Group Theory

Recap

Algebraic Structures with Single Binary Operation

[Set with Single Binary(Closed) Operation]

Algebraic Structure (Algebraic System):

- **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.

The algebraic structure is a type of non-empty set G which is equipped with one or more than one binary operation. Let us assume that * describes the binary operation on non-empty set G. In this case, (G, *) will be known as the algebraic structure. (1, -), (1, +), (N, *) all are algebraic structures.

(R, +, .) is a type of algebraic structure, which is equipped with two operations (+ and .)

In GATE Syllabus, We only have Algebraic Structures with Single Binary Operation.

Algebraic Structures with Single Binary Operation:

Magma/Groupoid
Semi Group
Monoid
Group
Abelian Group

In GATE Syllabus, We only have Algebraic Structures with Single Binary Operation.

Binary Operation == Closed Operation == Closure Property

Binary Operations

The formal definition of a group uses the notion of a *binary operation*. A *binary operation* $*$ on a set A is a map $A \times A \to A$, written $(a, b) \mapsto a * b$. Examples include most of the standard arithmetic operations on the real or complex numbers, such as addition $(a+b)$, multiplication $(a \times b)$, subtraction $(a-b)$. Other examples of binary operations (on suitably defined sets) are exponentiation a^b (on the set of positive reals, for example), composition of functions, matrix addition and multiplication, subtraction, vector addition, vector procuct of 3-dimensional vectors, and so on.

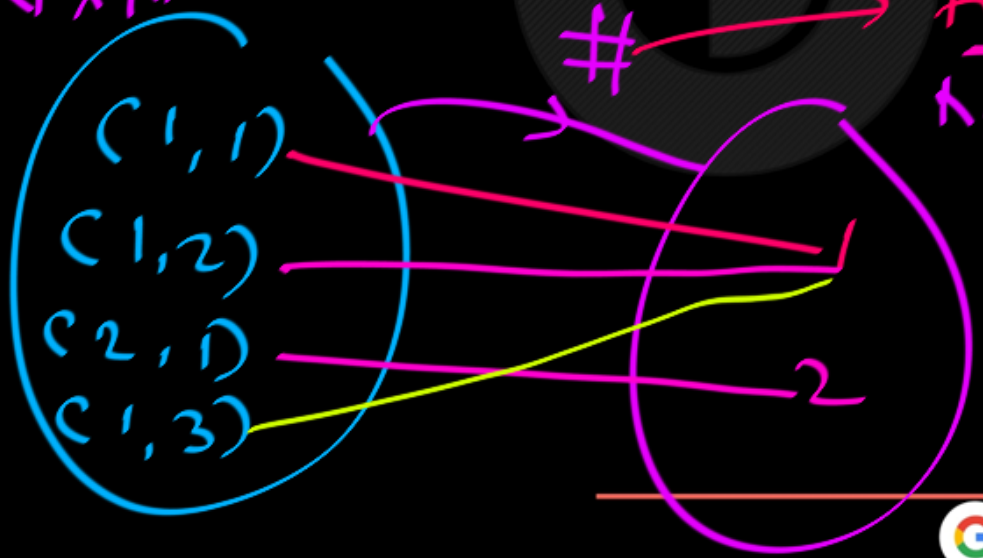
Eg: $(\mathbb{N}, \#)$

$\#$: binary op^n

$\# : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$\#(a, b) = a^b$

$\mathbb{N} \times \mathbb{N}$



$\#$ → function

$\mathbb{N}$

$(\mathbb{N}, \#)$

Base set

binary opn

a, b

$a \# b = a^b$

$2 \# 1 = 2 \; ; \; 1 \# 2 = 1$

Note: binary operation:

$$\# : A \times A \longrightarrow A$$

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

Base set: A

$(A, \#)$ structure

Q. Which of the following is/are Binary Operation on N?

1. +
2. -
3. *
4. /
5. <=
6. <
7. =

Q. Which of the following is/are Binary Operation on N?

1. +
2. -
3. *
4. /
5. <=
6. <
7. =

2 − 3 = −1 ∉ N

2/3 ∉ N

Boolean op^n / logical operations

Closed op^n

N × N → N

$(N, =)$ — Not Alg. Structure

$a = 2, \quad b = 3$

$a = b$ = false $\notin N$

equality in maths

$==$

Not in mathematics

$=$

↳ Assignment in C

Q: Base set = {T} — True

Which op^n is binary op^n?

① $\wedge$

② $\vee$

③ $\rightarrow$

④ $\leftrightarrow$

⑤ $\uparrow$

⑥ $\downarrow$

⑦ $+$

Q: Base set = {T} — True

Which op^n is binary op^n?

① $\wedge$ $T \wedge T = T$

② $\vee$ $T \vee T = T$

③ $\rightarrow$ $T \rightarrow T = T$

④ $\leftrightarrow$ $T \leftrightarrow T = T$

⑤ $\downarrow$

⑥ $\uparrow$ $T \uparrow T = F \notin$ Base set

⑦ $\oplus$ $T \oplus T = F \notin$ Base set

Which is Closes ?

Base set = $\{T\}$

(1) $(\{T\}, \wedge)$ $T \wedge T = T \in$ Base set

(2) $(\{T\}, \vee)$ $T \vee T = T \in$ " "

(3) $(\{T\}, \rightarrow)$ $T \rightarrow T = T \in$ " "

(4) $(\{T\}, \oplus)$ $T \oplus T = F \notin$ Base set

Note: Set S is "NOT closed" under #

iff

$\exists\, a, b$ such that $a \# b \notin S$

Same or different

Note: $(S, *)$ is **Not Closed** iff

$\exists a, b \in S$ such that $a * b \notin S$.

Eg: $(\{0, 1\}, \text{Addition})$

$a = 1; b = 1;$ $a + b = 1 + 1 = 2 \notin S$

$(\{0,1\}, +)$ — addition

— Not Closed

$0 + 0 = 0 \in$ Base Set

$0 + 1 = 1 \in$ " "

$1 + 0 = 1 \in$ " "

$1 + 1 = 2 \notin$ " "

So Not Closed

Not Closed

$\exists a, b \quad a+b \notin$ Base set

$a=1, b=1$

Definition A binary operation $*$ on a set A is *associative* if $a * (b * c) = (a * b) * c$ $\forall a, b, c \in A$.

Addition and multiplication (of numbers and matrices) are associative. Examples of nonassociative binary operations are subtraction (of anything), exponentiation of positive reals, and vector product.

Definition An *identity* for a binary operation $*$ on a set A is an element $e \in A$ such that $e * a = a = a * e$ $\forall a \in A$.

Examples are 0 for addition of numbers, 1 for multiplication of numbers, the identity $n \times n$ matrix for matrix multiplication. Not all binary operations have identities, however: an example is subtraction of numbers.

