Module 3 Group theory

31 August 2021 16:47

Set theory.

Set is a collection of well defined objects

X - is a set of prime numbers < 50

$X = \{x \mid x \text{ is prime}, x < 50\} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$

$Y = \{1, 3, 5, 7, 9, 11, 13, 15\}$

operation $*$ - $+, -, \times, /,$

$a*b = ab - 1.$

$a*b = a+b-ab$

Algebraic structure

Semigroup:

X is a set, $*$ is an operation.

for $a, b, c \in X$

$a*(b*c) = (a*b)*c$ - Associative law

$(X, *)$ is a semigroup.

N - set of natural numbers $N = \{1, 2, 3, 4, \ldots\}$

$*$ - operation as addition $+$

$3, 6, 11 \in N$, $3+(6+11) = (3+6)+11$

$(N, +)$ is the semigroup.

$(N, -)$, $3, 6, 11 \in N$. $3 - (6-11) = 3 - (-5) = 8$

$(3-6) - 11 = -3 - 11 = -14$

$3 - (6-11) \neq (3-6) - 11$

$\Rightarrow (N, -)$ is not a semigroup.

Y - Set of 2×2 matrices, Matrix multiplication is the operation

$A, B, C \in Y$ To prove $A \times (B \times C) = (A \times B) \times C$

$A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$ $B = \begin{pmatrix} 2 & 0 \\ -1 & 4 \end{pmatrix}$ $C = \begin{pmatrix} 3 & 1 \\ 2 & -2 \end{pmatrix}$

$A \times B = \begin{pmatrix} -1 & 12 \\ 3 & 4 \end{pmatrix}$ $B \times C = \begin{pmatrix} 6 & 2 \\ 5 & -9 \end{pmatrix}$ $_{-3+8}$ $_{1-8}$ $_{-25}$

$A \times (B \times C) = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 6 & 2 \\ 5 & -9 \end{pmatrix} = \begin{pmatrix} & \\ 17 & -5 \end{pmatrix}$

$$A \times (B \times C) = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ 5 & -9 \end{pmatrix} = \begin{pmatrix} & \\ 17 & -5 \end{pmatrix}$$

$$(A \times B) \times C = \begin{pmatrix} -1 & 12 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 2 & -2 \end{pmatrix} = \begin{pmatrix} 21 & -25 \\ 17 & -5 \end{pmatrix}$$

$A \times (B \times C) = (A \times B) \times C$

$(Y, \times)$ is semigroup.

Common Properties

$a, b, c \in X$, $*$ is an operation property

(i) $a, b \in X$, then $a * b \in X$ - closure

(ii) $a, b, c \in X$ " $a * (b * c) = (a * b) * c$ - associative

(iii) $a \in X$, $a * e = e * a = a$, e is an identity element.

(iv) $a \in X$ $a * b = b * a = e$, b is the inverse of a

(vi) $a, b \in X$ $a * b = b * a$ - Commutative

$\oplus$ is an operation

(vii) $a * (b \oplus c) = (a * b) \oplus (a * c)$ } distributive law.
$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$.

$* = +$ $\oplus = \times$

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

Monoid

A set Y with the operation $*$ $(Y, *)$ is a monoid then it satisfies associative law and identity element.

1) $(N, +)$
$a + (b + c) = (a + b) + c$ holds true for all elements of N.

