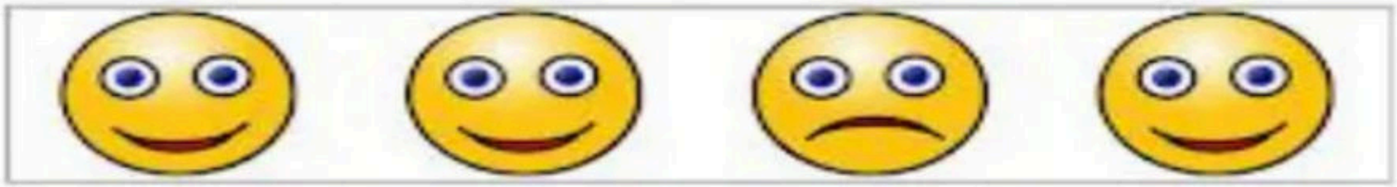
Doubt Clearing Session

Course on Discrete Mathematics for GATE 2023

Sanchit Jain • Lesson 24 • Sept 28, 2022

Find the odd one in the group



Group Theory

- Group theory is very important mathematical tool which is used in a number of areas in research and 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. E.g. can we use natural numbers in complex problem area like soft computing or studying black holes.

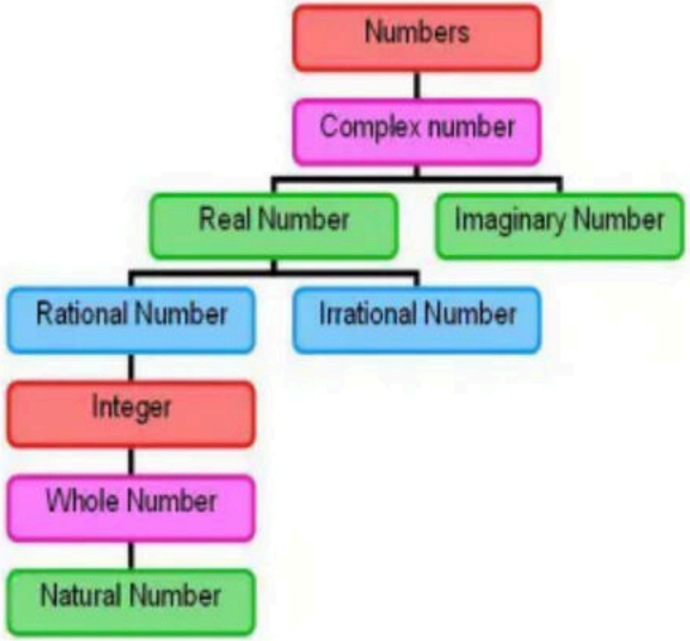
$$ds^2 = -\left(1 - \frac{2GM}{c^2 r}\right) dt^2 + \left(1 - \frac{2GM}{c^2 r}\right)^{-1} dr^2 + r^2 d\Omega^2$$

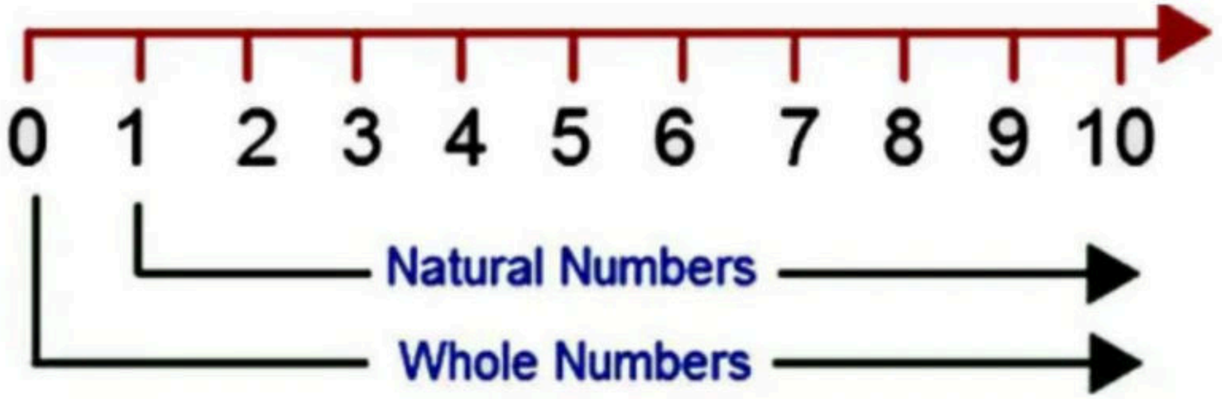
$$|\Delta F_{grav}| = \frac{2GMmd}{r_0^3}$$

