Group Theory

Questions

Order of an element, Subgroup

Cyclic Group, Subgroup generated by an element

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

3. List all of the elements in each of the following subgroups.

(a) The subgroup of $\mathbb{Z}$ generated by 7

(b) The subgroup of $\mathbb{Z}_{24}$ generated by 15

(g) The subgroup generated by 3 in $U(20)$

(h) The subgroup generated by 5 in $U(18)$

(i) The subgroup of $\mathbb{R}^*$ generated by 7

(j) The subgroup of $\mathbb{C}^*$ generated by i where $i^2 = -1$

(k) The subgroup of $\mathbb{C}^*$ generated by $2i$

(l) The subgroup of $\mathbb{C}^*$ generated by $(1+i)/\sqrt{2}$

(m) The subgroup of $\mathbb{C}^*$ generated by $(1+\sqrt{3}\,i)/2$

HW

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

(h) $U_{18} = \{1, 5, 7, 11, 13, 17\}$ → finite Group

operation : $\otimes_{18}$

$\langle 5 \rangle = ?$

$5^{-1} = 11$

$\langle 5 \rangle = \{5^1 = 5, 5^2 = 7, 5^3 = 17, 5^4 = 13, 5^5 = 11, 5^6 = 1 = e\}$ ← 5^{-1}

$5^4 = 5^2 \times 5^2 = 49 \bmod 18 = 13$

$5^2 = (5 \times 5) \bmod 18 = 7$; $5^3 = 5^2 \times 5 = 35 \bmod 18 = 17$

order of 5

$\langle 5 \rangle = \{1, 5, 7, 11, 13, 17\}$

So (5) = Generator

$5^{-1} = 11$; $\langle 11 \rangle = \langle 5 \rangle$

11 — Generator

Order of $5 = |\langle 5 \rangle| = 6$

U_{18} = Cyclic

Gen = 5, 11

5 has generated 6 elements.

$5^6 = 1$

smallest +ve int

$U_{18} = \{1, 5, 7, 11, 13, 17\}$ — $\otimes_{18}$ — cyclic group

gen = 5, 11

$= \{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\}$, $\otimes_{18}$

$= \{11^0, 11^1, 11^2, 11^3, 11^4, 11^5\}$, $\otimes_{18}$

$= \{5^1, 5^2, 5^3, 5^4, 5^5, 5^6\}$, $\otimes_{18}$

$U_{18} = \{1, 5, 7, 13, 11, 17\}$ (X) $_{18}$

$\langle 7 \rangle = \{7^1 = 7, 7^2 = 13, 7^3 = 1 = e\}$

7^{-1}

order of 7

$|7| = 3$

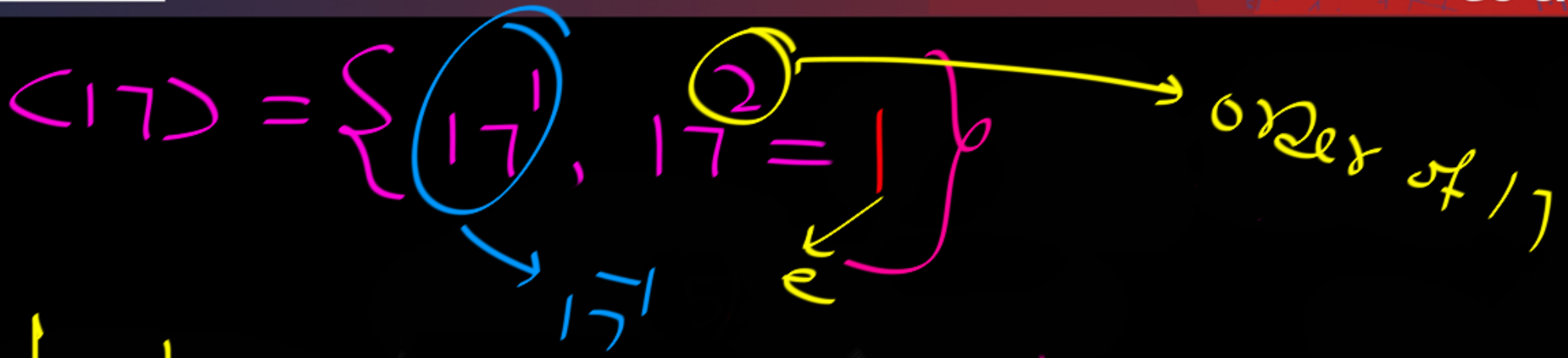
$7^{-1} = 13$

$|13| = 3$

$\langle 13 \rangle = \langle 7 \rangle$

7, 13

1 to + generators



$|\langle 17 \rangle| = 2$

17 is NOT gen.

$(\mathbb{C}^*, \times)$

↳ Non Zero Complex numbers ⟶ $ai + b$ (Real, Real)

↳ (Real) i + Real

$5i + 10$, $5i - 10$

5, i, $2i$

Every Real number is also Complex.

$(C^*, \times)$ — infinite Group ; $e = 1$

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

i^{-1}

order of i

$|i| = 4$

i = NOT Generator

Q : Group G, b is an element of G.

Order of identity element e = ? = 1 Always

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

$e^1 = e$

Smallest Positive integer

Q : Group G, b is an element of G.

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

$$\langle b \rangle = \{ b^n \mid n \in Z \} = \{ b^0, b^{\pm 1}, b^{\pm 2}, b^{\pm 3}, \cdots \}$$

$$\langle b^{-1} \rangle = \{ b^{-n} \mid n \in Z \} = \{ b^0, b^{\pm 1}, b^{\pm 2}, b^{\pm 3}, \cdots \}$$

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

Note: for any $b \in G$ group G

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

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

So order of b = $o(b^{-1})$

Q : Group G, If g is generator then inverse of g is also generator ?? → Yes.

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

Because "g" is also a "generator" of G

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

Q : For FINITE Group G, If order of "a" is same as Order of G then "a" is generator. → Yes.

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

$O(a) = O(G)$ = number of elements in G

means ⇒ "a" can generate all elements of G.

$O(a) = O(G)$ finite

So, a = generator

So, $\bar{a}^1 = 11$

Q : For Infinite Group G, If order of "a" is infinite then "a" is generator?? ⇒ NO.

Ex: $G = (Z, +)$

$\langle 2 \rangle = 2Z =$ even integers $\neq G$

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

2 is NoT Generator.

Q : Group G, "a" is an element of G.

Definition of "Subgroup generated by a" ?

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

(2) $\langle a \rangle = \{ a^n \mid n \in N \}$

(3) $\langle a \rangle = \{ a^n \mid n \in W \}$

(4) $\langle a \rangle = \{ \bar{a}^n \mid n \in N \}$

Not Correct for Group infinite

Q : Finite Group G, "a" is an element of G.

Definition of "Subgroup generated by a" ?

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

(2) $\langle a \rangle = \{ a^n \mid n \in N \}$

(3) $\langle a \rangle = \{ a^n \mid n \in W \}$

(4) $\langle a \rangle = \{ \bar{a}^n \mid n \in N \}$

Q: "finite" Group G, "a" is an element of G.

Definition of "Subgroup generated by a" ?

