Group theory

- Abstract Algebra is study of structure

① Lattice
② Boolean Algebra

- magma
- Semi group
- monoid
- group

} is structure

- Algebraic Structure (AS)

(Base set, *, #, ...)
- Base set: on the set we define these operation
- operation: ↓ these operation
- Algebraic Structure

ex: $(Z,+)$ → in gate we have Algebraic Structure with single binary operation.

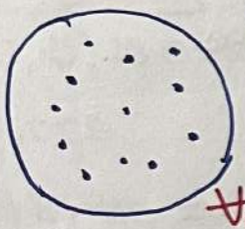
$(N,+,\times)$ (set of matrices, product)

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

Binary operation

① Closure property. : what happen inside a set ; Should remain inside the set.

Set S



$(S,\#)$ Structure

$\forall a,b \quad a\#b=c$

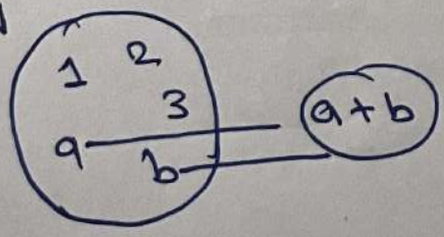
Take any a, b & perform operation & the result remain in "Set S" (Should belong)

} Closure property is satisfied by $(S,\#)$

ex: $(N,+)$ — Closure property so, Set of natural no. is closed under addition.

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

N



ex: $(\{1,2,3\}, +)$ — not closure property

$2+3=5 \notin$ Base set

ex: $(\mathbb{N}, -)$ → is not closed (not closure property)

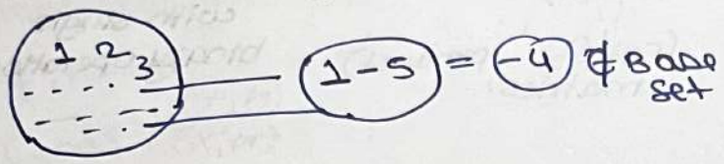
ex $(\{T,F\}, \wedge)$ — is closure property

F,F: $F \wedge F = F \in$ Base set (BS)

T,F: $T \wedge F : F \in BS$

F,T: $F \wedge T : F \in BS$

T,T: $T \wedge T : T \in BS$



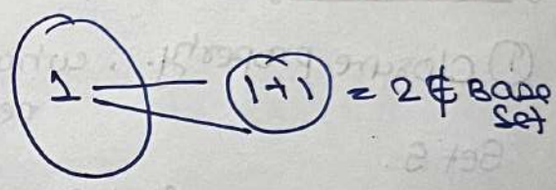
Integers are not closed under division

ex: $(\omega, -)$ — not closed

$a=1, b=2 \Rightarrow 1-2=1 \notin \omega$

ex: $(\{1\}, +)$ — not closed

Base set = {1} ← element



▸ Formal Definition

(set S, #)

Alg. Structure

Satisfy closure property

iff $\forall a,b \in S$

$a \# b \in S$.

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

Operation table

*	a	b
a	a	b
b	a	a

means

a*a=a

a*b=b

b*a=a

b*b=a

ex $(\{1,2\}, +)$

make operation table?

+	1	2
1	2	3
2	3	4

not closed.

4 ∉ to Base Set

In general cs:

Binary operation two operands.

$a+b$
$a*b$

unary operation

② one operand.

In Abstract Algebra.

- binary operation means closure property] "#" is binary operation on set S. iff $(S, \#)$ is closed.
  (Operation is closed)

ex: $(G, *)$ * is binary operation iff

$\forall a,b \in G \Rightarrow a*b \in G$.

Binary operation = closed operation

- Algebraic Structure By definition it must be closed

Associative property

ex: $(S, \#)$ is associative iff

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

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

ex: $(R, \div)$ not closed

/
Real

$a=0, b=0$

$\frac{a}{b} = \frac{0}{0} = ?$ Result (undefine)

ex: $(N, +)$ — Assoc.

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

$+, *$ → always Associative on whatever Baseset you take

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

$\forall a,b \in N$ then $a^2 \in N$ & $b \in N$

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

so, is closed.

is Associative?

$(a\#b)\#c$

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

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

$\Rightarrow a^4+b^2+2a^2b+c$

$a\#(b\#c)$

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

a^2+b^2+c

✗ not equal.

So, not Assoc.

Identity property — Doesn't affect the operation

ex: $5+0=5$
$9+0=9$
$5\times1=5$
$8\times1=8$

$(S,\#)$
Identity element "e":
$a\#e=a$
$e\#a=a$

note: it's fixed for all element

$(S,\#)$
Identity element "e" — fixed for all element "a"
$\forall a$;
$e\#a=a$
$a\#e=a$

ex: $(N,+)$ no identity element.
$N=\{1,2,3,\ldots\}$

$e+a=a$
fixed — anything $\in N$

$e\neq1 \therefore 1+2\neq2$
$e\neq2\ 2+3\neq3$

whole no.
ex: $(W,+)$
$e=0$ fixed for all
$0+5=5$
$0+6=6$

ex $(Z,-)$ is closed
→ not associative
$(5-4)-3 \neq 5-(4-3)$
→ doesn't have identity element
assume $e=0$
then
✓ $5-0=5$
✗ $0-5\neq5$

ex: $(Q,\times)$ is closed
↳ is Associ.
↳ $e=?$
$e=1$ — is the identity element
$a\times1=a$
& $1\times a=a$

ex: $(N,\#)$ $a\#b=\max(a,b)$
① understand operation
$-2\#2$ — nonsense as $-2\notin N$
$2\#2=\max(2,2)=2$
$2\#1=\max(2,1)$
$=2$

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

is closed $a, b \in N$

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

is there Identity element?

assume $e = ?$ so, yes $e = 1$

$e = 1 \Rightarrow a \# 1 = a$

$1 \# a = a$

is Assoc.? yes//

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

$3 \# 2$ $\quad$ $2 \# 3$

$3 = 3$

(ob) $2 \# 5$ } are same

$\#(2,5)$ }

ex: $(Z, \#)$ $a \# b =$ $a^2 + b$

is $e = ?$ (identity element)

assume $e = 0$ no, not identity element

$0 \# 5 = 5$ } $\neq$

$5 \# 0 = 25$ }

ex: $(\{\ldots\}, \text{set diff.})$ set set set

$(\{1,2,3\}, \text{set diff.})$ non sense.

element.

Binary operation

mapping/functn

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

iff $\#: S \times S \to S$

↳ mapping/functn.

ex: $(\{T, F\}, \wedge)$ binary operation

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

T, T	T
T, F	F
F, T	F
F, F	

How does it Relate to Closure property?

Co-domain is Base set.

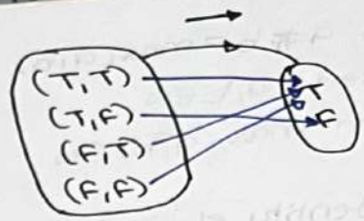
ex $(N, +)$

$+: N \times N \to N$

(1,1)	2
(1,2)	3
(2,1)	4
⋮	⋮

funct^n

ex: $(\{T,F\}, \rightarrow)$ is closed
↳ binary operation on $\{T,F\}$



$T \rightarrow T = T$
$T \rightarrow F = F$
$F \rightarrow T = T$
$F \rightarrow F = T$

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

ex: Set A
$(P(A), \setminus)$ → is closed.
$P(A)$ = Base set
$\setminus$ = set Diff.

Base set = $P(A)$ → elements subset of A

element in Base set: is subset of A

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

then $X \setminus Y \subseteq A$

Set Diff. is it Assoc.? (no)

$(\{a\} - \{a\}) - \{a\} = \phi$

$\neq$

$\{a\} - (\{a\} - \{a\}) = \{a\}$

Do you have identity element? (e?)

assume $e = \phi$ then $X - \phi = X$

$X \phi - X \neq X$

Practice Question

ex: which one is Binary operation on N?

① + ✓
② − 2−3 = −1 ∉ N
③ * ✓
④ / 2/3 ∉ N

⑤ ≤ } boolean operatn/ logical operatn
⑥ <
⑦ =

ex (N, =) — not Alg. structure
a=2, b=3
(a=b) = false ∉ N

ex: Base set {T}
which opn are binary opn?

① ∧ ✓
② ∨ ✓
③ → ✓
④ ↔ ✓

⑤ ⊕ T⊕T = F ∉ Base set
⑥ ↑ T↑T = F ∉ B.S
⑦ ↓

note
Set S is not closed under "#"
iff ∃a,b a#b ∉ S
there exist
a ∉ b can be same
(a ≠ b) Different

ex: ({0,1}, +) not closed
b/c 1+1 = 2 ∉ Base set

ex: Associative?
Base set {T, F}

⑤ → } not assoc.
⑥ ↑
⑦ ↓

① ∧
② ∨
③ ↔
④ ⊕

we will explore them in Digital logic why they are assoc.

i.e (F → T) → F
T → F
F

F → (T → F)
F → F
T

≠

↑ (NAND)
(a↑b)↑c ≟ a↑(b↑c)
$\overline{ab}\uparrow c$ ≠ $a\uparrow\overline{bc}$
$\overline{\overline{ab}c}$ ≠ $\overline{a\overline{bc}}$

ex: Identity property? Base set: {T, F}

① ∧ e = T
② ∨ e = F
⑧ → e ≠ F F → F ≠ F
& e ≠ T F → T ≠ F
④ ↔ e = T
T ↔ F = F
T ↔ T = T

⊗ ⊕

e=?

e=F

F ⊕ T = T

F ⊕ F = F

e

⊗ ↑ e=?

× e=F

F ↑ F ≠ F

× e=T

T ↑ T ≠ T

⊗ ↓

× e=F

F ↓ F ≠ F

× e=T

T ↓ T ≠ T

Imp. point

→ about Identity element

ex: can we have more than one Identity element? (no)

Proof: Assume e, f are too Identity element

- in every closed structure there is atmost one Identity element

$e = I_d$ $\quad f = I_d$

$e \# f = f$ $\quad e \# f = e$

$e \# f = e = f$ So, we can't have > 1 I_d element

$(S, \#)$ $\quad I_d = e \in S$

$\forall a \in S,$ $\boxed{\begin{array}{l} e \# a = a \\ a \# e = a \end{array}}$

$e \# e = e$

ex: $(N, +) \rightarrow e =$ ONE (Don't exist)

$(Z, +) \rightarrow e = 0$

ex: given operation table; set $\{a, b, c\}$ find identity element

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

$e = b$? ×

(no) b/c $b * a \neq a$

$e = c$? ×

$c * a \neq a$

$e = a$ → is identity element

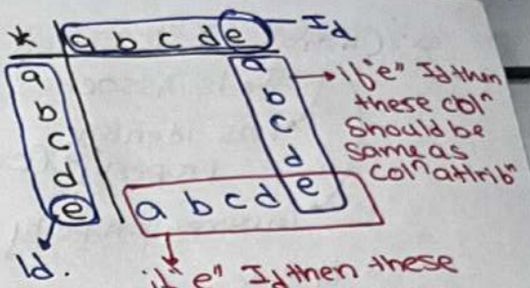
$a * a = a$ | $a * a = a$

$a * b = b$ | $b * a = b$

$a * c = c$ | $c * a = c$

Observation about "e" in operation

→ Identity element



Inverse property a, b, e ∈ S.

(S, #)

Inverse of 'a' = b iff

$$a \# b = e \;\&\; b \# a = e$$

then $b = a^{-1}$

ex: (Z, +) has inverse property

e = ?

e = 0

$5^{-1} = ?$

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

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

ex: (R, ×) has no inverse property

e = 1

$5^{-1} = ?$

$5 \times \bigcirc = e$

1/5

b/c "0"

$0 \times \bigcirc = 1$

DNE

(S, #) has inverse property iff

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

ex (N, +) has inverse property? no.

↳ has no identity element/ property

no identity property ⟶ no inverse property

ex (Q, ×) ... e = 1

↳ inverse property? no

$0 \times \bigcirc = 1$

DNE = 0^{-1}

$a \neq 0$

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

ex: $(R-\{0\}, \times)$ is closed
- is assoc.
- has identity property ($e=1$)
- Inverse property? yes.
  - $a \in Q$
  - $a^{-1} = \frac{1}{a}$

ex: if $a^{-1}=b$ then $b^{-1}=a$? yes.

