Group Theory

Next Topic

Power of an Element in Groups

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

Q: In a Groupoid, can we say that $(a*b)*c = a*(b*c)$? $\Rightarrow$ No

Q: In a Groupoid, can we say that

(a*a)*a = a*(a*a) ? $\Longrightarrow$ No

$(P\{1,2,3\}, -)$ — Groupoid

Set Diff

Not - Asso

|Base set| = 8

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

$(P\{1,2,3\}, -)$ $a = \{1\}$ "$-$"

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

$(\{1\} - \{1\}) - \{1\} \stackrel{?}{=} \{1\} - (\{1\} - \{1\})$

$\phi \neq \{1\}$

Q: In a Semi-Group, can we say that
$(a*a)*a = a*(a*a)$?

Reason: Associative property

$(a*a)*a = a*a*a$

$= a*(a*a)$

No need to put Parenthesis

$(G, *)$ — Group

$*$ → Group operation

$\forall a \in G$

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

$a^1 = a$

$a^2 = aa = a * a$

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

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

Group op^n

$\boxed{a^0 = e}$

Next, we introduce the concept of integral exponents of elements in a group. The concept plays an important role in the theory of cyclic groups.

Definition 14.2

For any $a \in G$ we define

$$\begin{array}{rcl} a^0 & = & e \\ a^n & = & a^{n-1}a, \quad for\ n \geq 1 \\ a^{-n} & = & (a^{-1})^n \quad for\ n \geq 1. \end{array}$$

$\varphi : \left(\{1, 2\}, \otimes_3 \right)$ — Group

$\Rightarrow e = 1$

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

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

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

$2^2 =$

$2 \otimes_3 2$

$= 4 \bmod 3$

$= 1$ ✓

$Q: (\underbrace{\{0, 1, 2\}}_{\to Z_3}, \oplus_3)$ — Group

$\oplus_3$ → Group operation

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

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

$\underbrace{1^2 = 1}$ in Number theory

Given $r \in \mathbb{Z}$ and $a \in G$, we write

$$a^r = \begin{cases} a * a * \cdots * a \ \ (r \text{ times}), & \text{if } r > 0 \\ e, & \text{if } r = 0 \\ a^{-1} * a^{-1} * \cdots * a^{-1} \ \ (-r \text{ times}), & \text{if } r < 0 \end{cases}$$

Q: $(W,+)$ — monoid; $0^{-1}=0$; $2^{-1}=$ DNE

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

$2^n = 2n$; $\boxed{0^{-1}=0}$

$\boxed{2^0 = e = 0}$

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

$n \geq 1$

$\boxed{2^0 = e = 0}$

$2^{-1} \Rightarrow$ Not Defined $\rightarrow$ Not Group

If $n > 0$ is an integer, we abbreviate $\underbrace{a * a * a * \cdots * a}_{n \text{ times}}$ by a^n. Thus $a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ times}}$

"Power of element" is Defined for any SemiGroup.

Associative

Theorem 14.4

Let a be an element of a group G and m and n denote integers. Then

(i) $a^n a^{-n} = e$.
(ii) $a^m a^n = a^{m+n}$
(iii) $(a^m)^n = a^{mn}$.

because of Associativity, Inverse

$a^3 a^2 = a^5 = (a\ a\ a)(a\ a) = (a\ a\ a\ a\ a)$

$a^m a^n = a^{m+n}$ ✓

$a^m a^{-n} = a^{m-n}$ ✓

$(a^m)^n = a^{mn}$ ✓

$$(a^2)^3 = a^2 \cdot a^2 \cdot a^2 = (aa)(aa)(aa)$$

$$= aaaaaa$$

$$= a^6$$

$$\boxed{a^2 a^{-2} = a^0 = e}$$

Q : $(\mathbb{N}, +)$ — Semigroup

$1^2 = 1 + 1 = 2$

2^0 = NOT Defined (because No identity element)

2^{-1} = " "