Q: Associative? Base set = {T, F}

1. $\wedge$
2. $\vee$
3. $\rightarrow$
4. $\leftrightarrow$
5. $+$
6. $\uparrow$
7. $\downarrow$

Q: Associative? Base set = {T, F}

1. ∧
2. ∨
3. ↓
4. ↔
5. +
6. ↑
7. →

Will Explore in Digital topic

Note: "$\rightarrow$" is Not Associative.

$$(F \rightarrow T) \rightarrow F \neq F \rightarrow (T \rightarrow F)$$

$$T \rightarrow F \qquad F \rightarrow F$$

$$F \neq T$$

↑ NAND:

$$(a \uparrow b) \uparrow c \stackrel{?}{=} a \uparrow (b \uparrow c)$$

$$\overline{ab} \uparrow c \qquad a \uparrow \overline{bc}$$

$$\overline{\overline{ab}\, c} \neq \overline{a\, \overline{bc}}$$

Which is Associative?

(1) $(\{T, F\}, \wedge)$

(5) $(\{T, F\}, \oplus)$

(2) $(\{T, F\}, \vee)$

(3) $(\{T, F\}, \rightarrow)$ Not Asso ; $(F \rightarrow T) \rightarrow F = F$

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

(4) $(\{T, F\}, \leftrightarrow)$

Which Satisfies Is property?

① $(\{T, F\}, \vee)$ $e = F$

② $(\{T, F\}, \uparrow)$ $e =$ DNE

③ $(\{T, F\}, \wedge)$ $e = T$

④ $(\{T, F\}, \downarrow)$ $e =$ DNE

⑤ $(\{T, F\}, \rightarrow)$ $e =$ DNE

⑥ $(\{T, F\}, \leftrightarrow)$ $e = T$ ✓

⑦ $(\{T, F\}, \oplus)$ $e = F$

Q: Identity Property ? Base Set = {T, F}

(1) $\wedge$

(2) $\vee$

(3) $\rightarrow$

(4) $\leftrightarrow$

Q: Identity Property ? Base Set = {T, F}

① $\wedge$

$e = T$

③ $\rightarrow$

$e \neq F$

$e \neq T$

$F \rightarrow F \neq F$

$F \rightarrow T \neq F$

② $\vee$

$e = F$

④ $\leftrightarrow$

$e = T$

$e \leftarrow \begin{matrix} T \leftrightarrow F = F \\ T \leftrightarrow T = T \end{matrix}$

Q: Identity Property ? Base set = {T, F}

1 ⊕ ⇒ e = f

2 ↑

⊕ e = f

f ⊕ T = T

f ⊕ f = f

↳ e

$\uparrow$:

$e = F$ ✗ $\quad F \uparrow F \neq F$

$e = T$ ✗ $\quad T \uparrow T \neq T$

$\downarrow$

$e = F$ ✗

$F \downarrow F \neq F$

$e = T$ ✗

$T \downarrow T \neq T$

Note: In Group Theory, for any "proof" Just Apply the Definition.

Group Theory

Next Topic

The Identity Property

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

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.)

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!)

Q: Can we have more than one Identity element?

Q: Can we have more than one Identity element? ⇒ No

Proof: Assume e, f are two Identity element.

$e = I_d$ so

$e \# f = f$

$f = I_d$ so

$e \# f = e$

$e \# f = e = f$

So we can not have > 1 Id. element.

$(S, \#)$

$Id : e \in S$

$\forall_{a \in S}$, $e \# a = a$

$a \# e = a$

$e \# e = e$

NOTE:

In EVERY Closed Structure, There is At Most One Identity Element.

Or

If there is Identity element then it is Unique.

$(N, +)$ — $e = 0$ DNE

$(Z, +)$ — $e = 0$ — Unique

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

find Id element ?

↳ Does not affect Operation.

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

find Id element ?

e = a ✓

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

b * a = b
c * a = c

Does not affect

e = b ?× b * a ≠ a

e = c ?× c * a ≠ a

Operation.

From the table we can see that:

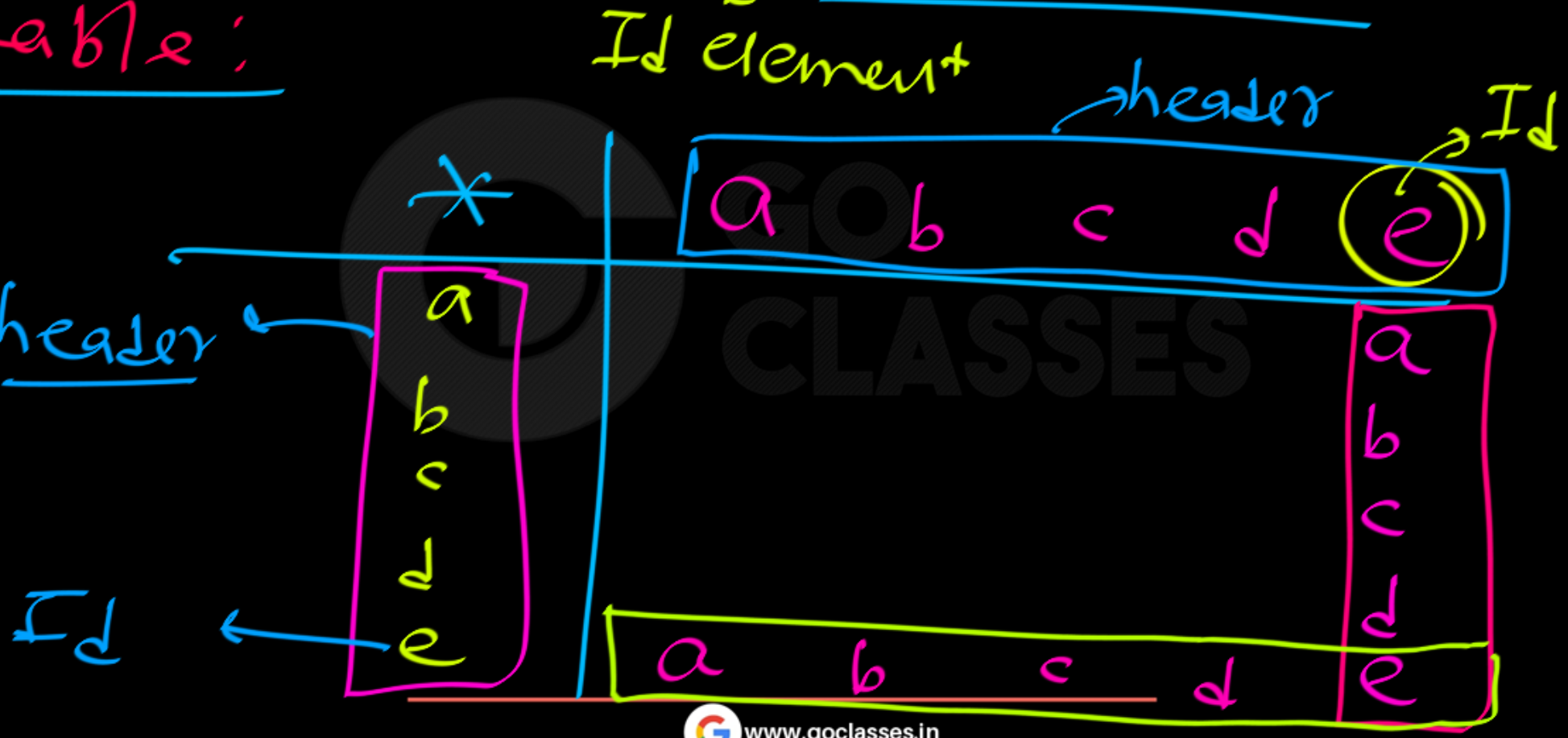
a*a=a a*a=a

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**!