① $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$

② $\langle a \rangle = \{ a^n \mid n \in N \}$

③ $\langle a \rangle = \{ a^n \mid n \in W \}$

④ $\langle a \rangle = \{ \bar{a}^n \mid n \in N \}$

$\langle a \rangle = \{ a^1, a^2, \ldots \}$ — n : $a = e$

order of a

Q: Infinite Group G, "a" is an element of G.

Definition of "Subgroup generated by a" ?

(1) $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ ✓

(2) $\langle a \rangle = \{ a^n \mid n \in N \}$ ✗

(3) $\langle a \rangle = \{ a^n \mid n \in W \}$ ✗

(4) $\langle a \rangle = \{ \bar{a}^n \mid n \in N \}$ ✗

Q: Infinite Group G; $a \in G$

$o(a) = 5$ then $a^5 = e$ → Smallest +ve integer

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

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

Subgroup generated by a

$\underline{Q}$: Infinite Group G ; $a \in G$

$o(a) = n \in N$ then

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

$= \{a^0, a^1, \dots, a^{n-1}\}$ $\longleftarrow$ a^{-1}

Q: finite group G ; $a \in G$

$|a| \leq |G|$?

Q: finite Group G ; $a \in G$

$|a| \leq |G|$? Yes.

$|a|$: number of elements that "a" can generate.

$|G|$: number of elements in G.

Group G

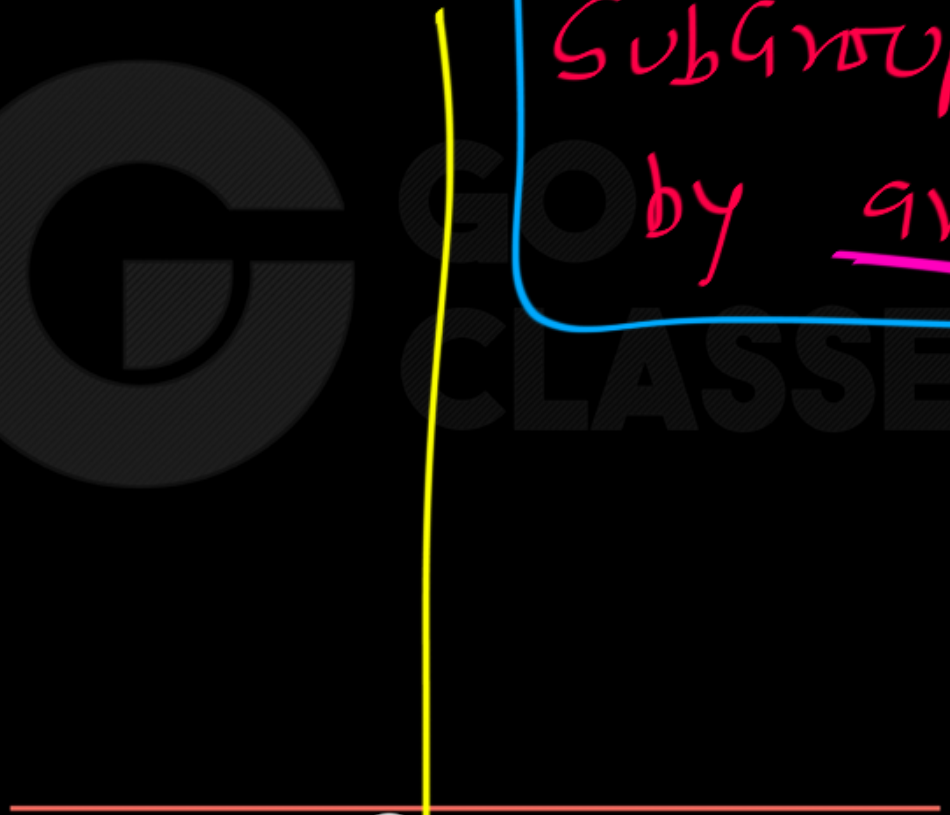
1. $1 \leq |a| \leq |G|$; $\forall a$
2. $a = e$; $|a| = 1$
3. $\forall a \neq e$; $2 \leq |a| \leq |G|$ ← e, a

Note: Group G

Subgroup

Very special Subgroup

Subgroup generated by an element



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

"G" = Subgroup of G ✓

"G" = Subgroup generated by some element

No

Note:

While creating "Subgroup generated by an element a",

Inverses are only needed if the group is infinite;

In a Finite group, the inverse of an element can be expressed as a positive power of that element.

Important

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 $\Rightarrow$

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

Group G, $\forall a \in G$

$|a|$ = Positive integer

→ Smallest Positive integer n such that $a^n = e$

$|a|$ → Number of elements generated by a ⇒ Positive integer

Q : Any Group G, "g" is an element of G, O(g) = n.

Then <g> is finite ? ⇒ Yes.

O(g) = n means

$|\langle g \rangle| = n$

Q : Any Group G, "g" is an element of G, O(g) = n.

Then the powers

$1, g, \ldots, g^{n-1}$ are distinct. ? Yes.

O(g) = n then

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

$O(g) = n$

$g^1, g^2, g^3, \ldots, g^n$ —— $\langle g \rangle$

Distinct

$O(g) = n$

$g^1, g^2, g^3, \ldots, g^n, g^{n+1} = g^1$

Distinct ? No

Q : Any Group G, “g” is an element of G.

If for some distinct integers m,n; g^m = g^n then

<g> is finite??

Q : Any Group G, "g" is an element of G.

If for some distinct integers m,n; g^m = g^n then

<g> is finite?? ⇒ Yes.

Idea: If $a^7 = a^{10} \Rightarrow \boxed{a^3 = e}$

$a^{10} = a^7 a^3 = a^7$

$\Rightarrow \boxed{a^3 = e}$

So, $O(a) \leq 3$

Any Group G; $a \in G$

let $m \neq n$

$a^m = a^n$

let $m > n$

then $a^{m-n} = e$; $a^{n-m} = e$

$\forall$

$o(a) \leq n-n$

order of a is Definitely finite.

Ex: $(C, C^*, X) = G \; ; \; i \in G$

$m \quad n$

$16 \neq 28$

$i^m = i^n$

$i^{16} = i^{28}$ ✓

$i^{16} = i^{28} \Rightarrow$ $i^{28} = i^{16} \cdot i^{12} = i^{16}$

$\Rightarrow i^{12} = e$

Order of $i \leq 12$ $\quad o(i) = 4$ ✓

"Smallest" the integer such that $i^n = 1$

Note: Any group G; $a \in G$

If $m > n$ integers and

$a^m = a^n$ then $a^{m-n} = e = a^{n-m}$

So

$$O(a) \leq m - n$$

Q : Any Group G, "g" is an element of G. If <g> is infinite then there is NO distinct integers m,n; such that g^m = g^n.

Yes. let $m > n$

$a^m = a^n \Rightarrow O(a) \leq m - n$ (finite)

Contrapositive:

$O(a) = \infty$ then for any $m \neq n$ $a^m \neq a^n$.

Note: Cyclic Group : G

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

$$G = \{g^n \mid n \in Z\}$$

Notice: Group G ; $a \in G$

$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ — subgroup of G

↓

Cyclic subgroup of G generated by a.

↳ "Individually"

Gen = a

Cyclic group ✓

Ex: $(Z, +)$ $\quad 2 \in Z$

$\langle 2 \rangle = \{0, +2, -2, +4, -4, +6, -6 \cdots\}$ = subgroup of Z

$\langle 2 \rangle$ → cyclic subgroup of Z generated by 2.

