Algebraic Structures

* Binary Operations

Combine two elements of the set to produce another element of the same set.

Binary Operators $+, -, \times, \div$

① Closure property
② Associative property
③ Identity property
④ Inverse Property
⑤ Commutative Property
⑥ Idempotent Property

① Closure = Algebraic Structures
② Closure + Associative = Semigroups
③ Closure + Associative + Identity = Monoids
④ Closure + Associative + Identity + Inverse = Groups
⑤ Closure + Associative + Identity + Inverse + Commutative = Abelian Groups

① Algebraic structure

↳ closure property.

↳ Let A be non empty set. An operation * is said to be closure on A if $\forall a, b \in A \quad a * b \in A$

eg. N, + Yes Z + Yes R + Yes

N, − No Z − Yes R − Yes

9 − 2 = 7
2 − 9 = −7 ✗

N, × Yes Z × Yes R × Yes

N, ÷ No Z ÷ No R ÷ No

$\frac{a}{0}$ ✗

② Semi groups

Let (A, *) be an algebraic structure, where * is a binary operation on A. (A, *) is called semigroups if the following conditions are satisfied.

1. closure property
2. Associative property.

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

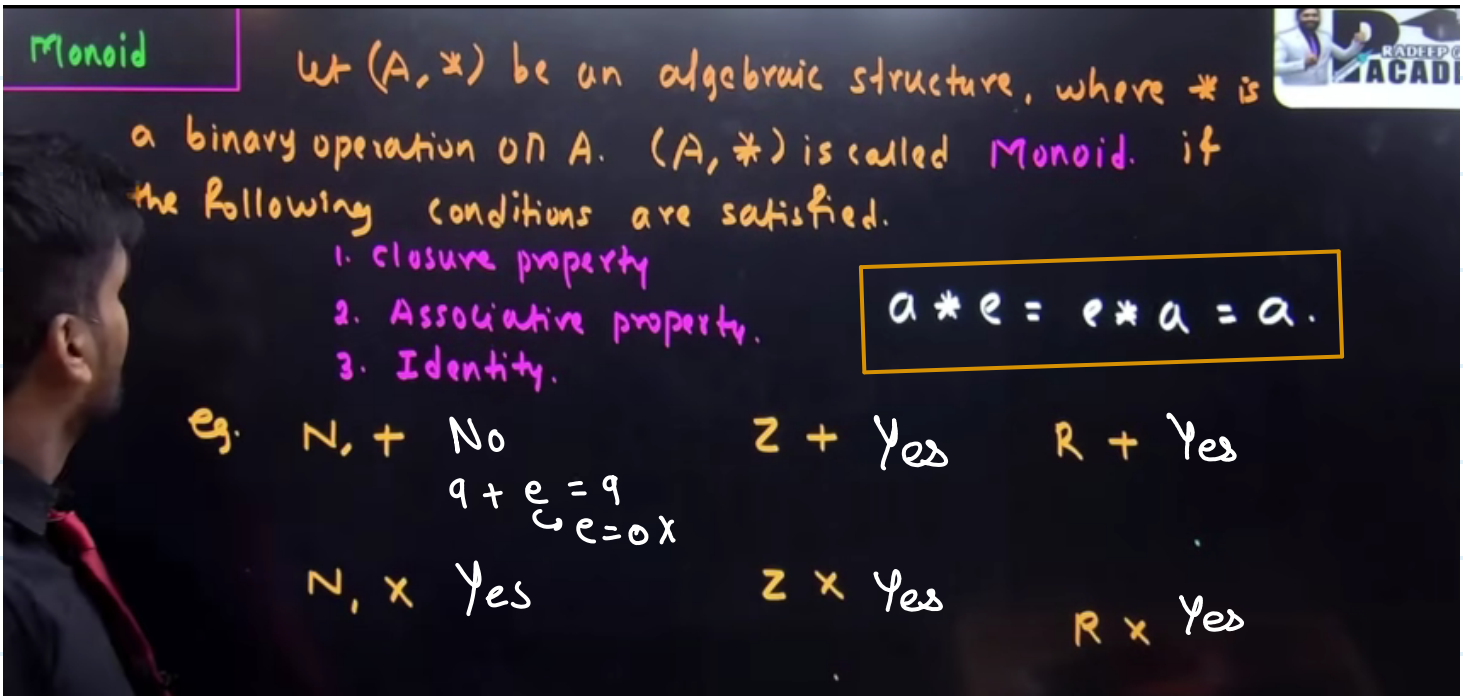