Observation about "e" in operation table:



Identity element e

$d * e = d$

$f * e = f$

$a * e = a$

$e * d = d$

$e * g = g$

$e * a = a$

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!

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

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

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

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

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

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

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

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!

Group Theory

Next Topic

The Inverse Property

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

In multiplication,

$3^{-1} = ? = \frac{1}{3}$

Inverse of 3 = b

$3 \times b = 1$ → e of mul

$\Rightarrow b = \frac{1}{3}$

for addition:

$3 + b = 0$ — e of +

$b = -3$

$3^{-1} = -3$ for + operation

$(S, \#)$ → base set

$a, b \in S$

Inverse of "a" = b iff

$a \# b = e$

and

$b \# a = e$

$b = \bar{a}'$

$(Z, +)$

$e = 0$

$5^{-1} = ?$

$5 + 5^{-1} = 0$

$5^{-1} = -5$

$a^{-1} = -a$

$5^{-1} + 5 = 0$

$5^{-1} = -5$

$(R, \times)$

$e = 1$

$5^{-1} = ?$

$5 \times \frac{1}{5} = 1$

$\frac{1}{5}$

The Inverse Property:

A set has the **inverse property** under a particular operation if **every** element of the set has an **inverse**. An inverse of an element is another element in the set that, when combined on the right or the left through the operation, always gives the **identity element** as the result. Again, this definition will make more sense once we've seen a few examples.

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), *y* represents the a special element called the **inverse** of *x* (see definition below), e represents the **identity element** of the set, and the symbol # represents our operation, then the **inverse property**, for A with the operation # would be:

For any element *x* of the set, there is another element *y* of the set so that $x\#y = e$ and $y\#x = e$.

(It is important to note that a set under an operation **must** have the **identity** PROPERTY before it can have the **inverse property**: if there is no **identity**, then the definition of the **inverse** doesn't make sense! So if a set under an operation does not have the **identity** PROPERTY, then we know already that it does not have the **inverse property**!)

$(S, \#)$ has inverse property iff

$\forall_{a \in S}$, a^{-1} exists.

$(Z, +)$ — Inverse Property? Yes

$2 + \bigcirc = 0$ $\quad -2 = \bar{2}^{1}$

$3 + \bigcirc = 0$ $\quad -3 = 3^{-1}$

$-10 + \bigcirc = 0$ $\quad 10 = (-10)^{-1}$

$\forall_{a \in Z}$

$\bar{a}^{1} = -a$

$\bar{0}^{1} = 0$

$(Z, +)$

$0^{-1} = ?$

$0 + 0 = 0$

$0 = 0^{-1}$

$(R, \times)$ — $e = 1$ | 0^{-1} = DNE

Reals

Inverse Property? No

$5 \times \bigcirc = 1$ $\quad \frac{1}{5} = 5^{-1}$

$6 \times \bigcirc = 1$ $\quad 6^{-1} = \frac{1}{6}$

$0 \times \bigcirc = 1$

$\bigcirc$? DNE

$(N, +)$ — Inverse property? No

No Identity property

No Identity Property ⟶

No Inverse property.

a) The set of **integers** has the **inverse property** under the operation of **addition**, because it has the **identity element** 0, and it is true that for **any** integer x, $x+(-x)=0$ and $-x+x=0$. So $\mathbf{-x}$ is the **inverse** for x in the set of **integers** under the operation of **addition** because it **gives the identity 0 as the result** whenever it acts on x from the right or the left.

b) The set of **natural numbers** does **not** have the **inverse property** under the operation of **addition**, because while $-x$ would normally be the **inverse** for x under addition, there are **no negative numbers in the set of natural numbers**. The **inverse** must be **in** the set in order for the **inverse property** to hold!

c) The set of **rational numbers** does **not** have the **inverse property** under the operation of **multiplication**, because the element 0 does not have an **inverse** ! The identity of the set of rational numbers under multiplication is 1, but there is **no** number we can multiply 0 by to get 1 as an answer, because 0 times anything (and anything times 0) is always 0!

d) If we let A be the set we get when we remove the number 0 from the set of **rational numbers**, then A **does** have the **inverse property** under the operation of **multiplication**, because it has the **identity element** 1 (we showed this in the last section), and it is true that for any rational number $x \neq 0$ (i.e. any element of A), $\frac{1}{x} \cdot x = 1$ and $x \cdot \frac{1}{x} = 1$. So $\frac{1}{x}$ is the **inverse** of x!

$(\mathbb{Q}, \times)$ — $e = 1$

Rationals

Inverse property? No

$0 \times \left(\frac{1}{0}\right) = 1$

$\frac{1}{0}$ DNE $= 0^{-1}$

$a \neq 0$

$a^{-1} = \frac{1}{a}$

$(R - \{0\}, \times)$ — Closed ✓

— Assoc ✓

— $e = 1$ — Id. Property ✓

— Inverse Property ?

$a \in R$

$a^{-1} = \frac{1}{a}$ ✓

: Yes

$(\mathbb{Q} - \{0\}, \times)$ — Closed ✓

— Assoc ✓

— $e = 1$ — Id. Property ✓

— Inverse Property ?

$a \in \mathbb{Q}$

$a^{-1} = \frac{1}{a}$ ✓

∴ Yes

e) The set of **real numbers** does **not** have the **inverse property** under the operation of **subtraction**, because it does **not** have an **identity element** (we showed this in the last section)! So it cannot have **inverse** S because the definition of an **inverse** requires the existence of an **identity element** to make sense!

This means that the **inverse property** only holds if **every single element in the set** has an **inverse**!

Also notice that the inverse must be the **same** on the right **and** on the left! If we have two elements, y and z so that $x\#y = e$ but $y\#x \neq e$ and $z\#x = e$ but $x\#z \neq e$, then we don't have an **inverse**. Neither y nor z is an **inverse**, because they don't give the **identity** as the result when they act on x **both** on the right **and** on the left.

Something else you should notice: if x is the **inverse** of y, then y is **always** the **inverse** of x. **Inverses always come in pairs!** (Although we **can** have an element be an **inverse** of itself – see below.)

One more important point: the **identity element** is always its **own inverse**. For example, if e is the identity element, then e#e=e. So by definition, when e acts on itself on the left or the right, it leaves itself unchanged and gives the identity element, itself, as the result!

Q: If $\bar{a}^1 = b$ then $\bar{b}^1 = a$?

Ans: Yes.