$a^{-1}=b$ means
$a \# b = e$, $b \# a = e$ → $b^{-1}=a$
means
$b \# a = e$
$a \# b = e$
$a^{-1}=b$

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

ex: I_d element $= e$
$e^{-1} = ? \; = e$

Prof: Assume $e^{-1}=b$ means
$e * b = e$
$b * e = e$
by definition of inverse

Since e is I_d
$e * b = b$ → $e=b$

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

ex: Is it possible for an element to have more than one inverse? (yes)

i.e
$(\{a,b,c,d,e\}, *)$ is closed
$e = Id$.

$\forall_{x,y}$ $x * y = e$
$x \neq e$
$y \neq e$
means
$e \times a = a$
$a \times e = a$

for others

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

$I_d = e$

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

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

$a * a^{-1} = e$, $a^{-1} * a = e$ } $a^{-1} = b, c$

note In any Structure,

$e^{-1} = e$

e: Identity element

$e^{-1} \neq$ some element Other than "e"

Commutative Property

"#" is commutative operatn iff $a\#b = b\#a$

$(S, \#)$ is commutative iff $\forall a,b \in S$ $a\#b = b\#a$

① $(N, +)$ ... is comm. $a+b=b+a$

② $(N, \times)$ — is comm. $a\times b = b\times a$

③ $(Z, -)$ - not comm. b/c $5-4 \neq 4-5$

④ $(R-\{0\}, \div)$ not comm.

Classification of Structure with Single Binary operatn

Algebraic Structure	properties.
① magma (Groupoid) ≡ Algebraic structure with Single Binary operatn	Closure property
② Semigroup	Closure + Asso.
③ Monoid	Closure + Assoc. + Identity
④ Group	Closure + Asso. + Identity + Inverse
⑤ Abelian group	Closure + Asso. + Identity + Inverse + Communicate

Abelian ≡ Commutative

ex: following are the example of Commutative monoids.

monoid — semigroup + identity

Represented as $(S, \#, e)$ ← identity

① $(N, \times, 1)$
② $(N, +, 0)$
$N = \{0, 1, 2, \ldots\}$
③ $(Z, \times, 1)$
④ $(Z, +, 0)$
⑤ $(Q, \times, 1)$
⑥ $(Q, +, 0)$
⑦ $(R, \times, 1)$
⑧ $(R, +, 0)$
⑨ $(P(A), \cap, A)$
⑩ $(P(A), \cup, \phi)$
⑪ $(\{T, F\}, \vee, F)$
⑫ $(\{T, F\}, \wedge, T)$

ex: $(Z, *)$; $a * b = a + b - 3$

① Closure property

If $a, b \in Z$

then $a + b - 3 \in Z$

② Asso.

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

$(a + b - 3) * c$ $\quad$ $a * (b + c - 3)$

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

③ Identity element

$e = ?$

$a * e = a$

$a + e - 3 = a$

$e = 3$

$e * a = a$

$e + a - 3 = a$

$e = 3$

④ Inverse property

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

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

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

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

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

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

⑤ Abelian group.

$a * b = a + b - 3$

$b * a = b + a - 3$

ex: $*: N \times N \to N$ & $m*n = m^n + n^m$

Base set N

& Structure $(N, *)$

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

① Closure

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

② commutative

$a*b = b*a$

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

③ Identity element; $e = ?$

$a*e = a$

$a^e + e^a = a$

$e = 1$?

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

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

④ Inverse property

no b/c Identity element doesn't exist

⑤ Asso.

ex. $1*2*3$

$(1*2)*3$

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

$3*3$

3^3+3^3

$\Rightarrow 54$

$\neq$

$1*(2*3)$

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

$1*17$

$1^{17}+17^1$

$\Rightarrow 18$

ex. Q: Set of Rational no. $\Rightarrow$ Abelian monoid.

① $(Q, *)$ & $a*b = \frac{ab}{4}$

① Closure?

$\frac{a}{b}, \frac{c}{d} \in Q$ then $\frac{(\frac{a}{b})(\frac{c}{d})}{4} \in Q$

② Asso.

$(a*b)*c$

$\frac{ab}{4} * c$

$\frac{abc}{16}$

$a*(b*c)$

$a * \frac{bc}{4}$

$\frac{abc}{16}$

$=$

③ Identity element

$a*e = a$

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

$e = 4$

verify $\frac{a}{b} \in Q$ $b \neq 0$

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

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

④ $a^{-1} = ?$ if $a \neq 0$ then

assume $a^{-1} = b$

$a*b = 4$

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

$a^{-1} = \frac{16}{a}$

$0^{-1} = ?$

$0*b = 4$

$\frac{0*b}{4} = 4$ } $b \in DNE$

⑤ Commutative

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

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

ex: True / false

✗ for any binary operation * on N, $a*a=a$ $\forall a \in N$

counter ex. $(N,+)$ $2+2 \neq 2$

every Structure has Idempotent } property false

$a \# a = a$ → Idempotent element

② * ... some binary operation

& '*' is commutative

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

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

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

order of a group

Order of any Structure

cardinality of Base Set

finite Structure : Base set is finite

↳ can never be empty

ex.

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

order = 2 ← no. of element in the set

ex: give a semi-group w/o an identity element

Semi-group But not monoid

ex: $(N,+)$

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

→ closed

→ Asso.

ex: $(S,*)$ & $|S|=1$

How many different binary opⁿ. we can define? only one binary opⁿ

$(S,*)$ — binary operatⁿ is a mapping/ functⁿ

$* : S \times S \longrightarrow S$

$(S=\{a\}, *)$ } only one possible

$a*a=a$

$(S,*)$ "no. of binary opⁿ" is same as "no. of functⁿ from $S\times S \longrightarrow S$"

$*: S\times S \longrightarrow S$

#functⁿ = # binary opⁿ $= |S|^{|S\times S|}$

So, $|S|=1 \longrightarrow$ #binary opⁿ $=1$

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

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

ex. $(S,*)$; $|S|=n$; no. of commutative binary opⁿ?

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

(a,a) — 2 choice
(b,b) — 2 choice
(a,b)
(b,a) — 2 choice's

a
b

#comm. binary opⁿ $= 2\times2\times2$

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

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

$\Rightarrow n^{\frac{n^2+n}{2}}$ no. of comm. binary operatⁿ

$|S|=n$

(1,1) — n choice
(2,2) — n choice
(3,3) — ---//---
(n,n) — n choice

n^n

(1,2)(2,1) — n choice } $n^{\left(\frac{n^2-n}{2}\right)}$

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

Properties of Monoid

- Identity is always unique (atmost 1)

- Left cancellation property.
  if $a \# b = a \# c$
  then $b = c$

- Right cancellation property
  If $a \# b = c \# b$
  then $a = c$

- Do we have left cancellation property in monoid. (no) In monoid we don't have left or Right cancellation property.

ex: $(N, *)$ $a * b = \max(a, b)$
↳ monoid; $e = 1$

Q: If $a*b = a*c$ then $b = c$? (no) so, no left cancellation.
$3*1 = 3*2$ But $1 \neq 2$
3 3

ex: $(Z, \times)$ — monoid; $e = 1$
↳ Associative
↳ Closed.

Q. In $(Z, \times)$, if $a \times b = a \times c \Rightarrow$ then $b = c$? no
$5 \times 6 = 5 \times b \Rightarrow b = 6$
but not always.

counter ex. $5 \times 0 = 6 \times 0$ But $5 \neq 6$
So, no Right cancellation

Idempotent property $\Rightarrow$ all element are Idempotent

$\forall a \quad a \# a = a$

ex: $(R - \{0\}, \times)$
no Idempontent property
$2 * 2 \neq 2$

ex: $(N, *)$, $a * b = \max(a, b)$
Idempotent property
$a * a = a$

$R^\circ = R - \{0\}$

$(R^\circ, \times)$ — no idempotent property

Idempotent element = 1

↳ not Idempotent element = $-1, 2$

$a \neq 1$

ex. $(\mathbb{Z}, \times)$ — $e = 1$ → Doesn't have inverse property

3^{-1} = Inverse of $3 = \frac{1}{3}$

$5^{-1} = \cdots = 5 = \frac{1}{5}$

$0^{-1} = \cdots = \text{ONE}$

ex: A binary operation $*$ on a set S is commutative if there exist $a, b \in S$ such that $a*b = b*a$ — false

Commutative

$\forall a,b \quad a*b = b*a$

not commutative: atleast one counter example

$\exists a,b \quad a*b \neq b*a$

ex: if G is a group But not Abelian then

① ~~$\forall a,b \cdot a*b \neq b*a$~~ is it possible that it's correct? — never.

② $\exists a,b \quad a*b \neq b*a$

where a, b are different

$a = x, b = e$

b/c group

$x*e = e*x = x$

$a = e, b = e$

$e*e = e*e$

$a = x, b = x$ then

$a*b = b*a$

$x*x = x*x$.

$a = x, b = x^{-1}$

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

In every group.

$a*e = e*a = a$

the commutative property will always be there

these will always be there but for remaining we don't know.

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

ex: (set of invertible $n \times n$ matrices, $\times$) is group But not Abelian group.
↳ matrix multiplication

① closed $M_{n\times n} P_{n\times n} = Q_{n\times n}$

② Associative $(MP)N = (M)(PN)$

③ Identity — Identity matrix.

④ Inverse

⑤ matrix mull is (not) Commutative
$AB \neq BA$

$IA = AI = A$ $\quad$ $AA^{-1} = A^{-1}A = I$

Practice Questn any non-empty set A

① $(P(A), \cup)$ ---- monoid $e = \phi$

② $(P(A), \cap)$ ---- monoid $e = A$

③ $(P(A), -)$ -- not Semi-Group (not monoid)
↓
Set diff. not Asso.

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

$P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$ (A)
↓ Base set
element of Base set.

Union $e = \phi$ $\quad$ Intersection $e = A$

Some Common group

✓ $(Z, +)$
✓ $(R, +)$
✓ $(Q, +)$
✓ $(C, +)$
↓
Set of Complex no.

$(N, +)$ X not group
↳ 'e' = DNE

$(\omega, +)$ X not group
↳ 3^{-1} = DNE

$(R, \times)$, $(Q, \times)$, $(Z, \times)$ } not group b/c 0^{-1} = DNE

✓ $(R^0, \times)$ --- $(R - \{0\}) = R^0$
✓ $(E^0, \times)$ --- $(E - \{0\}) = E^0$
✓ $(Q^0, \times)$ --- $(Q - \{0\}) = Q^0$

Some Imp. groups

Caddition modulo n,
Roots of unity)

① Root of unity (Roots of 1).

① $x=1$ then how many soln

$\Downarrow$

$x=\{1\}$

$(\{1\}, \times)$ Group; $e=1$

② $x^2=1 \Rightarrow \underbrace{x=\{1,-1\}}_{\text{Solution}}$ → Root's of unity

$(\{-1,1\}, \times)$ Group; $e=1$

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

order is 2 — $e^{-1}=e$ — $(-1)(\ )=1$, $\downarrow -1$

③ $x^3=1$

$x^3-1=0 \Rightarrow x^2(x-1)+x(x-1)+(x-1)$

$x^3-x^2+x^2-x+x-1$

(x^3-1)

$(x-1)(x^2+x+1)=0$

$x=1$ will satisfy

$x\neq 1$

$x^2+x+1=0$

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

$x=\frac{-1\pm\sqrt{1-4}}{2}$

$x=\frac{-1\pm\sqrt{-3}}{2}$

$\sqrt{-3} \Rightarrow \sqrt{3}\sqrt{-1}$

$\sqrt{-1}=i$

$x=\frac{-1\pm i\sqrt{3}}{2}$

$x^3=1 \Rightarrow \left\{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right\}$

$x=(1)^{1/3}$ → Cube root of 1

3 soln. → ω, ω^2

or

ω^2, ω.

$x=1,\omega,\omega^2$ → cube roots of unity → 1

these are the soln

Some Property

Add all the 3 sol.

$1+\omega+\omega^2=0$

$\omega^3=1$ put $x=\omega$

ex: $(\{1,\omega,\omega^2\}, \times)$ Abelian group.

