Group Theory

Lecture 1

Introduction to Abstract Algebra

Group Theory

Website : https://www.goclasses.in/

ABSTRACT ALGEBRA

INTRODUCTION TO GROUP THEORY

Group Theory

Topic 1

Introduction to Abstract Algebra

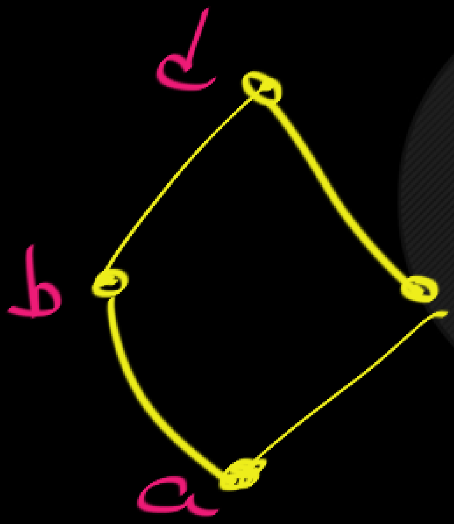
Website : https://www.goclasses.in/

Algebra: x, y, z, equations, Polynomials, $+, -, \ldots$

Abstract Algebra = Study of Abstract Structures

Abstract → ?

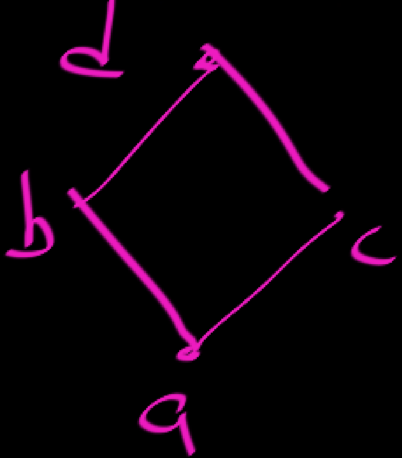
Abstract:



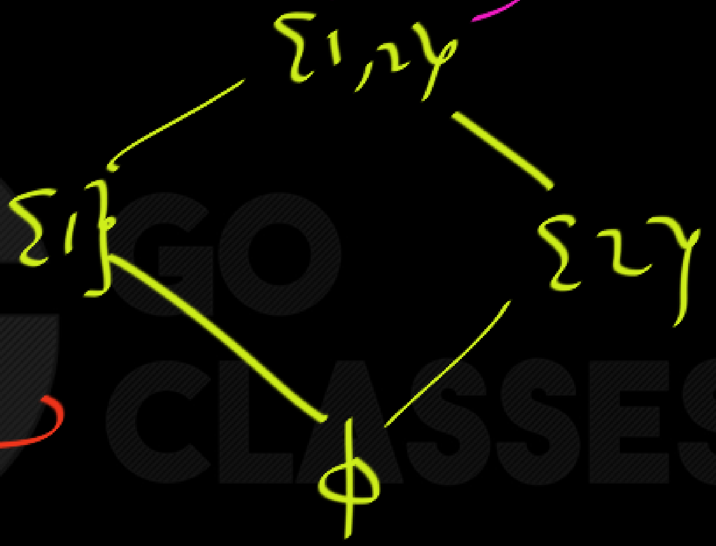
Hasse Diagram

c — **Boolean Algebra**

- Identity
- Absorption
- Distributive
- Commutative
- Complement
- De-morgan
- Idemptence



$(P\{1,2\}, \subseteq)$ — set Theory



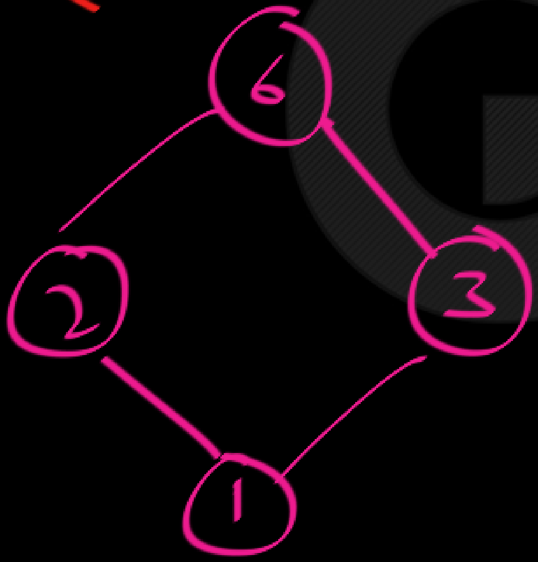
— boolean Algebra

Same Structure

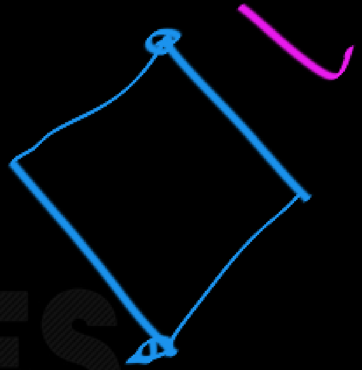
- Assoc ✓
- Comm ✓
- Distr ✓
- Demorg ✓

Number theory :

$(\{1, 2, 3, 6\}, |)$

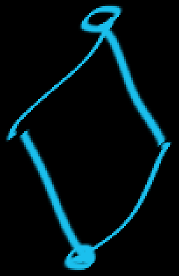


— Boolean Algebra

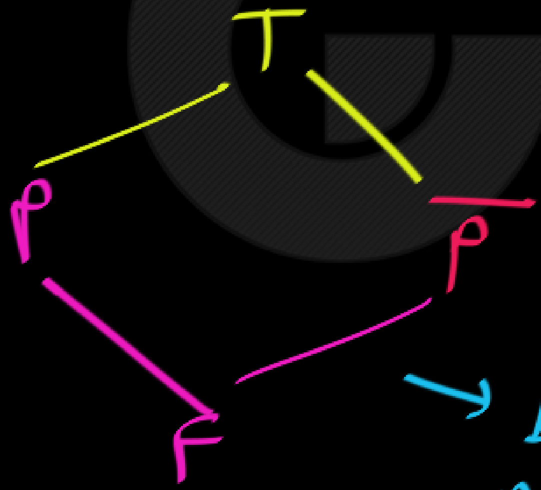


Propositional Logic :