$\bar{a}^1 = b$ means

$$\left.\begin{matrix} a \# b = e \\ b \# a = e \end{matrix}\right\} \rightsquigarrow \bar{b}^1 = a$$

$b^{-1} = a$ means

Definition of 'inverse'

$b \# a = e$

$a \# b = e$

$a^{-1} = b$

$b^{-1} = a$

$$(a^{-1})^{-1} = a$$

Q: Id element = e

$e^{-1} = ?$

$= e$

Proof: Assume $e^{-1} = b$, means

$$\left.\begin{matrix} e * b = e \\ b * e = e \end{matrix}\right\}$$ Definition of Inverse

$e * b = e$

$b * e = e$

by definition of Inverse

Since e is Id

$e * b = b$

$e = b$

So, $\boxed{e^{-1} = e}$

Hence proved

Note:

In poset "$\leq$" means POR.

Eg: $(N, \leq)$, $a \leq b$ iff $a \mid b$

Note:

In Group theory, "$*$" stands for "Binary Operation"

Q :

Is it **possible** for an element to have more than one inverse??

Q :

Is it **possible** for an element to have more than one inverse?? — Yes.

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

e = Id element

$\forall_{x,y}$

$x * y = e$

$x \neq e$
$y \neq e$

means

$e * a = a$
$a * e = a$

$a * b = e$
$b * a = e$

$a * c = e$
$c * a = e$

$b * c = e$
$c * b = e$

$(\{a, b, c, e\}, *)$ — Closed

Id = e

Inverse of $a = \bar{a}^{-1}$

$\bar{b}^{-1} = a, c, b$

$\bar{c}^{-1} = a, b, c$

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

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

$\bar{a}^{-1} = b, c, a$

Note: In Any Structure,

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

$e^{-1} \neq$ Some element other than e

e = Identity element

Proof: If $\bar{e}' = b$ then $b = e$

So, $\boxed{\bar{e}' = e}$

$Q : (\{a_1, a_2, a_3, \ldots, a_n, e\}, *)$

e = Id. element

$\forall_{x,y}$; $x * y = e$

$x \neq e, y \neq e$

$\Rightarrow$ closed

e = Id. $\checkmark$

$a_1^{-1} = a_1, a_2, \ldots, a_3$

$a_2^{-1} = a_1, a_2, \ldots, a_3$

a_1^{-1} ?

$a_1 * a_1^{-1} = e$

$a_1^{-1} * a_1 = e$

$\Rightarrow a_1^{-1} = a_1$

$a_1^{-1} = a_2$

$\vdots$

$a_1^{-1} = a_n$

Q :

Is it **possible** for an element to have more than one inverse??

Take a set S, and designate $e \in S$ the identity element. Define your binary operation $\oplus$ by $x \oplus y = e$ for all $e \neq x, y \in S$. Now every nonidentity element of the set is the inverse of every other nonidentity element.

Group Theory

Next Topic

The Commutative Property

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

is Commutative op^n : iff

$$a \# b = b \# a$$

a, b Commute

$(S, \#)$ is Commutative iff

$\forall_{a,b \in S}$ $a \# b = b \# a$

The property of Commutativity:

A set has the **commutative property** under a particular **operation** if the result of the operation is the same, even if you switch the order of the elements that are being acted on by the **operation**.

More formally, if x and y are variables that represent **any 2 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 **commutative property** , for A with the operation # would be:

$x\#y = y\#x$.

This means that the **commutative 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* and *y***, $x\#y$ will always give us the same result as $y\#x$.

$(N, +)$ — Comm

$a + b = b + a$

$(Z, -)$ — Not Comm

$5 - 4 \neq 4 - 5$

$(N, \times)$ — Comm

$a \times b = b \times a$

$(R - \{0\}, \div)$ — Not Comm

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

Properties

- **Commutative:** Let * be a binary operation on a set A.

  The operation * is said to be commutative in A if

  $a * b = b * a$ for all a, b in A

- **Associativity:** Let * be a binary operation on a set A.

  The operation * is said to be associative in A if

  $(a * b) * c = a *(b * c)$ for all a, b, c in A

- **Identity:** For an algebraic system (A, *), an element 'e' in A is said to be an identity element of A if

  $a * e = e * a = a$ for all $a \in A$.

- **Note:** For an algebraic system (A, *), the identity element, if exists, is unique.

- **Inverse:** Let (A, *) be an algebraic system with identity 'e'. Let a be an element in A. An element b is said to be inverse of A if

  $a * b = b * a = e$

Group Theory

Next Topic

Classification of Structures with single binary operation

Magma, Semi-Group, Monoid, Group, Abelian Group

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

Algebraic Structure	Properties
(1) Magma (Groupoid)	Closure property
(2) SemiGroup	Closure + Asso
(3) Monoid	Close + Asso + Identy
(4) Group	Close + Asso + Id + Inverse

Magma ≡ Algebraic Structure with Simple Binary op^{n}.

Closed

Mathematician in Group theory :

Abel

Abelian ≡ "Commutative"