eg. N, + Yes Z + Yes R + Yes

Z − No R − No

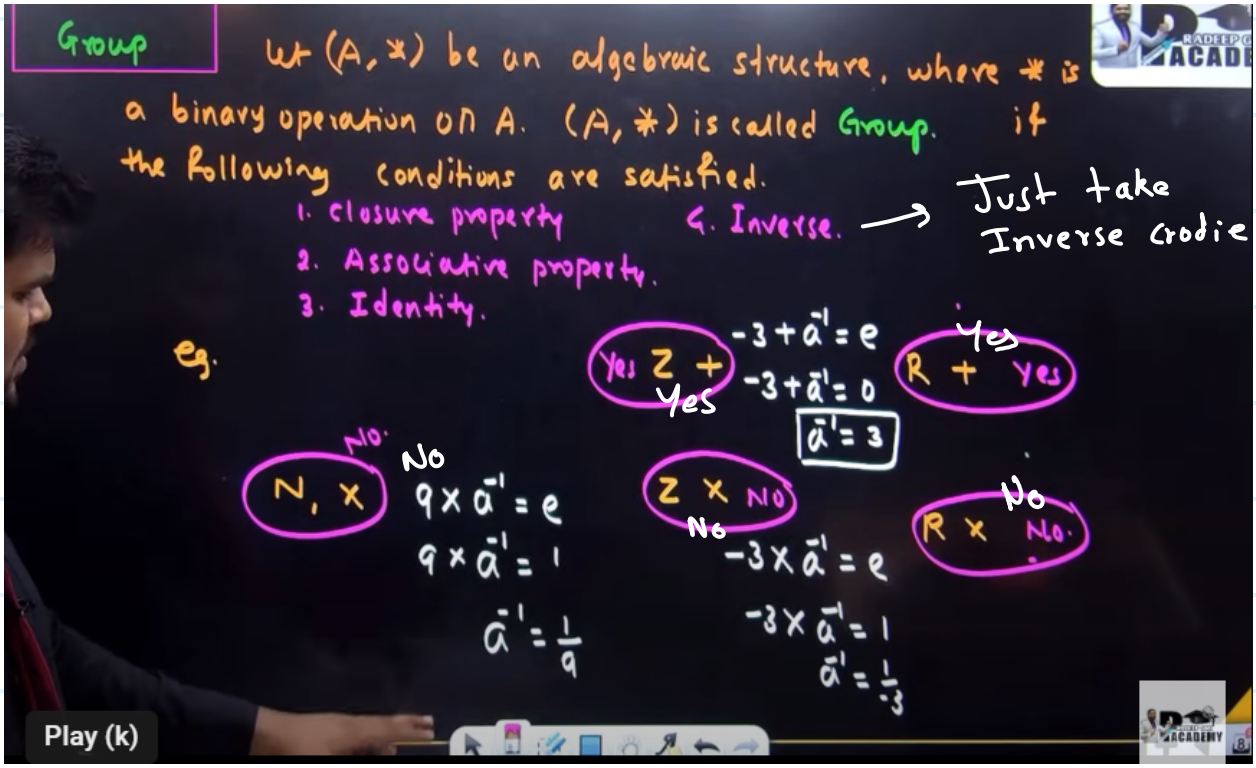
N, × Yes Z × Yes R × Yes

(−2 − 3) − 5 = −10
−2 − (3 − 5) = 0 ✗

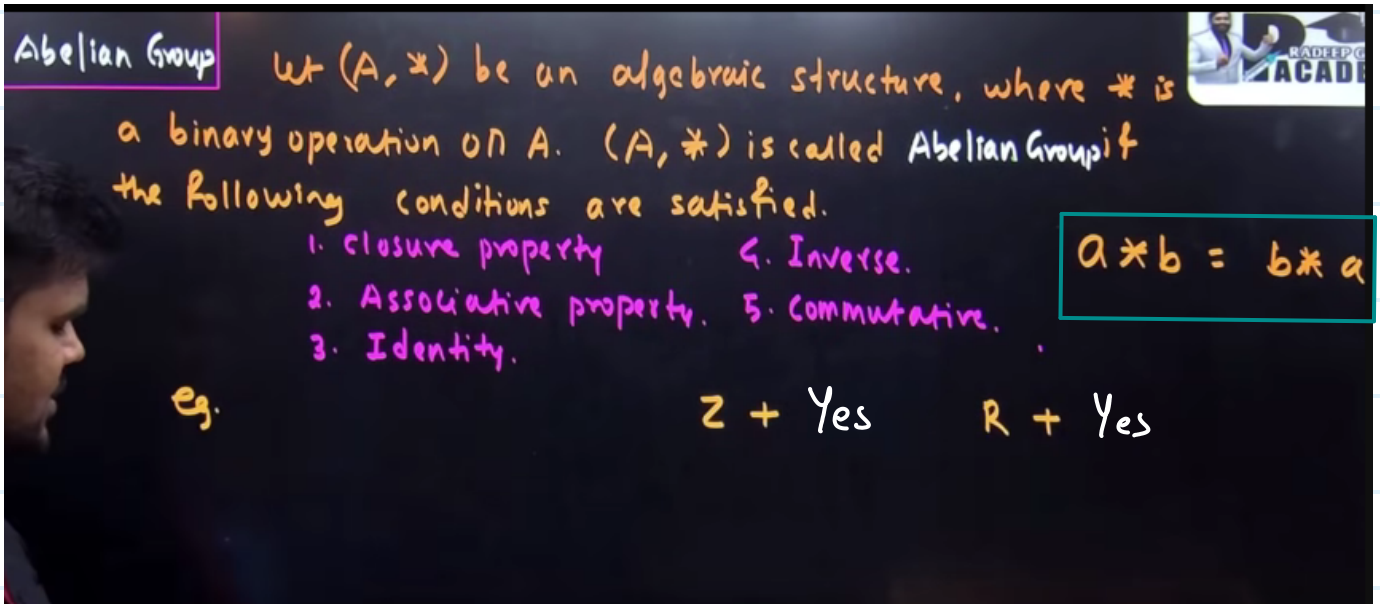
③


Monoid
Let (A, *) be an algebraic structure, where * is a binary operation on A. (A, *) is called Monoid. if the following conditions are satisfied.
1. Closure property
2. Associative property.
3. Identity.
a * e = e * a = a.
eg. N, + No
q + e = q
e = 0 x
Z + Yes
R + Yes
N, x Yes
Z x Yes
R x Yes

④


Group
Let (A, *) be an algebraic structure, where * is a binary operation on A. (A, *) is called Group. if the following conditions are satisfied.
1. Closure property
2. Associative property.
3. Identity.
4. Inverse. → Just take Inverse Crodie
eg.
Yes Z + Yes
-3 + ā¹ = e
-3 + ā¹ = 0
ā¹ = 3
R + Yes
N, x No
q x ā¹ = e
q x ā¹ = 1
ā¹ = 1/q
Z x No
-3 x ā¹ = e
-3 x ā¹ = 1
ā¹ = -1/3
R x No
Play (k)

⑤



$a,b \in o$
$a*b \in o$ ↑ Closure +

$(a*b)*c = a*(b*c)$ ↑ Associative +

$a*e = a$ ↑ Identity +

$a*a^{-1} = e$ ↑ Inverse +

$a*b = b*a$ ↑ Commutative

