

Name - Arya Kaur
 Roll no. - 16010421067
 Batch - A2

(Q) Closure Property

a, b are integers

$$a*b = a+b+2 \in \text{Integer}$$

$$a+b \in \mathbb{Z}$$

(Closure Property satisfies)

Associative Property

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

$$b*c = b+c+2$$

$$a*b = a+b+2$$

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

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

$$a+b+c+4 = a+b+c+4$$

Hence $*$ is associative

Existence of Identity

$$a*e = a$$

$$a+e+2 = a$$

$$e = -2 \text{ is identity element}$$

Existence of Inverse

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

$$a*a^{-1} = a+a^{-1}+2 = e$$

$$a+a^{-1} = -4$$

$$a^{-1} = -4-a$$

$$a^{-1} \in \mathbb{Z}$$

Set \mathbb{Z} is a group wrt. $*$

Q2) Z_7 under addition

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Closure Property - As all elements are of table Z_7 is satisfied

Associative Property

$$\begin{aligned}1 +_7 (2 +_7 3) \\= 1 +_7 (5) \\= 6\end{aligned}$$

$$(1 +_7 2) +_7 3$$

$$= 3 +_7 3$$

$$= 6$$

$$a +_7 (b +_7 c) = (a +_7 b) +_7 c$$

Z_7 is associative

Identity

From table we can see for Z_7 identity element is 0
 $a = 0$

Inverse Property

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

From table

$$0^{-1} = 0$$

$$1^{-1} = 6$$

$$2^{-1} = 5$$

$$3^{-1} = 4$$

$$4^{-1} = 3$$

$$5^{-1} = 2$$

$$6^{-1} = 1$$

Commutative property

The table is symmetric hence it is commutative

$\therefore \mathbb{Z}_7$ is an abelian group under addition.

$$\mathbb{Z}_7 - \{0\} = \{1, 2, 3, 4, 5, 6\}$$

For multiplication

*	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

This is associative
Identity element 1 at e=1

Inverse of each

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

$$2^{-1} = 4$$

$$3^{-1} = 5$$

$$4^{-1} = 2$$

$$5^{-1} = 3$$

$$6^{-1} = 6$$

(Q3) $S = \{1, 2, 3, 4, 5, 6, 12\}$

*	1	2	3	4	6	12
1	1	2	3	4	6	12
2	2	4	6	12	12	12
3	3	6	9	12	12	12
4	4	12	12	4	12	12
6	6	6	12	12	6	12
12	12	12	12	12	12	12

Closure property since all the elements of table is closure is satisfied

Associative property

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

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

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

* is associative

(S^*) is semigroup

$1 \in S$ is identity

$(S, *)$ is monoid

(Commutative property)

$$\text{LCM}(a, b) = \text{LCM}(b, a)$$

$$a * b = b * a$$

Hence $*$ is commutative

S is commutative monoid

Q4) $\mathbb{Z}_9 - \{0\}$ Multiplication modulo

*	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	0
2	2	4	6	8	1	3	5	7	0
3	3	6	0	3	6	0	3	6	0
4	4	8	3	7	2	6	1	5	0
5	5	1	6	2	7	3	8	4	0
6	6	3	0	6	3	0	6	3	0
7	7	5	3	1	8	6	4	2	0
8	8	7	6	5	4	3	2	1	0
9	0	0	0	0	0	0	0	0	0

Closure property - Since all elements of table $\mathbb{Z}_9 - \{0\}$, closure is satisfied

$$\begin{aligned} & 3 *_9 (4 *_9 5) \\ &= 3 *_9 2 \\ &= 6 \end{aligned}$$

$$\begin{aligned} & (3 *_9 4) *_9 5 \\ & 3 *_9 5 \\ & 6 \end{aligned}$$

Hence it is associative
 $(\mathbb{Z}_9 - \{0\})$ is semigroup

Exercise of Identity from table we observe 1 is
Identity element

\mathbb{Z}_9 is monoid

(Q5) zero divisors

(R, \oplus, \otimes) is ring

if $(a \otimes b) = 0$ co-identity wrt \otimes) but $a \neq 0$ & $b \neq 0$
then a and b are said to be zero divisors

Example

Zero divisor in $(\mathbb{Z}_{15}, \oplus)$

$$2 \otimes 7 = 0$$

$$4 \otimes 7 = 0$$

Units

(R, \oplus, \otimes) is ring and 1 is identity wrt \otimes if
 b is inverse of a wrt \otimes , then a and b are
called units

Example

Unit in $\text{Ring}(\mathbb{Z}_9, \oplus)$

$$2 \cdot 5 = 1$$

2 and 5 are units of \mathbb{Z}_9

Zero divisor of \mathbb{Z}_8

$$\{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16\}$$

Unit of \mathbb{Z}_{15}

$$\{1, 5, 7, 11, 13, 17\}$$

- a) (R, \oplus, \otimes) is field if
- (R, \oplus) is commutative group
 - $(R; \oplus, \otimes)$ is a commutative group where \oplus is identity
l.v.t \oplus
 - $a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$

Ring if

(R, \oplus) is commutative

(R, \otimes) is semigroup

$$a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$$

\mathbb{Z}_7

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

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	8	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Hence $(\mathbb{Z}_7^+, +)$ and $(\mathbb{Z}_7 - \{0\}, \cdot)$ are commutative groups

\mathbb{Z}_7 is a field