2 is gen of Z? No

$(\mathbb{Z}, +)$ — Cyclic Group ? Yes

Gen = 2

Note: Group G, $\forall a \in G$

$\langle a \rangle$ = Subgroup of G generated by a

$\langle a \rangle$ = Cyclic " " " " " "

$\langle a \rangle$ is Individually a Cyclic Group.

Cyclic Group

↓

a Group with at least one Generator

Vs

Cyclic Subgroup

↓

a Subgroup which (if you look individually) is cyclic.

Q:

Let G be a group under binary operation *. Let g ∈ G.

We define <g> as follows :

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$ = subgroup generated by a

Which of the following is/are true about <g> under binary operation * ?

A. <g> is also a group.

B. <g> is a cyclic subgroup of G.

C. <g> is abelian.

D. If H ≤ G and g ∈ H, then <g> ≤ H.

Q:

Let G be a group under binary operation *. Let $g \in G$.

We define <g> as follows :

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$ = subgroup generated by a

$\langle g \rangle$ → subgroup of g

Which of the following is/are true about <g> under binary operation * ?

A. <g> is also a group.

B. <g> is a cyclic subgroup of G. — gen = g

C. <g> is abelian. — every cyclic group is Abelian.

D. If $H \leq G$ and $g \in H$, then $\langle g \rangle \leq H$.

Ans : A,B,C,D

Exp :

This is a very basic and standard result in group theory.

Let G be a group and let g ∈ G. The cyclic subgroup generated by g is the subset :

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

The following four statements are true for <g> :

(i) The cyclic subgroup <g> generated by g is a subgroup of G.

(ii) g ∈ <g>.

(iii) If H ≤ G and g ∈ H, then <g> ≤ H. Hence <g> is the smallest subgroup of G containing g.

(iv) <g> is abelian.

(D) $H \leq G$ and $g \in H$ then

$\langle g \rangle \leq H$?

H is a subgroup containing g.

"Smallest" subgroup containing g.

$\langle g \rangle \leq H$

Ex: $(Z, +)$ —— $H = Z$

$H \leq Z$ ✓

$\langle 2 \rangle = 2Z$

→ Smallest subgroup of Z containing 2

$\langle 2 \rangle \leq H$

Let (G, $*$) be a group and a $\in$ G. We define the powers of a in G,

a^n for $n \in \mathbb{Z}$ as follows :

For $n \geq 0$, we can define a^n inductively: $a^0 = e_G$, the identity element of G; while a^{n+1} is defined to be $a^n * a$. For $n < 0$ we can define $a^n = \overline{a}^{-n}$, where $\overline{a}$ is the inverse of a in $(G, *)$.

For any element g $\in$ G, we define <g> as follows :

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

Continued on next page...

Which of the following is/are true about <g> ?

A. If <g> is a finite cyclic group, where g has order n. Then the powers

$\{1, g, \ldots, g^{n-1}\}$ are distinct.

B. If <g> is infinite cyclic and If m and n are integers and

$m \neq n$, then $g^m \neq g^n$.

C. Subgroups of cyclic groups are cyclic.

D. <g> is abelian.

Which of the following is/are true about <g> ?

A. If <g> is a finite cyclic group, where g has order n. Then the powers

$\{1, g, \ldots, g^{n-1}\}$

are distinct.

B. If <g> is infinite cyclic and If m and n are integers and

$m \neq n$, then $g^m \neq g^n$.

C. Subgroups of cyclic groups are cyclic.

D. <g> is abelian.

Q :

Order of generator of infinite group is definitely infinite ?

Q :

Order of generator of infinite group is definitely infinite ?

g

G

Yes.

$\langle g \rangle = G$

$O(g) = \infty$

Q :

Order of generator of finite group is finite ? Yes.

g , G , $|G| = n$

$|g| = n$

$\langle g \rangle = G$

$\langle g \rangle = |G|$

$\Rightarrow |g| = |G| = n$

Q :

Order of an element of infinite group is definitely infinite ?

Q :

Order of an element of infinite group is definitely infinite ?

No.

(C, c^*, x) — infinite group

$|i| = 4$; $\left|\frac{i+1}{\sqrt{2}}\right| = 8$

Q :

Order of an element of finite group is definitely finite ?

Q :

Order of an element of finite group is definitely finite ?

a ; a ; $|a| = n$

Yes.

$$1 \leq |a| \leq |a|$$

$a \neq e$; $\Rightarrow$ $2 \leq |a| \leq |a|$

Q :

It is possible that an infinite group has No generator?

Q :

It is possible that an infinite group has No generator? Yes.

≡

Is it Possible ∞ group is NOT Cyclic ? Yes.

$(R^*, \times)$ — NOT Cyclic

— No Generator

Q :

It is possible that a finite group has No generator?

Q :

It is possible that a finite group has No generator? ⇒ Yes

U_8 —— NOT cyclic

Q 1:

If identity element of a group G is the generator, then what is order of G ?

Q 1:

If identity element of a group G is the generator, then what is order of G ? = 1

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

Q 2: Let G be a group. Let a $\in$ G and a is inverse of itself. Then what is <a>?

$a = a^{-1}$

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

Q3 : Let G be a group which can be generated by some element "a" which is inverse of itself. Then what is order of G?

$a = a^{-1}$

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

$|G| \leq 2$

$|G| = 1$ or 2

Q 4 : Let G be a Cyclic Group then what is the number of Generators?

A. Even

B. Odd

C. Can be odd or even

Q 4 : Let G be a Cyclic Group then what is the number of Generators?

A. Even

B. Odd iff $|G| \leq 2$

C. Can be odd or even

$(\{e\}, *)$ — cyclic group gen = e

gen = 1

$(\{e, a\}, *)$ — cyclic group gen = a

gen = 1

Q 4 : Let G be a Cyclic Group of order more than 2 then what is the number of Generators?

A. Even

B. Odd

C. Can be odd or even

Q 4 : Let G be a Cyclic Group of order more than 2 then what is the number of Generators?

A. Even

B. Odd

C. Can be odd or even

Cyclic Group G ; $|G| > 2$

If a is Gen then so is a^{-1}.

Q: Is it possible $a = a^{-1}$ and a is Generator ?

No

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

Cyclic Group G ; $|G| > 2$

If a is gen then a^{-1} gen. ✓

If a is gen then $a \neq a^{-1}$.

every number of Generators $\in$ { Generators are in Pairs.

Cyclic Group G : $|G| > 2$

Generators :

a, a^{-1}

b, b^{-1}

c, c^{-1}

$\vdots$

$a \neq a^{-1}$

$b \neq b^{-1}$

$\vdots$

#Gen is even.

More abstract: suppose that the group G is cyclic; then, for each generator x, also x^{-1} is a generator, because $x^k = (x^{-1})^{-k}$.

Suppose $x = x^{-1}$; then $x^2 = 1$ (or e, if you prefer this notation; I don't) and therefore $|G| \leq 2$.

Thus, if $|G| > 2$, we have $x \neq x^{-1}$, for every generator x, and thus we can divide the generators into pairs.

Q 5:

Every two cyclic groups of same order are isomorphic?