$a + e = e + a = a \Rightarrow e = 0$

$(N, +)$ is a monoid, with 0 as identity element

2) $(N, \times)$, $a \times e = e \times a = a \Rightarrow e = 1$
$(N, \times)$ is a monoid with 1 as identity element

3) X - set of all 2×2 matrices

$+$ is the operation

$$\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} + \left[\begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} + \begin{pmatrix} 3 & 4 \\ -1 & 5 \end{pmatrix} \right] = \left[\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \right] + \begin{pmatrix} 3 & 4 \\ -1 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} + \begin{pmatrix} 4 & 4 \\ -2 & 7 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 0 & 6 \end{pmatrix} + \begin{pmatrix} 3 & 4 \\ -1 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} + \begin{pmatrix} 4 & 4 \\ -2 & 7 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 0 & 6 \end{pmatrix} + \begin{pmatrix} 3 & 4 \\ -1 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 7 \\ -1 & 11 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ -1 & 11 \end{pmatrix}$$

with respect to + (matrix addition), associative law is verified.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow a_1 = 0 \quad b + b_1 = b \Rightarrow b_1 = 0, \quad c_1 = 0 \quad d_1 = 0$$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ - identity element.}$$

$(X, +)$ is monoid.

||ly $(Y, \times)$, where Y is the set of 2×2 matrices,
$\times$ - is matrix multiplication $\quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

then $(Y, \times)$ is the monoid with identity element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$a e_1 + b e_3 = a$
$e_1 = 1 \quad e_3 = 0$.
$c e_2 + d e_4 = d$
$\Rightarrow e_4 = 1$
$e_2 = 0$

Groups

$(G, *)$ is a group if it satisfies

(i) closure $\quad a, b \in G$, then $a * b \in G$
(ii) Associativity
(iii) Identity element $\quad a * e = e * a = a$
(iv) Inverse $\quad a * b = b * a = e$.

$(N, +)$ $\quad 2, 3 \in N \quad 2 + 3 = 5 \in N$

$(2+3)+5 = 2+(3+5)$

0 is the identity element

$a + b = 0 \Rightarrow b = -a$ does not exist in $(N, +)$

$\therefore$ $(N, +)$ is not a group but semigroup, also monoid

Classification of groups

finite | infinite group.

The set is finite $\quad$ The set is infinite

Infinite group ex:

1 R is the set of real numbers

$*$ is defined as

infinite sets

R - Real numbers
R^+ - positive real nos
R^- - negative, R^* - nonzero real nos.
Z - set of integers
Z^+, Z^- - positive/negative
N - natural
Q - rational ..

1 R is the set of real numbers

N - natural
Q - rational ..

* is defined as

for $a, b \in R$, $a * b = a + b + 2ab$

1. Closure

$a, b \in R \quad a+b+2ab \in R$

2 Associativity

$a, b, c \in R$, To prove $a*(b*c) = (a*b)*c$

$LHS = a * (b * c)$

$= a * (b + c + 2bc)$

$= a + (b+c+2bc) + 2a(b+c+2bc)$.

$= a + b + c + 2(bc + ab + ac) + 4abc$ - (1)

$RHS = (a * b) * c$

$= (a+b+2ab) * c$

$= a+b+2ab + c + 2(a+b+2ab)c$

$= a+b+c+2(ab+ac+bc) + 4abc$ - (2)

from (1) & (2) LHS = RHS .

(iii) Identity element.

$a * e = e * a = a$

$\cancel{a} + e + 2ae = \cancel{a}$

$e(1+2a) = 0$

$1+2a \neq 0 \Rightarrow e = 0$ is the identity element

for $1+2a=0$, $a = -1/2 = -0.5$

$-0.5 * 0$

$-0.5 + 0 + 2(-0.5)0$

$= -0.5$

It holds, ∴ 0 is the element for all in R including $-1/2$

(IV) Inverse

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

$a + a^{-1} + 2aa^{-1} = e = 0$

$a^{-1}(1+2a) = -a$

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

for example for inverse of 3 is $\frac{3}{1+6} = 3/7$

Inverse ~~exists~~ except for $-1/2$

$-\frac{1}{2} * a^{-1} = 0$

$-\frac{1}{2} + a^{-1} + 2(-1/2)a^{-1} = 0$

$-1/2 = 0$ absurd $\Rightarrow -1/2$ does not have inverse

(V) Commutativity

(v) commutativity

$a * b = b * a$

$a + b + 2ab = b + a + 2ba$. It holds.

