Preliminaries:

1. Binary relation : A binary operation $*$ on a non-empty set A is a mapping from $A \times A$ to A. That is, $a * b \in A$ whenever $a, b \in A$.

Ex:- The operatn $+$ is binary opn on the set N

ex:- '$-$' on N $\longrightarrow$ Not

$2 - 5 = -3$ ✗

2. A binary operation $*$ on A is said to be
   i. Commutative: If for all $a, b \in A, a * b = b * a$
   ii. Associative : If for all $a, b, c \in A, a * (b * c) = (a * b) * c$

3. Identity element : An element $e \in A$ is said to be an identity element w.r.to the binary operation $*$ if $a * e = e * a$ for all $a \in A$.

A, $*$ 'e'

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

4. Inverse of an element: For a given element $a \in A$, an element $b \in A$ is said to be the inverse of a if $a * b = b * a = e$

A, $a \in A$,

$a * b = b * a =$ 'e' $\}$ $b = a^{-1}$

5. **Semigroup:** Let $(A,*)$ be an algebraic system. Then $(A,*)$ is said to be a semigroup if the following properties are satisfied
   i. Closure law $\rightarrow$ for any $a, b \in A$, $a * b \in A$
   ii. Associative law

$\rightarrow$ ① $(N, +)$ is semigp

② $(N, \cdot)$ is semigp

6. **Monoid:** Let $(A,*)$ be an algebraic system. Then $(A,*)$ is said to be a Monoid if the following properties are satisfied
   i. Closure law
   ii. Associative law
   iii. Identity Law $\rightarrow$ existance of identity elt

① $(N, +)$ is not monoid

② $(N, \cdot)$ is monoid

7. **Group:** Let $(A,*)$ be an algebraic system. Then $(A,*)$ is said to be a group if the following properties are satisfied
   i. Closure law
   ii. Associative law
   iii. Identity Law $\rightarrow$ existance of 'e'
   iv. Inverse law $\rightarrow$ every elt has inverse

① $(N, \cdot)$ is not a gp $\longrightarrow$ inverse fails (inverse of 2 is $\frac{1}{2} \notin N$)

② $(Z, +)$ is a gp $\rightarrow$ (inverse of 2 is -2)

③ $(R, \cdot)$ is not gp

④ $(R - \{0\}, \cdot)$ is gp

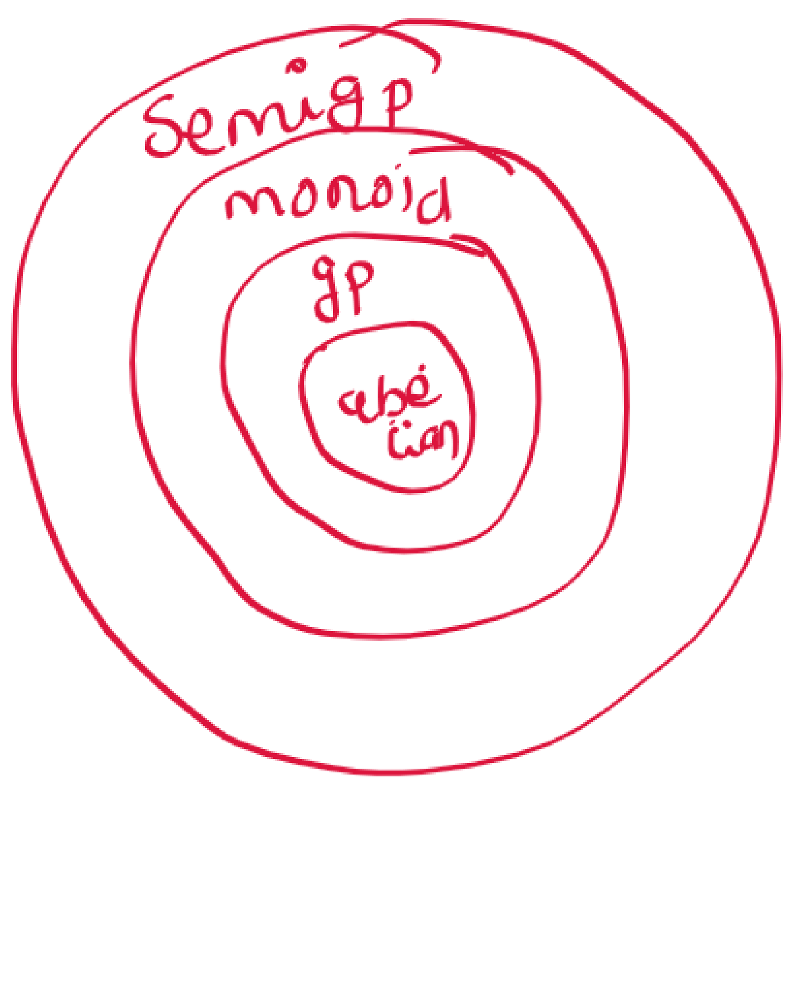
⑤ $(Q - \{0\}, \cdot)$ is gp

0

commutative gp

8. **Abelian group:** Let $(A,*)$ be an algebraic system. Then $(A,*)$ is said to be a group if the following properties are satisfied
   i. Closure law
   ii. Associative law
   iii. Identity Law
   iv. Inverse law
   v. Commutative law

ex:- $(Z, +)$



semigp monoid gp abelian

Properties:

Theorem 1: In a group $(G,*)$, the identity element is unique. $\rightarrow$ 'e'

Theorem 2: In a group $(G,*)$, inverse of an element is unique.