$(\{F, T, p, \overline{p}\}, \rightarrow$ is Tautology$)$



$\equiv$



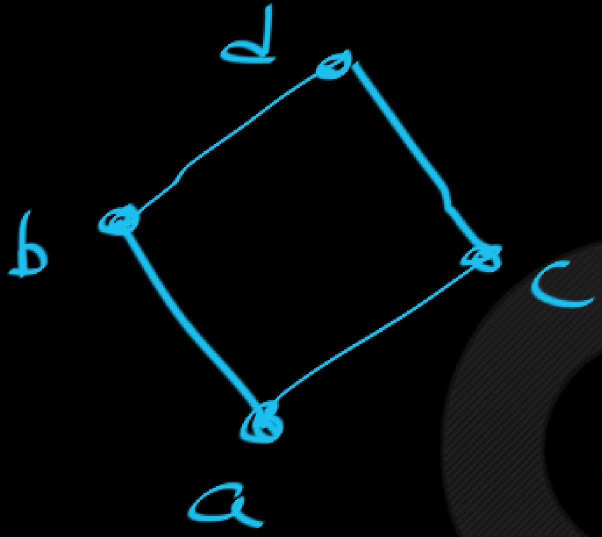
$\rightarrow$ boolean Algebra

$p, \overline{p}$ Not Comparable

$p \rightarrow \overline{p}$

$\overline{p} \rightarrow p$

Not Tauto



Abstract template

boolean Algebra

Dist

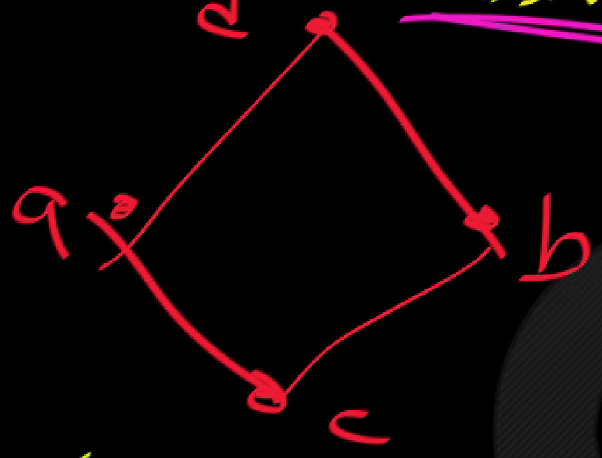
Comm

Demorgan

Abstract Concept

we will study.