- is closed ⇒ $\omega\cdot\omega=\omega^2$, $\omega\cdot\omega^2=\omega^3=1$, $1\cdot\omega^2=\omega^2$, $\omega^2\cdot\omega^2=\omega^4$, $\omega^3\cdot\omega \Rightarrow 1\cdot\omega=\omega$
- is Assoc.
- Identity element $e=1$
- Inverse ⇒ $1^{-1}=1$, $e^{-1}=e$, $\omega^{-1}\Rightarrow \omega\cdot\omega^2=1$, $(\omega^2)^{-1}\Rightarrow \omega^2\cdot\omega=1$
- Commuta.

④ $x^4=1 \Rightarrow x=\{1,-1,i,-i\}$ 4th Root of unity

$x^4=1 \Rightarrow x^4-1=0$

$a^2-b^2=(a+b)(a-b)$

$(x^2-1)(x^2-1)=0$

$x^2=1 \Rightarrow x=\pm 1$

$x^2=-1 \Rightarrow x=i,-i$

Property of i

$i=\sqrt{-1}$

$i^2=-1$

$i^3=i^2\cdot i=-i$

$i^4=i^2\cdot i^2=1$

$i^{18}=(i^9)(i^9)=-1$

1 $\quad$ -1

$(\{1,-1,i,-i\},\times)$ is Abelian group

- Asso.
- Closed $\Rightarrow -i\times -i=-1$
- Comm.
- Identity element $e=1$
- Inverse

- $1^{-1}=1 \quad (e^{-1}=e)$
- $(-1)^{-1} \Rightarrow (-1)(-1)=1$

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

- $i^{-1}=?$

$i\cdot(-i)=1$

$i^{-1}=-i \; ; \; (-i)^{-1}=i$

note

for all $n\geq 1$ nth Roots of unity is Abelian group under multiplication

Conclusion

① $x=1 \Rightarrow x=(\{1\},\times)$ Abelian group

② $x^2=1 \Rightarrow x=(\{1,-1\},\times)$ Abelian group

2 Root of unity

③ $x^3=1 \Rightarrow x=(\{1,\omega,\omega^2\},\times)$ Abelian group

$x=1^{1/3}$

3 Roots of unity

④ $x^4=1 \Rightarrow x=(\{1,-1,i,-i\},\times)$ Abelian group.

$x=1^{1/4}$

4th Root of unity

⋮

⑤ $x^n=1 \Rightarrow x=\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ Abelian group under multiplication.

n Soln

nth Root of unity

② Addition modulo 'n' (Z_n)

$n \in N$

$Z_n = \{0, 1, 2, \ldots, n-1\}$

↳ all the Remainder when divided by 'n'

i.e $Z_3 = \{0, 1, 2\}$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

operation: Addition %. n

$(Z_n, \oplus_n) \Rightarrow a \oplus_n b = (a+b) \%. n$

ex: $(Z_4, \oplus_4) = (\{0, 1, 2, 3\}, \oplus_4)$

① understand the operatn

$1 \oplus_4 3 = (1+3) \%. 4 = 4 \%. 4 = 0$

$3 \oplus_4 2 = 1$;

$0 \oplus_4 3 = 3$

④ inverse $(\{0, 1, 2, 3\}, \oplus_4)$ $e = 0$

- $0^{-1} = 0$ $(e^{-1} = e)$
- $1^{-1} = ? \Rightarrow 1 \oplus_4 (3) = 0$
- $2^{-1} = ? \Rightarrow 2 \oplus_4 (2) = 0$
- $3^{-1} = ? \Rightarrow 3 \oplus_4 (1) = 0$

So, $1^{-1} = 3$ & $3^{-1} = 1$ & $2^{-1} = 2$

In general: $(Z_n, \oplus_n)$ $n \in N$

$Z_n = (\{0, 1, 2, \ldots, n-1\}, \oplus_n)$

① closed

② Assoc.

③ $e = 0$

④ commu.

⑤ $a^{-1} = n - a$; $\forall a \neq 0$

$0^{-1} = 0$.

① closed ? yes

② Assoc. just like Addition

③ identity element $e = ?$ $\boxed{e = 0}$ $\Rightarrow 0 \oplus_4 2 = 2$

$0 \oplus_4 1 = 1$

X $1 \oplus_4 3 = 0$

1 is not the identity element.

⑤ commu.

$\Rightarrow a^{-1} = ?$

$a \oplus_n (\quad) = 0$

$\Rightarrow (a + (\quad)) \%. n = 0$

$n - a$

{as $m \bmod m = 0$}

Group property

① proof: let $(G,*)$ be a group
the identity element is unique.
always be unique.

$e, e' \Rightarrow$ Identity

$e = I_d$ | $e' = I_d$

$e * e' = e'$ | $e' * e = e$

so, $e * e' = \boxed{e' = e}$ is unique

② proof: that in a group every element has unique inverse?

- proof By contradiction

assume a has two inverse $\boxed{b, c}$

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

so, $\boxed{a*b=e}$; $\boxed{a*c=e}$

$\Rightarrow a*b = a*c$

multiple both side by a^{-1}

$\Rightarrow a^{-1} * (a*b) = a^{-1} * (a*c)$

B/c group is Asso. we can write like there

$(\underbrace{a^{-1}*a}_{e})*b = (\underbrace{a^{-1}*a}_{e})*c$

$e*b = e*c$

$\boxed{b=c}$

both inverse are Same

③ proof: that group has left cancellation property.

$\boxed{\text{if } a*b = a*c \text{ then } b=c}$

assume

$a*b = a*c$

$d \quad\quad d$

So, $a^{-1}d = a^{-1}d$

So, multiply by a^{-1}

$a^{-1} * (a*b) = a^{-1} * (a*c)$

Group is Associ.

$(\underbrace{a^{-1}*a}_{e})*b = (\underbrace{a^{-1}*a}_{e})*c$

$e*b = e*c$

$\boxed{b=c}$

④ Prove that group has Right cancellation property?

$a*b = c*b$

multiple both side by b^{-1}

$(a*b)*b^{-1} = (c*b)*b^{-1}$

b/c of Assoc.

$a*(b*b^{-1}) = c(b*b^{-1})$

$\boxed{a=c}$

In group:

if, $a*b = a*c \Rightarrow b=c$

if, $a*b = c*b \Rightarrow a=c$

But not $a*b = b*c \not\Rightarrow a=c$

- possible in Abelian group.

b/c group is not comm.

⑤ $(a^{-1})^{-1} = a$

$a=b^{-1}$ iff $b=a^{-1}$

⑥ prove $(ab)^{-1} = b^{-1}a^{-1}$

$ab = a*b$

let's $(ab)^{-1} = y$ ⟶ we need to find y.

means

$aby = e$

multiple both side by a^{-1}

$\Rightarrow (a^{-1}(a)by) = a^{-1}e$

e by a^{-1}

$\Rightarrow by = a^{-1}$

now, multiple by b^{-1} on both side

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

e $y = b^{-1}a^{-1}$

so,

$y = b^{-1}a^{-1}$

Associativity & parantheses

In propositional logic.

$F \wedge T \wedge F = F$

IS Associative

$(F \wedge T) \wedge F = F \wedge (T \wedge F)$

$F \to T \to F$ is Ambiguous.

→ not assoc.

$(F \to T) \to F$

$T \to F$

F

$F \to (T \to F)$

$F \to F$

T

if $(a \to b) \to c$ ≠ nonambiguous.

& $a \to (b \to c)$

- In no. theory.

$2+3+2$ is Asso.

$\Rightarrow 7$

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

$2-3-2$ is not Asso.

$(2-3)-2$

$\Rightarrow -3$

$2-(3-2)$

$= 1$

what properties do no. allow us to remove parentheses from expressions.

↳ Associativity : +, × (∧) → conjuction

Cayley table/ operation table/ multiplication table

A binary operation "*" on a finite sets can be displayed as cayley table

∧	F	T
F	F	F
T	F	T

Header

F∧T=F

ex $(\{T,F\}, \wedge)$ → closed

→ Asso.

→ Identity element $e=T$ it's monoid.

→ Inverse doesn't exist.

$F \wedge \underset{\text{DNE}}{?} = T$

$T^{-1}=T$

$F^{-1}=DNE$

ex: $(\{0,1\}, \times)$ → is monoid ($e=1$)

→ not a group.

×	0	1
0	0	0
1	0	1

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

$0 \times \underset{\text{DNE}}{?} = 1$

ex: $(\{1,-1\}, \times)$ → Asso.

→ group.

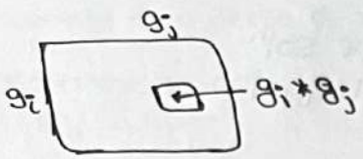
→ $e=1$ identity element

→ Inverse

×	-1	1
-1	1	-1
1	-1	1

- $1^{-1}=1$
- $(-1) \times \underset{-1}{?} = 1$
- $(-1)^{-1}=-1$

General



- Let G be a group with operation "*" & Cayley table

i.e abc → unambiguous. but it's fine b/c "*" is Associative. (given that it's a group)

$(ab)c = a(bc)$

$abc = a*b*c.$

Q. G is a group & $a, b \in G$

$ax=b$ & $xa=b$ has a unique sol^n

sol^n

$x = a^{-1}b$ & $x = ba^{-1}$

Group $(G, *)$

$ax=b$ then what is $x=?$

$ax=b$

$\Rightarrow a^{-1}ax = a^{-1}b$

$ex = a^{-1}b \Rightarrow x = a^{-1}b$ is a sol^n

↳ is it a unique sol^n

b/c of a^{-1} we can use it & also we don't need parantheses.

note

- Proof by Contradiction.

assume 2 sol^n of $ax=b$ → y, z

$x=y$ is solution means $ay=b$

$x=z$ is solution means. $az=b$

so, $ay = az \Rightarrow y = z$

In group $(G, *)$

- $ax=b$ has unique sol^n $x = a^{-1}b$
- $xa=b$ has unique sol^n $x = ba^{-1}$

In cayley table of group:

	y	z
a	b	b

$ax=b \Rightarrow$ has unique soln
↳ unique x will satisfy it

ex: in a Group $(G,*)$ $a \in G$ means $\exists a \in G$ then $a=?$ if $a^2=a$

Doesn't mean group is Idempotent. b/c we are not saying $\forall a$

$\Rightarrow a^2=a$
$\Rightarrow a \cdot a = a$
$\Rightarrow a \cdot a = a \cdot e$
$\Rightarrow a=e$

$a=ae$
$x=x \cdot e$

note
In group, $\forall a$
$a=ae$
$a=ea$
→ By definition of Identity element.

ex: In a group $(G,*)$

① $a*e=a$ for $\forall a \in G$ } By definition of Identity element.

② if $b*a=e$, then $a*b=e$

if $b*a=e$ then $a*b=?$

$\Rightarrow ba=e$ $\quad baa^{-1}=ea^{-1}$

$\Rightarrow b=a^{-1}$ $\quad b=a^{-1}$

x
$ba=e$
$b=ea^{-1}=a^{-1}$
unique soln

so, $ab=?$

$a \cdot a^{-1}=e$

ex: we know that In group $(G,*)$

$aa^{-1}=a^{-1}a$
$ae=ea$
} Do these imply Abelian? no.

these commutative properties are in every group.

Conclusion

① Identity & inverse of a element. is unique

② Both the cancellation law hold (left & Right)

③ $(a*b)^{-1} = b^{-1} * a^{-1}$

④ In a group, identity element is it's own inverse

$e^{-1} = e$

⑤ order of a group. the no. of element in a group.

⑥ Finite. group. if the order of the group G. is finite

Imp. Result.

① G is monoid, Identity element is unique.

② G is group;

(i) if $c \in G$ & $cc = c$ then $c = e$

(ii) For $\forall a, b \in G$ if $ab = ac$ then $b = c$ & if $ba = ca$ then $b = c$

(iii) $a \in G$ the inverse of a a^{-1} is unique.

(iv) $\forall a \in G$ we have $(a^{-1})^{-1} = a$

(v) $\forall a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$

(vi) $\forall a, b \in G$ the eqn $ax = b$ & $ya = b$ have unique Soln $x = a^{-1}b$ & $y = ba^{-1}$

ex. In a Group G;

a, b, c are different element of G.

is it possible that $a*b = a*c$? (no)

if $ab = ac$ then $b = c$

so contrapositive.

if $b \neq c$ then $ab \neq ac$

Cayley table of group

	b	c
a	(h)	≠ (g)

if $b \neq c$ then $ab \neq ac$

Checking Associative property in a cayley table → it's not simple to check assoc.