$\Rightarrow (R, *)$ is not a group

but $\{R - \{-1/2\}, *\}$ is an abelian group

Abelian group

group which satisfies commutative property.

Finite group

$S = \{1, -1, i, -i\}$ $*$ - multiplication

check whether $(S, \times)$ is a group

$\times$	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) closure

for any two elements its product also in S

(ii) Take any three elements

$1, i, -i$

$(1 \times i) \times -i = i \times -i = 1$

$1 \times (i \times -i) = 1 \times 1 = 1$

Associativity holds.

(iii) Identity element

$a * e = a$

$e = 1$ (from the table)

(iv) Inverse element

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

for 1

$1 \times 1 = 1$

Inverse of 1 is 1

-1

$-1 \times -1 = 1$

Inverse of -1 is -1

Inverse of $i = -i$

$i \times (-i) = 1$

Inverse of $-i = i$

$-i \times (i) = 1$

(v) abelian (commutativity)

$a * b = b * a$

$i \times -i = -i \times i = 1$

$(S, \times)$ is an abelian group.

Finite group - example 2:

Z_5 - Congruence modulo 5

$(Z_5, \times)$ is defined as $(i) \times_5 (j) = (i \times j) \bmod 5$

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

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

	[0]	[1]	[2]	[3]	[4]
[0]	0	0	0	0	0
[1]	0	1	2	3	4
[2]	0	2	4	1	3
[3]	0	3	1	4	2
[4]	0	4	3	2	1

(i) Closed

(ii) Associativity $1 \times_5 (2 \times_5 3) = 1 \times_5 1 = 1$

$(1 \times_5 2) \times_5 3 = 2 \times_5 3 = 1$

(iii) Identity - 1 .

(iv) Inverse

element	inverse
0	no-inverse
1	1
2	3
3	2
4	4

$\Rightarrow (Z_5, \times)$ is not a group as 0 does not have inverse

If we take $Z_5^* = Z_5 - \{0\} = \{1, 2, 3, 4\}$

5

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(i) closure

(ii) Associativity

(iii) identity - 1

(iv) inverse of 1 is 1, 2 is 3, 3 is 2, 4 is 1 .

$Z_6^* \rightarrow$

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

$(Z_5^*, \times)$ is a group

Consider $Z_4^* = \{1, 2, 3\}$

4

×	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$a * b \notin Z_4^*$ as $0 \notin Z_4^*$

It is not closed .

$(Z_4^*, \times)$ is not a group .

$(Z_5^*, \times)$ is a group.

$(Z_p^*, \times)$ is a group

for ex. P-prime

$(Z_{17}^*, \times)$, $(Z_{23}^*, \times)$ ... are all groups.

6 - 2×3, 3×2 (1×6)

9 - 3×3

21 - 3×7

17 - 1×17 - prime

$(Z_6, +)$

$(Z_6, +)$ 6 $Z_6 = \{0, 1, 2, 3, 4, 5\}$

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

Identity - 0

Inverse	
0	0
1	5
2	4
3	3

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

1 − 5
2 − 4
3 − 3
4 − 2
5 − 1

$(Z_6, +)$ is a group

Kelin 4

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(i) closed

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

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

(iii) Identity element is a

(iv) Inverse of every element is itself.

Order of the group :- The no. of elements in the group.

Order of the element (in any group) 'a' is, if $a^n = e$, order $= n$.

The least positive integer n such that $a^n = e$ is the order of a

If for addition, $a + a + \ldots n$ times $= 0$

$na = 0$ then n is the order of a

If for multiplication $a.a. \ldots n$ times $= 1$

$a^n = 1$. n is the order.