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

$\underline{i^{-1} = -i}$

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

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

$i \times i = 1 \quad -i$

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

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

$(-i)^{-4} = \left(\underline{(-i)^{-1}} \right)^4$

Group operation

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

$= (i)^4 = i \times i \times i \times i$

$= 1$

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

Group Theory

Next Topic

Subgroups

Subset which is a group(under same Operation)

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

Group $(G, *)$

Subgroup of G : $(H, *)$

$H \subseteq G$ and $(H, *)$ is a Group

Q: $G = (\{1, -1, i, -i\}, \times)$ — Group

$e = 1$

Which is a Subgroup of G?

1) $(\{1, -1\}, \times)$

3) $(\{1, 0\}, \times)$

2) $(\{1, i\}, \times)$

Q: $G = (\{1, -1, i, -i\}, \times)$ — Group

$e = 1$

Which is a Subgroup of G?

1) $(\{1, -1\}, \times)$

~~2)~~ $(\{1, 0\}, \times)$ Nonsense

Nonsense

~~3)~~ $(\{1, i\}, \times)$

Not a Group $i \times i = -1$

~~4)~~ $(\{0\}, +)$

Nonsense

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

e

Subgroups of G

1. $\{1\}$
2. $\{1, -1\}$
3. $\{1, -1, i, -i\}$

Not Subgroups of G

1. $\{-1\} \Rightarrow$ Not Closed
2. $\{i, -i\} \Rightarrow \times$
3. $\{1, i, -1\} \Rightarrow \times$

$H = (\{1, -i\}, \times)$ — Not closed

NOT Subgroup

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

$H = \{1, -i, -1\} \Rightarrow$ NOT a SubGroup

NOT closed $(-i) \times (-1) = i \notin H$

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

Subgroups :

1. $\mathbb{Z}$ ✓
2. $\{0\}$ ✓
3. $2\mathbb{Z}$ ✓
4. $3\mathbb{Z}$ ✓
5. $4\mathbb{Z}$
6. $n\mathbb{Z}$, $\forall n$

Note: $\mathbb{Z}_n = \{0, 1, --, n-1\}$

$$\boxed{\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}}$$

(Not needed for GATE)

$$\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$$

$2\mathbb{Z} = \{0, 2, -2, 4, -4, 6, -6, --\}$

$= \text{Even}$

$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\} = \text{multiple of } n.$

$2\mathbb{Z}$

$= \underline{\underline{\text{Even}}}$

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

$\mathbb{Z}/2\mathbb{Z} = \underline{\underline{\mathbb{Z}_2}}$

$= \underline{\underline{\{0, 1\}}}$

$\underline{\underline{\mathbb{Z}_2}}$

Q: $(\mathbb{Z}, +)$ — Group

$\forall n \in \mathbb{Z}$, $n\mathbb{Z}$ is a Subgroup of $(\mathbb{Z}, +)$

$n = 4$

$(4\mathbb{Z}, +)$ → Same operation

Subset

⇒ closed

⇒ $e = 0$

Asso-ciative

⇒ $(4n)^{-1} = -4n$

Group

Q: $G = (\mathbb{Z}, +)$

How many finite subgroups of G?

Ans: 1

$(\{0\}, +)$ ✓

Note: If operation "$*$" is understood/clear then we directly say "G is a Group" instead of saying "$(G, *)$ is a Group"

Idea: $(G = \{e, a_1, a_2, ---\}, *)$

Create Subgroup of G:

$H = \{ e, a_1, a_1^{-1}, a_1^2, a_1^3, a_1^4, \ldots \}$

Subset of G which is a "Group" (under $*$)

Idea to Create SubGroup H of G :

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, - - - - - Should be Taken.

because of inverse

because of closure

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

Create subgroup:

$H = \{0, 3, 3^2, 3^3, 3^4, 3^5, \ldots, 3^{-1},$

$6 \quad 9 \quad 12 \quad 15 \quad -3$

$(-3)^2, (-3)^3, \ldots$

$\ldots$

mandatory

If we take 3

$G = \{e, a, b, c, \dots\}$

Assume $a^{-1} = d$

Subgroup that contains "a":

$H = \{e, a, a^2, a^3, a^4, \dots, d, d^2, d^3, \dots$
$\dots\}$

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

"Subgroup of Group G" is a Subset which is also a group under same Operation.