Abstract

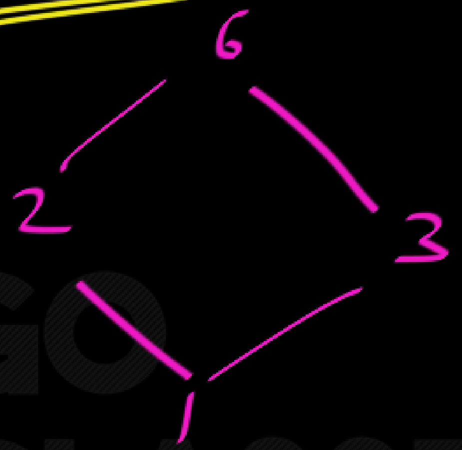


LUB $a \vee b$

GLB $a \wedge b$

Abstract

Specific



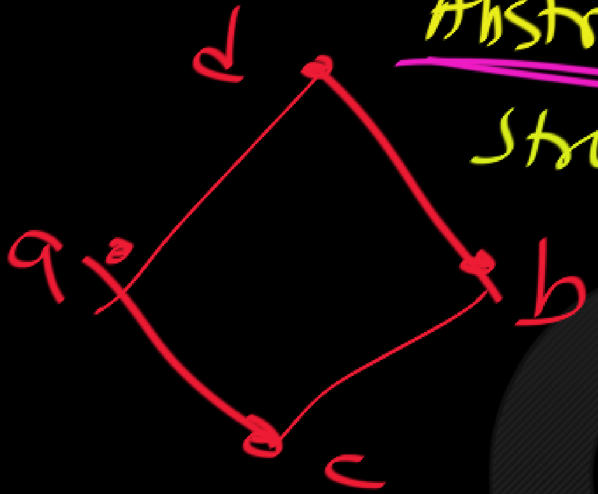
LUB = LCM

GLB = GCD

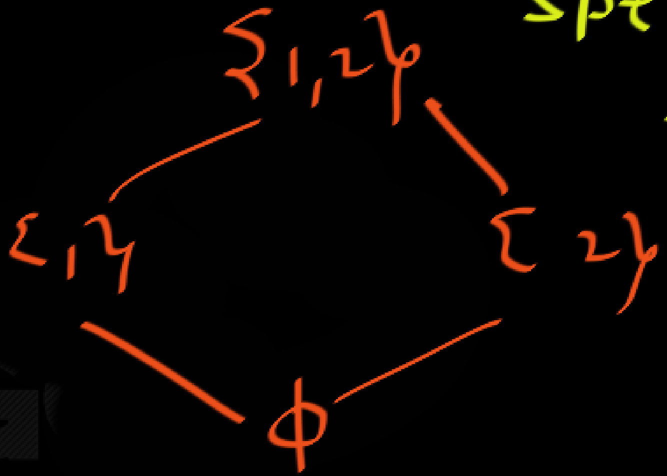
$LUB(3,2) = LCM(2,3) = 6$

$GLB(2,1) = GCD(2,1) = 1$

Abstract Structure



Specific Structure

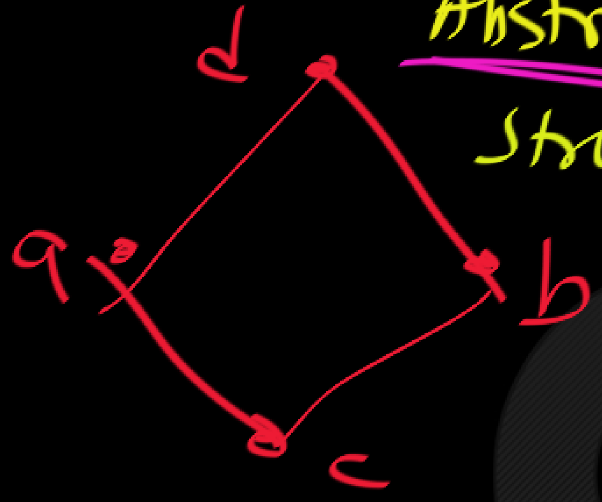


LUB $\quad a \vee b$

GLB $\quad a \wedge b$

LUB = Union

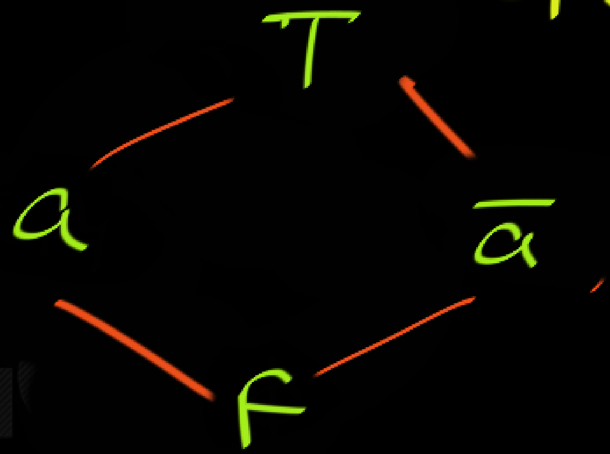
GLB = intersection



Abstract Structure

LUB $a \vee b$

GLB $a \wedge b$



Specific Structure

LUB = OR = Disjunction

GLB = AND = Conjunction

Abstract Concepts

Boolean Algebra / boolean lattice

LUB

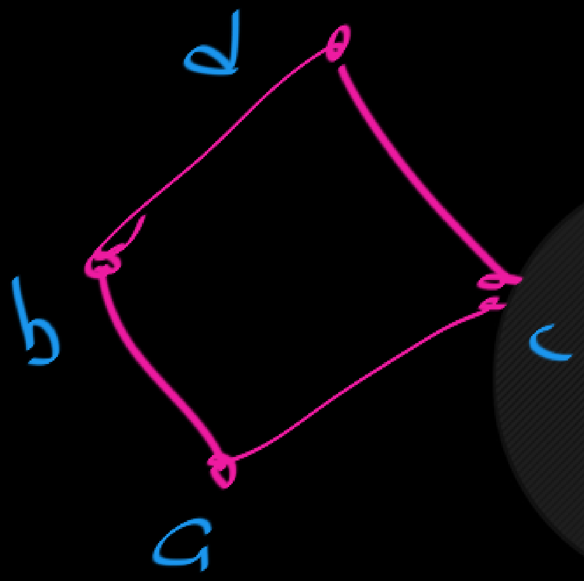
GLB

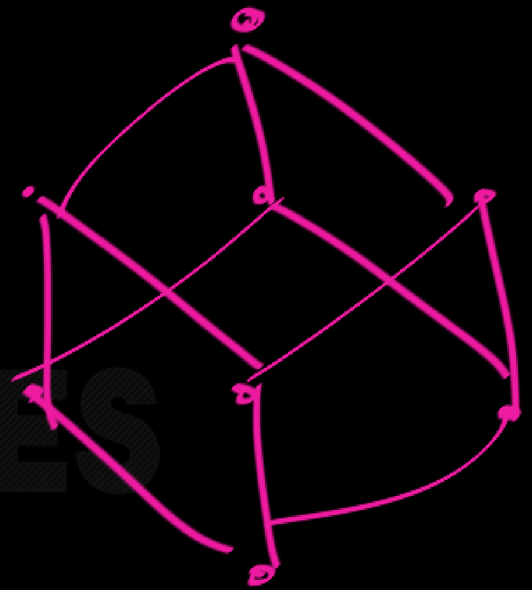
Specific Concepts

Prop. logic, set theory,

Union, intersection, LCM, GCD, AND, OR

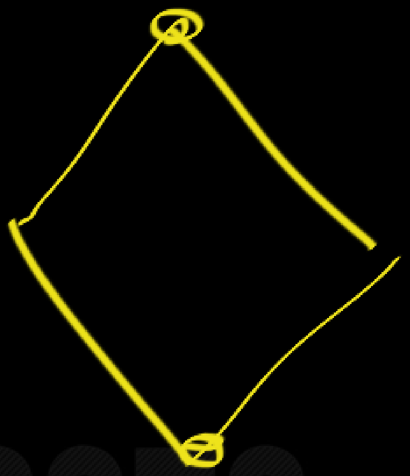
Boolean Algebra / Boolean Lattice :





Physics

Relation



Applications of Abstract Algebra

Abstract Algebra → Study of Abstract Structures

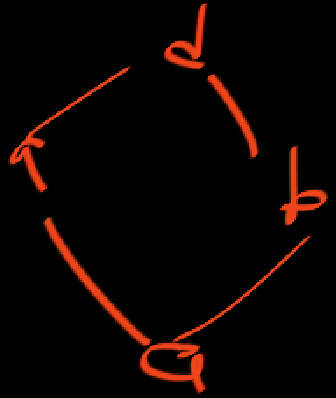
1. Chemistry
2. Physics
3. Cryptography
4. CS
5. mathematician

Google

$\boxed{\text{Group theory}}$

$(\{1, 2, 3, 6\}, |)$

$(P\{1, 2\}, \subseteq)$



$(\{T, F, a, \bar{a}\})$

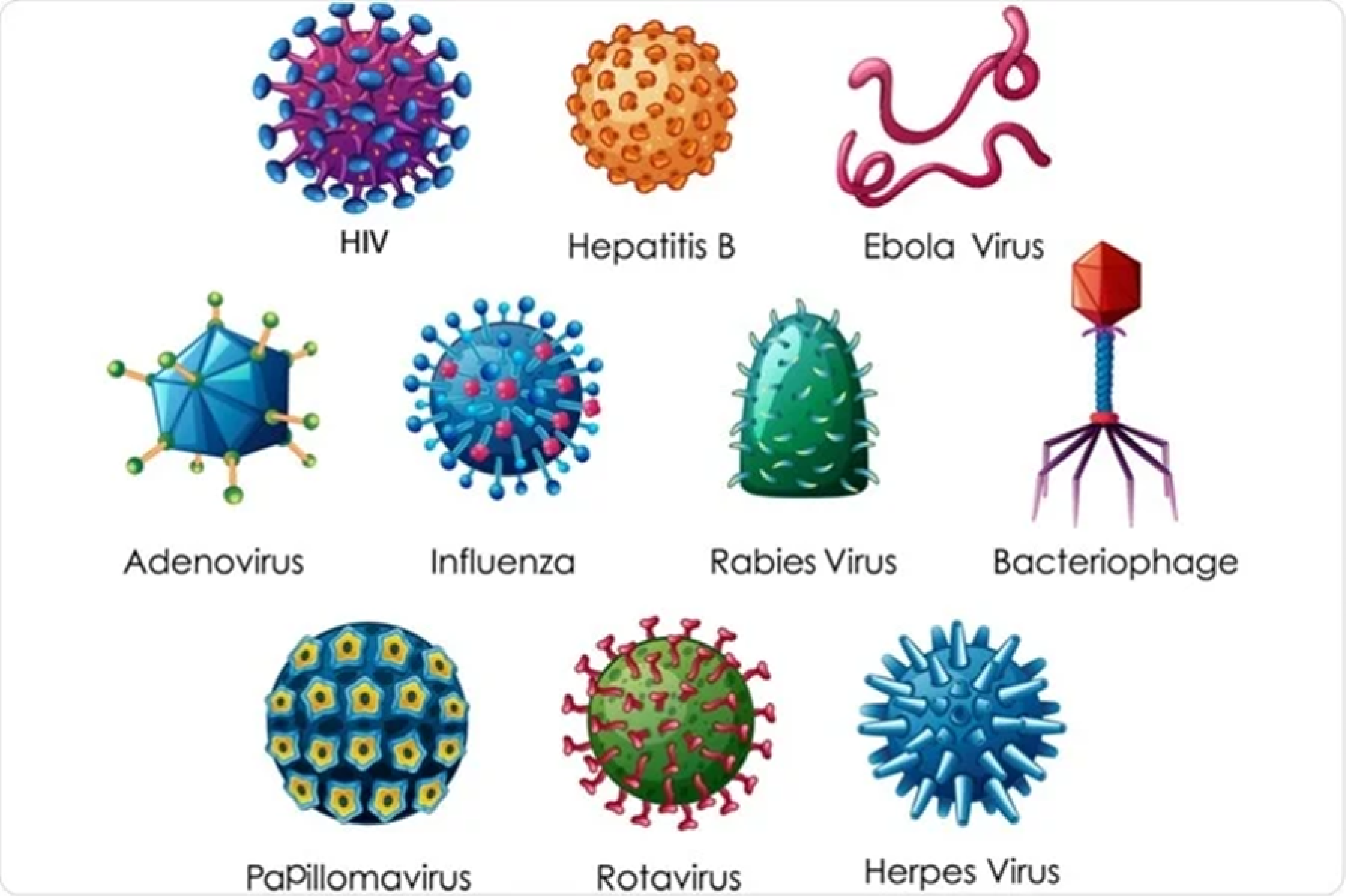
Chemistry:

Viruses — Divided in Categories based on their Structures

Abstract structure

→ Vaccine "V"

Chemistry


HIV
Hepatitis B
Ebola Virus
Adenovirus
Influenza
Rabies Virus
Bacteriophage
PaPillomavirus
Rotavirus
Herpes Virus

Abstract Algebra (AA)

1. What is AA?
2. Applications of AA
3. Why study AA
4. When did AA start?

IISc
MTech

Linear Algebra

1st class = Group, field, Ring

Abstract Algebra

Évariste Galois

गेलुआ

18 – 20 Years
Old

① linear equation:

$\boxed{ax^1 + b = 0}$ — Deg 1 Polynomial

Solution: $\boxed{x = \frac{-b}{a}}$ $a \neq 0$

Arithmetic

$x = \underbrace{+, -, \times, \div}$

② Deg ② Polynomial : (Quadratic equation)

$ax^2 + bx + c = 0 \longrightarrow$ Solution exist?

$$x = \boxed{\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$$

formula for Deg 2 polynomial

$x = (+, -, \div, \times, \sqrt{\ })$

③ Deg 3 polynomial:

$$\boxed{ax^3 + bx^2 + cx + d = 0} \rightarrow \text{formula exists}$$

Deg 4 polynomial → formula exists

formula for x = $\underbrace{+, -, \div, \times, \sqrt{\ }}$

Complex

$x = 1$

$0(x-1)\ 0(x-1)\ 0(x-1)$

Q: for Deg-5 polynomial, do we have a formula for x, in terms of $+, -, \times, \div, \sqrt{\ }$?

was open Question for 365 years.