Structure: $(S, \#)$ — binary operation

$(S, \#)$ is Associative iff $\forall a,b$ $(a\#b)\#c = a\#(b\#c)$

$(S=\{a,b,c\}, \#)$ — binary opⁿ

To check for Associative prop.:

$(x,y,z) \in S$ (∈S ∈S)

for every triple $(x\#y)\#z \stackrel{?}{=} x\#(y\#z)$

no. of triple: is. (x,y,z)

each × 4 choices have $\{a,b,c,d\}$ $\Rightarrow 4\times4\times4 = 64$ triple.

Time Compⁿ: $O(n^3)$

for every triple (x,y,z) you need to check. $(x\#y)\#z \stackrel{?}{=} x\#(y\#z)$

no. of triple: n^3

ex: Is these Structure Associative?

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

$S = \{a,b,c,d,e\} \Rightarrow |S| = 5$

it's not Associative

$(c*e)*e \stackrel{?}{=} c*(e*e)$

$a*e \stackrel{?}{=} c*c$

$d \neq b$

Note

To check associativity, never include Identity element. bic it will always satisfy.

ex: $(a\ e)b \stackrel{?}{=} a\ (e\ b)$ ←

$ab = ab$

Properties of cayley table of a group

→	T	F
T	T	F
F	T	T

T→F

F→T

ex: $(\{T,F\}, \rightarrow)$

Groupid, not even Semi-Group.

- Find Identity property "e" from cayely table

I_d	a	b	c
a	a	b	c
b	b		
c	c		

- Find commutative property from cayley table ⟷ Symmetric table (matrix)

	a	b
a		a*b
b	b*a	

// should be Same

- cayley table's of group's.

① cayley table we create for finite group. (Structure)

② each element in a row appear exactly once. & column.

③ every Row/column is simply a permutation of all element (every element appear exactly once)

④ Row & column of I_d element is Exactly Same as the Header.

note

cayley table of group

no Repetition in any Row, any column.

ex: $G: \{a,b,c,d\}$

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

Should not repeat.

& e=DNE

Identity element

ex:

	θ	a	b	c	d	e
θ	θ	a	b	c	d	e
a	a	θ	c	d	e	b
b	b	c	θ	e	a	d
c	c	d	e	θ	b	a
d	d	e	a	b	θ	c
e	e	b	d	a	c	θ

① closed

② Identity element = θ

③ Inverse
- $\theta^{-1} = \theta$
- $a^{-1} \Rightarrow a \cdot (?) = \theta$, a
- $b^{-1} = b$ $c^{-1} = c$ $d^{-1} = d$ $e^{-1} = e$

④ checking Assoc. for a,b,c

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

$c*c \stackrel{?}{=} a*e$

$\boxed{\theta \neq b}$

⑤ commutative

So, it's not a group

Q. $G = (\{e, a, b, c, d\}, *)$ be group.

if $ab = e$ (identity element)

$\boxed{a^{-1} = b \; ; \; b^{-1} = a}$

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

→ dX b/c of repeatation

"c" can't come here b/c of repeatation

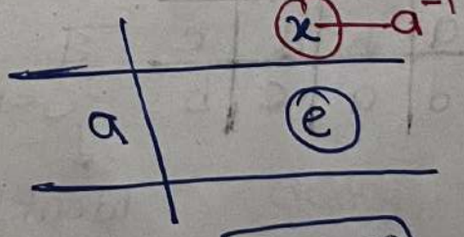
find inverse for every element
- $e^{-1} = e$
- $a^{-1} = b$
- $b^{-1} = a$
- $c^{-1} = d$
- $d^{-1} = c$

is the cayley table Abelian.

iff it's symmetric

∀ $\boxed{i^{th} \text{ Row} = i^{th} \text{ column}}$

e: Identity element



$\boxed{a*x = e}$

monoid vs group

ex: In a group
$a*a=a$ then $a=e$

$a*a=a$

$\not{a}*a=\not{a}*e$ (Group → left cancellation)

$a=e$

$a*e=a;\forall a$

(monoid with inverse) group

- unique identity
- unique inverse
- left cancelation
- Right cancelation.

vs

ex: In a monoid if $a*a=a$ then $a=e$

Counter example

$(\mathbb{N},*)$; $a*b=\max(a,b)$

$e=1$.

$5*5=\max(5,5)=5$

$5*5=5$ But $5\neq e$

monoid

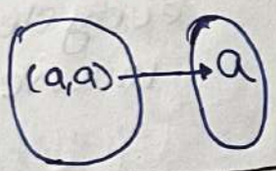
- unique identity
- Inverse may not exist for some element
- no left or Right cancellation

Group of Small Order

ex: How many different binary operation we can have with order 1 Structure. (function)

only one binary operation

i.e $(\{a\},*)$



ex: How many group of order 1 can you create. (non-isomorphic)

Group of order 1.

- $(\{T\},\wedge)$
- $(\{T\},\vee)$
- $(\{0\},+)$ .... infinite.

all of them are isomorphic

Isomorphic ≡ Same Structure

How many non-Isomorphic Groups of order 1 are there?

only 1.
Template.

	a
a	(a)

} is closed
↳ $e=a$
↳ $a^{-1}=a$
↳ Asso.
↳ comm.

So, every order 1 group is Abelian

Ex: How many non-isomorphic groups of order n.
≡ How many Abstract template of Groups of order n

Order 2 group → so one should be identity element.

	e	a
e	e	a
a	a	e

} only 1 template for group of order 1.

↳ is Abelian

Order 3 group → one of the element is identity element.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

} only 1 group of order 3

⇒ Abelian.

Order 4 groups

↳ 2 non-isomorphic groups

↳ and both are abelian. (Str+. 3 & (Str+. 1 or Str+. 2))

↳ 2 template of group

Str+3	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(e, x, y, z)

$x^{-1} = x$

$y^{-1} = y$.

$z^{-1} = z$

every element is inverse of itself.

Order 4 group

Str+.1	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

(e, x, y, z)

$x^{-1} = x$

these both are inverse of each other)

≡ are iso-morphic

Str+.2	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(e, x, y, z)

$x^{-1} = x$

inverse of each other.

Order 4 "Group" Templates.

only 2 non-isomorphic groups.

① $\{e, x, y, z\} \Rightarrow x^{-1}=x,\ y^{-1}=z$

② $\{e, x, y, z\} \Rightarrow x^{-1}=x,\ y^{-1}=y,\ z^{-1}=z$

} both are Abelian

gate 2007

- no. of different non-isomorphic Abelian group / group of order 4. (2)

ex: no. of different non-isomorphic non-Abelian group of order 4. (0)

note

group order	non-isomorphic groups	non-isomorph^n Abelian group
1	1	1
2	1	1
3	1	1
4	2	2

ex: $(\{0,1,2\}, \oplus_3)$ → group (order 3)

$\{0,1,2\}$ → Z_3

$\oplus_3$ → Addition modulo 3.

$\{0, 1, 2\}$

$e \quad x \quad y$

$x^{-1}=y,\ y^{-1}=x$

$1^{-1}=2$

$2^{-1}=1$

group of order 3 → only one template.

and that is also abelian.

$\{e, x, y\}$

e → Identity

$x^{-1}=y$ & $y^{-1}=x$

$(\{1, \omega, \omega^2\}, \times)$

$(\{0,1,2\}, \oplus_3)$

$(\{e, a, b\}, \#)$ $(a^{-1}=b,\ b^{-1}=a)$

e → Identity element

] Same Structure (isomorphic)

Power of element in group

ex: In groupoid, can we say that

① $(a*b)*c = a*(b*c)$ no

② $(a*a)*a = a*(a*a)$ no

Counter example

$(P\{1,2,3\}, -)$ → groupoid

↳ not-Asso.

$P\{1,2,3\}$ → Base set, $|\text{Base set}| = 8$

↳ set Diffe.

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

$(\{1\}-\{1\})-\{1\} \neq \{1\}-(\{1\}-\{1\})$

ex: In a semi-group, can we say.

③ $(a*a)*a = a*(a*a)$ yes

b/c of Assoc. property.

Power of element

ex: $(G, *)$ — Group $\forall a \in G$

↳ any group opn

$a^3 = a*a*a = aaa$

$a^1 = a$

$a^2 = aa = a*a$

$\vdots$

$a^n : a^{n-1}a, \forall n \geq 1$

$a^{-n} : (a^{-1})^n$ for $\forall n \geq 1$

$a^{-3} = (a^{-1})^3$

$= (a^{-1})*(a^{-1})*(a^{-1})$ → group opn

$a^0 = e$ → is definition

note

- Power is define for any semi-group
- So, whenever you have these Assoc. property you can have these powers.

ex: $(\{1,2\}, \otimes_3)$ → is group

↳ identity element $e = 1$

$1^5 = (1\times1\times1\times1\times1) \bmod 3 = 1$

$1^2 = 1 \otimes_3 1 = (1\times1) \bmod 3 = 1$

$1^3 = 1^2 \cdot 1 = 1\cdot1 = 1$

$2^2 = 2 \otimes_3 2$

$\Rightarrow (2\times2) \bmod 3 \neq 1$

ex: $(\{0,1,2\}, \oplus_3)$ → group ($\{0,1,2\} = Z_3$)

$2^2 = 2 \oplus_3 2 = 4 \bmod 3 = 1$

$1^2 = 1 \oplus_3 1 = 2 \bmod 3 = 2$

ex: $(\omega, +)$ → not a group
↳ but is monoid

$2^3 = 2+2+2 = 6$

$2^n = 2n$

$2^0 = e = 0$

2^{-1} = ONE (not a group)

"But" power of element is Defined for any semi-group (Associative)

theorem

$a \in G$ & Group G
m, n are Integers.

① $a^n a^{-n} = e$
② $a^m a^n = a^{m+n}$
③ $(a^m)^n = a^{mn}$

} b/c of Assoc. & Inverse.

ex: $a^3 a^2 = a^5 \Rightarrow (aaa)(aa) = (aaaaa)$

ex: $a^m a^{-n} \Rightarrow a^{m-n}$

ex: $(a^2)^3 \Rightarrow a^2 \cdot a^2 \cdot a^2$
$\Rightarrow (aa)(aa)(aa) \Rightarrow aaaaaa$

ex: $(N, +)$ → is semi group

$1^2 = 1+1 = 2$

2^0 = not define (b/c no identity element)

ex: $(\{1, -1, i, -i\}, \times)$ $i^{-1} = -i$

$i^{-3} = ? = (i^{-1})^3 = (-i)^3 = -i^3 = i$

$(-i)^{-5} = -i^{-5} = -(i^{-3} \cdot i^{-2})$
$= -(i \cdot i^{-2}) \Rightarrow (i)$

$i \times \bigcirc = 1$, $\bigcirc = -i$

$\Rightarrow \boxed{i^{-2} = (-i)^2 = -1}$

$(-i)^{-4} = ?$
$(-i)^{-4} = ((-i)^{-1})^4$

$\boxed{(-i)^{-1} = i}$
$\boxed{i^{-1} = -i}$

$\Rightarrow (i)^4 = i \times i \times i \times i$ (group operation)
$= 1$

$\boxed{a^{-5} = (a^{-1})^5}$

Subgroup

Subset which is a group (under same operatn).

Group $(G, *)$

Subgroup of G: $(H, *)$

$H \subseteq G$ & $(H, *)$ is a group

ex: $(\{1, -1, i, -i\}, \times)$ ---- group

↳ $e = 1$

note

if operatn "$*$" is understood then we directly say "G is a group" instead of saying "$(G, *)$ is a group"

- which is a subgroup?

① $(\{1, -1\}, \times)$

② $(\{1, 0\}, \times)$ → not even the subset

③ $(\{1, i\}, \times)$ there is not a group.

↳ it's not closed.

$i \times i = -1$.

④ $(\{0\}, +)$ nonsense bcz we are changing the operation

$G = \{1, -1, i, -i\}$ under mul

Subgroup of G

① $\{1\}$

② $\{1, -1\}$

③ $\{1, -1, i, -i\}$

it should be present as it's the identity element.

not subgroups of G.

① $\{-1\}$ → not closed.

② $\{i, -i\}$ → not closed.

③ $\{1, i, -i\}$ → not closed.

④ $\{1, -i\}$ → not closed.

$H = (\{1, -i\}, \times)$ ---- not closed.

$(-i) \times (-i) = -1 \notin H$.