a] Proof that the set Z of all integers with binary operation * defined by $a * b = a+b+1$ such that $\forall\ a,b \in z$ is an abelian gr.

→ $a * b = a + b + 1$

① Closure Property

$a, b \in z$

$a * b = a+b+1 \in z$

∴ Satisfies closure property

② Associative Property

$(a * b) * c = \overbrace{(a+b+1)}^{a} * b \; c$

$= a+b+1+c+1$

$= a+b+c+2$

$a * (b * c) = a * \overbrace{(b+c+1)}^{b}$

$= a+b+c+1+1$

$= a+b+c+2$

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

Satisfies associative property

③ Identity

$a * e = a$

$a + e + 1 = a$

$e = -1$

Satisfies Identity property

④ Inverse

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

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

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

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

Satisfies Inverse property

⑤ Commutative

$a * b = a+b+1$

$b * a = b+a+1$

$a * b = b * a$

Satisfies Commutative Property

$\therefore (Z, *)$ is an Abelian Group

* Addition Modulo

$a +_m b$

$a + b = r \; ; \quad 0 \le r \le m$

$5 +_3 9 = 2$ $\qquad$ $9+5=14 \Rightarrow 14 \div 3 = 4$, $14 - 12 = 2$; $3 \times 4 + 2$ → 2 = answer