$-i$

$-i$

example

1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

Order of the group is 4

Order of 1 is $1^n = 1 \Rightarrow n = 1$

$-1 \quad (-1)^n = 1 \Rightarrow n = 2$

$i \quad (i)^n = 1 \Rightarrow$

$i^4 = 1 \Rightarrow n = 4$

+	0	1	2	3	4	5

Z_6

$i^4 = 1 \Rightarrow n = 4$

$-i \quad (-i)^n = 1 \Rightarrow n = 4$

Z_6

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

Order of 0 is 1 $\quad 1 \cdot 0 = 0$

1 — 6 $\quad 1+1+1+1+1+1 = 0$, $6(1) = 0$

2 — 3 $\quad 2+2+2 = 0$

3 — 2 $\quad 3+3 = 0$

4 — 3 $\quad 4+4+4 = 0$

5 — 6 $\quad 5+5+5+5+5+5 = 0$

order.

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

5

Order of

1 — $1^n = 1 \Rightarrow n = 1$

2 — $2^n = 1 \Rightarrow n = 4$ $\quad 2 \times 2 \times 2 \times 2$

3 — $3^n = 1$ $\quad 3 \times 3 \times 3 \times 3 = 81$, $\underline{\underline{n=4}}$

4 — $4^n = 1$ $\quad 4 \times 4 \quad n = 2$.

Subgroups :-

$(G, *)$ is a group

$S \subset G$, S is the subset of G.

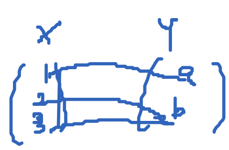
S itself is group, then S is the subgroup of G

S is to be proved as subgroup

$a, b^{-1} \in S$, we need to prove $a * b^{-1} \in S$

Permutation groups :-

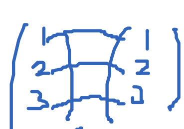
$f : X \to Y$



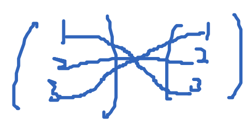
$f(x) = y$

$f(1) = a \quad f(2) = b \quad f(3) = b$ ..

$f : S \to S$, $\quad S = \{1, 2, 3\}$



f_1



f_2

$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\quad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad P_6 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$

$P_5 * P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$

$S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ is a set

The operation $*$ is defined as

$$P_1 * P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$$

$$P_3 * P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = P_2$$

$$P_3 * P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = P_6 \qquad P_2 * P_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = P_4$$

$$P_3 \times P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad P_3 * P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = P_1$$

inverse of P_3 is P_3.

To find inverse

P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_2	P_3	P_4	P_5	P_6
	P_4	P_4			
	P_5	P_4	P_6	P_2	P_4 P_5

$$P = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{matrix}$$

$$P^{-1} = \begin{pmatrix} 3 & 5 & & & & \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

$P_1 * (P_4 * P_6) = P_1 * P_3 = P_3$

$(P_1 * P_4) * P_6 = P_4 * P_6 = P_3$

$$F = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{bmatrix}.$$

Cyclic groups.

If an element a in a group $(G, *)$ in which all the elements in G are power of a, a is called the generator of G, and $g_1, g_2 \in G$, then $g_1 = a^m$, $g_2 = a^n$ ....

1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

i is the generator

$i^1 = i \quad i^2 = -1 \quad i^3 = -i \quad i^4 = 1$

$(-i)$ ~~is also~~ is also the generator

$(-i)^1 = -i \quad (-i)^2 = -1 \quad (-i)^3 = i \quad (-i)^4 = 1$

Every cyclic group is abelian :-

Let G be a group

a is the generator

$g_1 \,\&\, g_2 \in G$, then $g_1 = a^m$, $g_2 = a^n$

$g_1 * g_2 = a^m * a^n$

$= a^{m+n}$ if $*$ is multiplication.

$= a^{n+m}$

$= a^n \cdot a^m$

$= g_2 * g_1$

$\Rightarrow G$ is abelian

$A \times B$ is a set $A = \{1, 2, 3\}$ $B = \{4, 5\}$

$A \times B = \{(1,4) (1,5) (2,4) (2,5) (3,4) (3,5)\}$

Example

Let $Q \times Q$ is a set

for any two elements $(a, b), (x, y) \in Q \times Q$

$(a, b) * (x, y) = (ax, by)$

$= (ay, bx)$.

