DATE : / 20
PAGE No

Unit

Algebraic Structures

Group Theory

Today, It's used in a no. of areas in research & application. Using group theory, we can estimate the ~~strength~~ of a set with respect to an operator.

This idea will further help us in research field to identify the correct mathematical system to work in a particular research area. eg → can we use natural no. in complex problem area like soft computing or studying black holes.

let's define some structure of set & operator based on the properties & then check those properties on the basic number systems like natural no., integers, real no., etc.

Properties

(1) Closure property

Consider a non-empty set A & a binary operation * on A. A is said to be closed w.r.t. *, if $\forall a, b \in A$, then $a * b \in A$.

If, $a, b \in A$
then, $a * b \in A$

DATE : . / 20
PAGE No

Algebraic Structure

A non-empty set A is said to be an algebraic structure w.r.t. binary operation $*$, if A satisfy closure property w.r.t. $*$.

Natural No.	Integers	Real numbers.
$(N,+)$ ✓	$(Z,+)$ ✓	$(R,+)$ ✓
$(N,-)$ ✗	$(Z,-)$ ✓	$(R,-)$ ✓
$(N,\div)$ ✗	$(Z,\div)$ ✗	$(R,\div)$ ✗
$(N,\times)$ ✓	$(Z,\times)$ ✓	$(R,\times)$ ✓

Matrix	Even	Odd	Real − Zero
$(M,+)$ ✓	$(E,+)$ ✓	$(O,+)$ ✗	$(R-0,\times)$ ✓
$(M,\times)$ ✓	$(E,-)$ ✓	$(O,-)$ ✓	$(R-0,\div)$ ✓

(5) Associative property

Consider non-empty set A & a binary operation $*$ on A. A is said to be associative w.r.t. $*$ if, $\forall\ a,b,c \in A$ then, $(a*b)*c = a*(b*c)$

Semi-group

A non-empty set A is said to be a semigroup w.r.t. a binary operation $*$, if A satisfy closure and associative property w.r.t. $*$.

DATE : / 20
PAGE No

Natural no.	Integers	Real No.
$(N,+)$ ✓	$(Z,+)$ ✓	$(R,+)$ ✓
$(N,-)$ X	$(Z,-)$ X	$(R,-)$ X
$(N,\div)$ X	$(Z,\div)$ X	$(R,\div)$ X
$(N,\times)$ ✓	$(Z,\times)$ ✓	$(R,\times)$ ✓

Matrix	Even	Odd	Real - Zero
$(M,+)$ ✓	$(E,+)$ ✓	$(O,+)$ X	$(R-0,\times)$ ✓
$(M,\times)$ ✓	$(E,-)$ ✓	$(O,-)$ ✓	$(R-0,\div)$ X

③ **Identity Property**

Consider a non-empty set A & a binary operator $*$ on A. A is said to satisfy identity property w.r.t. $*$, if $\forall a \in A$,
there must be unique $e \in A$, such that
$a * e = e * a = a$

- There is exactly 1 identity element in set & will be same for all element in the set.

Monoid

A non-empty set A is said to be a monoid w.r.t. a binary operation $*$, if A satisfy closure, associative & identity property w.r.t $*$.

Add = $0=e$
Multiply = $1=e$

Natural	Integer	Real
$(N,+)$ ✗	$(Z,+)$ ✓	$(R,+)$ ✓
$(N,-)$ ✗	$(Z,-)$ ✗	$(R,-)$ ✗
$(N,\div)$ ✗	$(Z,\div)$ ✗	$(R,\div)$ ✗
$(N,\times)$ ✓	$(Z,\times)$ ✓	$(R,\times)$ ✓

Matrix	Even	Odd	Real - Zero
$(M,+)$ ✓	$(E,+)$ ✓	$(O,+)$ ✗	$(R-0,\times)$ ✓
$(M,\times)$ ✓	$(E,\times)$ ✗	$(O,\times)$ ✓	$(R-0,\div)$ ✗

Inverse Property

Consider a non-empty set A & a binary operation $*$ on A. A is said to satisfy inverse property w.r.t. $*$, if $\forall\, a \in A$

there must be unique element $a^{-1} \in A$, such that,

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

- Every element has exactly 1 unique inverse which is also present in the same set.
- If a is inverse of b, then b will also be inverse of a.
- No 2 elements can have same inverse.
- Identity element is its own inverse.