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

Q:

Any "Non-empty" subset H of Group G which satisfies

$\forall a,b \in H$ $\left\{\begin{array}{l} a * b \in H \\ a^{-1} \in H \end{array}\right\}$ then $e \in H$?

Ans: Yes.

Proof: H — "NonEmpty": M

So $\exists a \in H$

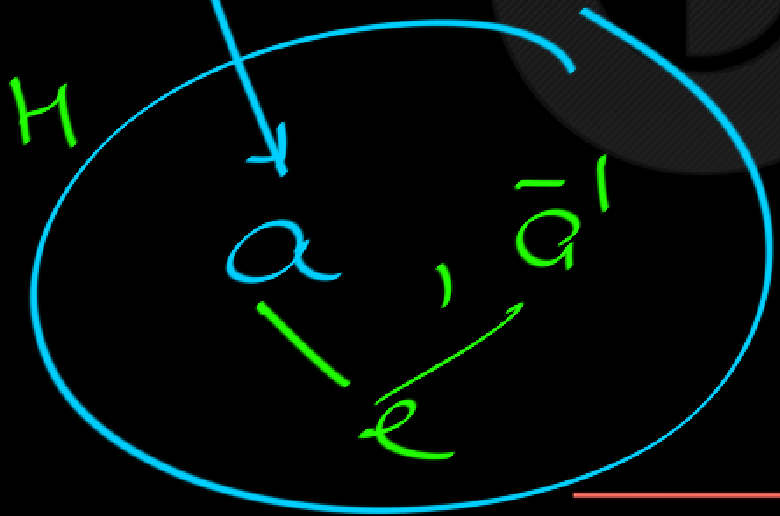
So $a^{-1} \in H$

So, $a * a^{-1} = e \in H$

NonEmpty $H \subseteq G$

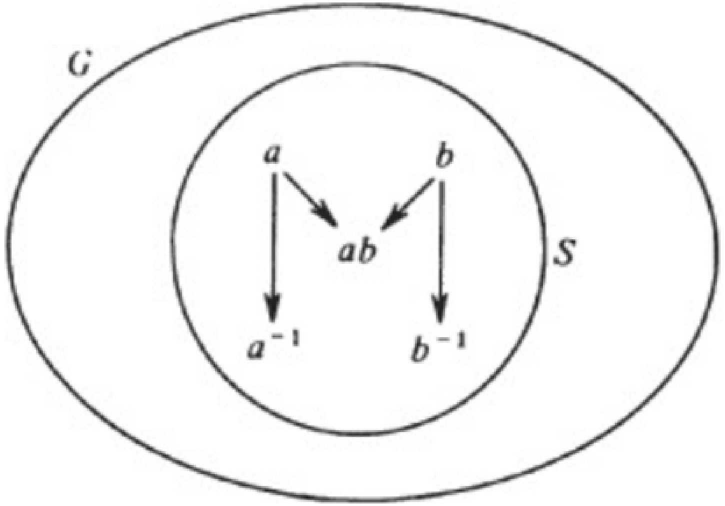
+ Closed

+ $a^{-1} \in H, \; \forall a \in H$



$a * a^{-1} = e \in H$

Let G be a group, and S a nonempty subset of G. It may happen (though it doesn't have to) that the product of every pair of elements of S is in S. If it happens, we say that S is *closed with respect to multiplication*. Then, it may happen that the inverse of every element of S is in S. In that case, we say that S is *closed with respect to inverses*. If both these things happen, we call S a *subgroup* of G.