Abelian Semigroup = Commutative semi; Group

Commutative

Close + Asso

Abelian monoid = Commutative monoid

Abelian Group : Commutative Group

Closure + Asso + Id + Inverse

+ Commutative

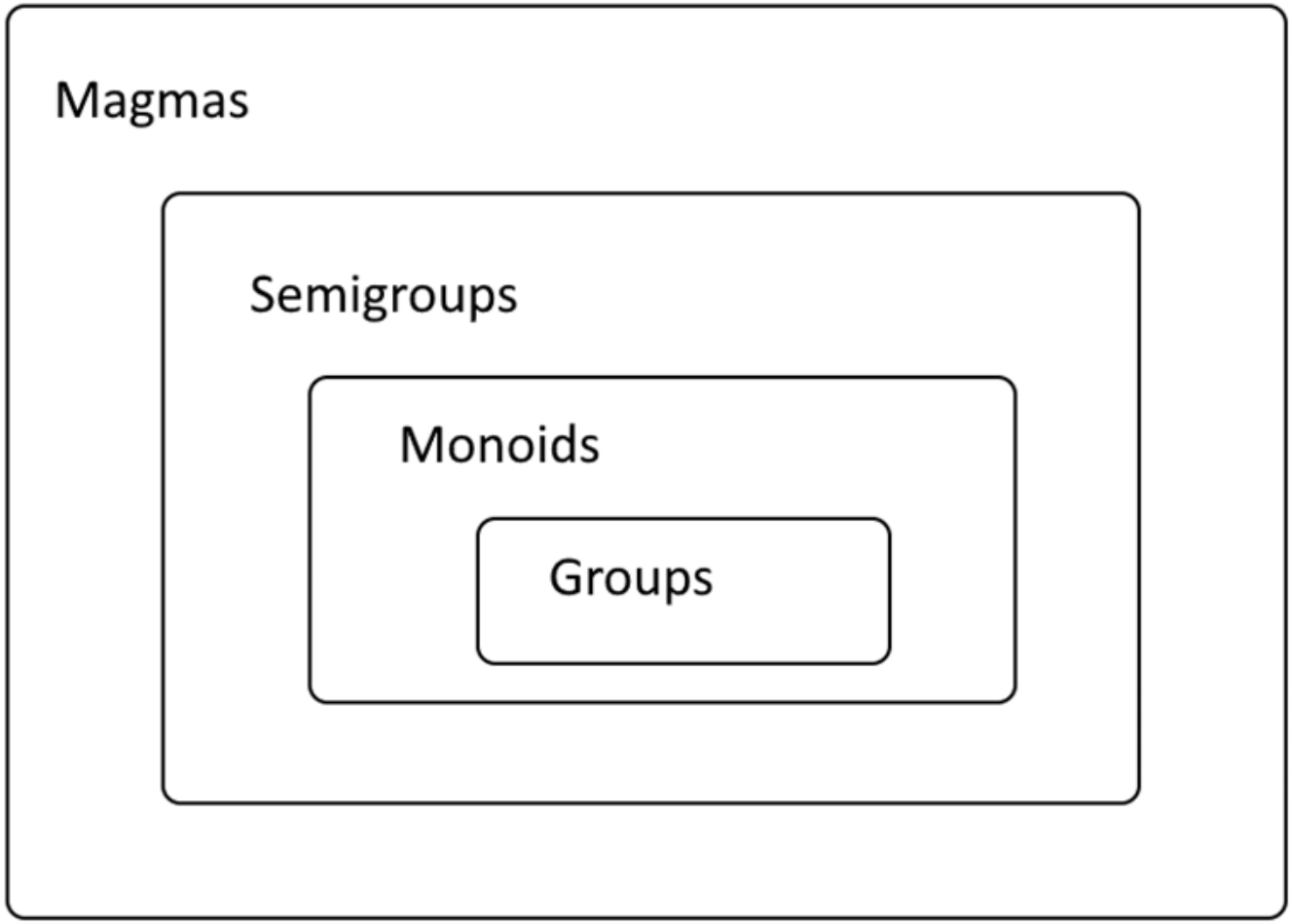
Group

Note. If we define a *binary algebraic structure* as a set with a binary operation on it, then we have the following schematic:

$$(\text{Binary Algebraic Structures}) \supseteq (\text{Semigroups}) \supseteq (\text{Monoids}) \supseteq (\text{Groups}).$$

= Magma (Groupoid)

1 binary operation +		
		magma
x+(y+z)=(x+y)+z	Associativity	semigroup
0+x=x+0=x	Identity	monoid
x+(-x)=(-x)+x=0	Inverse	group
x+y=y+x	Commutativity	abelian group


Magmas
Semigroups
Monoids
Groups

Groupoid / magma

- Definition; G be a non empty set and $*$ be a binary operation , then the structure (G,*) is called a groupoid, if $a * b \in G, \forall a, b \in G$ $i.e$ g is closed for the binary operation.
- Examples : (i)The structures $(N, +), (N, .), (Z. +), (Z, .), ((Q, +), (Q, .)$
- (ii) The set N is not a groupoid with respect to operation '–' .

Semi group

- **Semi Group:** An algebraic system (A, *) is said to be a semi group if
  1. * is closed operation on A.
  2. * is an associative operation, for all a, b, c in A.
- Ex. (N, +) is a semi group.
- Ex. (N, .) is a semi group.
- Ex. (N, −) is not a semi group. — Reason: Not Closed Not Asso.
- **Monoid:** An algebraic system (A, *) is said to be a **monoid** if the following conditions are satisfied.
  1) * is a closed operation in A.
  2) * is an associative operation in A.
  3) There is an identity in A.

$(Z, -)$ — Closed

Not Assoc

Magma

Monoid —— SemiGroup + Identity

↓

Represented as $(S, \#, e)$ — Identity

Example 2. The following are examples of (commutative) monoids: $(\mathbb{N}, \cdot, 1)$, $(\mathbb{N}, +, 0)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, \cdot, 1)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, \cdot, 1)$, $(\mathbb{R}, +, 0)$, $(\mathcal{P}(A), \cap, A)$, $(\mathcal{P}(A), \cup, \emptyset)$, for A a given set, as well as $(\{T, F\}, \vee, F)$ and $(\{T, F\}, \wedge, T)$.

$(N, \times, 1)$ — Commutative monoid

1 — e

$N = \{0, 1, 2, \ldots\}$

Q 3. Define the binary operation $*$ on $\mathbb{Z}$ by

$$x * y := x - 3 + y$$

for all $x, y \in \mathbb{Z}$. You will show that $(\mathbb{Z}; *)$ is an Abelian group. Since $x-3+y$ is an integer whenever x and y are integers, (G1) holds, so you will only need to verify (G2), (G3), (G4), and commutativity, using the steps below.

(a) Show that $*$ is associative.

(b) Show that $*$ is commutative.

(c) Find the identity element for $*$. [*Hint: Let e denote the identity. Use the equation $x * e = x$ to determine the value of e. Then show carefully that e is indeed an identity element for $*$.*]

(d) Let $x \in \mathbb{Z}$. Find the inverse, $\widehat{x}$, of x with respect to the identity element found in (c). [*Hint: Use the equation $x * \widehat{x} = e$ to find $\widehat{x}$ in terms of x. Then show that $\widehat{x}$ is indeed an inverse of x.*]

$(Z, *)$ $\quad a * b = a + b - 3$

① Closure ✓ If $a, b \in Z$

then $a + b - 3 \in Z$

② Asso: $(a * b) * c \overset{?}{=} a * (b * c)$

$(a * b) * c$

$a * (b * c)$

$(a + b - 3) * c$

$a * (b + c - 3)$

$a + b - 3 + c - 3 = a + b + c - 3 - 3$

$(\mathbb{Z}, *)$

$a * b = a + b - 3$

$b * a = b + a - 3$

$\Rightarrow$ Commutative

$e = ?$

$a * e = a$

$a + e - 3 = a$

$e = 3$

$e * a = a$

$e + a - 3 = a$

$e = 3$

Cross verify: $e = 3$

$\forall a \in Z$

$$a * 3 = a + 3 - 3 = a$$

Inverse property?

$\bar{a}^{-1}$?

$a * \bar{a}^{-1} = 3$

$a + \bar{a}^{-1} - 3 = 3$

$\bar{a}^{-1} = 6 - a$

Cross verify ✓

$\forall_{a \in Z}$

$a * (6 - a)$

$a + 6 - a - 3$

$= 3 = e$

$(Z, *)$ $\quad a * b = a + b - 3$

Abelian Group

$a^{-1} = 6 - a$ $\quad 10^{-1} = 6 - 10 = -4$

$(-10)^{-1} = 6 - (-10) = 16$

HW

Let $\star : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the binary operation:

$$m \star n = m^n + n^m$$

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

Prove or disprove the following:

1. $\star$ is associative.
2. $\star$ is commutative.

Base set N ; $(N, *)$

$a * b = a^b + b^a$

$(N, *)$ $\quad a * b = a^b + b^a$

① Closure — $a, b \in N$ then $a^b \in N$, $b^a \in N$

② Commutative — Asso? — Hw

$a * b = b * a$

$a^b + b^a = b^a + a^b$

No

Is $e = ?$ — No

$a * e = a$

$e^a + e^a = a$

No e

$e = 1$?