$$r_{Horizon} = \frac{2GM}{c^2}$$

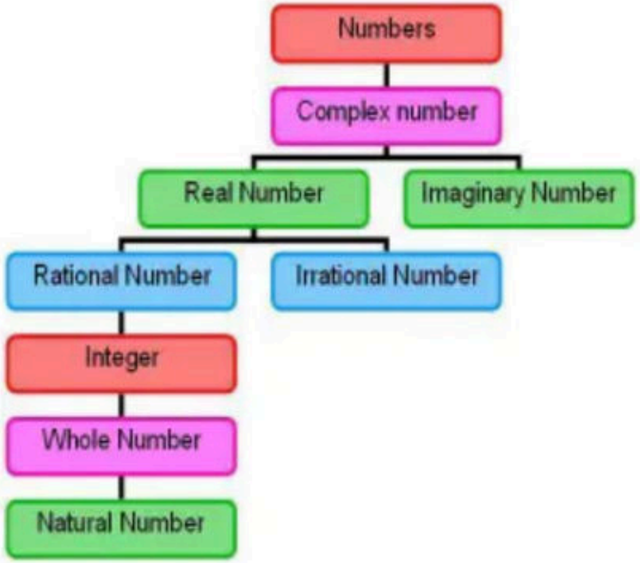
- Now we will directly study some of the basic set related properties and will define some structure of set and operator based on the properties and will check those properties on basics number systems like natural numbers, integers, real numbers etc.

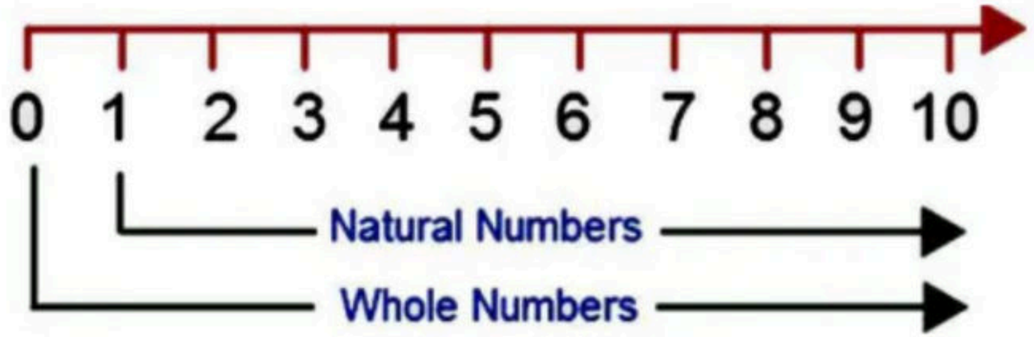
- **<u>Set of all-Natural number(N)</u>** - A natural number is a number that occurs commonly and obviously in nature. The set of natural numbers, can be defined as N = {1,2,3, 4.... ∞}



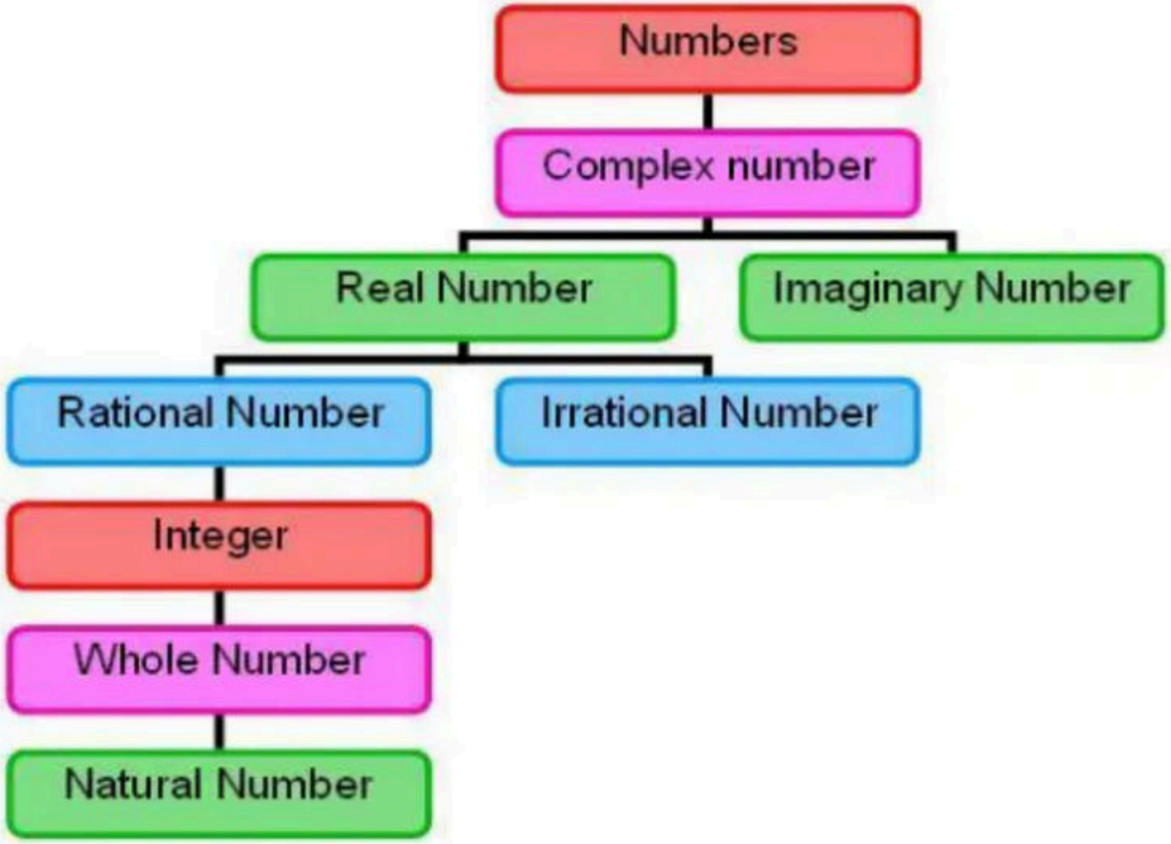


- **Set of all Integer(Z)** - An integer is a number that can be written without a fractional component.
- **Set of all Whole number(W)** - A whole number is a science expanded natural number. Set of natural number and zero





- **<u>Set of all Real number(R)</u>** - A real number is a value that represents a quantity along a continuous line, containing all of the rational numbers and all of the irrational numbers.