Group

A non-empty set A is said to be group w.r.t. a binary operator $*$, if A satisfy closure, associative, identity & inverse property w.r.t. $*$.

$a + (-a) = 0$

$a \times \frac{1}{a} = 1$

DATE : / 20
PAGE No

Natural	Integers	Real
$(N, +)$ X	$(Z, +)$ ✓	$(R, +)$ ✓
$(N, -)$ X	$(Z, -)$ X	$(R, -)$ X
$(N, \div)$ X	$(Z, \div)$ X	$(R, \div)$ X
$(N, \times)$ X	$(Z, \times)$ X	$(R, \times)$ X

Matrix	Even	Odd	Real - Zero
$(M, +)$ ✓	$(\mathcal{E}, +)$ ✓	$(O, +)$ X	$(R-0, \times)$ ✓
$(M, \times)$ X	$(\mathcal{E}, \times)$ X	$(O, \times)$ X	$(R-0, \div)$ X
(Non-singular Matrix), $\times$ ✓			

11

Conclusion

① If total no. of elements in a group is even then there exists at least one element in group who's inverse of itself.

② Sometime it's possible that every element is inverse of itself in a group.

③ In a group, $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in A$

④ **Cancelation property**

(i) $a * b = a * c \longrightarrow b = c$

(ii) $a * c = b * c \longrightarrow a = b$

$*$ is not multiplication, it's a binary operator

DATE : / 20
PAGE No

(5) Commutative property

Consider a non empty set A & a binary operation * on A. A is said to satisfy commutative property w.r.t. *, if $\forall\ a, b \in A$ such that, $a * b = b * a$.

Abelian group

A non-empty set A is said to be a abelian group w.r.t. binary operator *, if A satisfy closure, associative, identity, inverse and commutative property w.r.t. *.

Natural	Integer	Real
$(N, +)$ X	$(Z, +)$ ✓	$(R, +)$ ✓
$(N, -)$ X	$(Z, -)$ X	$(R, -)$ X
$(N, \div)$ X	$(Z, \div)$ X	$(R, \div)$ X
$(N, \times)$ X	$(Z, \times)$ X	$(R, \times)$ X

Matrix	Even	Odd
$(M, +)$ ✓	$(E, +)$ ✓	$(O, +)$ X
$(M, \times)$ X	$(E, \times)$ X	$(O, \times)$ X
(Non-singular, ×) X		

Real - Zero

$(R-0, \times)$ ✓

$(R-0, \div)$ X

DATE: / /
PAGE No

- finite group → Group with finite no. of elements.
- Order of group → denoted by, $O(G)$ = no. of elements in G.

If there is only 1 element in G, it must be an identity elements

Ques which is finite group?

{0}

+	0
0	0

Identity of + = 0

{0}

×	0
0	×

Identity of × = 1

{1}

+	1
1	2

2 isn't in group

{1}

×	1
1	1

{0,1}

+	0	1
0	0	1
1	1	2

×

{0,1}

×	0	1
0	×	×
1	×	1

multiply with 0 → ×

{-1,0,1}

+	-1	0	+1
-1	-2		
0			
+1			

-2 isn't in grp.

{-1,0,1}

×	-1	0	1
-1			
0			
1			

multiply

{-1,1}

+	-1	1
-1	-2	
1		

not in grp

{-1,1}

×	-1	1
-1	1	-1
1	-1	1

{-2,-1,0,1,2}

+	-2	-1	0	1	2
-2	-4				
-1					
0					
1					
2					

not in range.

×	-2	-1	0	1	2
-2	4				
-1					
0					
1					
2					

not in range
0 with multiply

DATE : / 20
PAGE No

$\{1, \omega, \omega^2\}$

X	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$\omega^3 = 1$

$\{-1, 1, i, -i\}$

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

$i = \sqrt{-1}$

$i^2 = -1$

Conclusion

→ It's very difficult to design finite group as with no. greater than 2 ∫ closure property fails with simple addition or multiplication.

→ So, we develop new modified addition & multiplication operators which satisfy all properties.