Q 5:

Every two cyclic groups of same order are isomorphic? Yes

$G = \{g^1, g^2, \ldots, g^n\}$

$H = \{a^1, a^2, \ldots, a^n\}$

same template.

same template

Note: for order n,

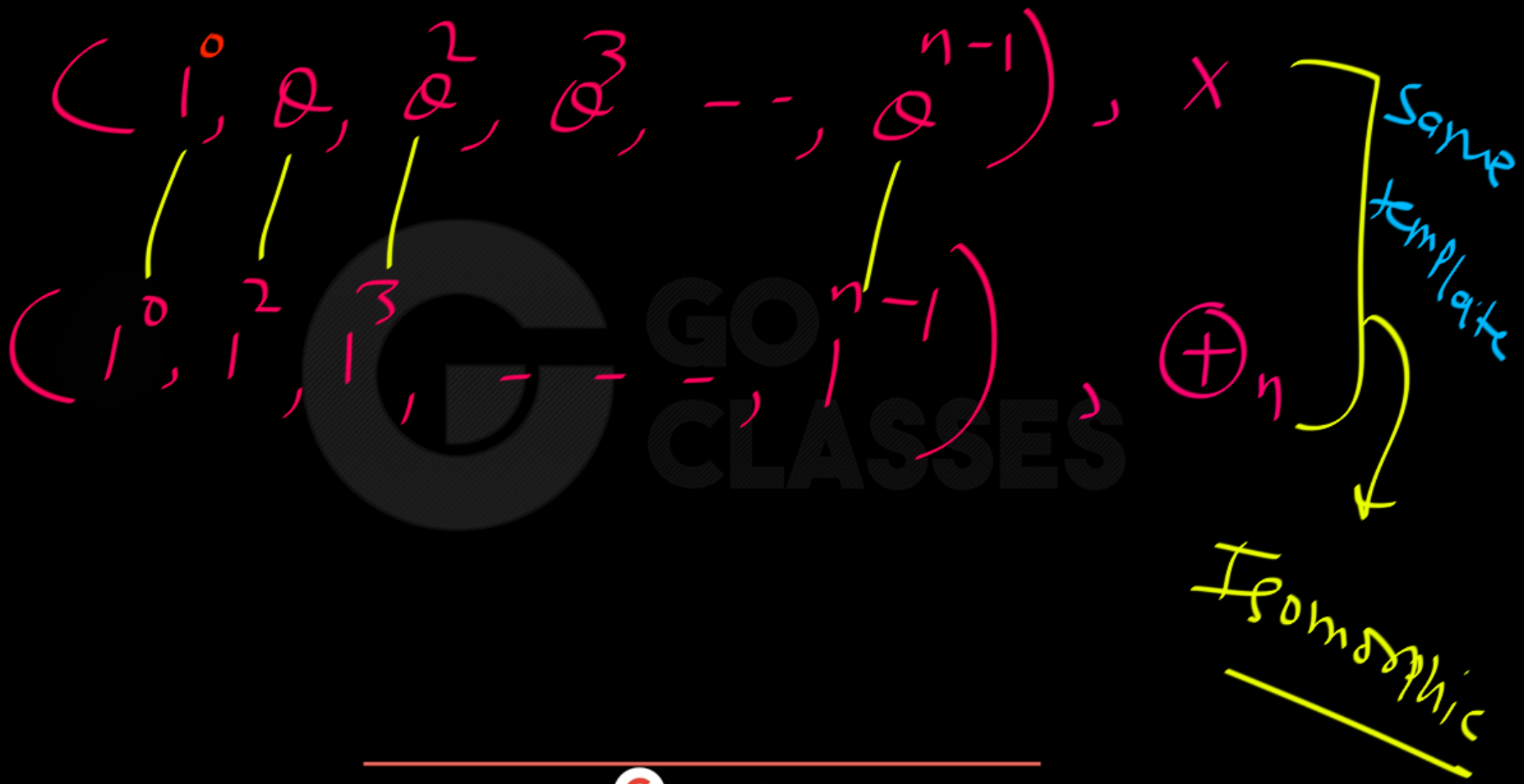
Give at least one cyclic group:

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

Note: for order n,

Give at least one cyclic group:

(n^{th} Roots of unity, $\times$)


$(i^0, \alpha, \alpha^2, \alpha^3, --, \alpha^{n-1}), \times$
$(1^0, 1^2, 1^3, --, 1^{n-1}), \oplus_n$
Same template
Isomorphic

Theorem:

Same Structure / same template

Any cyclic group is isomorphic to either $\mathbb{Z}$ *or* $\mathbb{Z}_n$.

Infinite cyclic Group $\equiv \mathbb{Z}, +$

finite cyclic Group of order $n \equiv \mathbb{Z}_n, \oplus_n$

Group Theory

Next Topic

Lagrange's Theorem

Order of Subgroup divides order of Group

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

Order of an element :

We denote by $|G|$ the size of a group G, and call this the order of G. The word order means something slightly different when used with particular group elements: the order of an element $g \in G$, written $o(g)$, is defined to be the smallest natural number such that $g^n = e$, if such an n exists. If not, we say g has infinite order.

Subgroup :

If $(G, *)$ is a group and $H \subset G$ is a subset such that $(H, *)$ satisfies the group axioms(properties), then we call H a subgroup of G, which we write as $H \leq G$.

Lagrange's Theorem:

If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Theorem 2.2.3. (Lagrange) *If S is a subgroup of the finite group G, then*

$$[redacted] = \frac{|G|}{|S|}$$ = Natural number

Thus the order of S divides the order of G.

Definition 2.5: If $x \in G$ and G is finite, the *order* of x is $|x| = |\langle x \rangle|$.

Corollary 2.2.4. *If $x \in G$ and G is finite, then $|x|$ divides $|G|$.*

Lagrange's Theorem:

Finite Group G ; $|G| = n$

If $H \leq G$ then $|H|$ Divides $|G|$

for any finite group G

$\langle a \rangle$ is a subgroup of G.

So $|\langle a \rangle|$ Divides $|G|$

$\Longrightarrow$ order of a

So, order of an element Divides order of group.

3.2.4 Lagrange's Theorem

Lagrange's Theorem states a very important relation between the orders of a finite group and any subgroup.

Theorem 3.15 (Lagrange's Theorem) *Let H be a subgroup of a finite group G. Then the order of H divides the order of G.*

Corollary 3.16 *let g be an element of the finite group G. Then the order of g divides the order of G.*

Subgroup except G

4.4.26 Group Theory: GATE CSE 2018 | Question: 19 top

https://gateoverflow.in/204093

Let G be a finite group on 84 elements. The size of a largest possible proper subgroup of G is _____

Subgroup except G

4.4.26 Group Theory: GATE CSE 2018 | Question: 19 top

https://gateoverflow.in/204093

Let G be a finite group on 84 elements. The size of a largest possible proper subgroup of G is _____

Ans : 42

4.4.26 Group Theory: GATE CSE 2018 | Question: 19 top

https://gateoverflow.in/204093

Let G be a finite group on 84 elements. The size of a largest possible [redacted] subgroup of G is _____

Ans : 84

NOTE: Lagrange's Theorem is only one way.

If H is subgroup then |H| Divides |G|.

Converse is NOT True.

finite Group G ; d Divides |G|

then ∃ subgroup of order d ?

Not Necessarily.

Eg: There is a Group of order 12 for which there is No subgroup of order 6.

the converse of Lagrange's theorem is not true?

NOT Required for GATE.