Break

1. **Closure property: -** Consider a non-empty set A and a binary operation * on A. A is said to be closed with respect to *, if ∀ a, b ∈ A, then a*b ∈ A.

2. **Algebraic Structure: -** A non-empty set A is said to be an algebraic structure with respect to a binary operation *, if A satisfy closure property with respect to *.

		Algebraic Structure
1	(N, +)	
2	(N, -)	
3	(N, /)	
4	(N, x)	
5	(Z, +)	
6	(Z, -)	
7	(Z, /)	
8	(Z, x)	
9	(R, +)	
10	(R, -)	
11	(R, /)	
12	(R, x)	
13	(M, +)	
14	(M, x)	
15	(E, +)	
16	(E, x)	
17	(O, +)	
18	(O, x)	
19	(R-0, x)	
20	(R-0, /)	
21	(Non-Singular Matrix, x)	

1. **Associative property**: - Consider a non-empty set A and a binary operation * on A. A is said to be associative with respect to *, if ∀ a, b, c ∈ A, then (a*b) *c = a*(b*c)

2. **Semi-Group**: - A non-empty set A is said to be a Semi-group with respect to a binary operation *, if A satisfy closure, Associative property with respect to *.

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

$\frac{1}{2} \div 3 = 1 \div \frac{2}{3}$

$\frac{1}{6} \neq \frac{3}{2}$

		Algebraic Structure	Semi Group
1	(N, +)	Y	✓
2	(N, -)	N	✗
3	(N, /)	N	✗
4	(N, x)	Y	✓
5	(Z, +)	Y	✓
6	(Z, -)	Y	✗
7	(Z, /)	N	✗
8	(Z, x)	Y	✓
9	(R, +)	Y	✓
10	(R, -)	Y	✗
11	(R, /)	N	✗
12	(R, x)	Y	✓
13	(M, +)	Y	✓
14	(M, x)	Y	✓
15	(E, +)	Y	✓
16	(E, x)	Y	✓
17	(O, +)	N	✗
18	(O, x)	Y	✓
19	(R-0, x)	Y	✓
20	(R-0, /)	Y	✗
21	(Non-Singular Matrix, x)	Y	✓

1. **Identity property: -** Consider a non-empty set A and a binary operation * on A. A is said to satisfy identity property with respect to *, if ∀ a ∈ A, there must be unique e ∈ A, such that
a*e = e*a = a

$+ \rightarrow 0$

$\times \rightarrow 1$

$\cup \rightarrow \phi$

$(Z, +)$ $\quad e \times a = a \times e = a$ $\quad . \rightarrow \in$

$\cap \rightarrow U$

2. There is exactly one Identity element in the set and will be same for all element in the set.

$\begin{bmatrix} m \end{bmatrix} \times \begin{bmatrix} \cdots \end{bmatrix} = m$

3. **Monoid: -** A non-empty set A is said to be a Monoid with respect to a binary operation *, if A satisfy closure, Associative, identity property with respect to *.

$\begin{bmatrix} \quad \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

		Algebraic Structure	Semi Group	Monoid
1	(N, +)	Y	Y	✗
2	(N, -)	N	N	✗
3	(N, /)	N	N	✗
4	(N, x)	Y	Y	✓
5	(Z, +)	Y	Y	✓
6	(Z, -)	Y	N	✗
7	(Z, /)	N	N	✗
8	(Z, x)	Y	Y	✓
9	(R, +)	Y	Y	✓
10	(R, -)	Y	N	✗
11	(R, /)	N	N	✗
12	(R, x)	Y	Y	✓
13	(M, +)	Y	Y	✓
14	(M, x)	Y	Y	✓
15	(E, +)	Y	Y	✓
16	(E, x)	Y	Y	✗
17	(O, +)	N	N	✗
18	(O, x)	Y	Y	✓
19	(R-0, x)	Y	Y	✓
20	(R-0, /)	Y	N	✗
21	(Non-Singular Matrix, x)	Y	Y	✓

1. **Inverse property: -** Consider a non-empty set A and a binary operation * on A. A is said to satisfy inverse property with respect to *, if ∀ a ∈ A, there must be unique element $a^{-1} \in A$, such that $a * a^{-1} = a^{-1} * a = e$

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

2. Every element has a exactly one unique inverse which is also present in the same set.

$M \times M^{-1} = I$

$2 \times \boxed{\frac{1}{2}} = 1$

3. If a is the inverse of b, then b will be invers one a.

4. No two elements can have the same inverse

$0 \times \square = 1$

5. Identity element is its own inverse.

$M + [M] = (:)$

6. **Group: -** A non-empty set A is said to be a group with respect to a binary operation *, if A satisfy closure, Associative, identity, inverse property with respect to *.