$15 +_5 25 = 0$

* Multiplication Modulo

$a \times_m b = r \qquad 0 \le r \le m$

$3 \times_4 5 = 3$ $\qquad$ $3 \times 5 : 15 \div 4 = 3$, $15 - 12 = 3$

Q] Show that $(G, +_8)$ is an abelian group where $G = (0,1,2,3,4,5,6,7)$

$+_8$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

① Closure Property

$a, b \in G$

$a +_8 b \in G$

$\therefore$ Satisfies closure

② Associative Property

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

$(1 +_8 2) +_8 3 = 3 +_8 3 = 6$

$1 +_8 (2 +_8 3) = 1 +_8 5 = 6$

$\therefore$ Satisfies Associative

③ Identity Property

Identity element $= 0$

Satisfies Identity

④ Inverse

$0 +_8 0 = 0$

$1 +_8 7 = 1$ Satisfies ✓

⑤ Commutative

$1 +_8 2 = 3$ satisfies

$2 +_8 1 = 3$

$\therefore G, +_8$ is abelian group

P.T. $G = (1, 2, 3, 4, 5, 6)$ is Abelian group of order 6 wrt $\times_7$.

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Now prove all properties.

* Cyclic Group

A group G is said to be cyclic if for some a in G, every element x in G can be expressed as a^n

eg:- $A\{1, 2, 3, 4, 5, 6\} \times_7$

$3^1 = 3$

$3^2 = 3 \times_7 3 = 2$

$3^3 = 3^2 \times_7 3 = 6$

$3^4 = 3^3 \times_7 3 = 4$

$3^5 = 3^4 \times_7 3 = 5$

$3^6 = 3^5 \times 3 = 1$

$7 \overline{)18} \; \frac{2}{4}$

$\therefore$ 3 is a generator

* Subgroups

A → Group

B is a subset of A

Then B → Subgroup

⟶ Proper Subgroup

$A < G$

$G = \{1\ 2\ 3\ 4\}$

$A = \{1\ 3\}$

* Coset

Coset
↙ ↘
Right Left

Let H be a subgroup of a group $(G, *)$

$Ha = \{h * a \mid h \in H\}$

↳ Ha is called a right coset of H in G.

$aH = \{a * h \mid h \in H\}$

↳ aH is called a left coset of H in G.

If $Ha = aH \Rightarrow$ Normal Subgroup

★ Groups and Coding

- Weight ⇒ No. of 1's

Eg:- $x = 01000$, weight $x = 1$

$x = 011100$, weight $x = 3$

* Hamming Distance

Eg:- $x = 011$, $Y = 001$

$x \oplus y = 010$

weight $(x \oplus y) = 1$ or $|x \oplus y| = 1$

This distance blw x & Y is Hamming Distance

Encoding function

$e: B^m \rightarrow B^n$, where e is (m,n) encoding function

- Detection of errors

Let $e: B^m \rightarrow B^n$ is an encoding fn & the min. dist of e is $k+1$, then e can detect k or less errors.

If min dist e is $2k+1$ then it can correct k or less errors

* Parity Check Matrix

$H = \left[\begin{array}{c} \\ \hline \text{Identity Matrix} \end{array}\right] \begin{matrix} \} m \\ \} n \end{matrix}$

eg: $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ $\begin{matrix} \} m=2 \\ \} n=5 \end{matrix}$

$e : B^n \to B^n$

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

$e(0,0) = 00\,x_1x_2x_3$

$[x_1x_2x_3] = [0\ 0]\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

$= [0\oplus 0 \quad 0\oplus 0 \quad 0\oplus 0]$

$= [0\ 0\ 0]$

$\therefore e(0,0) = 00000$

$e(0,1) = 01\,x_1x_2x_3$

$[x_1x_2x_3] = [0\ 1]\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = [0\oplus 0 \quad 0\oplus 1 \quad 0\oplus 1]$