Ans: No = Proven by Galois.

Deg-5 Polynomial

No Arithmatic "formula for x

proven by Galois

Group

"Galois":—

1. No Appreciation for his mathematics
2. Love troubles
3. political Extrimist/Activist

Galois' writings [edit]

In 1830 Galois (at the age of 18) submitted to the Paris Academy of Sciences a memoir on his theory of solvability by radicals; Galois' paper was ultimately rejected in 1831 as being too sketchy and for giving a condition in terms of the roots of the equation instead of its coefficients. Galois then died in a duel in 1832, and his paper, "*Mémoire sur les conditions de résolubilité des équations par radicaux*", remained unpublished until 1846 when it was published by Joseph Liouville accompanied by some of his own explanations.[4] Prior to this publication, Liouville announced Galois' result to the Academy in a speech he gave on 4 July 1843.[5] According to Allan Clark, Galois's characterization "dramatically supersedes the work of Abel and Ruffini."[6]

Évariste Galois

A different theory according to the The Evariste Galois Archive, particularly in their page regarding the duel, about the death of Galois is the following.

> The most likely reason is: He was weary of life, because of his unhappy love affair, his fruitless efforts for gaining recognition for his mathematical work, his financial and work situation and he felt finished up a blind alley in politics as well. So his duel was like a staged suicide.

https://hsm.stackexchange.com/questions/9/why-was-%C3%89variste-galois-killed

If he had known that his work would be of great significance to mathematics, life would have been more meaningful for him. As it was, he died a very disappointed man.

Abstract Algebra :

Study of Abstract Structures

What is Abstract Algebra?

If you ask someone on the street this question, the most likely response will be: “Something horrible to do with x, y and z”.

If you’re lucky enough to bump into a mathematician then you might get something along the lines of: “Algebra is the abstract encapsulation of our intuition for composition”.

By composition, we mean the concept of two object coming together to form a new one. For example adding two numbers, or composing real valued single variable functions.

As we shall discover, the seemly simple idea of composition hides vast hidden depth.

Abstract Algebra:

1. Lattice ✓
2. boolean Algebra ✓

Ring
field
Vector

not in GATE Syllabus

magma
semiGroup
monoid
Group

Structures

GATE Syllabus

Algebraic Structure : (AS)

(Base set , *, #, - - -)

Operations

AS

Algebraic structure:

$(Z, +)$ — GATE

$(Z, \underbrace{+, \times, -}_{\text{operations}})$ — Base set: Z

$(N, +, \times)$

(Set of matrices, product) — GATE

Algebraic Structures with Single binary operation :

GATE Syllabus

$(N, +)$, $(\{T, F\}, \wedge)$

$(N, \times)$

$(R, +)$

In mathematics, an **algebraic structure** consists of a nonempty set A, a collection of operations on A of finite arity, and a finite set of identities, known as axioms, that these operations must satisfy.

An algebraic structure is understood to be an arbitrary set, with one or more operations defined on it. And algebra, then, is defined to be the study of algebraic structures.

Algebraic Structures:

Examples of algebraic structures with a single binary operation are:

- Magma
- Quasigroup
- Monoid
- Semigroup
- Group

Group Theory

GATE Syllabus

Set Theory

Already studied

Examples involving several operations include:

- Ring
- Field
- Module
- Vector space
- Algebra over a field
- Associative algebra
- Lie algebra
- Lattice
- Boolean algebra

GATE Syllabus

Group Theory

Topic 2

Algebraic Structures with Single Binary Operation

Magma, Semi-Group, Monoid, Group

Website : https://www.goclasses.in/

Now, we will start what matters in GATE or any other exam.

Group Theory

Next Topic

Binary Operation

(The Closure Property)

Website : https://www.goclasses.in/

The Property of Closure

A set has the **closure property** under a particular **operation** if the result of the operation is always an element in the set. If a set has the **closure property** under a particular **operation**, then we say that the set is **"closed under the operation."**

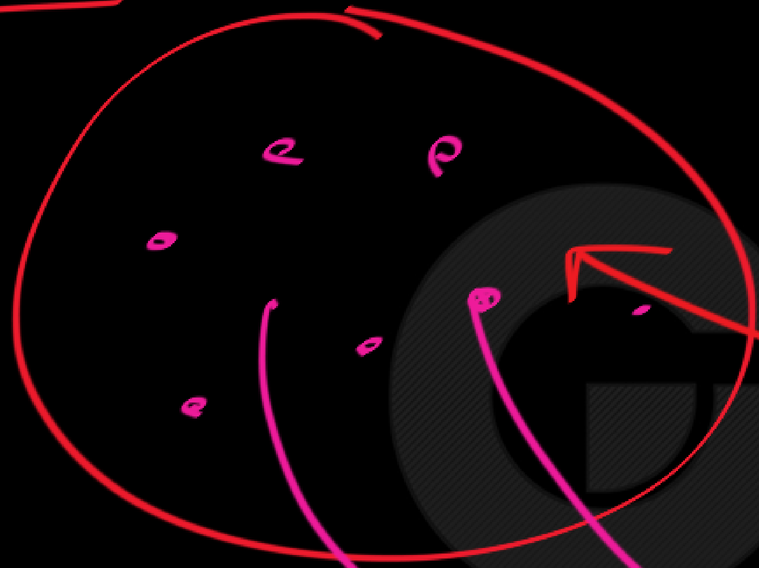
It is much easier to understand a property by looking at examples than it is by simply talking about it in an abstract way, so let's move on to looking at examples so that you can see exactly what we are talking about when we say that a set has the **closure property**:

what happens inside a set, should remain inside the set.

Set S

$(S, \#)$

Structure



$\forall a, b$

$a \# b = c$

result

Closure Property is satisfied by $(S, \#)$

$(N, +)$ — Closure property

$\forall a, b \quad a \in N, b \in N, \quad a + b \in N$

N is closed under +

N

1, 2, 3,
4, a
b

$a + b$ = result $\in N$

$(\{1, 2, 3\}, +)$ — Closure property ✗

$2 + 3 = 5 \notin$ Base set

$a = 1, b = 1$

$1 + 1 = 2 \in$ Base set $\not\Rightarrow$ Closure property

$(\{T, F\}, \wedge)$ — Closure ✓

$\{T, F\}$

F, F : $F \wedge F = F \in$ Base set

F, T : $F \wedge T = F \in$ " "

T, F : $T \wedge F = F \in$ " "

T, T : $T \wedge T = T \in$ " "

$(N, -)$ — Closed? No

$1 - 1 = 0 \notin N$

1, 2, 3, ...