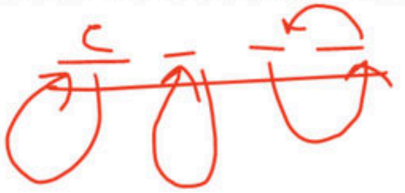
$-56 + \boxed{56} = 0$

$23 + \boxed{-23} = 0$

$42 \times \boxed{\frac{1}{42}} = 1$

		AS	Semi Group	Monoid	Group
1	(N, +)	Y	Y	N	X
2	(N, -)	N	N	N	X
3	(N, /)	N	N	N	X
4	(N, x)	Y	Y	Y	X
5	(Z, +)	Y	Y	Y	✓
6	(Z, -)	Y	N	N	X
7	(Z, /)	N	N	N	X
8	(Z, x)	Y	Y	Y	X
9	(R, +)	Y	Y	Y	✓
10	(R, -)	Y	N	N	X
11	(R, /)	N	N	N	X
12	(R, x)	Y	Y	Y	X
13	(M, +)	Y	Y	Y	✓
14	(M, x)	Y	Y	Y	X
15	(E, +)	Y	Y	Y	✓
16	(E, x)	Y	Y	N	X
17	(O, +)	N	N	N	X
18	(O, x)	Y	Y	Y	X
19	(R-0, x)	Y	Y	Y	✓
20	(R-0, /)	Y	N	N	X
21	(Non-Singular Matrix, x)	Y	Y	Y	✓

1. If the total number of elements in a group is even then there exists at least one element in the group who is the inverse of itself.



2. Some time it is also possible that every element is inverse of itself in a group.

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

4. Cancelation law holds good

   1. $a * b = a * c \rightarrow b = c$
   2. $a * c = b * c \rightarrow a = b$

1. **Commutative property: -** Consider a non-empty set A and a binary operation * on A. A is said to satisfy commutative property with respect to *, if ∀ a, b ∈ A, such that a* b = b*a

2. **Abelian Group: -** A non-empty set A is said to be a group with respect to a binary operation *, if A satisfy closure, Associative, identity, inverse, commutative property with respect to *.

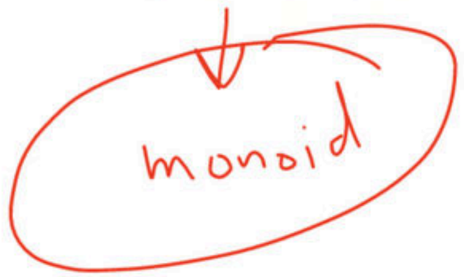
$A_1 \times A_2 = A_2 \times A_1$

		AS	SG	Monoid	Group	Abelian Group
1	(N, +)	Y	Y	N	N	✗
2	(N, -)	N	N	N	N	✗
3	(N, /)	N	N	N	N	✗
4	(N, x)	Y	Y	Y	N	✗
5	(Z, +)	Y	Y	Y	Y	✓
6	(Z, -)	Y	N	N	N	✗
7	(Z, /)	N	N	N	N	✗
8	(Z, x)	Y	Y	Y	N	✗
9	(R, +)	Y	Y	Y	Y	✓
10	(R, -)	Y	N	N	N	✗
11	(R, /)	N	N	N	N	✗
12	(R, x)	Y	Y	Y	N	✗
13	(M, +)	Y	Y	Y	Y	✓
14	(M, x)	Y	Y	Y	N	✗
15	(E, +)	Y	Y	Y	Y	✓
16	(E, x)	Y	Y	N	N	✗
17	(O, +)	N	N	N	N	✗
18	(O, x)	Y	Y	Y	N	✗
19	(R-0, x)	Y	Y	Y	Y	✓
20	(R-0, /)	Y	N	N	N	✗
21	(Non-Singular Matrix, x)	Y	Y	Y	Y	✗

Break

Q let A = {1, 3, 5, ……., ∞} and B = {2, 4, 6, ……., ∞}, what is the highest structure achieved by anyone of them?

1) (A,+) **2)** (A,*) **3)** (B,+) **4)** (B,*)



a) Algebraic Structure

b) Semi Group

c) Monoid

d) Group

Q Consider a set of natural numbers N, with respect to *, such that $a * b = a^b$ which of the following is true?

a) semi group but not monoid

b) A monoid but not a group

c) A group

d) not a semi group

N^N

A.S

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

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

$(a^b)^c = a^{b^c}$

$a^{bc} \neq a^{b^c}$

Q let {p, q, r, s} be the set. A binary operation * is defined on the set and is given by the following table:

*	p	q	r	s
p	p	r	s	p
q	p	q	r	s
r	p	q	p	r
s	p	q	q	q

Which of the following is true about the binary operation?

a) it is commutative but not associative

b) it is associative but not commutative

c) it is both associative and commutative

d) it is neither associative nor commutative

Q Consider a set of integers Z, with respect to *, such that a * b = max (a, b) which of the following is true?