↳ not subgroup

ex: $(\mathbb{Z}, +)$

Subgroup: ① $\mathbb{Z}$

② $\{0\}$

③ $2\mathbb{Z}$

④ $3\mathbb{Z}$

⑤ $4\mathbb{Z}$

⑥ $n\mathbb{Z}$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$\mathbb{Z}_n$ (or) $\mathbb{Z}/n\mathbb{Z}$

$2\mathbb{Z} = \{0, 2, -2, 4, -4 \ldots\}$ | $n\mathbb{Z} = \{nx / x \in \mathbb{Z}\}$

↳ even no.

multiple of n.

$2\mathbb{Z}$
all even no.
$\Rightarrow \{0, -2, 2, -4, 4 \ldots\}$

$\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$
$\{0, 1\}$

ex: $(\mathbb{Z}, +)$ ....group.
$\forall n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$

$n = 4$
$(4\mathbb{Z}, +)$ → is closed → it's a group
- is a subset & is a same operation
- $e = 0$
- Inverse $(4n)^{-1} = -4n$
- Assoc.

ex: $G: (\mathbb{Z}, +)$
How many finite subgroups of G? (1)
$(\{0\}, +)$

Idea $(G: \{e, a_1, a_2 \ldots\}, *)$
Create subgroup of G.
$H = \{e, a_1, a_1^{-1} \ldots\}$
- if you take a_1 comes as pair
- should also be taken
- subset of G which is a group (under $*$)

if you take a_1
$H = \{e, a_1, a_1^{-1}, a_1^2, a_1^3 \ldots\}$
$a_1^{-1}, a_1^2, a_1^3 \ldots$ will come bcoz of a_1

it should follow
it should contain
1. identity property
2. closure property
3. inverse property

1. take "e" of G in H
2. if $a_1 \in H$ then $a_1^{-1}, a_1^2, a_1^3, a_1^4 \ldots$ should be taken
   - a_1^{-1}: bcoz inverse property
   - a_1^2: bcoz closure property

ex: $(\mathbb{Z}, +)$
Create subgroup:
$H = \{0, 3, 3^2, 3^3, 3^4 \ldots, 3^{-1}, (-3)^2, (-3)^3, \ldots\}$
- -3
- $3^{-1}, (-3)^2, (-3)^3$: bcoz closure property
- 0: mandatory
- $3, 3^2, 3^3, 3^4 \ldots$: if we take 3, we need to take these bcoz of

ex: $G = \{e, a, b, c, \ldots\}$ assume $a^{-1} = d$. Subgroup that contain "a" $H = \{e, a, a^2, a^3, \ldots\}$

note

Any non-empty subset H of Group G which satisfies.

$\forall a, b \in H \{ a * b \in H, a^{-1} \in H \}$ then $e \in H$?

yes

b/c H is non empty.

non Empty $H \subseteq G$
- closed
- $a^{-1} \in H, \forall a \in H$

Proper subgroup → $H \subset G$

↳ H is subgroup of G & $H \neq G$

note

$(G, *)$ ... group

① $(\{e\}, *)$ — Trivial subgroup

② $(G, *)$ — Subgroup of G.

ex: Z_9 under operation $+$

$(Z_9, \oplus_9)$ → is group

the subset $\{0,3,6\}$] $(\{0,3,6\}, \oplus_9)$ ... proper subgroup

↳ closed

↳ $e = 0$

$3^{-1} = 6$

& $6^{-1} = 3$

- A very special subgroup

Subgroup generated by an element

$(\mathbb{Z}, +)$ → is a group

Subgroup generated by 2 ≡ $\langle 2 \rangle$ ≡ Smallest subgroup that contains 2 (denoted as.)

$\langle 2 \rangle = \{0, 2, 4, 6, 8, \ldots, -2, -4, -6, \ldots\}$

$= 2\mathbb{Z}$

$\langle 2 \rangle = \{2^0, 2^1, 2^2 \ldots, 2^{-1}, 2^{-2} \ldots\}$

So $\langle 2 \rangle = \{2^n / n \in \mathbb{Z}\}$

ex: $(\{1, i, -1, -i\}, \times)$

Subgroup generated by $|a| = 2$

$\langle i \rangle = \{e=1, i, i^2, i^3, \ldots, i^{-1}, i^{-2}, \ldots\}$

$= \{1, i, -1, -i\} =$ G itself

Subgroup generated by -1

$\langle -1 \rangle = \{(-1)^0, (-1)^1, (-1)^2, \ldots\}$

$= \{1, -1, 1, \ldots\}$

So, $\langle -1 \rangle = \{1, -1\}$

$\langle 1 \rangle = \{1\} = \{1^0, 1^1, 1^2 \ldots 1^{-1}, 1^{-2} \ldots\}$

$= \{1, 1, 1 \ldots\}$

So, $\langle 1 \rangle = \{1\}$

Very Imp note .....

$(G, *)$ — group, let $a \in G$

$\langle a \rangle$ = subgroup generated by a

= Smallest subgroup that contain a

$\langle a \rangle = \{a^n / n \in \mathbb{Z}\}$

Group G, $|G|$: order of G [ord (G)]

(Cardinality of G)

Observation: $G = \{1, -1, i, -i, x\}$ → so Generator of G is $i, -i$

$\langle 1 \rangle = \{1\}$
$\langle -1 \rangle = \{1, -1\}$ } 1, -1 can't generator "G"

$\langle i \rangle = G$
$\langle -i \rangle = G$ } i, -i can generate whole "G"

- i is generator of G as it can generate whole G.
- -i is also generators of G.

Generator Group$(G, *)$

$g \in G$ is generator of G.

iff $\boxed{G = \langle g \rangle}$

ex: $(\mathbb{Z}, +)$ $\begin{cases} \langle 1 \rangle = \mathbb{Z} \\ \langle -1 \rangle = \mathbb{Z} \end{cases}$

Generator?

$\langle 1 \rangle = \{1^0, 1^1, 1^2, 1^3, \ldots, 1^{-1}, 1^{-2} \ldots\}$

$\langle 1 \rangle = \{0, 1, 2, 3, \ldots, -1, -2, -3 \ldots\}$

Subgroup generate by 2

$\langle 2 \rangle = \{2^0, 2^1, 2^2 \ldots, 2^{-1}, 2^{-2} \ldots\}$

$= \{0, 2, 4, 6, 8 \ldots\ldots -2, -4, \ldots\}$

$\langle 2 \rangle = 2\mathbb{Z} \neq \mathbb{Z}$

↳ not generator of 2

ex: $G: (\{0, 1, 2, 3\}, \oplus_4)$ → e=0

Generator? are 1, 3

$\langle 0 \rangle = \{0\}$

✓ $\langle 1 \rangle = \{0, 1, 2, 3\} = G$

$\langle 2 \rangle = \{0, 2\}$

✓ $\langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, \ldots 3^{-1}, 3^{-2} \ldots\}$

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

$1^0 = e = 0$
$1^1 = 1$
$1^2 = 2$
$1^3 = 3.$

$3^2 = (3+3) \bmod 4 = 2$
$3^3 = 9 \bmod 4 = 1.$

note Group $(G, *)$

① $\langle e \rangle = \{e^0, e^1, e^2 \ldots\ldots e^{-1}, e^{-2} \ldots\}$

$\langle e \rangle = \{e, e, e, \ldots\ldots \overset{\downarrow}{e} \ldots\ldots\}$

$\boxed{\langle e \rangle = \{e\}}$

② $\langle a \rangle = \langle a^{-1} \rangle$

$\{e, a^1, a^2, a^3, \ldots\ldots a^{-1}, a^{-2} \ldots\} = \langle a \rangle$

Same !!

$\{e, a^{-1}, a^{-2}, \ldots\ldots, a, a^2 \ldots\} = \langle a^{-1} \rangle$

Coprime OR Relatively Prime

- Coprime / relatively prime / mutually prime

Int a, b

a, b are coprime iff

$\boxed{GCD(a, b) = 1}$

ex: $9, 10$ are coprime

$GCD(9, 10) = 1$.

ex: which the integer less than 12 are relatively prime to 12

~~1~~ ~~2~~ ~~3~~ ~~4~~ ~~5~~ ~~6~~ ~~7~~ ~~8~~ ~~9~~ ~~10~~ ~~11~~

ex: which the no. less than (7) are relatively prime to 7

~~1~~ 2 ~~3~~ ~~4~~ 5 ~~6~~

(7) → prime no.

all less than 7 are coprime

ex: which the integer less than P are relatively prime to P

$\boxed{1, 2, \ldots\ldots P-1}$

ex: P (Prime no.) is always coprime with n if $1 \leq n < P$?

$\boxed{1, 2, \ldots\ldots P-1}$ prime no. P is coprime with each of them

multiplication modulon group (U_n)

U_n: the group of unit's in the Integer mod n).

In previous classes

$Z_n = \{0, 1, 2, \dots, n-1\}$

$(Z_n, \oplus_n)$ ... group

↓ Set of possible Integer when you divide by n

$a \oplus_n b = (a+b) \bmod n$.

ex $Z_4 = \{0,1,2,3\}$ $\otimes_4$

$Z_4 = \{0,1,2,3\} = \{0, 1, \dots 4-1\}$

- $a \otimes_4 b = (a \times b) \bmod 4$
- $3 \otimes_4 2 = (3 \times 2) \bmod 4$
  $\Rightarrow 6 \bmod 4 = 2$
- $3 \otimes_4 3 = 9 \bmod 4 = 1$

(e=1) identity element

$a \otimes_4 1 = a \bmod 4 = a$

↓

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

2^{-1}?

$2 \otimes_4 0 \neq 1$

$2 \otimes_4 1 = 2 \neq e$

$2 \otimes_4 2 = 0 \neq e$

$2 \otimes_4 3 = 2 \neq e$

$2^{-1} = DNE$

$3^{-1} = 3$

is monoid.

$(Z_4 = \{0,1,2,3\}, \otimes_4)$

- is closed
- is Assoc.
- identity element (e=1)
- doesn't have inverse property.
- is commutative.

ex: $0 \otimes_4 ? = 1$

DNE

$0^{-1} = DNE$

$1^{-1} = 1$

$2^{-1} = DNE$

$3^{-1} = 3$

- $(Z_n, \oplus_n)$ → is not group

it's commutative monoid.

ex: How to convert Z_n into a group under multiplicatn mod n operatn.

$\otimes_4$ → mul mod n

inverse ≡ multiplicative inverse.

i.e $(Z_4, \otimes_4)$

0^{-1} : DNE } problem
2^{-1} : DNE

3^{-1} : 3
1^{-1} : 1 — unit no. which have inverse

$(\{1,3\}, \otimes_4)$
- it's a Abelian group.
- consider as U_4
- ↳ there is group.
- it is closed i.e $1 \otimes_4 1 = 1$, $1 \otimes_4 3 = 3$, $3 \otimes_4 3 = 1$, $3 \otimes_4 1 = 3$
- also Asso.
- e = 1
- is inverse ex: $1^{-1} = 1$ & $3^{-1} = 3$
- is commu.

$(Z_4, \otimes_4)$

0, 1, 2, 3 — {1,3} → unit group. U_4

ex: $(Z_6, \otimes_6)$ — not a group.

2^{-1} : $2 \otimes_6 ? \neq e$ DNE

Problem

Clored, Asso., e=1

0^{-1} : DNE
1^{-1} : 1
2^{-1} : DNE
3^{-1} : DNE
4^{-1} : DNE
5^{-1} : 5

0, 2, 3, 4 don't have inverse under $\otimes_6$

Convert into group.

$(U_6 = \{1,5\}, \otimes_6)$ → is group

as $1^{-1} = 1$ & $5^{-1} = 5$.

Converting to group ($\{1,3,5,7\}$ are unit group.)

ex $(Z_8, \circledast_8)$

$(Z_8 = \{0,1,2,3,4,5,6,7\}, \otimes_8)$ → is clored
- ↳ Asso.
- ↳ e = 1.
- ↳ no inverse for {0, 2, 4, 6}

& $1^{-1} = 1$, $3^{-1} = 3$
& $5^{-1} = 5$, $7^{-1} = 7$

$(U_8 = \{1,3,5,7\}, \otimes_8)$ is a group

Conclusion: $(Z_n, \otimes_n)$ — not a group.

Problem? Inverse property

convert ↓ group.