$[x_1x_2x_3] = [0\ 1\ 1]$

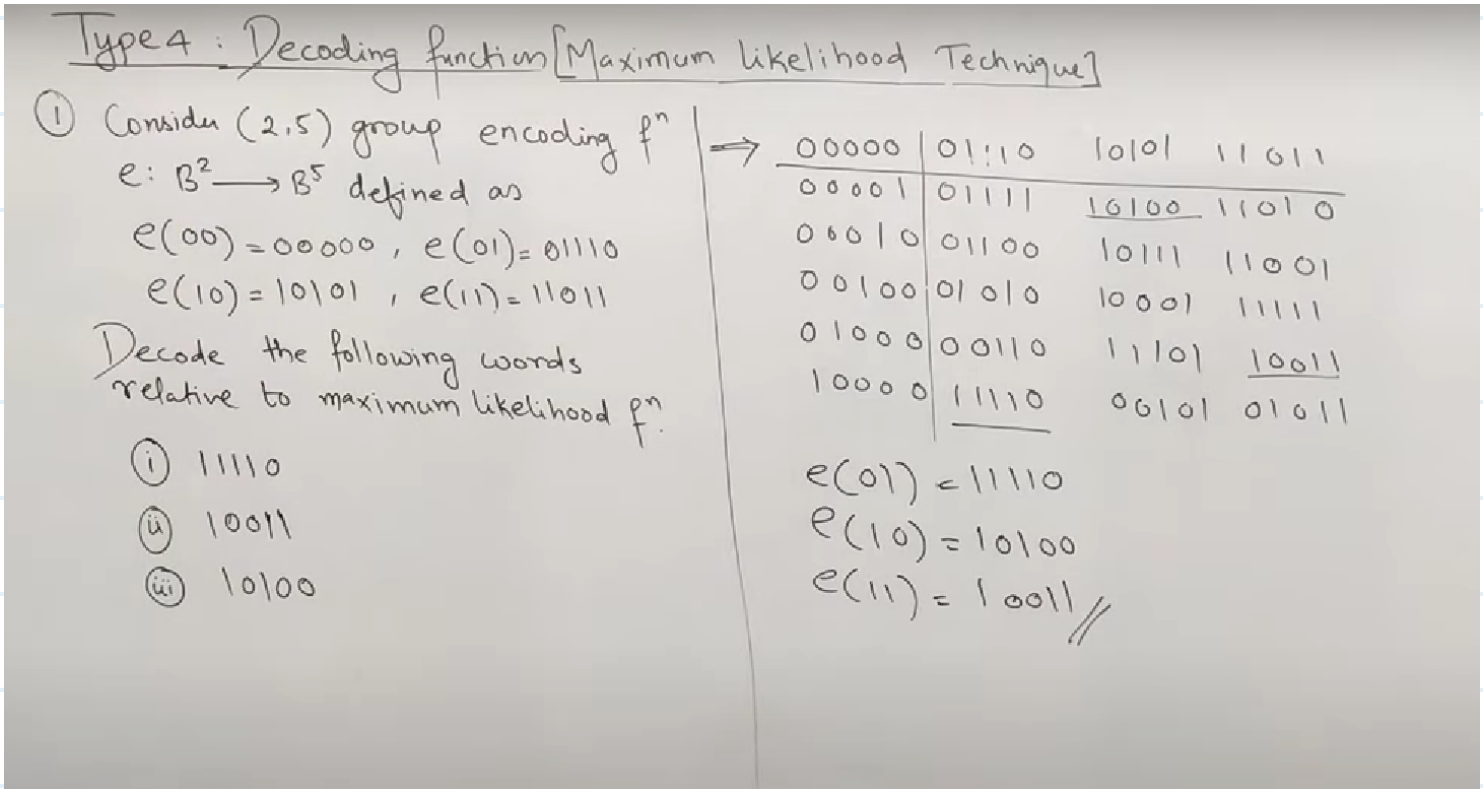
$e(01) = 01011$

Similarly,

$\therefore e(10) = 10110$

$\therefore e(11) = 11101$

* Maximum Likehood Decoding Technique



Type 4 : Decoding function [Maximum likelihood Technique]

① Consider (2,5) group encoding fn
e: $B^2 \longrightarrow B^5$ defined as
e(00) = 00000 , e(01) = 01110
e(10) = 10101 , e(11) = 11011

Decode the following words relative to maximum likelihood fn.

(i) 11110
(ii) 10011
(iii) 10100

→

00000	01110	10101	11011
00001	01111	10100	11010
00010	01100	10111	11001
00100	01010	10001	11111
01000	00110	11101	10011
10000	11110	00101	01011

e(01) = 11110
e(10) = 10100
e(11) = 10011 //