a) Algebraic structure

b) semi-group

c) Monoid

d) group

Q Consider a set of integers Z, with respect to *, such that a * b = min (a, b) which of the following is true?

a) Algebraic structure

b) semi-group

c) Monoid

d) group

Q which of the following is not a group?

a) {……. -6, -4, -2, 0, 2, 4, 6, ……}, +

b) {…. -3k, -2k, -k, 0, k, 2k, 3k, ….}, + [$k \in Z$]

c) {2^n, $n \in Z$}, *

d) set of complex number, *

Q Consider the set of all integers(Z) with the operation defined as $m * n = m + n + 2, m, n \in Z$

if (z, *) forms a group, then determine the identity element

a) 0 **b)** -1 **c)** -2 **d)** 2

$m * n = m + n + 2$

$m * e = m + e + 2$ — (1) $\quad m * e = m$ (2)

$m = m + e + 2$

$e = -2$

Q Consider a set of positive rational number with respect to an operation *, such that a*b = (a.b)/3, it is known that the it is an abelian group, which of the following is not true?

a) identity element e = 3

b) inverse of a = 9/a

c) inverse of 2/3 = 6

d) inverse of 3 = 3

Break

Q The binary operator ≠ is defined by the following truth table **(GATE-2015) (1 Marks)**

Which one of the following is true about the binary operator ≠?

(A) Both commutative and associative

(B) Commutative but not associative

(C) Not commutative but associative

(D) Neither commutative nor associative

p	q	P ≠ q
0	0	0
0	1	1
1	0	1
1	1	0

Q Which of the following properties a Group G must hold, in order to be an Abelian group? **(Net Dec 2015)**

(a) The distributive property

(b) The commutative property

(c) The symmetric property

a) (a) and (b)

b) (b)

c) (a) and (b)

d) (a), (b) and (c)

Q A binary operation α on a set of integers is defined as $x * y = x^2 + y^2$. Which one of the following statements is TRUE about *? **(GATE-2013)**

(1 Marks)

(A) Commutative but not associative

(B) Both commutative and associative

(C) Associative but not commutative

(D) Neither commutative nor associative

Q Which one of the following in NOT necessarily a property of a Group? **(GATE-2009) (2 Marks)**

(A) Commutativity

(B) Associativity

(C) Existence of inverse for every element

(D) Existence of identity

Q Consider the set H of all 3 × 3 matrices of the type

$$\begin{matrix} a & f & e \\ 0 & b & d \\ 0 & 0 & c \end{matrix}$$ where a, b, c, d, e and f are real numbers and abc ≠ 0.

Under the matrix multiplication operation, the set H is **(GATE-2005) (2 Marks)**

(A) a group

(B) a monoid but not a group

(C) a semigroup but not a monoid

(D) neither a group nor a semigroup

Q Consider the set $\sum^*$ of all strings over the alphabet $\sum = \{0, 1\}$. $\sum^*$ with the concatenation operator for strings **(GATE-2003) (1 Marks)**

(A) does not form a group

(B) forms a non-commutative group

(C) does not have a right identity element

(D) forms a group if the empty string is removed from $\sum^*$

Q Which of the following is true? **(GATE-2002) (2 Marks)**

(A) The set of all rational negative numbers forms a group under multiplication.

(B) The set of all non-singular matrices forms a group under multiplication.

(C) The set of all matrices forms a group under multiplication.

(D) Both (2) and (3) are true.

Q Which of the following statements is FALSE? **(GATE-1996) (1 Marks)**

a) The set of rational numbers is an abelian group under addition

b) The set of integers in an abelian group under addition

c) The set of rational numbers form an abelian group under multiplication

d) The set of real numbers excluding zero is an abelian group under multiplication

Q Let A be the set of all non-singular matrices over real number and let $*$ be the matrix multiplication operation. Then **(GATE-1994) (2 Marks)**

a) A is closed under $*$ but $\langle A,* \rangle$ is not a semigroup.

b) $\langle A,* \rangle$ is a semigroup but not a monoid.

c) $\langle A,* \rangle$ is a monoid but not a group.

d) $\langle A,* \rangle$ is a group but not an abelian group.

Break

- **Finite Group: -** A group with finite number of elements is called a finite group.

- **Order of group: -** Order of a group is denoted by O(G) = no of elements in G
  - If there is only one element in the Group, it must be an identity element.

Q Check out which of the following is a finite group?

1- {0}, +

+	0
0	

2- {0}, *

*	0
0	

3- {1}, +

+	1
1	

4- {1}, *

*	1
1	

5- {0,1}, +

+	0	1
0		
1		

6- {0,1}, *

*	0	1
0		
1		

7- {-1, 0, 1}, +

+	-1	0	1
-1			
0			
+1			

8- {-1, 0, 1}, *

*	-1	0	1
-1			
0			
1			

Q Check out which of the following is a finite group?

9- {-1, 1}, +

+	-1	1
-1		
1		

10- {-1, 1}, *

*	-1	1
-1		
1		

11- {-2, -1, 0, 1, 2}, +

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

Q Check out which of the following is a finite group?