$= (ax, ay + b)$

$= (ax + ay, by)$

$*$ is defined as $(a, b) * (x, y) = (ax, ay + b)$..

To prove/disprove properties:

(i) $(a, b), (x, y) \in Q \times Q$, $(ax, ay + b) \in Q \times Q$ – closure

(ii) $(a, b), (x, y), (p, q) \in Q \times Q$

$\big((a, b) * (x, y)\big) * (p, q) = (ax, ay + b) * (p, q)$

$= (axp, axq + ay + b)$ — ①.

$(a, b) * \big((x, y) * (p, q)\big) = (a, b) * (xp, xq + y)$

$= (axp, a(xq + y) + b)$ — ②

① = ②

Associative law holds $\Rightarrow$ Semigroup.

(iii) Identity element:

$(a, b) * (e_1, e_2) = (a, b)$

$(ae_1, ae_2 + b) = (a, b)$

$\Rightarrow ae_1 = a$. $ae_2 + b = b$

$e_1 = 1$

$(e_1, e_2) = (1, 0)$ is the identity element $\Rightarrow$ Monoid.

iv) Inverse

$$(a, b) * (a^{-1}, b^{-1}) = (e_1, e_2)$$

$$(a a^{-1}, a b^{-1} + b) = (e_1, e_2)$$

$$a a^{-1} = e_1 = 1 \qquad a b^{-1} + b = e_2 = 0$$

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

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

$(a^{-1}, b^{-1}) = (\frac{1}{a}, \frac{-b}{a})$ is the inverse of (a, b), $a \neq 0$.

(v) Commutative

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

$$(a, b) * (c, d) = (ac, ad + b) \quad — ①$$

$$(c, d) * (a, b) = (ca, cb + d) \quad — ②$$

① ≠ ② i.e, $ad + b \neq cb + d \Rightarrow$ not Commutative $\Rightarrow$ not abelian.

cyclic group: examples.

If order of a group is 3, it must be cyclic.

a, b, c are the elements

i.e a, b, e

$a * b = e \quad b * a = e$

$a * a \in G \quad a * a = a$ or b or e

if I take $a * a = b$. $a^2 = b$

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

$$a^3 = e$$

The three elements ~~are~~ $(a, \underset{=b}{a^2}, a^3 = e)$.

a^2, $a^4 = (a^2)^2$

Any group of order 6, If a is the generator,

a^1, a^2, a^3, a^5, has 4 generators.

$(Z_5, +_5)$

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

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

Let 2 as the generator

$2^1 = 2$

3 4 0 1 2

4 0 1 2 3 $\quad 2^1 = 2$

Set + operation + properties $\Rightarrow$ group
$\downarrow$
Subset + operation + exclude associative $\Rightarrow$ subgroup.

closure + identity + inverse $\Rightarrow a, b \in H,\ a * b^{-1} \in H$

Example 4.2 If G is an abelian group with identity e, prove that all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

To prove identity

$e \in H$ if $e^2 = e \Rightarrow e \in H$

$e.e = e \Rightarrow e = 1$ is the identity element.

Inverse

$x \in H, \quad x^2 = e$

$x.x = e$

$x^{-1}.x.x = x^{-1}.e$ [premultiply with x^{-1}]

$e.x = x^{-1} \Rightarrow x = x^{-1}$ inverse exists for all $x \in H$

To prove closure

if $x, y \in H$ then $xy \in H$

$xy = yx \quad \because H$ is abelian

$= y^{-1}x^{-1} \quad y = y^{-1}, x = x^{-1}$

$= (xy)^{-1} \quad \because (xy)^{-1} = y^{-1}x^{-1}$

$xy . xy = 1$

$(xy)^2 = 1 = e \quad xy \in H$

$\Rightarrow H$ is closed.