Take all element that have inverse (unit group) U_n } $(U_n, \otimes_n)$

observation:
- which element have inverse?

ex: $Z_4 = \{0,1,2,3\}, \otimes_4$

(0,2) don't have inverse
↳ they are not coprime or relatively prime to 4.
$GCD(2,4) = 2$; $GCD(0,4) = 4$

(1,3) have inverse
↳ bcz they are coprime to 4
$GCD(1,4) = 1$, $GCD(3,4) = 1$

$Z_n, \otimes_n$ → (m) $\in Z_n$ has multiplicative inverse.
↳ Closed
Asso.
$e = 1$.

m, n are co-prime
↳ m is unit

$(Z_n, \otimes_n)$ → not group

collect unit. → $(U_n, \otimes_n)$ Abelian group.

$U_n = \{m \in Z_n \mid m \text{ is unit}\}$

(or)

$U_n = \{y \mid y \in \{1, 2, \ldots n-1\}$
y is coprime with n.

ex $(G_{14}, \otimes_{14})$ not group.

↓

$(U_{14} = \{1,3,5,9,11,13\}, \otimes_{14})$ be group

- $(Z_n, \oplus_n)$ is Abelian group
- $(Z_n, \otimes_n)$ not a group but monoid
- $(U_n, \otimes_n)$ is group.

ex: $(Z_8, \otimes_8) \rightarrow (U_8 : \{1,3,5,7\}, \otimes_8)$ → is Abelian group.

Cayley table

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

- group
- Closed
- e=1.
- inverse
- comm.
- Asso.

$3 \otimes_8 3 = 1$

$3 \otimes_8 5 = 7$

$5 \otimes_8 3 = 7$

$U_8 : \{1,3,5,7\}$ ..... group of order 4

$U_{10} : \{1,3,7,9\}$ ..... group of order 4

$U_{12} : \{1,5,7,11\}$ ..... group of order 4.

- So there means atleast 2 of them as a same template (Isomorphic).

As we know

Group of order 4.

only Two template's.

① $\{e, x, y, z\}$ (e: id) $\rightarrow x^{-1}=x \,/\, y^{-1}=y \,/\, z^{-1}=z \,/\, e^{-1}=e.$

② $\{e, x, y, z\}$ (e: id) $\rightarrow x^{-1}=y \,/\, y^{-1}=x \,/\, z^{-1}=z$

$U_8 : \{1,3,5,7\}$

$3^{-1}=3 \,/\, 5^{-1}=5 \,/\, 7^{-1}=7$

↓

Template 1

$U_{10} : \{1,3,7,9\}$

$3^{-1}=7 \,/\, 7^{-1}=3 \,/\, 9^{-1}=9$

↓

Template 2

$U_{12} : \{1,5,7,11\}$

$5^{-1}=5 \,/\, 11^{-1}=11 \,/\, 7^{-1}=7$

↓

Template 1.

So, $U_8 \equiv U_{12}$ → same template, same structure, Isomorphic.

$U_8 \not\equiv U_{10}$ → Diff. structure

ex: Group G;
$a \in G$ & a is inverse of itself $\Big] \; a^{-1} = a$

then $\langle a \rangle$?

$\langle a \rangle = \{a^0 = e, a^1 = a, a^{-1} = a, a^2 = e$
$a^3 = a, a^{-2} = e \ldots .\}$

if $a = a^{-1}$
then
$a^2 = a \cdot a$
$= a \cdot a^{-1} = e$

$(G, *)$; $a \in G$ $\boxed{a^{-1} = a}$ → means.

$\langle a \rangle = \{a, e\}$

$\langle e \rangle = \{e\}$

$a^2 = e$

$a^{-2} = (a^{-1})^2 \Rightarrow a^2 = e$

$a^3 = a^2 \cdot a = e \cdot a = a$

a) Group $(G, *)$, let $a \in G$ $a^{-1} = a$
then $a = e$?
(no)

for $e \Rightarrow \boxed{e^{-1} = e}$

But $a^{-1} = a \not\Rightarrow e^{-1} = e$

ex: Group G which can be generated by element "a" & $a^{-1} = a$ then order of G $\Big]$ Group $(G, *)$; $\langle a \rangle = G$

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

a is generator of G
$\langle a \rangle : G$

$a^{-1} = a$
$\langle a \rangle = \{a, e\}$
$\langle e \rangle = \{e\}$

$|G| \leq 2$
$\boxed{|G| = 1 \text{ or } 2}$

$G(\{e\}, *)$
(or) $G(\{e, a\}, *)$

Order of an Element

Size of Subgroup generated by an element.

ex: $(\{1,-1,i,-i\},\times)=G \Rightarrow \langle i\rangle = G$, $\langle -i\rangle = G$

order of $G = 4 = |G|$

order of $1 = |\langle 1\rangle| = |\{1\}| = 1$

order of $-1 = |\langle -1\rangle| = |\{1,-1\}| = 2$

order of $i = |\langle i\rangle| = 4$; $|-i| = 4$

note

Group $(G,*)$; $a \in G$

order of $a = |\langle a\rangle|$

$|a| = |\langle a\rangle| = o(a)$

order of a.

ex: $(U_{10}:\{1,3,7,9\},\otimes_{10})$

$|U_{10}| = 4$

$|1| = |e| = |\langle e\rangle| = |\{e\}| = 1$

$|3| = |\langle 3\rangle| = |\{1,3,9,7\}| = 4$

$|3|$ is a generator.

$3^3 = (3\times 3\times 3)\%.10 = 7$

$3^{-1} = (3\times y)\%.10 = 7$ ↳ 7

$G(\{1,3,7,9\},\otimes_{10})$

$3^{-1} = 7$ | $7^{-1} = 3$

$\langle 7\rangle = \langle 3\rangle = \{1,3,7,9\}$

$|7| = 4$.

So, 7 is also a generator.

$|g| = |\{1,9\}|$ $\boxed{g^{-1}=g}$

$|g| = 2$

g is not a generator.

if $\boxed{a^{-1}=a}$ then $\langle a\rangle = \{a,e\}$

$\boxed{e^{-1}=e}$ ⇓ $\langle e\rangle = \{e\}$

ex. Group $(G,*)$; $a \in G$; $a^{-1}=a$

$|\langle a\rangle| = ?$

$|\langle a\rangle| \leq 2$ { $a=e$ $|\langle a\rangle| = 1$; $a \neq e$ $|\langle a\rangle| = 2$ }

Observation → $\{0,1,2,\ldots\}$

ex: $(\mathbb{Z}_{10}, +_{10})$ $e=0$

In no. theory 0^0 = undefined

but in group theory $0^0 = e$

① $\langle 0\rangle = \{0^0=0\}$ ↳ e ; $\langle e\rangle = \{e\}$

$\langle 0\rangle = \{0^n \mid n\in\mathbb{Z}\}$

note ..... assume we have

① $\langle a\rangle = \{a^0=e, a^1=a, a^2=b, a^3=e \mid a^4=a, a^5=b \ldots\}$

So now we will not get any new element.

Smallest the powers such that u get identity element

$a^3 = a^2 \cdot a$

$b\cdot a = e$

② b is working as a^{-1} then $b = a^{-1}$

Group:

ex: $a^5 = e$

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

$a^4 \cdot a = e \Rightarrow a^{-1} = a^4$

• should we check for $a^{-1}, a^{-2}, \ldots$ (n≥0) b/c

$a^2 = b$ → a^{-1} nothing new

If $a^3 = e$ then $a^{-1} = a^2$

$a^{-1}, a^{-2}\ldots$

a^2 a^4

---

② $\langle 1\rangle = \{1^0=0, 1^1=1, 1^2=2, 1^3=3, \ldots 1^{10}=0\}$ → nothing new you will get $1^{11}, 1^{12}, \ldots$

$1^{10} = e \Rightarrow 1^{-1} = 1^9$

$\langle 1\rangle = \mathbb{Z}_{10}$ is a generator.

③ $\langle 2 \rangle = \{2^0 = 0 = e, 2^1 = 2, 2^2 = 4, 2^3 = 6, 2^4 = 8, 2^5 = 0 = e, 2^6 = 2, \ldots\}$

not +ve.

nothing new.

as, $2^5 = e$

$\Rightarrow 2^4 \cdot 2 = e$

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

$2^{-2} = (2^{-1})^2$

$= (2^4)^2 = 2^8$

$\Rightarrow 2^5 \cdot 2^3 = 6.$

$2^5 = e$, $2^3 = (2+2+2)\%10$

not a generator.

$\langle 2 \rangle = \{2, 4, 6, 8, e\}$

$|\langle 2 \rangle| = 5$

④ $\langle 3 \rangle = \{3^0 = 0, 3^1 = 3, 3^2 = 6, 3^3 = 9, 3^4 = 2, 3^5 = 5, 3^6 = 8, 3^7 = 1, 3^8 = 4, 3^9 = 7$

$3^{10} = 0\}$

Smallest +ve integer to get identity element

$3^5 = 3^4 \cdot 3 \Rightarrow 2 \cdot 3$

$(2+3) \bmod 10 = 5.$

$\langle 3 \rangle = Z_{10}$

$|\langle 3 \rangle| = 10$

$|3|$ = Smallest +ve integer n such that $\boxed{3^n = e}$

$\langle a \rangle = \{a^1, a^2, \ldots a^{r-1}, a^r = e\}$ smallest +ve integer.

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

order of $a = r$.

Conclusion

- order of an Element

Group $(G, *)$; $a \in G$

① if $a = e$; $|e| = 1$

② $a \neq e$ then $\underbrace{|a|}_{r} = |\langle a \rangle|$

Smallest +ve 'n' such that $a^n = e$

another definition

$|\langle a \rangle|$: size of subgroup generated by a.

if $\underbrace{|a| = n}$ then $\boxed{a^{-1} = a^{n-1}}$

means.

$a^n = e$

ex. $(\{1,-1,i,-i\},\times)$

$|i| = \{i^1, i^2, i^3, i^4 = e\}$
$= 1$

$i \quad -1 \quad -i$

$|i| = 4$

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

Q. $(\mathbb{Z},+)$ ... infinite group.

$\langle 2 \rangle = \{2^1 = 2, 2^2 = 4, 2^3 = 6 \dots$
$2^0 = 0, 2^{-1} = -2, 2^{-2} = -4 \dots\}$

$\langle 2 \rangle = 2\mathbb{Z}$

$|2| \infty$

Smallest +ve 'n'
$2^n = 0$? no such "n"

note

① if there is no +ve integers n such that $a^n = e$ then we will say that order of a is infinite
so, "a" can generate "∞" no. of element

② if $a^n = e$ → is smallest +ve integer

then
$\langle a \rangle = \{a^1, a^2, \dots a^{n-1}, a^n = e\}$
$a^{-1} \quad a^0$

③ for infinite group; take care. →
order of an element can be finite (or) infinite

$\langle a \rangle = \{a^n / n \in \mathbb{Z}\}$

$|a|$ = Smallest +ve integer 'n'

$a^n = e$

④ in finite group,
order of every element is finite.

ex: $(\mathbb{Z},+)$ group

$|0| = 1$

$a \neq 0$
$|a| = \infty$
$\langle a \rangle = a\mathbb{Z}$

Cyclic group

↳ group with atleast one generator

ex: $(\{1,3,5,7\}, \otimes_8)$ → is cyclic group? (no)

$\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{1,3\}$ $|3| = 2$

$\langle 7 \rangle = \{1,7\}$ $|7| = 2$

$|5| = 2$

ex: $(\{1,2,3,4\}, \otimes_5)$ is cyclic group?

$\langle 1 \rangle = \{1\}$

$\langle 2 \rangle = \{2, 4, 3, 1\}$ (3 → 2^{-1})

$|2| = 2^{(4)} = 1$

$|2| = 4$.

So, 2, 3 are generator.

$2^3 = 8 \bmod 5 = 3$

$2^4 = 16 \bmod = 1$.

ex: $(Z_n, \oplus_n)$ is cyclic group?

↳ generator = 1 (iff) $n \geq 2$

$Z_1 = \{0\}$ .... cyclic → generator = 0

$Z_2 = \{0,1\}$ ... cyclic → generator = 1

ex: Z is cyclic. It is generated by 1.

↳ + (we are talking about these operatn)

Z_n is cyclic. It's generated by 1.