$a * 1 = a + 1 \neq a$

$a * 1 = a + 1$

a

$a + 1$

$= a + 1$

$e = 2$; $a * 2 = a^2 + 2^a \neq a$

Inverse prop ——— No

Asso: 1, 2, 3

$(1 * 2) * 3$ | $1 * (2 * 3)$

$3 * 3$ | $1 * (2^3 + 3^2)$

$3^3 + 3^3 = 54$ | $= 2^3 + 3^2 + 1 \neq 54$

$(N, *)$

$a * b = a^b + b^a$

Commutative magma

HW

6. $*$ is a binary operation defined on Q. Find which of the following binary operations are commutative and which of them are associative?

(i) $a * b = a - b$

(ii) $a * b = \frac{ab}{4}$

(iii) $a * b = a + b + ab$

(iv) $a * b = (a - b)^2$

(v) $a * b = a + ab$

(vi) $a * b = \frac{a + b}{2}$

Q = set of Rationals

$(\mathbb{Q}, *)$ $\quad a * b = \frac{ab}{4}$

(1) $3 * 4 = \frac{3 \times 4}{4} = 3$

(2) Closure ✓ $\quad \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$

then $\frac{\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)}{4} \in \mathbb{Q}$ ✓

(3) Asso

$(a * b) * c \stackrel{?}{=} a * (b * c)$

$\left(\frac{ab}{4}\right) * c \qquad a * \left(\frac{bc}{4}\right)$

$\frac{abc}{16} \qquad \frac{abc}{16}$

(4) $e = ?$

$$a * e = a$$

$$\frac{ae}{4} = a$$

$$e = 4$$

Verify

$b \neq 0$

$$\frac{a}{b} \in Q$$

$$\left(\frac{a}{b}\right) * 4 \stackrel{?}{=} \frac{a}{b}$$

$$\frac{\frac{a}{b} * 4}{4} = \frac{a}{b}$$

(5) $\bar{a}^1 = ?$

$\bar{a}^1 = b$

$a * b = 4$

$\frac{ab}{4} = 4 \Rightarrow b = \frac{16}{a}$

$\bar{0}^1 = ?$

$0 * b = 4$

$\frac{0 \times b}{4} = 4$

$b = DNE$

$\bar{0}^{-1} = DNE$

If $a \neq 0$

$$\bar{a}^{-1} = \frac{1}{a}$$

$(Q, *)$

$a * b = \frac{ab}{4}$

Abelian monoid

$(Q - \{0\}, *)$

$a * b = \frac{ab}{4}$

$e = 4, \quad \bar{a}^1 = \frac{16}{a}$; Commutative

Abelian Group

$a * b = b * a$

$\frac{ab}{4} = \frac{ba}{4}$

State whether the following statements are true or false with reasons.

(i) For any binary operation $*$ on $\mathbb{N}$, $a * a = a \, \forall a \in \mathbb{N}$.

(ii) If $*$, a binary operation $*$ on $\mathbb{N}$ is commutative then, $a * (b * c) = (c * b) * a$.

State whether the following statements are true or false with reasons.

(i) For any binary operation $*$ on $\mathbb{N}$, $a * a = a \forall a \in \mathbb{N}$.

(ii) If $*$, a binary operation $*$ on $\mathbb{N}$ is commutative then, $a * (b * c) = (c * b) * a$.

(i) $\Rightarrow$ $(\mathbb{N}, +)$

$2 + 2 \neq 2$

So (i) is false

(iii) $*$ — Some operation

↓ binary

If $*$ is Commutative then

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

$*$ — Commutative

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

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

A *semigroup* is a nonempty set G with an associative binary operation. A *monoid* is a semigroup with an identity. A *group* is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$. In a semigroup, we define the property:

(*iv*) Semigroup G is *abelian* or *commutative* if $ab = ba$ for all $a, b \in G$.

The *order* of a semigroup/monoid/group is the cardinality of set G, denoted $|G|$. If $|G| < \infty$, then the semigroup/monoid/group is said to be *finite*.

Order of any Structure :

Cardinality of Base Set.

finite Structure : base set is finite.

(Can never be empty.)

Structure $(\{T, F\}, \wedge)$

Order $= 2$

A semigroup is a nonempty set S together with an associative binary operation on S.

Q 1 :
Give an example of a semigroup without an identity element.
i.e. A Semi-Group BUT not Monoid.

$(N, +)$

$(N, *)$ $\quad a * b = \min(a, b)$

Closed

Assoc

A semigroup is a nonempty set S together with an associative binary operation on S.

Ans 1 :
Give an example of a semigroup without an identity element.

Solution $\mathbb{Z}^+ = \{1, 2, 3, ...\}$ is a semigroup without identity with binary operation usual addition.

Question:

Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer the question if S has exactly 2 elements; exactly 3 elements; exactly n elements.

How many different commutative binary operations can be defined on a set of 2 elements? on a set of 3 elements? on a set of n elements?

Q: $(S, *)$ $|S| = 1$

How many different binary op^{n} we can Define?

$S = \{a\}$

$(S, *)$ —— binary op^n is a mapping/function.

$$* : S \times S \rightarrow S$$

function

$(S = \{a\}, *)$

$a * a = a$

One binary operation Possible

$(S, *)$ "no. of binary opn"