$\Rightarrow H$ is a subgroup

Example 4.3 If G is the set of all ordered pairs (a, b), where $a(\neq 0)$ and b are real and the binary operation $*$ on G is defined by

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

show that $(G, *)$ is a non-abelian group. Show also that the subset H of all those elements of G which are of the form $(1, b)$ is a subgroup of G.

(i) Closure

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

a & c are real $\Rightarrow ac$ is real

$bc + d$ also real.

$\Rightarrow (ac, bc + d) \in H$

(ii) Associativity

$(a, b) * [(c, d) * (f, g)] = (a, b) * (cf, df + g) = (acf, bcf + df + g)$ — ①

$[(a, b) * (c, d)] * (f, g) = (ac, bc + d) * (f, g) = (acf, (bc + d)f + g) \rightarrow$ ②

① = ② $\Rightarrow$ Associativity holds.

(iii) Identity :-

$(a, b) * (e_1, e_2) = (a, b)$

$(ae_1, be_1 + e_2) = (a, b) \Rightarrow ae_1 = a \Rightarrow e_1 = 1$

$be_1 + e_2 = b \Rightarrow b + e_2 = b \Rightarrow e_2 = 0$

The identity element is $(1, 0)$

(iv) Inverse

$$(a,b) * (a^{-1}, b^{-1}) = (e_1, e_2) = (1,0)$$

$$(aa^{-1},\ ba^{-1}+b^{-1}) = (1,0) \Rightarrow aa^{-1} = 1, \quad ba^{-1}+b^{-1} = 0$$

$$a^{-1} = 1/a \qquad \frac{b}{a} + b^{-1} = 0$$

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

inverse of (a,b) is $(1/a, -b/a)$

(v) Commutative

$$(a,b) * (c,d) = (ac,\ bc+d) \qquad ac = ca$$

$$(c,d) * (a,b) = (ca,\ da+b) \qquad bc+d \neq da+b$$

$\Rightarrow$ It is not commutative.

$\Rightarrow$ G is non abelian group.

To prove the set of all element $(1,b) \in H$ is a subgroup

$(1,a),\ (1,b) \in H$

To prove $(1,a) * (1,b)^{-1} \in H$

$(1,a) * (\frac{1}{1}, -\frac{b}{1})$

$= (1,\ a-b)$ $\qquad$ a, b are real; a − b is real

$(1,\ a-b) \in H$.

$\Rightarrow H$ is a subgroup.

Homomorphism:

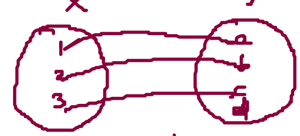
$y = f(x)$ $\qquad$ X - domain - set of values

Y - co-domain - ″

$f: X \to Y$

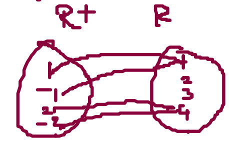
f is 1-1 (one-one)

f is onto



1-1
not onto

$f(x) = x^2$

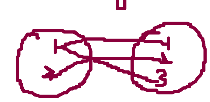


not 1-1

$f: R \to R$, $f(x) = x^2$ is not 1-1 & onto $\qquad$ $f(x) = f(y)$

$f: R^+ \to R^+$ $f(x) = x^2$ is 1-1 and onto $\qquad$ $\Rightarrow x = y$ then 1-1

f is 1-1 & onto $\Rightarrow$ f is bijective



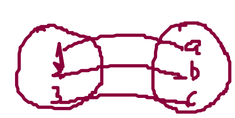
onto
not 1-1

$(G, *)$ is a group. $(G_1, \circ)$ is another group

$f: G \to G_1$ defined by $f(a * b) = f(a) \circ f(b)$

f is group homomorphism

f is 1-1 & onto then it is bijective..



1-1

Results:

f is 1-1 & onto then it is bijective.