$1 - 5 = -4$

$(W, -)$ — Closed ✗

$a=1,\ b=2\ ;\ 1-2=-1 \notin W$

Formal Definition:

(Set S, #) satisfy closure property

Alg. Structure

iff $\forall a, b \in S$

$a \# b \in S$

a) The set of **integers** is **closed** under the **operation** of **addition** because the sum of any two integers is always another integer and is therefore in the set of integers.

b) The set of **integers** is **not** **closed** under the **operation** of **division** because when you divide one integer by another, you don't always get another integer as the answer. For example, 4 and 9 are both integers, but 4 ÷ 9 = 4/9. 4/9 is **not** an integer, so it is **not** in the set of integers!

$(Z, \div)$ – Not closed

$a = 2, \ b = 3$ $\quad a \div b = 2 \div 3 = \frac{2}{3} \notin Z$

c) The set of **rational numbers** is closed under the operation of **multiplication**, because the product of any two rational numbers will always be another rational number, and will therefore be in the set of rational numbers. This is because multiplying two fractions will always give you another fraction as a result, since the product of two fractions a/b and c/d, will give you ac/bd as a result. The only possible way that ac/bd could not be a fraction is if bd is equal to 0. But if a/b and c/d are both fractions, this means that neither b nor d is 0, so bd cannot be 0.

d) The set of **natural numbers** is **not** closed under the operation of **subtraction** because when you subtract one natural number from another, you don't always get another natural number. For example, 5 and 16 are both natural numbers, but 5 – 16 = – 11. – 11 is **not** a natural number, so it is **not** in the set of natural numbers!

$(\{1\}, +)$ — Not Closed

$(\{0\}, +)$ — Closed ✓

$0 + 0 = 0 \in$ Base set

Base set $= \{1\}$ — element

$1 + 1 = 2 \notin$ Base set

e) The set $\{1,2,3,4\}$ is **not** **closed** under the **operation** of addition because $2 + 3 = 5$, and 5 is **not** an element of the set $\{1,2,3,4\}$.

$(\{a, b\}, *)$

$*$	a	b
a	a	$\boxed{b}$
b	a	a

operation table

means

$a*a = a$

$a*b = b$

$b*a = a$

$b*b = a$

mean

$a*b$ ✓

$b*a$ ✗

f) The set {a,b,c,d,e} has the following **operation table** for the **operation** *:

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

Closed ?

f) The set {a,b,c,d,e} has the following **operation table** for the **operation** *:

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

Closed ? ✓

$a * e = d$

$c * d = e$

$(\{1, 2\}, +)$ Make operation table?

$+$	1	2
1	2	3
2	3	4

"Not closed"

g) The set {a,b,c,d,e} has the following **operation table** for the **operation** $:

$	a	b	c	d	e
a	b	f	e	a	h
b	d	a	c	h	e
c	c	d	b	g	a
d	g	e	d	c	b
e	e	b	h	d	c

$a \$ e = h \notin$ Base set

So Not closed.

The set{a,b,c,d,e} is **not closed** under the **operation** $ because there is **at least one** result (all the results are shaded in orange) which is **not** an element of the set {a,b,c,d,e}. For example, according to the chart, a$b=f. But f is **not** an element of {a,b,c,d,e}!

"In General CS":

binary operation : two operands

$a + b$

$a * b$

unary operation : -2 → one operand

ternary operation : ? :   a ? b : c

Abstract Algebra:

binary operation "#":

$\bigcirc \# \bigcirc$

$\Rightarrow$ Closure property

is binary operation on set S

iff

(S, #) is closed.

binary operation $\equiv$ Closed operation

Definition. *Let G be a set. A* **binary operation** *is a map of sets:*

$$* : G \times G \to G.$$

For ease of notation we write $*(a, b) = a * b \ \forall a, b \in G$. Any binary operation on G gives a way of *combining* elements. As we have seen, if $G = \mathbb{Z}$ then $+$ and $\times$ are natural examples of binary operations. When we are talking about a set G, together with a fixed binary operation $*$, we often write $(G, *)$.

$(G, *)$

$*$ is binary operation iff

$\forall a, b \in G, \; a * b \in G$

$+$ is binary operation on $\{1,2\}$ $\Rightarrow$ No.

$+$ is binary operation on N. ✓

Algebraic Structure :

by definition, must be closed.

$(N, +)$ ✓ $(Z, -)$ — Not AS

$(Z, -)$ ✓

Algebraic systems

- **N = {1,2,3,4,.....∝ } = Set of all natural numbers.**
  Z = { 0, ±1, ±2, ±3, ±4 , ... ∝} = Set of all integers.
  Q = Set of all rational numbers.
  R = Set of all real numbers.
- **Binary Operation:** The binary operator * is said to be a binary operation (closed operation) on a non empty set A, if
  $a * b \in A$ for all $a, b \in A$ (Closure property).
  Ex: The set N is closed with respect to addition and multiplication
  but not w.r.t subtraction and division.
- **Algebraic System:** A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.
  Ex: (N, +), (Z, +, −), (R, +, . , −) are algebraic systems.

$(\mathbb{Z}, -)$ — Closed ✓

$\forall a, b \in \mathbb{Z}$ ✓ $a - b \in \mathbb{Z}$

$2 - 3 = -1 \in \mathbb{Z}$

$3 - 2 = 1 \in \mathbb{Z}$

"$-$" is binary operation on $\mathbb{Z}$.

$(\mathbb{Z}, -) \rightarrow$ Alg. Structure.

Group Theory

Next Topic

The Associative Property

Website : https://www.goclasses.in/

if x, y and z are variables that represent **any 3 arbitrary elements** in the set we are looking at (let's call the set we are looking at A), and the symbol # represents our operation, then the **associative property** for A with the operation # would be:

$$(x\#y)\#z = x\#(y\#z).$$

This means that the **associative property** only holds for the set A and the operation # if, **no matter what elements we take from A and put in place of *x*, *y* and *z***, $(x\#y)\#z$ will always give us the same result as $x\#(y\#z)$.

Remember that the parentheses just tell us **which pair to do first**.

$(S, \#)$ is **Associative** iff

$\forall a, b, c \in S$

$$(a \# b) \# c = a \# (b \# c)$$

Let's look at some examples so that we can understand the associative property more clearly:

First let's look at a few infinite sets with operations that are already familiar to us:

a) The set of **natural numbers** is **associative** under the operation of **addition**, because it is true that for **any** two natural numbers x, y, and z, $(x+y)+z = x+(y+z)$.

$(N, +)$ — Assoc

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

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

c) The set of **rational numbers** is **associative** under the operation of **multiplication**, because it is true that for **any** three rational numbers x, y and z, (xy)z=x(yz). (Again, notice that we don't always write out the operation symbol for multiplication. It is traditional when we write multiplication to leave the multiplication symbol out so that x×y is just written xy.)

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

d) The set of **real numbers** is **not** associative under the operation of **subtraction**, because for any three real numbers x, y and z, there are many cases where $(x - y) - z \neq x - (y - z)$! For example:

$$(2 - 5) - 12 = (-3) - 12 = -15$$

$$2 - (5 - 12) = 2 - (-7) = 2 + 7 = 9$$

$-15 \neq 9$!

So $(2 - 5) - 12 \neq 2 - (5 - 12)$

So $(x - y) - z = x - (y - z)$ is **not** true for **all** real numbers x, y and z!