Let $a \in G$ and a has 2 inverses b and c

$a*b = b*a = e$ — (1) $\qquad a*c = c*a = e$ — (2)

consider $b = b*e$

$= b*(a*c) \quad (\because e = a*c)$

$= (b*a)*c \quad (\because$ associative$)$

$= e*c \quad (\because b*a = e$

$= c$

$\therefore b = c$

$(\mathbb{Z}, +)$

$2 \rightarrow -2$

$2+(-2) = 0$

$(-2)+2 = 0$

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

Theorem 3: In a group $(G,*)$, $(a^{-1})^{-1} = a$ for all $a \in G$.

Proof:- let $a^{-1} = x$ (Denoting

By defn of inv ; $a*x = x*a = e \quad (\because x$ is inverse of $a)$

Thus a is inverse of $x \Rightarrow x^{-1} = a$

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

Theorem 4: In a group $(G,*)$, $(a*b)^{-1} = b^{-1}*a^{-1}$ for all $a \in G$.

Proof:-

Let $x = a*b$ and $y = b^{-1}*a^{-1}$

T.P.T y is inverse of x (P.T $x^{-1} = y$)

ie T.P.T $x*y = y*x = e$

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

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

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

$= a*a^{-1}$

$= e$

Similary we can show that $y*x = e$

$\therefore x*y = y*x = e$

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

NOTE

$a, b, c \in G$

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

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

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

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

Theorem 5: In a group $(G,*)$,

i. $a * b = a * c \Rightarrow b = c$. (Left cancellation law)
ii. $a * b = c * b \Rightarrow a = c$. (Right cancellation law)

$\cancel{a} * b = \cancel{a} * c \Rightarrow b = c$

$a * \cancel{b} = c * \cancel{b} \Rightarrow a = c$

Proof :-

Given $a * b = a * c$

operate on left side by a^{-1}

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

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

$e * b = e * c$ (Inverse law $a^{-1} * a = e$

$b = c$ (Identity law

Hence the proof

ii) Given $a * b = c * b$

Operate on right by b^{-1}

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

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

$a * e = c * e$

$a = c$

Theorem 6: In a group $(G,*)$, the equations $a * x = b$ and $y * a = b$ where $a, b \in G$ have unique solution in G

$a * x = b$ This eqn has a unique soln x'

Proof:-

consider $a * x = b$

Existence of soln :-

$a * x = b$

operate on left by a^{-1}

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

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

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

$\boxed{x = a^{-1} * b}$

since $a \in G$, $a^{-1} \in G$ (inverse law)

$a^{-1} \in G$, $b \in G \Rightarrow a^{-1} * b \in G$ ($\because$ closure

uniqueness :-

Let x_1 & x_2 be 2 soln of the $a * x = b$

$a * x_1 = b$ — (1) and $a * x_2 = b$ — (2)

$(1) = (2) \Rightarrow a * x_1 = a * x_2$

$x_1 = x_2$ (left cancellatn law)

Similarly we can prove for the eqn $y * a = b$

① In a gp $(G, *)$, if $(a*b)^2 = a^2*b^2$ $\forall$ (for all) $a, b \in G$. Then P.T G is abelian gp

Soln

Given that $(a*b)^2 = a^2 * b^2$ for all $a, b \in G$

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

$$\cancel{a}*(b*a)*b = \cancel{a}*(a*b)*b$$

$$(b*a)*\cancel{b} = (a*b)*\cancel{b}$$

$b*a = a*b$ for all $a, b \in G$

$\therefore$ commutative law is satisfied

$\therefore$ G is abelian

② Let G be a group in which every element is inverse of itself, Then S.T G is abelian

Soln

$a^{-1} = a$ $\forall$ $a \in G$ (given

Consider $a*b = (a*b)^{-1}$ ($\because$ given

$= b^{-1}*a^{-1}$ ($\because$ Thm 4)

$= b*a$

$a*b = b*a$

$\therefore$ Abelian

③ If a group $(G, *)$ has even no of elts, then S.T atleast one elt must be its own inverse

Proof

$$G = \{e, a_1, a_2 \ldots, a_{2n-1}\}$$

$$\begin{cases} a_1^{-1} = a_2 \\ a_3^{-1} = a_4 \\ \vdots \\ a_{2n-3}^{-1} = a_{2n-2} \\ a_{2n-1}^{-1} = a_{2n-1} \end{cases}$$

Subgroup

Let $(G, *)$ be a group. H be a nonempty subset of G. H is said to be a subgroup of G if H itself forms a group under the same operation

Ex:-

① $(Q, +)$ is group

$(Z, +)$ is a subgroup of $(Q, +)$

② $(Z, +)$ is a group

$A = \{$set of all even integers$\} = \left\{\begin{matrix} 0, 2, 4, 6, 8, \ldots \\ -2, -4, -6, \ldots \end{matrix}\right\}$

$A \subseteq Z$

* $(A, +)$ is a group. $\therefore (A, +)$ is a subgroup of $(Z, +)$

* $B = \{$set of odd integers$\}$

$(B, +)$ is not a subgroup of $(Z, +)$