12- {-2, -1, 0, 1, 2}, *

*	-2	-1	0	1	2
-2					
-1					
0					
1					
2					

13- {1, ω, ω^2}, *

*	1	ω	ω^2
1			
ω			
ω^2			

14- {-1, 1, i, -i}, *

*	-1	1	i	-i
-1				
1				
i				
-i				

1. **<u>Conclusion</u>: -** it is very difficult to design finite group as with number greater than 2 closure property fails with simple addition and multiplication operation.

2. So we will try to develop new modified addition and multiplication operators with which closure and other properties can be satisfied.

Break

- **<u>Addition modulo</u>: -** addition modulo is a binary operator denoted by $+_m$ such that

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

- $a +_m b = a + b - m$ if $(a + b >= m)$

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

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

- **<u>Multiplication modulo</u>: -** Multiplication modulo is a binary operator denoted by $*_m$ such that

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

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

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

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

Q Check out which of the following is a group?

1- $\{0,1,2,3\}, +_4$

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

2- $\{0,1,2,3\}, *_4$

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

3- $\{1,2,3\}, +_4$

$+_4$	1	2	3
1			
2			
3			

4- $\{1,2,3\}, *_4$

$*_4$	1	2	3
1			
2			
3			

5- $\{0,1,2,3,4\}, +_5$

$+_5$	0	1	2	3	4
0					
1					
2					
3					
4					

6- $\{0,1,2,3,4\}, *_5$

$*_5$	0	1	2	3	4
0					
1					
2					
3					
4					

7- $\{1,2,3,4\}, +_5$

$+_5$	1	2	3	4
1				
2				
3				
4				

8- $\{1,2,3,4\}, *_5$

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

9- $\{0,1,2,3,4,5,6\}, +_7$

$+_7$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

10- $\{0,1,2,3,4,5,6\}, *_7$

$*_7$	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

11- $\{1,2,3,4,5,6\}, +_7$

$+_7$	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

12- $\{1,2,3,4,5,6\}, *_7$

$*_7$	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

13- $\{1,3,5,7\}, *_8$

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

14- $\{1,2,4,7,8,11,13,14\}, *_{15}$

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

15- $\{1,2,3,4\ldots\ldots,p-1\}, *_p$

16- $\{0,1,2,3,4\ldots\ldots,p-1\}, *_p$

17- $\{1,2,3,4\ldots\ldots,p-1\}, +_p$

18- $\{0,1,2,3,4\ldots\ldots,p-1\}, +_p$

Break

Q $\{0,1,2,3,4,5\}, +_6$ is a group which of the following is not true?

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

$+_6$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Q $\{1,2,3,4,5,6\}$, $*_7$ is a group which of the following is not true?

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

$*_7$	1	2	3	4	5	6
1						
2						
3						
4						
5						
6						

Q $\{1,3,5,7\}, *_8$ is a group which of the following is not true?

a) $1^{-1} = 1$ **b)** $3^{-1} = 3$ **c)** $5^{-1} = 5$ **d)** $7^{-1} = 7$

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

Q $\{1,2,4,7,8,11,13,14\}$, $*_{15}$ is a group which of the following is not true?

a) $2^{-1} = 8$ **b)** $4^{-1} = 4$ **c)** $7^{-1} = 13$ **d)** $11^{-1} = 14$

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

Break

Q The set {1, 2, 3, 5, 7, 8, 9} under multiplication modulo 10 is not a group. Given below are four plausible reasons. Which one of them is false? **(GATE-2006) (1 Marks)**

(A) It is not closed

(B) 2 does not have an inverse

(C) 3 does not have an inverse

(D) 8 does not have an inverse

$*_{10}$	1	2	3	5	7	8	9
1							
2							
3							
5							
7							
8							
9							

Q The set {1, 2, 4, 7, 8, 11, 13, 14} is a group under multiplication modulo 15. The inverses of 4 and 7 are respectively **(GATE-2005) (2 Marks)**

(A) 3 and 13 **(B)** 2 and 11 **(C)** 4 and 13 **(D)** 8 and 14

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

Q The following is the incomplete operation table a 4-element group.

(GATE-2004) (2 Marks)

The last row of the table is

(A) c a e b **(B)** c b a e **(C)** c b e a **(D)** c e a b

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b				
c				

Q Consider the binary operation $\oplus$ over set $Z_n = \{0, 1, 2, \ldots\ldots, n-1\}$

$a \oplus b = a + b$ if $(a + b < n)$

$a \oplus b = a + b - n$ if $(a + b >= n)$

a) it is closed

b) it does not form a group

c) it forms a group but not an abelian group

d) it is an abelian group

Break

Sub Group

1. The subset of a group may or may not be a group.
2. When the subset of a group is also a group then it is called sub group.
3. The identity element of a group and its sub group is always same.
4. Union of two subgroup may or may not be a subgroup.
5. Intersection of two subgroup is always a subgroup.
6. Lagrange's theorem: - the order of a group is always exactly divisible by the order of a sub group.