INTRODUCTION

A CLT group is a finite group which satisfies the converse of Lagrange's theorem and so has a subgroup of order d for every positive divisor d of the group order. A CLT number is a natural number n such that every group of order n is CLT. These numbers have been characterized by Berger [2] and Struik [10]. The numbers less than or equal to 100 which are not CLT are 12,24,36,48,56,60,72,75, 80,84 and 96. (In fact, see Pazderski [6], groups of other orders less than or equal to 100 are all supersolvable). This paper lists the corresponding non-CLT groups, 24 in all, after first proving some

0092-7872/83/1102-0111$3.50/0

NOTE: for Abelian Group ;

Converse of lagrange's Theorem is True.

NOTE: If G is a finite Abelian Group and d Divides $|G|$ then there exists at least one Subgroup of order d.

4.4.28 Group Theory: GATE CSE 2020 | Question: 18 top

https://gateoverflow.in/333213

Let G be a group of 35 elements. Then the largest possible size of a subgroup of G other than G itself is _____.

Ans: 7

Q: $|G| =$ Prime p $\quad a \neq e$

$|e| = 1$

$|a| = ?$

Q: $|G| =$ Prime p $\quad a \neq e$

$|e| = 1$ ✓ $\quad 2 \leq |a| \leq |G|$

$|a| = ?$ By lagrange's theorem, $|a|$ will Divides $|G| = p$; $|a| = p$

$a \neq e$ So $\quad 2 \leq |a| \leq |G|$ Prime p

$|a|$ Divides p and $|a| \geq 2 \Rightarrow |a| = p$

G = order prime p ; $\forall\, a \neq e$

$|a| = p$ means $\langle a \rangle = G$

Every element other than e is a Generator.

So G is cyclic ✓

Corollary 2.2.5. *If $|G| = p$ a prime, then G is cyclic.* So G Abelian.

Proof. Let $x \in G$, $x \neq 1$. Then $|x| = p$, because p is a prime. Hence $\langle x \rangle = G$ and therefore G is cyclic. □

Theorem 2.3.2. *Every subgroup of a cyclic group is cyclic.*

Theorem 1. Let p be a prime. Prove that every group of order p^2 is abelian.

Prime p :

order p group ⟶ Abelian

" p^2 " ⟶ "

Note: p = prime

Order p group ⟶ Cyclic

Order p^2 group ⟶ Cyclic

Ex: U_8

$|U_8| = 2^2$ — Prime

Not Cyclic

4.4.29 Group Theory: GATE CSE 2021 Set 1 | Question: 34 top

https://gateoverflow.in/357417

Let G be a group of order 6, and H be a subgroup of G such that $1 < |H| < 6$. Which one of the following options is correct?

A. Both G and H are always cyclic
B. G may not be cyclic, but H is always cyclic
C. G is always cyclic, but H may not be cyclic
D. Both G and H may not be cyclic

$|H| = 2, 3$ → Every group of order 2, 3 is cyclic

4.4.29 Group Theory: GATE CSE 2021 Set 1 | Question: 34

top

https://gateoverflow.in/357417

Let G be a group of order 6, and H be a subgroup of G such that $1 < |H| < 6$. Which one of the following options is correct?

A. Both G and H are always cyclic
B. G may not be cyclic, but H is always cyclic
C. G is always cyclic, but H may not be cyclic
D. Both G and H may not be cyclic

H — subgroup of G So

$|H|$ Divides $|G| = 6$

4.4.24 Group Theory: GATE CSE 2014 Set 3 | Question: 3 top

https://gateoverflow.in/2037

Let G be a group with 15 elements. Let L be a subgroup of G. It is known that $L \neq G$ and that the size of L is at least 4. The size of L is _____.

5

$L \leq G$, $|L|$ Divides 15

$|L| = 1, 3, 5, 15$

$5 \geq 4$

$L \neq G$

Group Theory

Next Topic

Classification of Groups of Specific Orders

Order 1 and all prime orders (1 group: 1 abelian, 0 nonabelian)

All groups of prime order p are isomorphic to C_p, the cyclic group of order p.
A concrete realization of this group is Z_p, the integers under addition modulo p.

Order 1 or prime $\Rightarrow$ Cyclic group
$\Leftrightarrow$
Abelian group.

Q: Order of $G = 17$; How many Non-Isomorphic Groups of order 17?

Q: Order of $G = 17$; How many Non-Isomorphic Groups of order 17 ?

$17 \Rightarrow$ 0 1

$|G| = 17 =$ Prime order $\Rightarrow$ G cyclic $\equiv Z_{17}$

Every cyclic Group of order n or Isomorphic $\equiv Z_n$

Q: Order of $G = 4$; How many Non-Isomorphic Groups of order 177 ?

Ans: 2 (templates)

Order 4 (2 groups: 2 abelian, 0 nonabelian)

1 cyclic, 1 Noncyclic.

template 1 : (e, x, y, z) $x = x^{-1}$, $y^{-1} = z$

cyclic — Gen = y, z

template 2 : (e, x, y, z) $\forall a$ $a^{-1} = a$

not cyclic

Order 1 to 5 $\not\Rightarrow$ Abelian

2, 3, 5 Prime order $\Rightarrow$ Cyclic & Abelian

1, 4 $\Rightarrow$ Abelian

Order 6 (2 groups: 1 abelian, 1 nonabelian)

Smallest Non-Abelian Group ⇒ S_3

#Non-Abelian Groups:

Order	#Non Abel Groups
1	0
2, 3, 5, 7, 11, 13	0
4	0
6	1

Classification of Groups of Order $n \leq 8$

n=1: The trivial group $\langle e \rangle$ is the only group with 1 element.

n=2,3,5,7: These orders are prime, so Lagrange implies that any such group is cyclic. By the classification of cyclic groups, there is only one group of each order (up to isomorphism):

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z}, \quad \mathbb{Z}/7\mathbb{Z}.$$

n=4: There are two groups of order 4:

n=6: There are two groups of order 6:

Group Theory

Next Topic (VERY Important)

Alternate Definitions of "Abelian Group"

MUST Understand Proofs. New variations can be created.

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

Abelian Group :

A Group with Commutative property.

$$a * b = b * a \quad \forall_{a,b}$$

NOTE: If I ask whether a Group is Abelian?

Target: $ab = ba$

Q 1: Group G, $a, b \in G$

$\forall_{a,b} \quad (a * b)^{-1} = b^{-1} * a^{-1}$

then G is Abelian ?

Q 1: Group G, $a, b \in G$

$\forall_{a,b}$ $(a * b)^{-1} = b^{-1} * a^{-1}$ — property of EVERY Group

then G is Abelian ? — No

Q 2:

2.7. *If G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, then show that G must be abelian.*

Q 2:

2.7. *If G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, then show that G must be abelian.*

Group G ; $\forall_{a,b}$ $(ab)^2 = a^2b^2$

Target : $ab = ba$

$(ab)^2 = a^2 b^2$ Group

$abab = aabb$

$a^{-1}abab\,b^{-1} = a^{-1}aabb\,b^{-1}$

$ba = ab$

$(ab)^2 = a^2 b^2$ Group

$abab = aabb$

Left Cancellation $bab = abb$

Right "

$ba = ab$ & Abelian

Note: Group G ; $\forall a, b$

$(ab)^2 = a^2 b^2 \Longrightarrow$ Abelian

$(ab)^2 = a^2 b^2 \Longleftarrow$ Abelian

Abelian iff $(ab)^2 = a^2 b^2$ $\forall a, b$

If group G is Abelian :

$$ab = ba$$

$$abb = bab$$

$$aabb = abab$$

$$a^2b^2 = (ab)^2$$

Q 2:

2.7. *If G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, then show that G must be abelian.*

Solution: $abab = a^2b^2$ apply a^{-1} from left and b^{-1} from right. We obtain $ba = ab$ for all $a, b \in G$.
Hence G is abelian.

