-1} = a^{-1}$

$\Rightarrow ba^{-1}b^{-1}b = a^{-1}b$

$\Rightarrow ba^{-1} = a^{-1}b$

7.

a. $\{0\}; \{0,6\}; \{0,4,8\}; \{0,3,6,9\}; \{0,2,4,6,8,10\}; \mathbb{Z}_{12}$

b. $\{1\},; \{1,10\}; \{1,3,4,5,9\}; \mathbb{Z}_{11}^{*}$

c. $\{\pi_0\}; \{\pi_0, \pi_1, \pi_2\}; \{\pi_0, r_1\}; \{\pi_0, r_2\}; \{\pi_0, r_3\}; S_3$