↳ $\oplus$

ex: Group of nth roots of unity is a cyclic group? (operatn is ⇒ mul.)

generator

$\{1\} \longrightarrow g = 1$

$\{1,-1\} \longrightarrow g = -1$

$\{1, \omega, \omega^2\} \longrightarrow g = \omega, \omega^2$

$\{1,-1,i,-i\} \longrightarrow g = i, -i$

note ..... Cyclic group means ∃ generator "g"

- Cyclic group "G"

  $G = \langle g \rangle = \{g^0, g^{\pm 1}, g^{\pm 2}, g^{\pm 3}, \ldots\}$

- nth Root of unity

  $\{1, \theta, \theta^2, \theta^3 \ldots \theta^{n-1}\}$ cyclic group. generator = θ

ex: every Z_n is a cyclic group (yes) (operatⁿ is $\oplus_n$)

i.e $Z_8 = \{1^0, i, i^2, \ldots, i^8\}$

ex: every U_n is a cyclic group? — operatⁿ $\otimes_n$

(no)

$(\{1,2,3,4\}, \otimes_5) = U_5 =$ cyclic

U_8: not cyclic.

ex: Z_7^* in Z_7 regarded as a group using "mul" $\Rightarrow Z_7^* = U_7$ & operatⁿ $= \otimes_7$

$\Rightarrow$ cyclic.

$U_7 = \{1,2,3,4,5,6\}, \otimes_7$

generator

$\langle 1 \rangle = \{1\}$

$|2| = 2^n = 1$

$|2| = 3$ So, 2 is not a generator.

$\langle 2 \rangle = \{2,4,1\}$

$|4| = 3$. So, 4 is not a generator.

$|3| = 3^6 = 1$

$3^6 = 3^5 \cdot 3$

$= 5 * 3$

$= 15 \bmod 7 = 1$

So, 3 is a generator.

& $3^{-1} = 5$ So, 3, 5 are generator.

$|6| = 2$ So, 6 is not a generator.

note

ex: finite group G, $|G| = n$

$\forall a$, $a^n = ?$

So, $\forall a$ $\boxed{a^n = e}$

i.e $U_7 = \{1,2,3,4,5,6\}, \otimes_7$

$|U_7| = 6$

$1^6 = 1$	$4^6 = 1$
$2^6 = 1$	$5^6 = 1$
$3^6 = 1$	$6^6 = 1$

ex: Every cyclic group is Abelian? (yes)

cyclic group 'G' means $\exists$ generator 'g'

$G = \langle g \rangle = \{g^0, g^1, g^2 \cdots, g^r \cdots\}$

Cyclic group G.

$G = \{g^n / n \in \mathbb{Z}\}$

$(a, b \in G)$; $a = g^m$, $b = g^p$

is $ab = ba$? yes //

$g^m g^p \quad g^p g^m$

$g^{p+m} = g^{p+m}$

So, every cyclic group is Abelian group.

ex: Every Abelian group is cyclic? (no)

Counter ex: $(U_8, \circledast_8) = \{1, 3, 5, 7\}, \circledast_8$

Abelian — but not cyclic

ex: order of smallest group that is not cyclic? (4)

- Order 1, 2, 3 are cyclic.

↓ Check.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$a^1 = a \mid a^2 = b \mid a^3 = a^2 \cdot a = e$

ex: order of Smallest group that is not cyclic but Abelian? (4).

ex: If e is the generator then G=?

Trivial group.

$|G| = 1$ $(G = \{e\}, *)$

Otherwise, 'e' cannever be the generator.

Practice Questn

(a) the subgroup of Z generated by 7 → operatn +

$(\mathbb{Z}, +)$

$\langle 7 \rangle = 7\mathbb{Z}$

$\langle n \rangle = n\mathbb{Z}$

$\langle 0 \rangle = \{0\}$

$|7| = \infty$

$|n| = \infty \; ; \; n \neq 0$

(b) $(\mathbb{Z}_{24}, \oplus_{24})$

$\langle 15 \rangle = \{15^1, 15^2 = 6, 15^3 = 21, 15^4 = 12 \ldots\ldots\}$

$15^3 = (15^2) \cdot 15 \Rightarrow (6 + 15) \bmod 24$

$15^4 = 15^2 \cdot 15^2 = 6 \cdot 6$

$= (6+6) \bmod 24 = 12$

$15^2 = (15+15) \bmod 24 = 6.$

$|15| = 8$ so, 15 is not a generator.

(c) U_{20} ; $\langle 3 \rangle = ?$

operatn is $\otimes_{20}$

$\langle 3 \rangle = \{3^1 = 3,$

$3^2 = 9$

$3^3 = 7$

$3^4 = 1 \}$

3^{-1}

$3^4 = 3^3 \cdot 3^1$

$= 7 \cdot 3$

$= 21 \bmod 20 = 1$ ← identity element

$|3| = 4$

? it's not a generator

as $|U_{20}| = |\{1, 3, 7, 9, 11, 13, 17, 19\}| = 8$

(d) operatn "mul"

R^*: non zero Reals

(i) the subgroup R^* generated by 7

$(R^*, *)$ $\langle 7 \rangle = ?$

$\langle 7 \rangle = \{7^n \mid n \in \mathbb{Z}\}$

$\langle 7 \rangle = \{7^0 = 1$

$7^1 = 7$

$7^2 = 49$

$7^3, 7^4, \ldots\ldots\}$

$7^{-1} = \frac{1}{7} \ldots\ldots$

$|7| = \infty$

& 7 is not a generator.

$(R^*, *)$ is cyclic group? (no) generator exist.

↳ no, g such that $\forall a$, $g^n = a$, for some n.

② the subgroup C^* generated by $\frac{(1+i)}{\sqrt{2}}$

C^*: non zero complex no.

$(C^*, *) \quad \left\langle \frac{1+i}{\sqrt{2}} \right\rangle$

$\left(\frac{1+i}{\sqrt{2}}\right)^0 = 1 \;/\; \left(\frac{1+i}{\sqrt{2}}\right)^1 = \frac{1+i}{\sqrt{2}} \;/\; \left(\frac{1+i}{\sqrt{2}}\right)^2 = \frac{2i}{2} = i$ $\quad (1+i)^2 = 1+2i+i^2$, $(a+b)^2 = a^2+2ab+b^2$

$\left(\frac{1+i}{\sqrt{2}}\right)^3 = \left(\frac{1+i}{\sqrt{2}}\right)\cdot\left(\frac{1+i}{\sqrt{2}}\right)^2 \Rightarrow \frac{i-1}{\sqrt{2}}$ (i)

$\left|\frac{1+i}{\sqrt{2}}\right| = 8$

$\left(\frac{1+i}{\sqrt{2}}\right)^4 = \left(\frac{1+i}{\sqrt{2}}\right)^2 \cdot \left(\frac{1+i}{\sqrt{2}}\right)^2 = i \cdot i = (-1)$

$\left(\frac{1+i}{\sqrt{2}}\right)^8 = 1 = e$

$(C^*, *)$ — "∞" group

$\left|\frac{i+1}{\sqrt{2}}\right| = 8$

$\left\langle \frac{1+1}{\sqrt{2}} \right\rangle = \{d, d^2 = i, d^3, d^4 = -1, \ldots d^8 = 1\}$

assumed

C^*: nonzero complex no.

↓

$ai + b$

Real Real.

every Real no. is also complex.

③ $(C^*, *)$ — infinite group; $e = 1$

$\langle i \rangle = ? = \{i^1 = i, i^2 = -1, i^3 = -i, i^4 = e = 1\}$

order of 'i'

$|i| = 4$

④ Group G, b is an element of G

order of identity element? (1) always.

$\langle e \rangle = \{e\}$

$e^n = e$

↳ Smallest +ve Integer.

ex: Group G, b is an element of G

order of b = order of b^{-1}

$\langle b \rangle = \{b^n / n \in \mathbb{Z}\} = \{b^0, b^{+1}, b^{+2} \dots\}$

$\langle b^{-1} \rangle = \{b^{-n} / n \in \mathbb{Z}\} = \{b^0, b^{+1}, b^{+2} \dots\}$

note

$\langle b \rangle = \langle b^{-1} \rangle$

so there

$ord(b) = ord(b^{-1})$

$|\langle b \rangle| = |\langle b^{-1} \rangle|$

ex: Group G, if g is generator.

then its inverse of g is also generator?

yes.

For any element a, $\langle a \rangle = \langle a^{-1} \rangle$

Bic "g" is also a "generator" of G.

$\langle g \rangle = \langle g^{-1} \rangle = G$

ex: for finite group G, if

order of a = order of G

then "a" is generator

(yes)

$O(a) = O(G)$

↳ finite

So, a = generator.

also a^{-1} = generator.

"Finite" Group G, $a \in G$

$O(a) = O(G)$ = no. of element in G

means ⇒ a can generate all element of a

ex: for infinite group G.

if order of a is infinite then

'a' is generator? (no)

$G(\mathbb{Z}, +)$

$\langle 2 \rangle = 2\mathbb{Z}$ = even no. $\neq G$

Order of $2 = \infty$ But $\langle 2 \rangle \neq G$

So, 2 is not a generator

ex. definition of subgroup

"a" is an element of G

(a) $\langle a \rangle = \{a^n / n \in \mathbb{Z}\}$

(b) $\langle a \rangle = \{a^n / n \in \mathbb{N}\}$

(c) $\langle a \rangle = \{a^n / n \in \omega\}$

(d) $\langle a \rangle = \{a^{-n} / n \in \mathbb{N}\}$

not correct for infinite group

• all are correct for finite group.

Q. Infinite group G, $a \in G$

$O(a) = 5$ then $a^5 = e$ → smallest true integer.

$\langle a \rangle = \{a^1, a^2, a^3, a^4, a^5 = e\}$

Subgroup generated by a

a^{-1}

Q. finite group G, $a \in G$

$|a| \leq |G|$? yes → no. of element in G

no. of element that "a" can generate

note

Group G

① $1 \leq |a| \leq |G|$; $\forall a$

② $a = e$; $|a| = 1$

③ $\forall a \neq e$; $2 \leq |a| \leq |G|$

e, a

- Finite group ; $\forall a \in G$

$a^{-1} = a^{n-1}$, where $n = O(a)$

$n = O(a)$ means. $a^n = e$

"mul" by a^{-1} on both sides

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

- Group G, $\forall a \in G$

$|a|$ = true integer.

→ Smallest positive integer "n"

no. of element generated by a = true integers.

$a^n = e$

note

Group G.

Subgroup

Subgroup generated by an element

→ very special subgroup

ex: Group $G = U_8 = \{1, 3, 5, 7\}$

✓ "G" = Subgroup of G

✗ "G" = Subgroup generated by some element (x)

• Any Group G, "g" is an element of G, O(g)=n

① $\langle g \rangle$ is finite? (yes)

$O(g)=n$ means $|\langle g \rangle|=n$

② then the powers $e, g, \dots g^{n-1}$ are distinct (yes)

$O(g)=n$

$\langle g \rangle = \{g^0, g^1, \dots g^{n-1}\}$

(or)

$O(g)=n$

$\langle g \rangle = \{g^1, g^2 \dots g^n\}$ are distinct.

ex. • Any group G, "g" is an element of G.

if for some distinct integers m, n.

$g^m = g^n$ then $\langle g \rangle$ is finite? (yes)

Idea

if $a^7 = a^{10}$ then $\Rightarrow$ $a^3 = e$

$a^{10} = a^7 \cdot a^3 = a^7$

$a \in G$

let $m \neq n$

$a^m = a^n$

then $a^{m-n} = e$;

$a^{n-m} = e$

order of "a" is definitely finite.

ex. $(\mathbb{C}^*, \times) = G$; $i \in G$

16 ≠ 28

m n

$i^m = i^n$

$i^{16} = i^{28}$

$i^{16} = i^{16} \cdot i^{12}$

$e = i^{12}$

$i^{28} = i^{16} \cdot i^{12}$

order of $i \leq 12$

↓

Smallest +ve integer such that $a^n = 1$

note

Any group G; $a \in G$

if $m > n$ integer &

$a^m = a^n$ then

$a^{m-n} = e = a^{n-m}$

So, $O(a) \leq m-n$

ex: Any Group G & $g \in G$.
if $\langle g \rangle$ is infinite then there is no distinct integers m, n such that $g^m = g^n$

(⇒) let $m > n$
$a^m = a^n \Rightarrow O(a) \leq m-n$ → finite.