Addition modulo

It's a binary operator.

denoted by $+_m$

$a +_m b = a + b$ if $(a + b < m)$

$a +_m b = a + b - m$ if $(a + b \geq m)$

eg. $\{0, 1, 2, 3\}, +_4$

$m = 4$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	4-4 = 0
2	2	3	4-4 = 0	5-4 = 1
3	3	4-4 = 0	5-4 = 1	6-4 = 2

closure ✓

associative ✓

Identity ✓

Inverse ✓

DATE: / 20
PAGE No

Multiplication modulo

Binary operator denoted by $*_m$

$a *_m b = a * b$ if $(a * b < m)$

$a *_m b = (a * b) \% m$ if $(a * b \geq m)$

↓ module (remainder)

eg. $\{1,2,3,4\}, *_5$

$*_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\{0,1,2,3\}$

dues.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\{1,2,3\}$

$*_4$	1	2	3
1	1	2	3
2	2	0	
3	3		

0 isn't a group

$+_5$	1	2	3
1			
2			
3			

add^n & 0 isn't present → X

$*_4$	0	2	2
0			
2			
2			

multiply & 0 → X

$\{1,3,5,7\}$

$*_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$\{1 \text{ --- } p-1\}, \times_p$ ✓

or $\{1 \text{ --- } p-1\}, +_p$ ✓

no 0 with $\times$, and 0 must in $+$

DATE: / / 20
PAGE No

Ques Which is not true for $\{0,1,2,3,4,5\}, +_6$

a) $1^{-1}=5$ b) $2^{-1}=4$ c) $3^{-1}=6$ d) $0^{-1}=0$

→ not in range & isn't an inverse

$+_6$	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

inverse, $0^{-1}=0$, $1^{-1}=5$, $2^{-1}=4$, $3^{-1}=3$, $4^{-1}=2$, $5^{-1}=1$

Sub group

① a subset of group may or may not be a group.
if it's a group, then it's called subgroup.

② Identity element of group & its subgroup is always same.

③ Union of 2 subgroups, may or may not be a subgroup.

④ Intersection of 2 subgroups, it's always subgroup.

⑤ Lagrange's theorem → the order of a group is always exactly divisible by the order of sub group.

DATE : / 20
PAGE No

Ques $G = \{1, 3, 5, 7\}, *_8$

a) $\{0, 1\}$ b) $\{1, 3\}$ c) $\{1, 5\}$ d) $\{1, 7\}$

0 isn't in range

	1	3
1	1	3
3	3	1

	1	5
1	2	6
5	6	2

	1	7
1	1	7
7	7	1

Ques Elements in group = 84. Size of largest subgroup of group is 42.

84 can be divisible by →

1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84

Order of element

$(A, *)$ be a group, then $\forall a \in A$ order of a is denoted by $O(a)$.

(1) $O(a) = n$ (smallest +ve integer) such that $a^n = e$.

(2) Order of identity element is always one.

(3) Order of element & its inverse is always same.

(4) Order of element in an infinite group does not exist or infinite except identity.

eg.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$a^2 = a \times a$ but in this $a^2 = a * a$ any operation

$1^1 = 1$, $1^2 = 2$, $1^3 = 3$, $1^n = 0$

$a^n = e \longrightarrow$ $O(0) = 0$, $O(1) = 4$, $O(2) = 2$, $O(3) = 4$

DATE : / 20
PAGE No

Ques find order $\{1, \omega, \omega^2\}$

X	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	+1
ω^2	ω^2	+1	ω

in multiply, identity = 1.

$\omega^1 = \omega$
$\omega^2 = \omega^2$
$\omega^3 = 1$

$(\omega^2)^1 = \omega^2$
$(\omega^2)^2 = 1/\omega^3$
$(\omega^2)^3 = \omega$

$(1)^1 = 1$
$1^2 = \omega$
$1^3 = \omega^2$

$O(\omega) = 3$ $O(\omega^2) = 2$ $O(1)^1 = 1$

Generating element or generator

An element 'a' is said to be a generating elements, if every element of A is an integral power of a, i.e., every element of A can be represented using power of a.

$A = \{a^1, a^2, a^3, \dots\}$

Cyclic group

A group $(A, *)$ is said to be a cyclic group if it contains at least 1 generator.

① If element is generator, then its inverse is also generator.

② Order of a cyclic group is always the order of generating element.

Ques. $G = \{1, 2, 4, 5, 7, 8\}$, $*_{15}$ is a cyclic group. find generators.