Q 3:

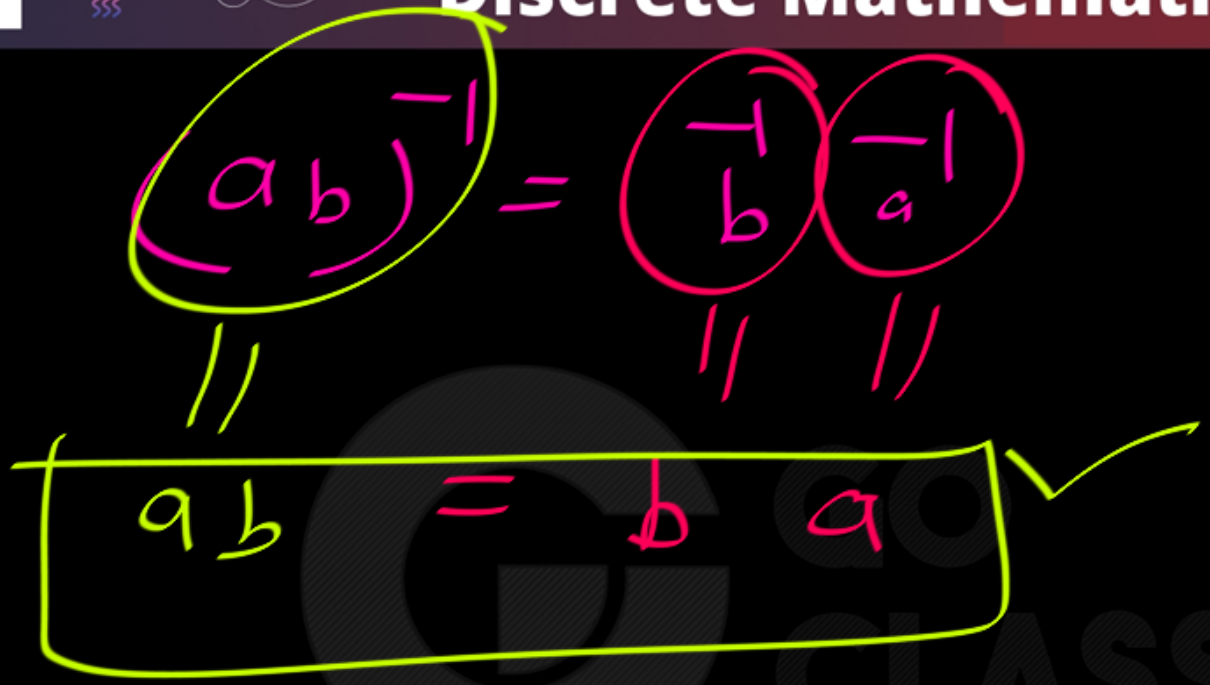
2.14. *Show that if every element of the group G is its own inverse, then G is abelian.*

Q 3:

2.14. *Show that if every element of the group G is its own inverse, then G is abelian.*

$\forall a$, $a^{-1} = a$ ✓ Target $\Rightarrow$ $ab = ba$

Group $\Rightarrow$ $(ab)^{-1} = b^{-1}a^{-1}$ → for EVERY group


$(ab)^{-1} = b^{-1} a^{-1}$
$ab = ba$

Note:

$\forall a, \quad a = a^{-1}$

$\Longleftrightarrow$

$\forall a, \quad a^2 = e$

Same

Q: Group $(G, *)$; $\forall a$, $a^2 = e$

then G is Abelian? Yes.

$a^2 = e \Rightarrow \boxed{a = a^{-1}} \forall a$

Q: If a Group is Abelian then

$\forall a, \quad a = \bar{a}^{1}$?

Q: If a Group is Abelian then

$\forall a, \quad a = \bar{a}^1$? = No

Ans:

$U_5 = \{1, 2, 3, 4\}, \times_5$

Abelian ← Order 4

But $\bar{2}^1 = 3$

$\bar{2}^1 \neq 2$

NOTE:

$\forall a,\ a^{-1} = a \Longrightarrow$ Abelian

$\forall a,\ a^{-1} = a \not\Longleftarrow$ Abelian

Q:

A group is Abelian iff $\forall a, \bar{a}^{-1} = a$.

False

Counter Ex: U_5

Q:

A group is Abelian if $\forall a, \bar{a}^{-1} = a$.

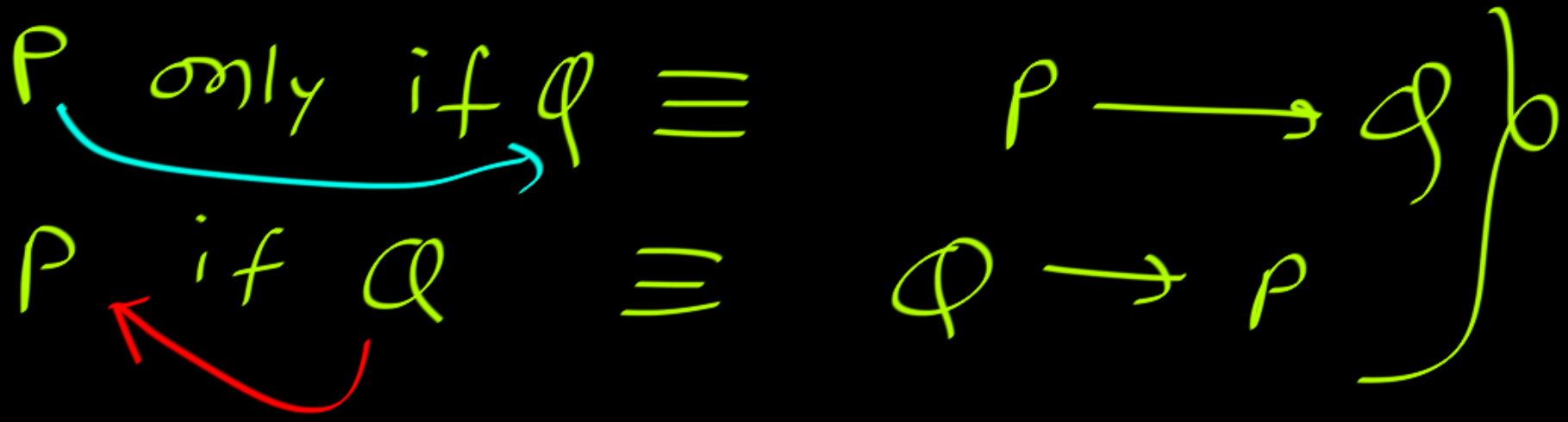
True

True

Q:

A Group is Abelian only if $\forall a, \bar{a}^{-1} = a$.