Contrapositive.
$O(a) = \infty$ then for any $m \neq n$
$a^m \neq a^n$

ex: $(\mathbb{Z}, +)$ $2 \in \mathbb{Z}$
$\langle 2 \rangle = \{0, \pm 2, \pm 4, \ldots\}$ is subgroup of $\mathbb{Z}$

is 2 generator of $\mathbb{Z}$? (no)
But $(2\mathbb{Z}, +)$ — cyclic group? yes
Generator: 2

note .....
Group G, ~~then~~
$\langle a \rangle$ = Subgroup of G generated by a
$\langle a \rangle$ = cyclic subgroup of G generated by a
is individually a cyclic group.

Cyclic group	Vs	Cyclic Subgroup
• a group with atleast one generator		• a subgroup which (if you look individually is cyclic).

ex: $\langle g \rangle = \{g^n / n \in \mathbb{Z}\}$ subgroup generated by g

(a) $\langle g \rangle$ is group & abelian
(b) $\langle g \rangle$ is a cyclic subgroup of G
(c) If $H \leq G$ & $g \in H$ then $\langle g \rangle \leq H$. → Smallest subgroup containing 'g'

H is a subgroup containing 'g' → $\langle g \rangle \leq H$

ex: $(\mathbb{Z}, +)$ → $H = \mathbb{Z}$, $H \leq \mathbb{Z}$

$\langle 2 \rangle = 2\mathbb{Z}$
Smallest subgroup of $\mathbb{Z}$ containing 2
$\langle 2 \rangle \leq H$

ex: order of generator of infinite group is definitely infinite? (yes) $\langle g\rangle = G$

$O(g) = \infty$

ex: order of element of infinite group is infinite? (no)

ex: $(\mathbb{C}^*, *)$ — infinite group

$|i| = 4$; $\left|\frac{i+1}{\sqrt{2}}\right| = 8$

ex: order of generator of finite group is finite? (yes)

$|G| = n$.

$|g| = n$. so $\langle g\rangle = G$

ex: order of element of finite group is finite? (yes)

$1 \leq |a| \leq |G|$

ex: its possible that an infinite group has no generator? yes

≡ is it possible ∞ Group

$(R^*, \times)$ — not cyclic

↳ no generator.

ex. is it possible that a finite group has no generator? yes.

U_8 — not cyclic.

ex: Group G, $a \in G$ & $a = a^{-1}$ then $\langle a\rangle$?

$\langle a\rangle = \{e, a\}$

- G be cyclic group then no. of Generators.
  - odd (iff) $|G| \leq 2$
  - even otherwise $|G| > 2$

if a is generator then a^{-1} gen. } (even) generator are in pair.

if a is gen. then $a \neq a^{-1}$

ex: every two cyclic group of same order are isomorphic?
↳ have same template

note .....
for order n, given atleast one cyclic group (nth roots of unity, ×)
(∞) $(\mathbb{Z}_n, \oplus_n)$

- Any cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}_n$

Infinite cyclic group $\equiv \mathbb{Z}, +$

finite cyclic group of order $n \equiv \mathbb{Z}_n, \oplus_n$

Lagrange's theorem ← it's one copy

↳ order of subgroup(s) divides order of group(G)

$\frac{|G|}{|S|}$ = natural no.

another Definition
↳ for any finite group G
$\langle a \rangle$ is a subgroup of G.
So, $|\langle a \rangle|$ Divides $|G|$
order of a
So, order of an element Divides order of group.

- Converse is not true.
finite Group G, d Divides $|G|$
then ∃ subgroup of order d?
not necessarily

note .....
For Abelian group.
Converse of lagrange's theorem is true.

- If G is a finite Abelian group & d divide's $|G|$ then there exist atleast one subgroup of order d.

ex: $|G|$ = prime (p) $G \neq e$ so, $2 \leq |a| \leq |G|$ prime p

$|e| = 1$

$|a|$ = ? By lagrange' theorem

$|a|$ will Divides $|G| = p$

$|a| = p$

$|a|$ Divides p $\Big\}$ $|a| = p$

$\not\leq |a| \geq 2$

G = order prime $\forall a \neq e$.

$|a| = p$ means $\langle a \rangle = G$

every element other than 'e' is a generator

So, G is cyclic

$\because$ every cyclic is Abelian

So, G is Abelian also

- Theorem:

every subgroup of a cyclic group is cyclic

- Theorem:

Let 'p' be a prime. then every group of order p^2 is abelian.

note ..... p = Prime

Order p group ⟶ cyclic

Order p^2 group ⟶ cyclic

counter ex: U_8 $|U_8| = 2^3$

U_8 → not cyclic

2^3 → prime

- Order 1 (or) prime $\Rightarrow$ cyclic group

$\Downarrow$

abelian group.

Ex: Order of G: 17
how many non-isomorphic group of order 17? (1)

$|G| = 17$ (prime order) $\Rightarrow$ G cyclic $\equiv Z_{17}$

every cyclic group of order n are isomorphic $= Z_n$

→ if order of G: 4
then
Order 4 (2 groups; 2 abelian)
1 cyclic & 1 non-cyclic

template 1
(e, x, y, z)
$x^{-1} = x$
$y^{-1} = z$
gen. $= y, z$

template 2
(e, x, y, z)
$\forall_a \; a^{-1} = a$

Order 1 to 5 $\Rightarrow$ Abelian.

(2, 3, 5) Prime order $\Rightarrow$ cyclic $\Rightarrow$ Abelian

(1, 4) → Abelian.

Order 6: (2 group; 1 abelian, 1 non-abelian)

Smallest non-Abelian Group $\Rightarrow$ order 6

non-Abelian groops.

Order	#non-Abelian groops
1	0
(prime) → 2, 3, 5, 7, 11, ...	0
4	0
6	1
⋮	

Very. Imp.

Alternate Definition of Abelian group

• another definition.

ex:. Group G, such that $(ab)^2=a^2b^2$ then G is abelian?

$\forall a,b\ (ab)^2=a^2b^2$

$\Downarrow$

$abab=aabb$

we can a^{-1} from LHS & b^{-1} from RHS (we can do these b/c it's a group)

$\underbrace{a^{-1}}_{e}aba\underbrace{bb^{-1}}_{e} = a\underbrace{aa}_{e}b\underbrace{bb^{-1}}_{e}$

So, $\boxed{ba=ab}$

Target: $\boxed{ab=ba}$

So,

$(ab)^2=a^2b^2 \Rightarrow$ Abelian

$(ab)^2=a^2b^2 \Leftarrow$ Abelian

prove

$ab=ba$

$abb=bab$

$aabb=abab$

$\boxed{a^2b^2=(ab)^2}$

ex:. if every element of group G is it's own inverse. then G is abelian.

$\forall a, \boxed{a^{-1}=a}$

Target $\Rightarrow \boxed{ab=ba}$

group $\boxed{(ab)^{-1}=b^{-1}a^{-1}}$ $\xrightarrow{\text{the A/C to ques'n}}$ $\boxed{ab=ba}$

every element is inverse of itself.

for every group these will happen.

$\forall a\ a=a^{-1}$ $\Big\}$ Same.

$\Vert\!\Vert$

$\forall a,\ a^2=e$

ex:. if a group is Abelian then $\forall a,\ a=a^{-1}$? (no)

$U_5=\{1,2,3,4\}, \otimes_5$

$\downarrow$ abelian

Order 4

But $2^{-1}=3$

$2^{-1}\neq 2$

note

$\forall a, a^{-1}=a \Rightarrow$ Abelian

$\forall a, a^{-1}=a \not\Leftarrow$ Abelian

ex:
A group is Abelian iff/only if $\forall a, a^{-1}=a$

False

ex
A group is Abelian if $\forall a, a^{-1}=a$

True

ex: Does every subgroup of an abelian group have to be abelian? yes

Group G Abelian : $\forall a,b$ $\boxed{ab=ba}$

Subgroup (H) $\forall x,y$ $\boxed{xy=yx}$ b/c operation are same.

$(G,*)$ $a,b \in G$ $\boxed{a*b=b*a}$ Since G Abelian

$(H,*)$ $a,b \in H$ $\boxed{a*b=b*a}$ So H is Abelian

ex: Group G, $x,y,z \in G$

then $xy=zx \rightarrow y=z$

then G is abelian.

Target $ab=ba$

$\cancel{b}ab=ba\cancel{b}$

So, $\boxed{ab=ba}$

$\boxed{ax=ya \Rightarrow x=y}$ → Abelian

$\boxed{ax=ya \Rightarrow y=x}$ ← Abelian.

If Abelian : $\boxed{ab=ba}$

$\Rightarrow ax=ya$

$\Rightarrow \cancel{a}x=\cancel{a}y$ (b/c of ^sso.)

$\boxed{x=y}$

Group G is Abelian iff

$\forall a,b,x$

$ax=ba \rightarrow x=b.$

note .....

- $ax=bx \rightarrow a=b$ } in group these is allowed
- $\cancel{a}x=\cancel{a}y \rightarrow x=y$ }
- $\cancel{a}x=ya \not\rightarrow x=y$ } not allowed in group.
- $a\cancel{x}b=c\cancel{x}d \rightarrow ab=cd$

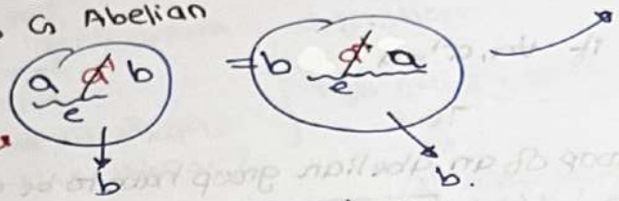
ex: Group G, $x,y,z \in G$

$xyz = ayc \rightarrow xz = ac$

then is G Abelian

Target: $ab = ba$

proof:



Putting a^{-1} in middle

nooo you can do the middle cancelation

So, middle cancellation $\rightleftharpoons$ Abelian

ex: Group G is abelian iff $(ab)^{-1} = a^{-1}b^{-1}$

given: $(ab)^{-1} = a^{-1}b^{-1}$ → Target $ab = ba$

$\Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1}$

$\Rightarrow (ab)^{-1} = (ba)^{-1}$

$\Rightarrow (ab)^{-1} = (ab)^{-1}$

both have same inverse

⇓

then they are also same

$ab = ba$

In Group; if $a \neq b$ then $a^{-1} \neq b^{-1}$ b/c Inverse of every element is unique.

$\forall a,b \quad (ab)^{-1} = a^{-1}b^{-1}$ $\rightleftharpoons$ Abelian

given Abelian $ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1}$

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

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

A/c to question

as we know

Intersection of Subgroup

↳ Intersection of 2 subgroup is also a subgroup.

ex: Group $(G,*)$

Subgroup $(H,*)$, $(L,*)$

$(H \cap L,*)$ — is subgroup

① Identity element
$e \in H$, $e \in L$
$e \in H \cap L$

② Closure: $\forall a,b \in (H \cap L)$ → $a,b \in H \Rightarrow ab \in H$, $a,b \in L \Rightarrow ab \in L$ } $ab \in H \cap L$
$\Rightarrow a*b \in H \cap L$

$a \in H \cap L \Rightarrow a^{-1} \in H \cap L$
$a \in H \Rightarrow a^{-1} \in H$
$a \in L \Rightarrow a^{-1} \in L$ } $a^{-1} \in H \cap L$

Subgroup

- But union of 2 subgroup may not be subgroup

ex: $(\mathbb{Z},+)$
$\Rightarrow (3\mathbb{Z},+)$, $(4\mathbb{Z},+)$ } subgroup
$(3\mathbb{Z} \cup 4\mathbb{Z},+)$ → not even closed.
$3+4 \notin 3\mathbb{Z} \cup 4\mathbb{Z}$

Alternative Definition of Subgroup

① Alternative Definition:
Group $(G,*)$,
A subgroup of G is a non-empty subset $H \subset G$ such that.

① $x,y \in H \Rightarrow x*y \in H$
Closure property

② $x \in H \Rightarrow x^{-1} \in H$
Inverse property

② Another Definition (merge both condition)

Group $(G,*)$, A subgroup of G is a subset $H \subset G$. such that

$\forall a,b.\ a*b^{-1} \in H$

note ----

If G is finite group then To check (H) is subgroup of G or not
(should be non-empty)
Only closure property of H is need to be checked

Note If G is Group,
$H \subseteq G$
↓
Subset

→ To check if H is subgroup:
↳ Subset which is a group

① $e \in H$
② closure of H
③ Inverse property of H.

→ To check if H is subgroup & G is finite group.

① closure of H
② non-empty.