Q consider a group G = {1,3,5,7}, $*_8$ which of the following sub set of this set does not form is sub group?

a) {0,1}

$*_8$	0	1
0		
1		

b) {1,3}

$*_8$	1	3
1		
3		

c) {1,5}

$*_8$	1	5
1		
5		

d) {1,7}

$*_8$	1	7
1		
7		

e) {1,3,7}

$*_8$	1	3	7
1			
3			
7			

Q Let G be a group with 15 elements. Let L be a subgroup of G. It is known that L != G and that the size of L is at least 4. The size of L is _____. **(GATE-2014) (1 Marks)**

(A) 3 **(B)** 5 **(C)** 7 **(D)** 9

Q Let G be a finite group on 84 elements. The size of a largest possible proper subgroup of G is _____ . **(GATE-2014) (1 Marks)**

Q let (A, *) be a group of prime order, how many proper-subgroups are possible for A?

a) 0 **b)** 1 **c)** P-1 **d)** P

Break

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

1. O(a) =n (smallest positive integer), such that $a^n = e$
2. Order of identity element is always one.
3. Order of an element and its inverse is always same.
4. Order of an element in an infinite group does not exist or infinite expect identity.

Q consider a group {0,1,2,3}, $+_4$ and find the order of each element?

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

Q consider a set on cube root of unity $\{1, \omega, \omega^2\}$, * and find the order of each element?

*	1	ω	ω^2
1			
ω			
ω^2			

Q consider a set on forth root of unity {-1, 1, I, -i}, * and find the order of each element?

*	-1	1	i	-i
-1				
1				
i				
-i				

Break

Generating element or Generator: - A element ‘a’ is said to be a generating element, if every element of A is an integral power of a, i.e. every element of A can be represented using power of a.

$A = \{a^1, a^2, a^3, a^4, a^5....\}$

Cyclic group: - A group (A, *) is said to be a cyclic group if it contains at least one generator.

1. In a cyclic group if an element is a generator than its inverse will also be a generator.

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

Q consider a group {1,2,4,7,8,11,13,14}, $*_{15}$ and find the order of each element?

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

Q For the composition table of a cyclic group shown below

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

Which one of the following choices is correct?

(GATE-2009) (2 Marks)

(A) a, b are generators

(B) b, c are generators

(C) c, d are generators

(D) d, a are generators

Break

Number of generators

Lagrange's theorem: - let A be a cyclic group of order n, number of Generator in A is denoted by $\phi(n) = \{n(p_1-1)\ (p_2-1)\ (p_3-1)\ \ldots\ldots\ldots\ (p_k-1)\} / (p_1p_2p_3\ldots\ldots\ldots p_k)$

Q let G be a cyclic group, O(G) = 8, number of generators in G =?

Q let G be a cyclic group, O(G) = 12, number of generators in G =?

Q let G be a cyclic group, O(G) = 70, number of generators in G =?

Q let G be a cyclic group, O(G) = 23100, number of generators in G =?

Break

Q Let s = set of all integers. A binary operation * is defined by

$a * b = a + b + 3$

consider the following statements

S_1: (S,*) is a group

S_2: -3 is identity element of (S, *)

S_3: the inverse of -6 is 0

which of the following are true

a) Only S_1 and S_2

b) Only S_2 and S_3

c) Only S_1 and S_3

d) Only S_1 ,S_2 and S_3

Q $(D_{12}, *)$ where a*b = g.c.d of (a, b) $\forall_{a,b} \in D_{12}$ then $(D_{12}, *)$ is

a) a semigroup but not monoid

b) a monoid but not a group

c) a group

d) not a semi group

Gcd(a, b)	1	2	3	4	6	12
1						
2						
3						
4						
6						
12						

Q In a group (G, *) if a*a = a, then proof that a = e, where e is identity element of a?

Q In a group if $x' = x$ for $\forall\ a \in G$ in G, then G is an abelian group?

Q In a group (G, *) , if $(a*b)^2 = a^2 * b^2$, then prove that G is an abelian group?

Break

Q Let G be an arbitrary group. Consider the following relations on G:

- **R_1:** $\forall a, b \in G$, aR_1b if and only if $\exists g \in G$ such that $a = g^{-1}bg$
- **R_2:** $\forall a, b \in G$, aR_2b if and only if $a = b^{-1}$

Which of the above is/are equivalence relation/relations? **(GATE-2019) (2 Marks)**

(A) R_1 and R_2 **(B)** R_1 only **(C)** R_2 only **(D)** Neither R_1 nor R_2

Q There are two elements x, y in a group $(G, *)$ such that every element in the group can be written as a product of some number of x's and y's in some order. It is known that $x * x = y * y = x * y * x * y = y * x * y * x = e$ where e is the identity element. The maximum number of elements in such a group is _____. **(GATE-2014) (2 Marks)**

Q Consider the set S = {1, ω, ω2}, where ω and w^2 are cube roots of unity. If * denotes the multiplication operation, the structure (S, *) forms **(GATE-2010) (1 Marks)**

(A) A group **(B)** A ring **(C)** An integral domain **(D)** A field

A **ring** is a set R equipped with two binary operations[a] + (addition) and · (multiplication) satisfying the following three sets of axioms, called the **ring axioms**

1. R is an abelian group under addition, meaning that:
   - $(a + b) + c = a + (b + c)$ for all a, b, c in R (that is, + is associative).
   - $a + b = b + a$ for all a, b in R (that is, + is commutative).
   - There is an element 0 in R such that $a + 0 = a$ for all a in R (that is, 0 is the additive identity).
   - For each a in R there exists $-a$ in R such that $a + (-a) = 0$ (that is, $-a$ is the additive inverse of a).
2. R is a monoid under multiplication, meaning that:
   - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, c in R (that is, · is associative).
   - There is an element 1 in R such that $a \cdot 1 = a$ and $1 \cdot a = a$ for all a in R (that is, 1 is the multiplicative identity).[b]
3. Multiplication is distributive with respect to addition, meaning that:
   - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all a, b, c in R (left distributivity).
   - $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, c in R (right distributivity).