$(\mathbb{R}, \div)$ — Group! — No

Real

$a = 0, b = 0$

$\frac{a}{b} = \frac{0}{0} =$ Result?

undefines

$(\mathbb{N}, \#)$ $\quad a \# b = a^2 + b$

① $\boxed{\text{Understand}}$ the operation:

$2 \# 2 = 2^2 + 2 = 6$

$1 \# 2 = 1^2 + 2 = 3$

$2 \# 1 = 2^2 + 1 = 5$

$(N, \#)$ $a \# b = a^2 + b$

① Closed? ✓ $a, b \in N$

then $a^2 \in N$, $a^2 + b \in N$

② Asso?

$\forall a, b, c$ $(a \# b) \# c \stackrel{?}{=} a \# (b \# c)$

$(a \# b) \# c \qquad a \# (b \# c)$

$(a^2 + b) \# c \qquad a \# (b^2 + c)$

$(a^2 + b)^2 + c \neq a^2 + b^2 + c$

$= a^4 + b^2 + 2a^2 b + c$

So Not Asso.

Group Theory

Next Topic

The Identity Property

Website : https://www.goclasses.in/

Identity element : Does not affect the operation.

$5 + 0 = 5$
$9 + 0 = 9$

$5 \times 1 = 5$
$9 \times 1 = 9$

$(S, \#)$

Identity element "e" :

$a \# e = a$
$e \# a = a$

Note: $(S, \#)$

Identity element "e" — fixed for all elements "a"

$\forall_a$;

$$\boxed{\begin{aligned} e \# a &= a \\ a \# e &= a \end{aligned}}$$

The Identity Property:

A set has the **identity property** under a particular operation if there is an element of the set that leaves every other element of the set **unchanged** under the given operation.

More formally, if x is a variable that represents **any arbitrary element** in the set we are looking at (let's call the set we are looking at A), and the symbol # represents our operation, then the **identity property**, for A with the operation # would be:

There is some particular element of the set A called the **identity element** (which will denote by the letter e), so that $x\#e = x$ and $e\#x = x$ for **any element of A that we plug in for the variable *x*.** (It is important to understand here that e represents a **specific fixed** element of the set A, but x represents a variable that can **change** and take on the values of **any** element of the set A.)

$(N, +)$ — No identity element

$N = \{1, 2, 3, --\}$

$e + a = a$

fixes anything $\in N$

$e \neq 1$: $1 + 2 \neq 2$

$e \neq 2$: $2 + 3 \neq 3$

$(W, +)$ — $e = 0$ fixed for all

$0 + 5 = 5$; $5 + 0 = 5$

$0 + 6 = 6$; $6 + 0 = 6$

$0 + 100 = 100$; $100 + 0 = 100$

$(\mathbb{Z}, -)$ — Closed ✓ ; Not Asso

Identity ? ✗

$e = 0$?

$a - 0 = a$ ✓

$\boxed{0 - a \neq a}$

✗

Identity e

$a \# e = a$

and

$e \# a = a$

$(\mathbb{Z}, -)$ — Not Asso

$(5-4)-3 \neq 5-(4-3)$

$-2 \neq 4$

c) The set of **natural numbers** does **not** have an identity element under the operation of **addition**, because, while it is true that for **any** whole number x, $0+x=x$ and $x+0=x$, **0** is **not** an element of the set of **natural numbers**!

d) The set of **rational numbers** does have an identity element under the operation of **multiplication**, because it is true that for **any** rational number x, $1x=x$ and $x \cdot 1=x$. So **1** is the **identity element** for the **rational numbers** under the operation of **multiplication** because it **does not change** any rational number when it is multiplied by it on the left or on the right. (Again, notice that we don't always write out the operation symbol for multiplication. It is traditional when we write multiplication to leave the multiplication symbol out so that $1\times x$ is just written $1x$.)

$(\mathbb{Q}, \times)$ — Closed ✓

— Asso ✓ (mul is Asso)

— e? $= 1$ ✓

$e = 1$ ✓

$a \times 1 = a$

$1 \times a = a$

Q: $(\mathbb{N}, \#)$ $a \# b = \max(a, b)$

① Understand operation:

$-2 \# 2$ — Nonsense

$2 \# 2 = \max(2,2) = 2$

$2 \# 1 = \max(2,1)$
$= 2$

$1 \# 2 = 2$

$(N, \#)$; $a \# b = \max(a, b)$

① Closed ✓ $a, b \in N$

then $\max(a, b) \in N$

② Asso? ✓ ✓

$(2 \# 3) \# 2$ $\quad$ $2 \# (3 \# 2)$

$= 3 \# 2 = 3$ $\quad = \quad$ $3 \Leftarrow 2 \# 3$

$(N, \#)$; $a \# b = \max(a, b)$

$e = ?$ — yes

$e = 1$? ✓

$1 \# a = a$ ✓

$a \# a = a$ ✓

$(\mathbb{Z}, \#)$ $a \# b = \max(a, b)$

$e = ?$

for 3, $e = 2$

for 2, $e = 1$

for -10, $e = -13$

wrong

fixes for all.

$(\mathbb{Z}, \#)$; $a \# b = a^2 + b$

$e = 1 = $ No

$e = 0$?

No

$0 \# 5 = 5$

$0 \# a = a$

$5 \# 0 \neq 5$

$a \# 0 \neq a$

({ $\underset{\downarrow}{\circ}$, $\underset{\downarrow}{\circ}$, $\underset{\downarrow}{\circ}$, - - - } , set difference)

set set set

({1, 2, 3}, set difference) $\Rightarrow$ Nonsense

elements

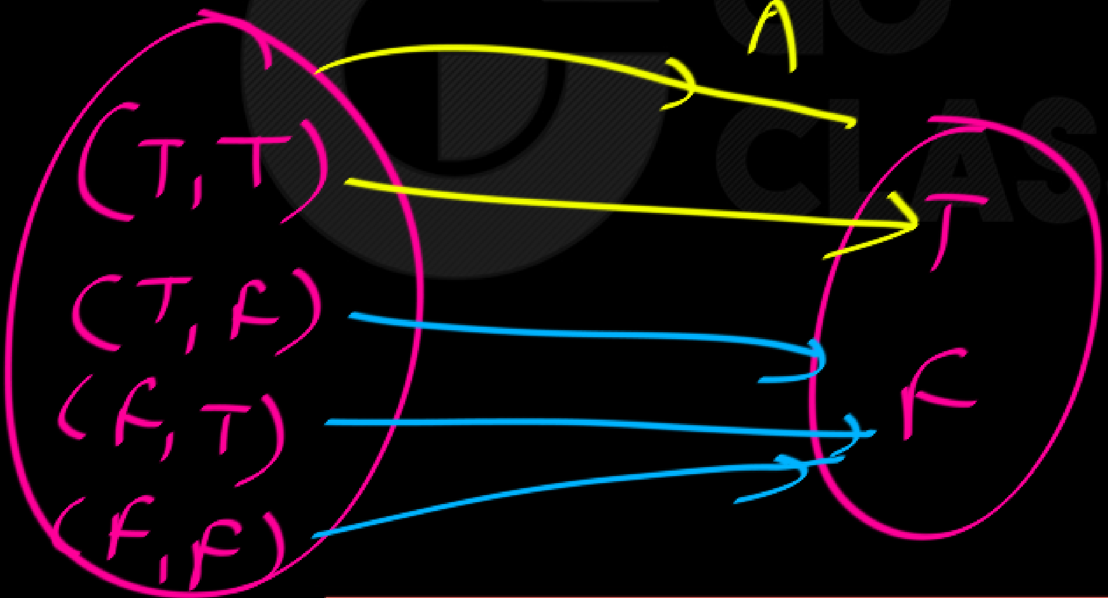
Binary operation $\Rightarrow$ mapping / function