False


P only if Q ≡ P → Q
P if Q ≡ Q → P

Q 3:

2.14. *Show that if every element of the group G is its own inverse, then G is abelian.*

Solution: For all $x, y \in G$ we have $(xy)^{-1} = xy$ and $x^{-1} = x$ and $y^{-1} = y$. Then $(xy)^{-1} = xy$. This implies $y^{-1}x^{-1} = xy$. Hence $yx = xy$

Q 5:

Does every subgroup of an abelian group have to be abelian?

Q 5:

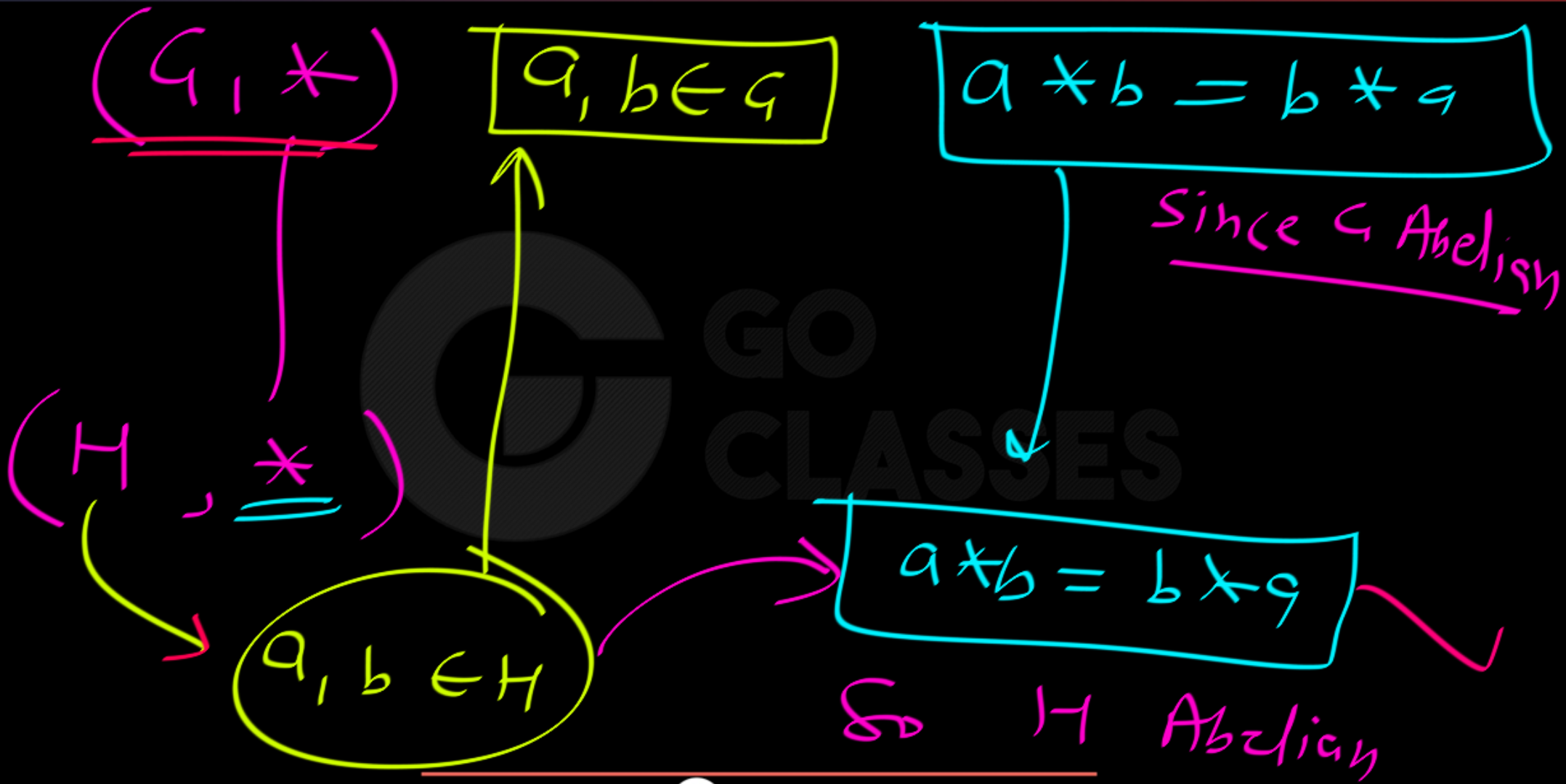
Does every subgroup of an abelian group have to be abelian? — Yes.

Group G Abelian ⇒ $\forall a, b$ $ab = ba$

Subgroup H

$\forall x, y$ $xy = yx$

because operation is same.


(G, *)
a, b ∈ G
a * b = b * a
Since G Abelian
(H, *)
a, b ∈ H
a * b = b * a
So H Abelian

Q 5:

Does every subgroup of an abelian group have to be abelian? YES.

If G is an abelian group and H is a subgroup, suppose $x, y \in H$. Then in particular $x, y \in G$, so $xy = yx$. Since x, y were arbitrary, H is abelian.

or

Just use proof by contradiction. Suppose H is not abelian and thus contains two non-commuting members x and y. Then $xy \neq yx$. But x and y are also in G, and thus G is not abelian. Contradiction. Therefore H is abelian.

GATE CSE 2022 | Question: 17

asked in **Set Theory & Algebra** Feb 15 • edited Feb 19 by **soujanyareddy13**

2

Which of the following statements is/are TRUE for a group G?

A. If for all $x, y \in G,\ (xy)^2 = x^2y^2$, then G is commutative.

B. If for all $x \in G,\ x^2 = 1$, then G is commutative. Here, 1 is the identity element of G.

C. If the order of G is 2, then G is commutative.

D. If G is commutative, then a subgroup of G need not be commutative.

GATE CSE 2022 | Question: 17

asked in **Set Theory & Algebra** Feb 15 • edited Feb 19 by **soujanyareddy13**

2

Which of the following statements is/are TRUE for a group G?

A. If for all $x, y \in G,\ (xy)^2 = x^2y^2$, then G is commutative.

B. If for all $x \in G,\ x^2 = 1$, then G is commutative. Here, 1 is the identity element of G.

C. If the order of G is 2, then G is commutative.

D. If G is commutative, then a subgroup of G need not be commutative.

Note: In Group.

$ax = bx \Rightarrow a = b$ ⟵

$ax = ay \Rightarrow x = y$ ⟵

$ax = ya \not\Rightarrow x = y$

In Group:

$a * b = c * d \not\Rightarrow ab = cd$

Q 6:

Let G be a group as following :

G is a group such that $x, y, z \in G$

$xy = zx$ implies $y = z$

Is G abelian ??

If $xy = zx \implies y = z$

Target: $ab = ba$

Proof:

~~$bab = bab$~~ ✓

So $\boxed{ab = ba}$

$ax = ya \implies x = y$ $\implies$ Abelian

$\impliedby$

If Abelian: $ab = ba$

$ax = (ya) = ay \implies x = y$

Group G is Abelian iff $\forall a, b, x$

$ax = ba$

implies $x = b$

Q 7:

Let G be a group as following :

G is a group such that $x, y, z \in G$

$xyz = ayc$ implies $xz = ac$

where $x, y, z, a, c \in G$

Then G is a Commutative Group? Yes.