1-1
onto

Results :-

* e is the identity element $(G, *)$
  e_1 is " " " $(G_1, \cdot)$

  then $f(e) = e_1$

* a has inverse a^{-1} in G then

$$f(a^{-1}) = [f(a)]^{-1}$$

Kernal of a homomorphism

Set of all elements a of G such that $f(a) = e_1$

kernal is a subgroup.

To prove, $a, b \in G$, $a, b \in$ kernal of f $K(f)$

$$f(a) = e_1, \quad f(b) = e_1$$

To prove $a * b^{-1} \in K(f)$ for proving $K(f)$ is a subgroup

$$f(a * b^{-1}) = f(a) \cdot f(b^{-1})$$
$$= e_1 \cdot [f(b)]^{-1}$$
$$= e_1 \cdot e_1^{-1}$$
$$= e_1 \cdot e_1 = e_1$$

$a * b^{-1} \in K(f) \Rightarrow K(f)$ is a subgroup

To find Kernal

Let $f : C \to R$, defined as $f(a+ib) = a$, $*$ - addition

$$f((a+ib) + (c+id)) = f((a+c) + i(b+d)) = a+c$$

$$f(ia + ib) = f(i(a+b)) = 0$$

Set of all purely imaginary numbers form a kernal.

Cosets :- Co-set

a is the element of $(G, *)$, H is a subset of G

The coset aH is defined as $aH = \{a * h \mid h \in H\}$

aH - left coset

$Ha = \{h * a \mid h \in H\}$ - right coset.

$H = \{h_1, h_2 \cdots h_m\}$

$H = \{h_1, h_2 \ldots h_m\}$

$aH = \{a*h_1, a*h_2, \ldots a*h_m\}$

$Ha = \{h_1*a, h_2*a \ldots h_m*a\}$

Lagrange theorem

Group Code:-

Transmitter → Encoder → channel → Decoder → Receiver

Binary number System = $+_2$ - additive arithmetic modulo 2 has $\{0,1\}$

$1+1 = 2 \pmod 2 = 0$

$1+0 = 1$

$0+0 = 0$

$B = \{0, 1\}$

Any message conveyed as sequence of 0's and 1's

Sending message has 3 digits as $(000)\ (001) \ldots = B^3$

B^3 - ordered triple

B^5 - ordered 5 tuple $(00101, 11011, \ldots)$

$f : B^3 \to B^5$, operation $+_2$ In general $e : B^m \to B^n$

$x \in B^3$ is called string

(i) Weight of the string x - no. of 1's in x. 110010 - weight 3

(ii) The distance b/w two strings x & y is the no of positions in which they differ

$x = (001011)$ $y = (101111)$

distance is 2

(iii) $e : B^m \to B^n$

G - generator matrix $[I_m | A]$, I_m - $m \times m$ unit matrix

A - $m \times (n-m)$

2×3

Ex

$e : B^2 \to B^5$

Ex

$e : B^2 \to B^5$ $\qquad 2 \times 3$

$e(B^2) = B^5$

$e(B^2) = B^2 G = B^5$

$$(0\ 1)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = (0\ 1\ 0\ 0\ 1)$$

$$(1\ 1)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = (1\ 1\ 1\ 1\ 1)$$

first m digits is the original string of B^2

Generator matrix - encoder

Parity check matrix

$G = [I_m \mid A]$, $H = [A^T \mid I_{n-m}]$

$$= \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}_{3\times 5}$$

r = received code

$= (0\ 1\ 0\ 0\ 1)$

$$r^T = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}_{5\times 1}$$

$$H r^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = (0\ 0\ 0)$$

a .

e Wrong output $r = (0\ 1\ 0\ \boxed{1}\ 1)$

$$H r^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}_{3\times 5}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}_{5\times 1} = (0\ 1\ 0)_{3\times 1}$$

Original message $= (0\ 1\ 0\ 0\ 1)$

Example 4.1 A binary symmetric channel has probability $p = 0.05$ of incorrect transmission. If the code word $c = 011\ 011\ 101$ is transmitted, what is the probability that (a) we receive $r = 011\ 111\ 101$? (b) we receive $r = 111\ 011\ 100$? (c) a single error occurs? (d) a double error occurs? (e) a triple error occurs?