$(S, \#)$; $\#$ is binary operation

iff $\# : \underbrace{S \times S \longrightarrow S}$

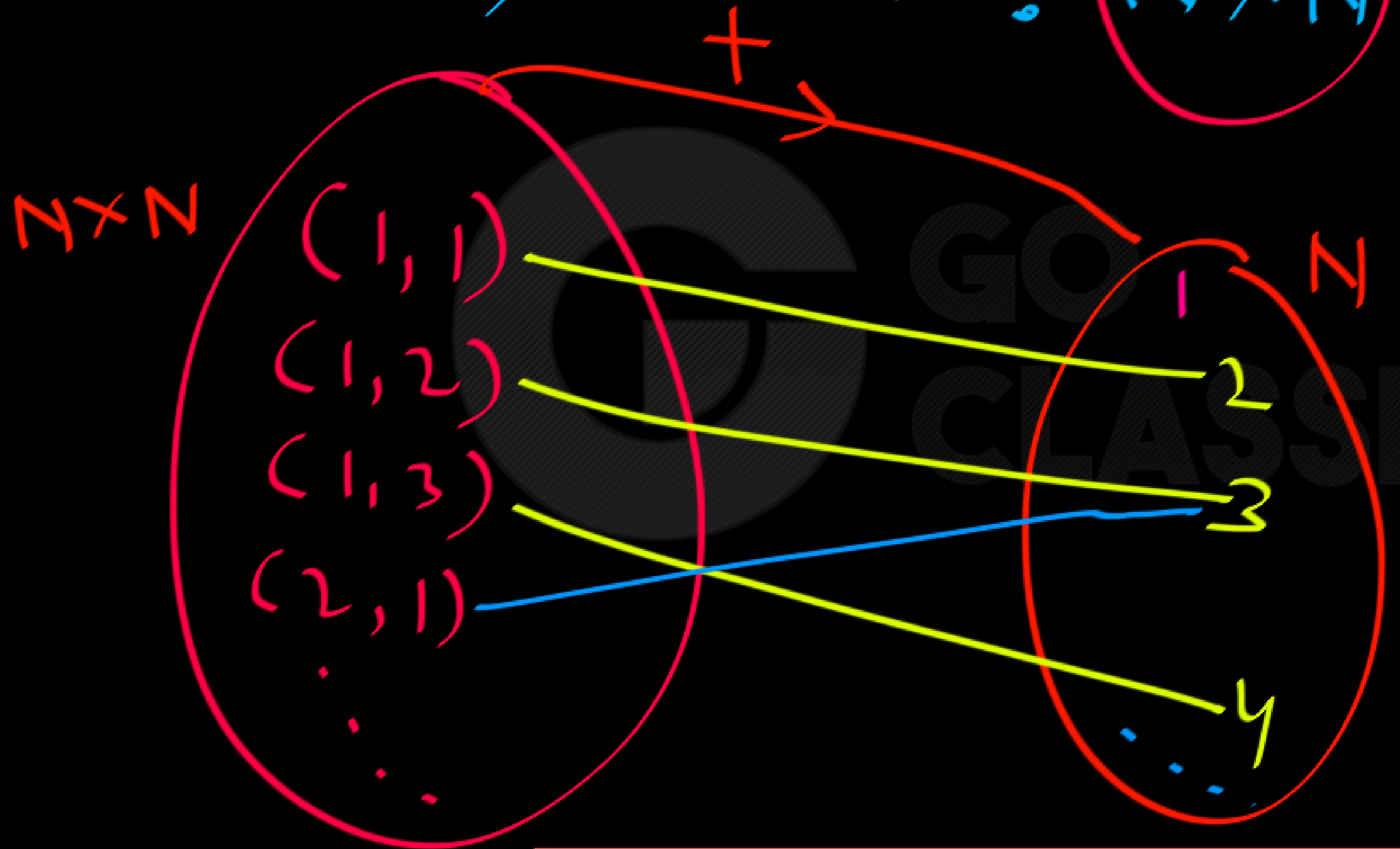
$(S = \{T, F\}, \wedge)$ binary operation

$\wedge : S \times S \to S$



$(N, +)$

$+ : N \times N \longrightarrow N$



$\#$ is binary operation on S iff

$\#: S \times S \rightarrow S$

mapping/function

How does it relate to Closure Property ?

is binary operation on S iff

$\# : S \times S \rightarrow S$

↳ mapping/function

How does it relate to closure property? $\Rightarrow$ Co-Domain is base set.

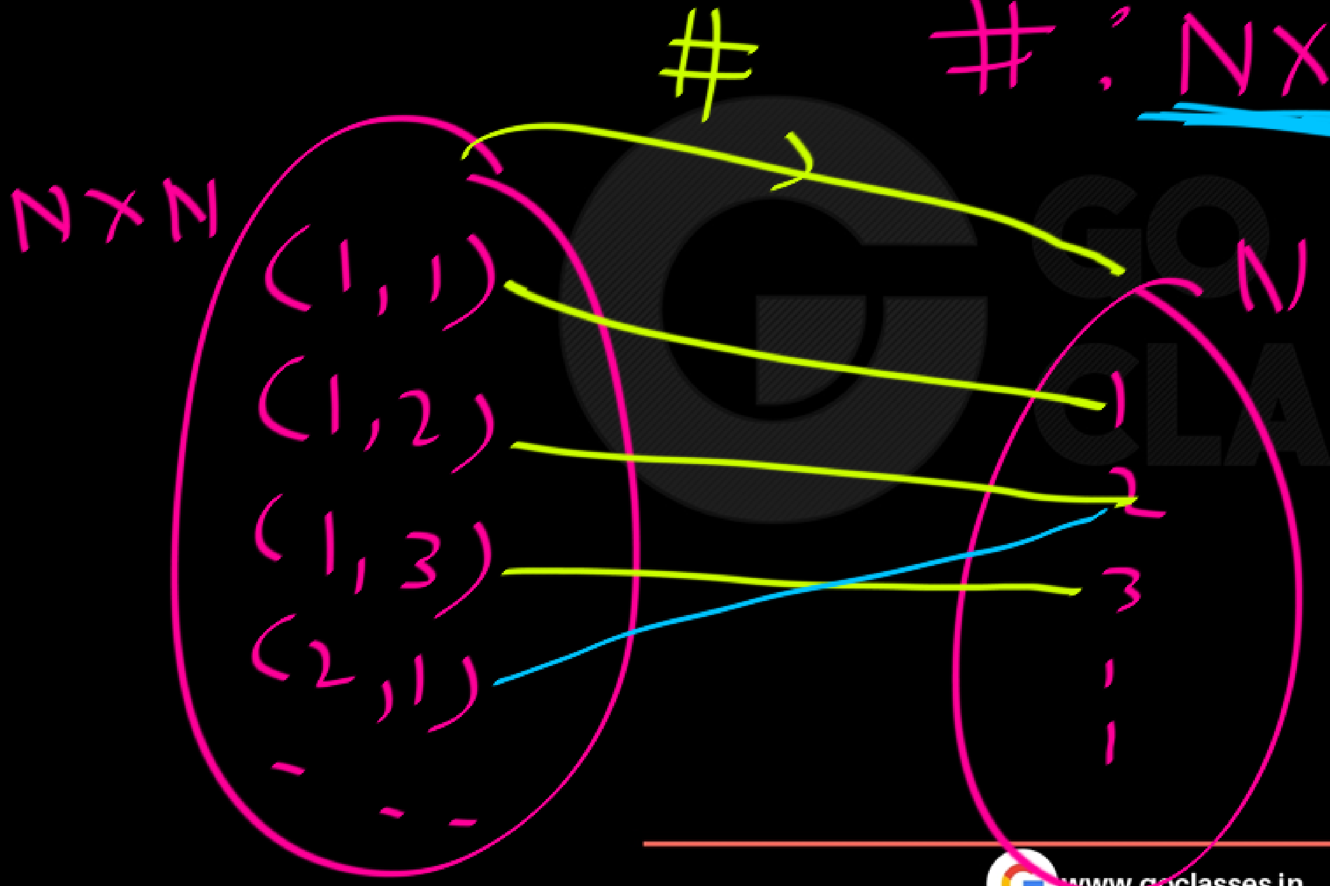
$(S, \#)$

$\# : S \times S \longrightarrow S$

(a, b)