An *integral domain* is a nonzero commutative ring in which the product of any two nonzero elements is nonzero. Equivalently:

- An integral domain is a nonzero commutative ring with no nonzero zero divisors.
- An integral domain is a commutative ring in which the zero ideal {0} is a prime ideal.
- An integral domain is a nonzero commutative ring for which every non-zero element is cancellable under multiplication.
- An integral domain is a ring for which the set of nonzero elements is a commutative monoid under multiplication (because a monoid must be closed under multiplication).
- An integral domain is a nonzero commutative ring in which for every nonzero element r, the function that maps each element x of the ring to the product xr is injective. Elements r with this property are called *regular*, so it is equivalent to require that every nonzero element of the ring be regular.
- An integral domain is a ring that is isomorphic to a subring of a field. (Given an integral domain, one can embed it in its field of fractions.)

Informally, a field is a set, along with two operations defined on that set: an addition operation written as $a + b$, and a multiplication operation written as $a \cdot b$, both of which behave similarly as they behave for rational numbers and real numbers, including the existence of an additive inverse $-a$ for all elements a, and of a multiplicative inverse b^{-1} for every nonzero element b. This allows one to also consider the so-called *inverse* operations of subtraction, $a - b$, and division, a / b, by defining:

$$a - b = a + (-b),$$
$$a / b = a \cdot b^{-1}.$$

Classic definition [edit]

Formally, a field is a set F together with two binary operations on F called *addition* and *multiplication*.[1] A binary operation on F is a mapping $F \times F \to F$, that is, a correspondence that associates with each ordered pair of elements of F a uniquely determined element of F.[2][3] The result of the addition of a and b is called the sum of a and b, and is denoted $a + b$. Similarly, the result of the multiplication of a and b is called the product of a and b, and is denoted ab or $a \cdot b$. These operations are required to satisfy the following properties, referred to as *field axioms* (in these axioms, a, b, and c are arbitrary elements of the field F):

- Associativity of addition and multiplication: $a + (b + c) = (a + b) + c$, and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Commutativity of addition and multiplication: $a + b = b + a$, and $a \cdot b = b \cdot a$.
- Additive and multiplicative identity: there exist two different elements 0 and 1 in F such that $a + 0 = a$ and $a \cdot 1 = a$.
- Additive inverses: for every a in F, there exists an element in F, denoted $-a$, called the *additive inverse* of a, such that $a + (-a) = 0$.
- Multiplicative inverses: for every $a \neq 0$ in F, there exists an element in F, denoted by a^{-1} or $1/a$, called the *multiplicative inverse* of a, such that $a \cdot a^{-1} = 1$.
- Distributivity of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

This may be summarized by saying: a field has two operations, called addition and multiplication; it is an abelian group under addition with 0 as the additive identity; the nonzero elements are an abelian group under multiplication with 1 as the multiplicative identity; and multiplication distributes over addition.

Even more summarized: a field is a commutative ring where $0 \neq 1$ and all nonzero elements are invertible.

Alternative definition [edit]

Fields can also be defined in different, but equivalent ways. One can alternatively define a field by four binary operations (addition, subtraction, multiplication, and division) and their required properties. Division by zero is, by definition, excluded.[4] In order to avoid existential quantifiers, fields can be defined by two binary operations (addition and multiplication), two unary operations (yielding the additive and multiplicative inverses respectively), and two nullary operations (the constants 0 and 1). These operations are then subject to the conditions above. Avoiding existential quantifiers is important in constructive mathematics and computing.[5] One may equivalently define a field by the same two binary operations, one unary operation (the multiplicative inverse), and two constants 1 and -1, since $0 = 1 + (-1)$ and $-a = (-1)a$.[nb 1]

Q Which one of the following is false? **(GATE-1996) (2 Marks)**

(A) The set of all bijective functions on a finite set forms a group under function composition.

(B) The set {1, 2, ……., p-1} forms a group under multiplication mod p where p is a prime number

(C) The set of all strings over a finite alphabet ∑ forms a group under concatenation

(D) A subset S≠∅ of G is a subgroup of the group if and only if for any pair of element a, b ∈ S, $a * b^{-1} \in S$

Q Some group (G,o) is known to be abelian. Then, which one of the following is true for G? **(GATE-1994) (2 Marks)**

A) $g = g^{-1}$ for every $g \in G$

B) $g=g^2$ for every $g \in G$

B) $(goh)^2=g^2oh^2$ for every $g, h \in G$

D) G is of finite order