P = Prob. of occurrence of error $= 0.05$, q = Prob of sending correct one $= 0.95$

a)

$c = 011\ 011\ 101$

$r = 011\ 111\ 101$

Required prob $= P$(1 error and 8 non errors) $= 0.05 \times 0.95 \times 0.95 \ldots$ 8 times.

$= 0.05\,(0.95)^8$

b) $r = 111\ 011\ 100$ - 2 errors

Reqd. Prob $= (0.05)^2\,(0.95)^7$

c) a single error occurs.

c) a Single error occurs

P(error in 1st position) or Second position or .... 9th pos)

$= 9\,(0.05)\,(1-0.05)^8$

1 2   2 3   3 4
1 3   2 4
1 5   2 9   8 9
1 9

$= {}^9C_2$

$= \frac{9 \times 8}{1 \times 2}$

$= 36$

d) double error

Req. Prob $= {}^9C_2\,(0.05)^2\,(0.95)^7$

$= 36\ (\quad)(\quad)$

e) triple error

Prob $= {}^9C_3\,(0.05)^3\,(0.95)^6$.

$= \frac{9 \times 8 \times 7}{1 \times 2 \times 3}\,(\;"\;)\,(\;"\;)$

Example 4.2 The (9, 3) three times repetition code has the encoding function $e = B^3 \to B^9$, where $B = (0, 1)$.

(a) If d: $B^9 \to B^3$ is the corresponding decoding function, apply 'd' to decode the received words (i) 111 101 100, (ii) 000 100 011; (iii) 010 011 111 by using the majority rule.

(b) Find three different received words r for which $d(r) = 000$

111 101 100 — 101 ...

$d(r) = 000$ $r =$ 010 000 100

111 000 000

101 000 010 ...

Example 4.3 Find the code words generated by the encoding function e: $B^2 \to B^5$ with respect to the parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{array}{c} \begin{array}{cc} A^T & I_{m-m} \end{array} \\ \left[\begin{array}{cc|ccc} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right] \end{array}$$

Generator matrix $G = [I_m \mid A]$

$$= \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$B^2 = (00, 01, 10, 11)$

$e(00) = (00)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0\,0\,0\,0\,0)$.

$e(1,1) = (1\,1)\,(\qquad) = (1\,1\,0\,0\,0)$ ...

1. Show that the set of all polynomials in x with real coefficients and degree less than or equal to 2 under the operation of addition is a group.

2. If α, β are elements of the symmetric group S_4, given by $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$. Find αβ, βα, α^2 and α^{-1}. Find also the orders of α, β and αβ.

3. Show that the group {(1,2,3,4,5,6),$\times_7$} is cyclic. How many generators are there for this group? What are they?

4. If C^* is the multiplication group of non-zero complex numbers and if the mapping $f: C^* \to C^*$ is defined by $f(z) = z^4$, show that f is a homomorphism also find the kernel of f.

5. Find the left cosets of {0, 3} in the group $(Z_{6,} +_6)$.

6. Find the codewords generated by the encoding function $e : B^4 \to B^7$ with the generator matrix G for any five strings of B^4 and verify it with the corresponding parity check matrix.

$$G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right).$$

7. with the given $G = \left(\begin{array}{ccc|ccccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \end{array}\right)$, Check the following

Strings whether they can be the output of the encoding function. If not find the corrected one and its input string

[Hint: to be found the following.

the mapping $e : B^m \to B^n$

The strings of B^n.

The parity check matrix

for the given r. get corrected and find $d(r)$-input.

Given r

{01010101, 00100100, 11111111, 10011010, 01100101}