$*_{15}$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	10	14	1
4	4	8	1	5	13	2
5	5	10	5	10	5	10
7	7	14	13	5	4	11
8	8	1	2	10	11	4

① $2^{-1} = 8$, $8^{-1} = 2$, $1^{-1} = 1$, $4^{-1} = 4$

~~so 4 generators~~

② Neither element gives whole set $\{1,2,4,5,7,8\}$

③ No cyclic group.

Number of generator

Let A be a cyclic group of order n, no. of generator in A is denoted by

$$\phi(n) = \{ n(p_1-1)(p_2-1)(p_3-1)\cdots(p_k-1) \} / (p_1 \cdot p_2 \cdot p_3 \cdots p_k)$$

Ques Order of group = 8, no. of generators.

2	8
2	4
2	1

$2 = p_k$ ↓ prime factor

$$\phi(8) = \frac{8(2-1)}{2} = 4 \times 1 = 4.$$

DATE : / 20
PAGE No

Ques $O(G) = 12$, generators $\phi = ?$

2	12
2	6
3	3
	1

$$\phi(12) = \frac{12(2-1)(3-1)}{2\times 3} = \frac{12\times 1\times 2}{2\times 3} = 4$$

Coset

Let H be a subgroup of group G & $a \in G$, then the set
$aH = \{ah \mid h \in H\}$ is called left coset of H in G
$Ha = \{ha \mid h \in H\}$ " " right " " " " "

$aH \subset G$, $Ha \subset G$, $\forall a \in G$.

- $eH = H = He$, the left & right coset of H corresponding to identity e coincide with H.

Hence, H itself is a left as well as right coset of H in G.

eg. $G = (Z, +)$ & $H = 2Z$

$\{-\infty, \dots -2, -1, 0, 1, 2, \dots \infty\}$ $\{-\infty \dots -4, -2, 0, 2, 4, \dots -\infty\}$

$H+0 = H$
$H+1 = \{-\infty \dots -3, -1, 1, 3, \dots \infty\}$
$H+2 = \{-\infty \dots -6, -4, -2, 0, 2, 4, 6 \dots \infty\} = H$

hence, repetitive,
H has only 2 cosets, i.e; H and H+1.

DATE : / 20
PAGE No

Ques. cosets of $3\mathbb{Z}$ in group $(\mathbb{Z}, +)$

$H = 3\mathbb{Z} = \{-\infty \dots -6, -3, 0, 3, 6, \dots \infty\}$

$H+0 = H = 0+H$

$H+1 = \{-\infty \dots -5, -2, 1, 4, 7, \dots \infty\} = 1+H$

$H+2 = \{-\infty, \dots -4, -1, 2, 5, 8 \dots \infty\} = 2+H$

$H+3 = \{-\infty, \dots -6, -3, 0, 3, 6 \dots \infty\} = H$

3 cosets, $\boxed{H, H+1 \text{ and } H+2.}$

Ring

A ring is an algebraic ~~structure~~ system $(R, +, \cdot)$ where R is a non-empty set & $+$ and $\cdot$ are 2 binary operations and if following conditions are satisfied:

conditions

(1) • $(R, +)$ is an abelian group.

(2) • $(R, \cdot)$ is semigroup.

(3) • operation $\cdot$ is distributive over $+$,

→ $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

→ $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$

eg. $(\mathbb{Z}, +, \times)$ is a ring.

Integral Domain

A ring becomes integral domain, if it's a commutative ring with unity & without zero divisor :-

conditions

(1) $(D, +)$ is an abelian group

(2) $(D, \cdot)$ is semigroup with commutative & with unity, without zero divisor if $a.b = 0$, then $a = 0$ or $b = 0$

DATE / 20
PAGE No

eg. $(Z, +, \times)$
$(Q, +, \times)$ (rational)
$(R, +, \times)$
$(C, +, \times)$ (complex)
$(Z, +_3, \times_3)$

$(Z, +_3, \times_3)$

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

→ abelian group

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

→ semigroup
→ commutative
→ $a \cdot b = 0$ $(a=0, b=0)$

Field

A field is an algebraic system $(R, +, \cdot)$ where R is non-empty set & $+$ & $\cdot$ are 2 binary operations & by the following conditions are satisfied —

1. $(R, +)$ is an abelian group
2. $(R, \cdot)$ is an abelian group (inverse should exist for every non-zero element)
3. The operation $\cdot$ is distributive over $+$.
   → $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$
   → $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$

eg: $(R, +, \times)$
$(Q, +, \times)$
$(Z_3, +_3, \times_3)$