$(N, \#)$ $\quad a \# b = \max(a, b)$

$\# : N \times N \rightarrow N$



$(a, b) \rightarrow c$

$a \in N$, $b \in N$

$c \in N$

$(N, \#)$ $\quad a \# b = \max(a, b)$

$2 \# 5 = \max(2,5) = 5$

$\#(2,5) = 5$

Same

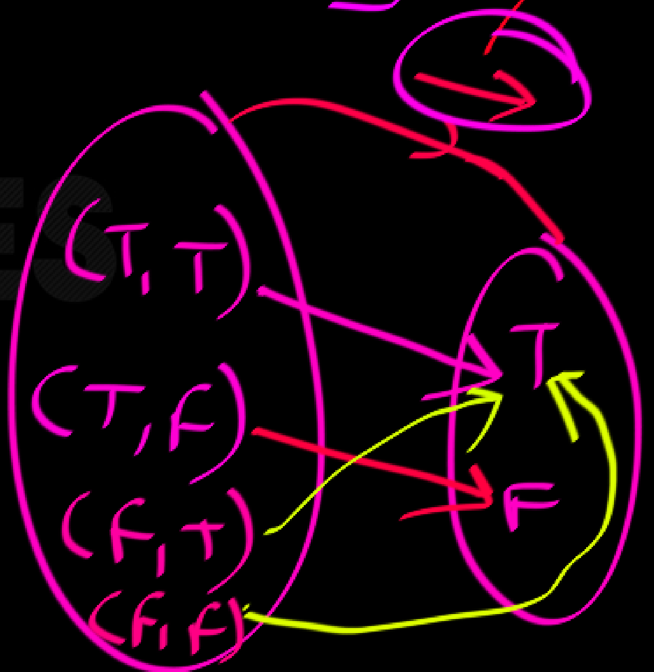
$\#(1, 100) = 100$

function from $N \times N$ to N.

$(\{T, F\}, \rightarrow)$ — Closed ✓ f

binary op^n on $\{T, F\}$

$T \rightarrow T = T$	$\rightarrow (T, T) = T$
$T \rightarrow F = F$	$f(T, T) = T$
$F \rightarrow T = T$	$\rightarrow (T, F) = F$
$F \rightarrow F = T$	$\rightarrow (F, T) = T$



Q: Set A ;

$(P(A), \setminus)$ — Closed

$P(A)$: Base Set

$\setminus$: Set Difference

$X, Y \subseteq A$

$X \setminus Y \subseteq A$?

elements in Base set = subsets of A

Base set $= P(A) \rightarrow$ elements $=$ subsets of A

$\boxed{X, Y \subseteq A}$ means $X, Y \in P(A)$

then

$X \setminus Y \subseteq A$

$(P(A), \setminus)$ — Asso! — No

set Difference

$A = \{a, b, c\}$

$P(A) = \{x \mid x \subseteq A\}$

Base set

$$\underbrace{(\{a\}-\{a\})-\{a\}}_{\phi} \overset{?}{=} \underbrace{\{a\}-(\{a\}-\{a\})}_{\{a\}}$$

$$\phi \neq \{a\}$$

$(P(A), \setminus)$

e? — No.

$e = \phi$?

$X - \phi = X$ ✓

$\phi - X \neq X$

e) The set of **real numbers** does **not** have an **identity element** under the operation of **subtraction**, because for any real number x, there is **no single** real number e such that $x - e = x$ and $e - x = x$! It is true that $x - 0 = x$ for any x, but then $0 - x \neq x$! In fact, the only thing we could put in for e that would make sure $e - x = x$ is $2x$. But then our e would **change** for each value of x.

For example, if $e=2x$:

If $x=1$, then $e=2$, but if $x=2$, then $e=4$.

So e would **not** be the **same** for **every single** element of the set of real numbers!

So we **don't** have an **identity element** for the set of **real numbers** under the operation of **subtraction**!

This means that the identity property only holds for the set A and the operation # if, **no matter what elements we take from A and put in place of *x***, *x*#e always has the result *x* and e#*x* always has the result *x*. This element e must be the **same** element for **every different** element we put in for *x*.

You should also be aware that **it is only possible to have one identity element for each set**. So if we've already found one identity element, we can stop. There won't be another one to find in that set under that particular operation.

(Notice that we **must** have e*e=e in order for e to be the identity element. The equations e**x*=*x* and *x**e=*x* **must** be true when we **plug in e for *x***, because e is one of the elements of the set we are looking at, and **every single element** of the set must make the equations true!)

Let's look at a few simple sets with operation tables and check to see if they have the identity property.

f) Here is an operation table for the set {a,b,c} and the operation *:

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

From the table we can see that:

a*a=a   a*a=a

a*b=b   b*a=b

a*c=c   c*a=c

So the element a must be our **identity element** because a*x=x and x*a=x for every element of the set {a,b,c} that we put in for x! The element a **doesn't change** any element that it operates on with the operation *! So the set {a,b,c} under the operation * defined by the operation table above does have the **identity property**!

g) Here is an operation table for the set {a,b,c} and the operation ~:

~	**a**	**b**	**c**
a	c	c	b
b	c	a	a
c	b	a	b

Remember, in order to be the **identity element**, an element must leave **every** single element in the set {a,b,c} **unchanged** both when it operates on it from the left **and** when it operates on it from the right!

a~a=c So a~a≠a! a~a=c So a~a≠a!

a~b=c So a~b≠b! b~a=c So b~a≠b!

a~c=b So a~c≠c! c~a=b So c~a≠c!

So the element a cannot be the **identity element**, because it **changes** every single element when it acts on it with the operation~!

b~a=c So b~a≠a! a~b=c So a~b≠a!

b~b=a So b~b≠b! b~b=a So b~b≠b!

b~c=a So b~c≠c! c~b=a So c~b≠c!

So the element b cannot be the **identity element**, because it changes every single element when it acts on it with the operation~!

$c \sim a = b$ So $c \sim a \neq a$! $a \sim c = b$ So $a \sim c \neq a$!

$c \sim b = a$ So $c \sim b \neq b$! $b \sim c = a$ So $b \sim c \neq b$!

$c \sim c = b$ So $c \sim c \neq c$! $c \sim c = b$ So $c \sim c \neq c$!

So the element c cannot be the **identity element**, because it **changes** every single element when it acts on it with the operation~!

So there is **no identity element** for this set {a,b,c} under the operation ~ represented by the table above!