Proof:

$a\,\bar{a}\,b = b\,\bar{a}\,a$

b ← $a\,\bar{a}\,b$ = $b\,\bar{a}\,a$ → b

$ab = ba$

Target $\boxed{ab = ba}$

Middle Cancellation $\Longrightarrow$ Abelian

$\Longleftarrow$

Abelian:

$$a * b = c * d$$

$$abx = cdx$$

$$\boxed{ab = cd}$$

Q 7:

Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$

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

$b^{-1} a^{-1} = a^{-1} b^{-1} \Rightarrow (ab)^{-1} = (ba)^{-1}$

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

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

$ab = ba$

Target $ab = ba$

In Group ; If $a \neq b$ then $a^{-1} \neq b^{-1}$

because Inverse of Every element is Unique.

$(ab)^{-1} = a^{-1}b^{-1}, \forall a, b \Rightarrow$ Abelian

$\Leftarrow$

Abelian $\quad ab = ba \rightarrow (1)$

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

$= \quad (ab)^{-1} = a^{-1}b^{-1}$

Q 7:

Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$

Ans:

$$ab = ba \overset{\text{by inversing}}{\iff} b^{-1}a^{-1} = a^{-1}b^{-1} \iff (ab)^{-1} = a^{-1}b^{-1}.$$

Another short proof:

$$ab = ((ab)^{-1})^{-1} = (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba.$$

Group Theory

Next Topic

Intersection of Subgroups

(Intersection of two subgroups is also a subgroup)

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

Give an example of G, H, K where the union HUK is not a subgroup.

There are many examples on this: Consider the group $(\mathbb{Z}, +)$. Now $(3\mathbb{Z}, +)$ and $(4\mathbb{Z}, +)$ are its subgroups, but is their union also a subgroup of $(\mathbb{Z}, +)$?

$(\mathbb{Z}, +)$

$(3\mathbb{Z}, +)$

$(4\mathbb{Z}, +)$

Subgroup

$((3\mathbb{Z} \cup 4\mathbb{Z}), +)$

Not even closed

$3 + 4 \notin 3\mathbb{Z} \cup 4\mathbb{Z}$

NOTE:

For any group G;

Union of two subgroups is may NOT be a subgroup.

Note: Group $(G, *)$

Subgroup $(H, *)$, $(L, *)$

$(H \cap L, *)$ — Subgroup

- Closed ?
- e ?
- Inverse ?

(1) $e \in H$, $e \in L$

$e \in H \cap L$

(2) Closure: $\forall a, b \in H \cap L \Rightarrow a * b \in H \cap L$

Subgroup

$a, b \in H \Rightarrow ab \in H$

$a, b \in L \Rightarrow ab \in L$

$\Rightarrow ab \in H \cap L$

(3) $a \in H \cap L \Longrightarrow a^{-1} \in H \cap L$

$a \in H \Rightarrow a^{-1} \in H$

$a \in L \Rightarrow a^{-1} \in L$

$\Rightarrow a^{-1} \in H \cap L$

↳ subgroup

Proposition. *$H, K \subset G$ subgroups $\Rightarrow$ $H \cap K \subset G$ is a subgroup.*

Proof. 1. As H, K subgroups, $e \in H$ and $e \in K \Rightarrow e \in H \cap K$.

2. $x, y \in H \cap K \Rightarrow x * y \in H$ and $x * y \in K \Rightarrow x * y \in H \cap K$.

3. $x \in H \cap K \Rightarrow x^{-1} \in H$ and $x^{-1} \in K \Rightarrow x^{-1} \in H \cap K$.

This result clearly extends to any collection of subgroups of G.

Group Theory

Next Topic

Alternate Definitions of "Subgroup"

(Skip the proofs. Not required.)

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

Subgroups

Definition. *Let $(G, *)$ be a group. A* ***subgroup*** *of G is a subset $H \subset G$ such that*

1. $e \in H$
2. $x, y \in H \Rightarrow x * y \in H$
3. $x \in H \Rightarrow x^{-1} \in H$

A subgroup is naturally a group under the induced binary operation. It clearly has the same identity element.

Subgroups

Non-empty

Alternative

Definition. *Let $(G, *)$ be a group. A **subgroup** of G is a subset $H \subset G$ such that*

[redacted]

2. $x, y \in H \Rightarrow x * y \in H$

3. $x \in H \Rightarrow x^{-1} \in H$

A subgroup is naturally a group under the induced binary operation. It clearly has the same identity element.

Subgroups

Another Alternative

Non-empty

Definition. *Let $(G, *)$ be a group. A **subgroup** of G is a subset $H \subset G$ such that*

[redacted]

2. $x, y \in H \Rightarrow x * y \in H$

3. $x \in H \Rightarrow x^{-1} \in H$

mix/merge

$\forall a, b$

$a * b^{-1} \in H$

A subgroup is naturally a group under the induced binary operation. It clearly has the same identity element.

Subgroups and subgroup tests

A subgroup of a group G is a subset of G which is a subgroup in its own right (with the same group operation). There are two subgroup tests.

Proposition 3.9 (First Subgroup Test) *A non-empty subset H of a group G is a subgroup of G if, for any $h, k \in H$, we have $hk \in H$ and $h^{-1} \in H$.*

Subgroups and subgroup tests

Proposition 3.9 (First Subgroup Test) *A non-empty subset H of a group G is a subgroup of G if, for any $h, k \in H$, we have $hk \in H$ and $h^{-1} \in H$.*

Proof We have to show that H satisfies the group axioms. The conditions of the test show that it is closed under composition (G0) and inverses (G3). The associative law (G1) holds in H because it holds for all elements of G. We have only to prove (G2), the identity axiom.

We are given that H is non-empty, so choose $h \in H$. Then by assumption, $h^{-1} \in H$, and then (choosing $k = h^{-1}$) $1 = hh^{-1} \in H$.

Subgroups and subgroup tests

A subgroup of a group G is a subset of G which is a subgroup in its own right (with the same group operation). The following is another subgroup test :

We can reduce the number of things to be checked from two to one:

Proposition 3.10 (Second Subgroup Test) *A non-empty subset H of a group G is a subgroup of G if, for any $h,k \in H$, we have $hk^{-1} \in H$.*

Proof Choosing $k = h$, we see that $1 = hh^{-1} \in H$. Now using 1 and h in place of h and k, we see that $h^{-1} = 1h^{-1} \in H$. Finally, given $h,k \in H$, we know that $k^{-1} \in H$, so $hk = h(k^{-1})^{-1} \in H$. So the conditions of the First Subgroup Test hold.

Note: If G is group; $H \subseteq G$

$\subseteq$: subset

To check if H is subgroup:

1. $e \in H$
2. Closure of H
3. Inverse property of H

subset which is group

Note: If G is a finite group; $H \subseteq G$ (H is a subset)

To check if H is subgroup:

1. Closure of H
2. Non-empty

Important: If G is finite group

then To check H is subgroup of G or not ?

H is non-empty

Only closure property of H is need to check

Although the above theorem is obvious it shows what must be checked to see if a subset is a subgroup. This checking is simplified by the next two theorems.

Theorem 2.1.2. *If S is a subset of the group G, then S is a subgroup of G if and only if S is nonempty and whenever $a, b \in S$, then $ab^{-1} \in S$.*

Theorem 2.1.3. *If S is a subset of the finite group G, then S is a subgroup of G if and only if S is nonempty and whenever $a, b \in S$, then $ab \in S$.*