11. Sub Group : A non empty sub set H of a group G is a sub group of G if H is closedunder products and inverses .

i.e. $a, b \in H \Rightarrow ab \in H \text{ and } a^{-1} \in H$

The sub groups H = G and {e} are called trivial or improper sub groups of G and the sub groups $H \neq G$ and {e} are called nontrivial or proper sub groups of G. It can be easily seen that the identity of a sub group H is the same as the identity of group and the inverse of a in H is the same as the inverse of a in G.

Example : The set {1, –1} is a sub group of the multiplicative group {1, –1, i, –i}

(ii) The set of even integers {0, ± 2, ± 4, …} is a subgroup of the set of additive group Z = { 0, ± 1, ± 2, ….} of integers.

Note: $(G, *)$ — Group

① $(\{e\}, *)$ — Trivial subgroup

② $(G, *)$ — subgroup of G

Proper Subgroup: $\Rightarrow$ any subgroup other than G.

H is subgroup of G

and $H \neq G$

In Z_9 under the operation $+_9$, the subset {0, 3, 6} forms a proper subgroup.

$(Z_9, \oplus_9)$ — Group

$(\{0, 3, 6\}, \oplus_9)$ — proper subgroup

Closed

$e = 0$

$3^{-1} = 6$; $6^{-1} = 3$

Group Theory

Next Topic

A VERY Special Subgroup

Subgroup generated by an element

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

$(\mathbb{Z}, +)$ — Group

Subgroup Generated by 2 $\equiv$ Smallest subgroup that contains 2

$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, \ldots, -2, -4, -6, \ldots\} = 2\mathbb{Z}$

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

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

$\langle 2 \rangle = \{2^n \mid n \in Z\}$ ✓

Eg: $(\{1, i, -1, -i\}, \times) = G$

Subgroup generated by Iota? ≡

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

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

$\langle 1 \rangle = \{1\} = \{1^6, 1^1, 1^2, 1^{-1}, 1^{-2}, \ldots\}$

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

$1, 1, 1, 1, 1, \ldots$

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

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

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

Note: $(G, *)$ – Group, let $a \in G$

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

= Smallest subgroup that contains a

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

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

Example 2.1: *Examples of subgroups.*

1. Both $\{1\}$ and G are subgroups of the group G. Any other subgroup is said to be a *proper subgroup*. The subgroup $\{1\}$ consisting of the identity alone is often called the *trivial subgroup*.

2. If a is an element of the group G, then

$e = a^0$

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, a^4, \ldots\}$$

are all the powers of a. This is a subgroup and is called the *cyclic subgroup* generated by a.

Observation:

$G = (\{1, -1, i, -i\}, \times)$

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

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

1, −1 cannot generate G.

$\langle i \rangle = G$

$\langle -i \rangle = G$

i, −i can generate whole G.

i Can Generate whole G.

So, i is Generator of G

$-i$ Can Generate whole G.

So, $-i$ is Generator of G.

$G = (\{1, -1, i, -i\}, \times)$

Generators of G = i, $-i$

Generator: Group $(G, *)$

$g \in G$ is "Generator" of G

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

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

Generators? $\Rightarrow$ $\underbrace{1}$, $\underbrace{-1}$

$$\boxed{\begin{aligned} \langle 1 \rangle &= \mathbb{Z} \\ \langle -1 \rangle &= \mathbb{Z} \end{aligned}}$$

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

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

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

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

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

$\longrightarrow$ NOT Generator of $\mathbb{Z}$

$Q: G = \{0, 1, 2, 3\}, \oplus_4 \longrightarrow e = 0$

Generators? $\Rightarrow$ 1, 3

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

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

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

$1^0 = e = 0$

$1^1 = 1$

$1^2 = 2$

$1^3 = 3$

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

$$= \{e = 0, 3, 2, 1, 1, \ldots\} = G$$

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

Note: Group $(G, *)$

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

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

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

(2) $\underline{\langle a \rangle} = \langle a^{-1} \rangle$ ✓

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

$\|$

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