is same as "number of

functions from $S \times S \longrightarrow S$

$* : S \times S \longrightarrow S$

$\#functions = \#binary\ op^n = |S|^{|S \times S|}$

$|S| = 1 \longrightarrow$ # binary op^n $= 1$

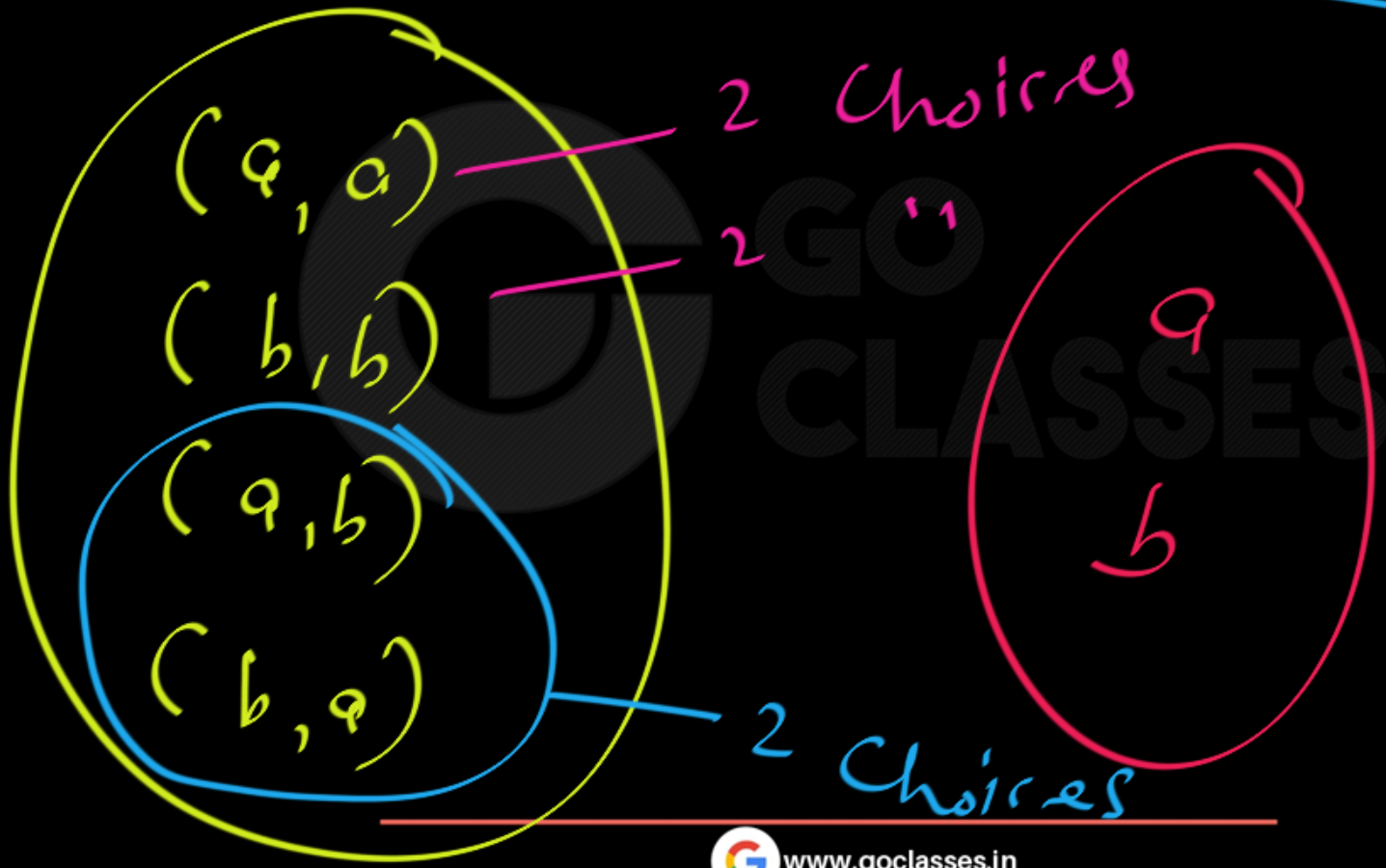
$|S| = 2 \longrightarrow$ " $= 2^{(2^2)} = 16$

$|S| = n \longrightarrow$ " $= n^{(n^2)}$

Q: $(S, *)$; $|S| = n$

Commutative binary op^n ?

$(S = \{a, b\}, *)$ — Commutative



Comm binary $= 2^3$

$= 2 \times 2 \times 2$

$= 8$

$|S| = n$

$(1,1)$ —— n choices

$(1,2)$ —— n choices

$\vdots$

(n,n) —— n choices

$\Big\}\ n^n$

$\frac{n^2-n}{2}$

$\{(1,2), (2,1)$ —— n choices $\}$

$\vdots$

$\Big\}\ n^{\left(\frac{n^2-n}{2}\right)}$

$$n^n \times n^{\left(\frac{n^2-n}{2}\right)}$$

$$= n^{n + \frac{n^2-n}{2}}$$

$$= n^{\frac{2n+n^2-n}{2}}$$

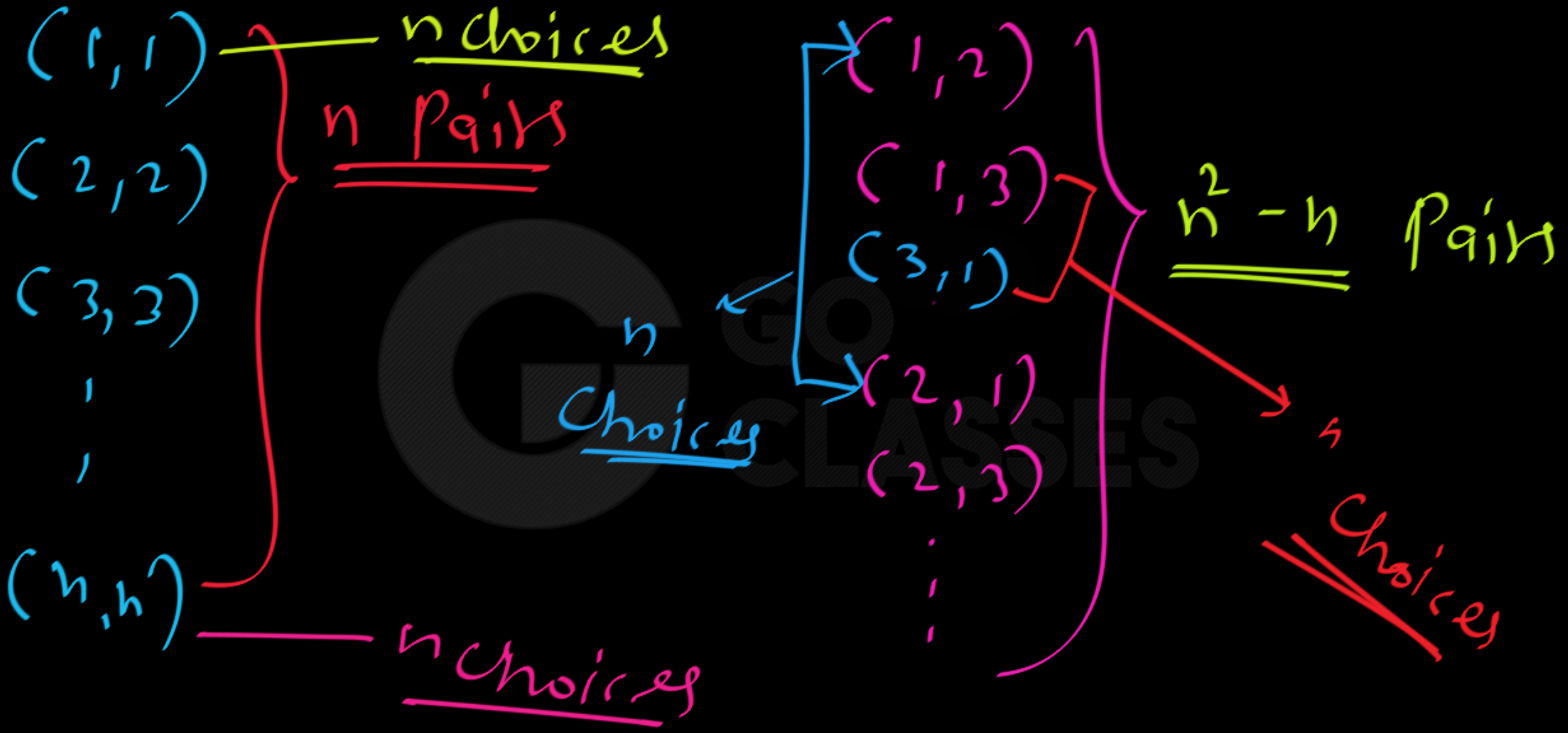
$$= n^{\frac{n^2+n}{2}}$$

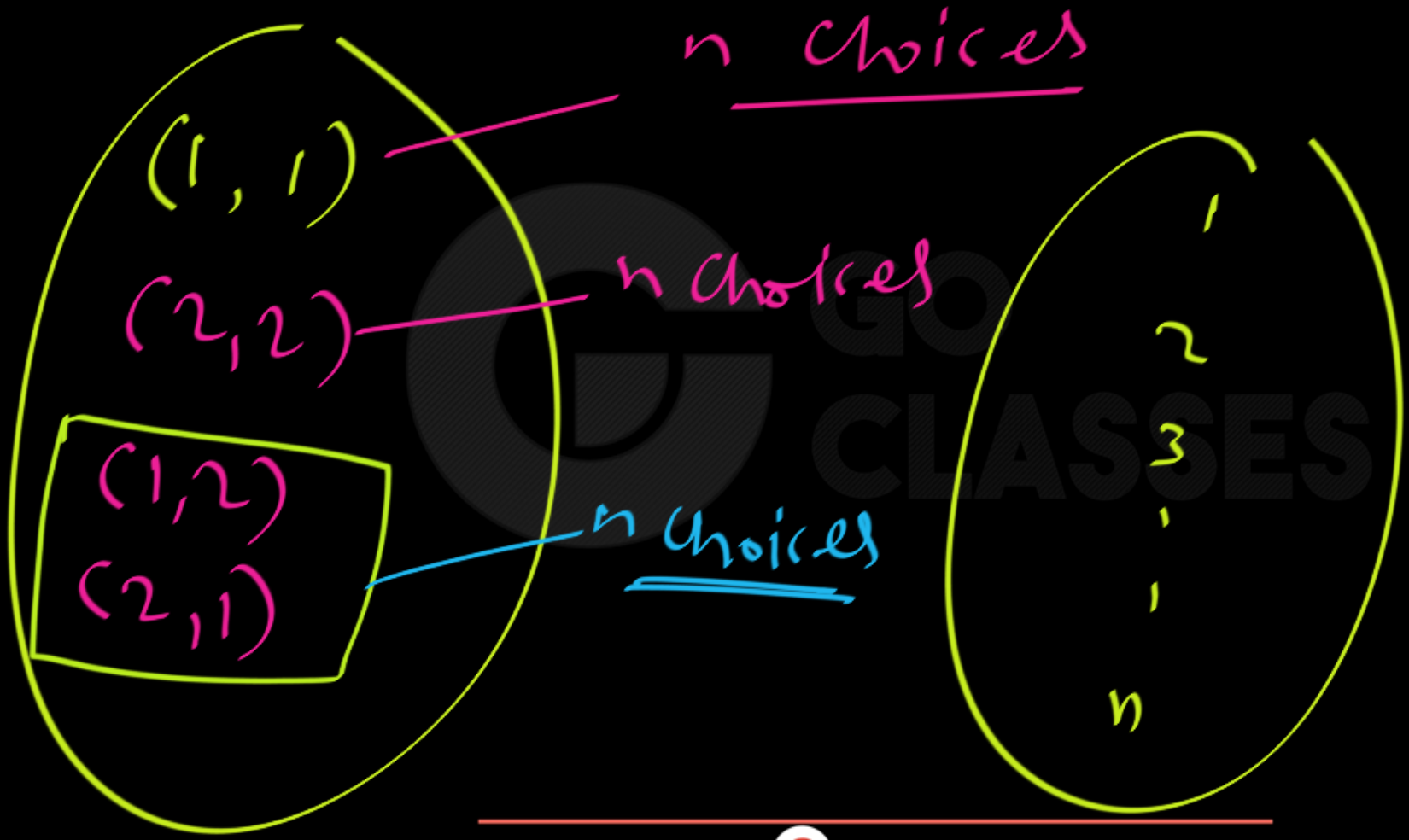
$|S| = n$

$S = \{1, 2, 3, \ldots, n\}$

$|S \times S|$ = no. of pairs $= n^2$ pairs

$(1,1), (1,2), \ldots, (2,1), (2,2) \ldots\ldots$


(1,1)
(2,2)
(3,3)
(n,n)
n choices
n pairs
n choices
n
choices
(1,2)
(1,3)
(3,1)
(2,1)
(2,3)
n² - n pairs
n
choices


n choices
(1, 1)
n choices
(2,2)
(1,2)
(2,1)
n choices
1
2
3
n

$n^n \times n^{\frac{n^2-n}{2}} = n^{\frac{n^2+n}{2}}$

n^n → (a, a) pairs

$n^{\frac{n^2-n}{2}}$ → (a, b) pairs, $a \neq b$

$n^{\frac{n^2+n}{2}}$ = Number of Commutative binary ops

Question related to monoid: HW

1. Is Identity element unique?
2. Do we have Left Cancellation Property in Monoid?
3. Do we have Right Cancellation Property in Monoid?

Left Cancellation Property :

If $a \# b = a \# c$

then $b = c$?

Right Cancellation Property :

If $a \# b = c \# b$

then $a = c$?

Group Theory

Next Topic

Groups

Closed, Associative, Identity, Inverse

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

Fundamental Definition. *A* ***group*** *is a set G, together with a binary operation $*$, such that the following hold:*

1. *(Associativity):* $(a * b) * c = a * (b * c)\ \forall a, b, c \in G$.
2. *(Existence of identity):* $\exists e \in G$ *such that* $a * e = e * a = a\ \forall a \in G$.
3. *(Existence of inverses): Given* $a \in G, \exists b \in G$ *such that* $a * b = b * a = e$.

Group

- **Group:** An algebraic system (G, *) is said to be a **group** if the following conditions are satisfied.

  1) * is a closed operation.

  2) * is an associative operation.

  3) There is an identity in G.

  4) Every element in G has inverse in G.

- **Abelian group (Commutative group):** A group (G, *) is said to be ***abelian*** (or ***commutative)*** if

  $a * b = b * a$.

Semigroup, Monoid, Group :

Let G be a non-empty set and * be a binary operation defined on G.

A semigroup is a nonempty set G with an associative binary operation.
A monoid is a semigroup with an identity.
A group is a monoid such that each $a \in G$ has an inverse $a^{-1} \in G$.

Abelian Group :

Group G is abelian or commutative if $a*b = b*a$ for all $a, b \in G$.
An Abelian group is a group satisfying the commutative law.

Cardinality/Order :

The order of a semigroup/monoid/group is the cardinality of set G, denoted $|G|$.
If $|G| < \infty$, then the semigroup/monoid/group is said to be finite.

Relation between different algebraic structures :

If we define a binary algebraic structure as a set with a binary operation on it, then we have the following schematic:

(Binary Algebraic Structures) $\supseteq$ (Semigroups) $\supseteq$ (Monoids) $\supseteq$ (Groups) $\supseteq$ (Abelian Group) .