GROUP THEORY

BINARY OPERATION

Let A be a nonempty set. A mapping $f: A \times A \to A$ is called a binary operation. We normally denote binary operation using $*$ or $\cdot$.

PROPERTIES OF BINARY OPERATIONS

Let $*: G \times G \to G$ be a binary operation where G is a nonempty set.

① **CLOSURE PROPERTY**

$*$ is closed if for any $a, b \in G$, then $a * b \in G$.

② **ASSOCIATIVE PROPERTY**

$a * (b * c) = (a * b) * c$ for any $a, b, c \in G$.

③ **EXISTENCE OF IDENTITY ELEMENT**

There exists an element $e \in G$ such that

$a * e = e * a = a \quad \forall a \in G$

The element 'e' is called the identity element of G.

④ **EXISTENCE OF INVERSE**

For any $a \in G$, if there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$, then a^{-1} is called the inverse of a.

⑤ **COMMUTATIVE OR ABELIAN PROPERTY**

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

⑥ **DISTRIBUTIVE PROPERTY**

$a * (b \cdot c) = (a * b) \cdot (a * c)$ Left Distributive law

$(b \cdot c) * a = (b * a) \cdot (c * a)$ Right Distributive law

for any $a, b, c \in G$

⑦ **CANCELLATION PROPERTY**

$a * b = a * c \Rightarrow b = c$ Left cancellation law

$b * a = c * a \Rightarrow b = c$ Right Cancellation law

for any $a, b, c \in G$

⑧ **IDEMPOTENT PROPERTY**

$a * a = a \quad \forall a \in G$.

EXAMPLES

1. The operation '$-$' on N is not closed since $2,3 \in N$ but $2-3=-1 \notin N$
2. The operation $*$ defined by $a*b=\frac{a+b}{2}$ is closed in R but not in Z.
3. Addition and multiplication are commutative on Z whereas subtraction is not.
4. Matrix multiplication on the set of all 2×2 matrices is not commutative but is associative.

   For eg., $\begin{pmatrix}1&2\\3&4\end{pmatrix}\begin{pmatrix}5&6\\0&-2\end{pmatrix}=\begin{pmatrix}5&2\\15&10\end{pmatrix}$

   but $\begin{pmatrix}5&6\\0&-2\end{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{pmatrix}23&24\\-6&-8\end{pmatrix}$ $\therefore$ Not commutative
5. For Z, '0' is the identity element under addition and '1' is the identity element under multiplication.
6. For any $a\in Z$, $-a$ is the inverse of a under addition since $a+(-a)=(-a)+a=0$
7. $+$ and $-$ in Z do satisfy both the cancellation laws. But matrix multiplication does not satisfy cancellation law.

   For eg., Let $A=\begin{pmatrix}1&1\\0&0\end{pmatrix}$ $B=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $C=\begin{pmatrix}0&-3\\1&5\end{pmatrix}$

   Then $AB=AC=\begin{pmatrix}1&2\\0&0\end{pmatrix}$

   But $B\neq C$

PROBLEMS

1) Let $*$ be a binary operation defined on $R-\{1\}$ defined by $x*y=x+y-xy$. Show that $*$ is commutative and associative. Find the identity element and indicate inverse of each element.

Solution

(i) To P.T. $a*b=b*a$ for any $a,b\in R-\{1\}$

$$\begin{aligned}LHS &= a*b\\ &= a+b-ab\\ &= b+a-ba\\ &= b*a\\ &= RHS.\end{aligned}$$

$\therefore$ $*$ is commutative

(ii) To P.T. $a*(b*c) = (a*b)*c$ for any $a,b,c \in R-\{1\}$

$LHS = a*(b*c) = a*(b+c-bc) = a+b+c-bc-a(b+c-bc)$

$= a+b+c-ab-bc-ca+abc$

$RHS = (a*b)*c = (a+b-ab)*c = a+b-ab+c-(a+b-ab)c$

$= a+b+c-ab-bc-ca+abc$

$LHS = RHS \therefore$ * is associative

(iii) To P.T. $\exists$ an element $e \in R-\{1\}$ such that $a*e=a$ for any $a \in R-\{1\}$.

Let $a \in R-\{1\}$

Consider $a*e=a$

$\Rightarrow a+e-ae=a$

$\Rightarrow e(1-a)=0$

$\Rightarrow e=0$ ($\because a \neq 1$ as $a \in R-\{1\}$)

$\in R-\{1\}$

$\therefore 0 \in R-\{1\}$ is the identity element

(iv) To P.T. for $a \in R-\{1\}$, $\exists$ an element $a^{-1} \in R-\{1\}$ such that $a*a^{-1} = a^{-1}*a = e$

Let $a \in R-\{1\}$

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

$\Rightarrow a+a^{-1}-aa^{-1}=e$

$\Rightarrow a+a^{-1}(1-a)=0$

$\Rightarrow a^{-1} = \frac{-a}{1-a} \in R-\{1\}$

$\therefore$ Inverse element for a is $\frac{-a}{1-a}$

[Reason: If $\frac{-a}{1-a}=1$, then $-a=1-a$ $\Rightarrow 0=1$ which is impossible $\therefore \frac{-a}{1-a} \neq 1$]

2) Let * denote a binary operation on N given by $x*y=x$. Show that * is not commutative but is associative. Which elements are idempotent?

Solution

(i) Let $a,b \in N$.

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

$\therefore a*b \neq b*a$ Hence * is not commutative.

(ii) To P.T. $a*(b*c) = (a*b)*c$ for any $a,b,c \in N$

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

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

$\therefore$ LHS = RHS Hence $*$ is associative

(iii) For any $a \in N$, $a*a = a$ (by definition)

$\therefore$ All the elements are idempotent.

3) Let $x*y = \text{lcm}(x,y)$ where $*$ is a binary operation on I the set of positive integers. S.T. $*$ is commutative and associative. Find the identity element and also state which elements are idempotent.

Solution

(i) Let $a,b \in I$

$a*b = \text{lcm}(a,b) = \text{lcm}(b,a) = b*a$

$\therefore a*b = b*a$ for any $a,b \in I$

$\therefore *$ is commutative

(ii) Let $a,b,c \in I$

$a*(b*c) = a*\text{lcm}(b,c) = \text{lcm}(a, \text{lcm}(b,c))$

$(a*b)*c = \text{lcm}(a,b)*c = \text{lcm}(\text{lcm}(a,b), c)$

Note that $a*(b*c) = (a*b)*c$ since lcm of 3 integers taken in any order will be the same.

(iii) For any $a \in I$, to prove that $\exists$ an element $e \in I$ such that $a*e = e*a = a$

Consider $a*e = a$

$\Rightarrow \text{lcm}(a,e) = a$

$\Rightarrow e = 1 \in I$ is the identity element.

(iv) $a*a = \text{lcm}(a,a) = a$ for any $a \in I$

$\therefore$ Each element in I is idempotent.

4) Prove that the set N satisfies associative and identity properties under the operation $x*y = \max(x,y)$

Solution

(i) Let $a,b,c \in N$.

$a*(b*c) = a* \max(b,c) = \max(a, \max(b,c))$

$(a*b)*c = \max(a,b)*c = \max(\max(a,b), c)$

$\therefore a*(b*c) = (a*b)*c$ since maximum of 3 natural numbers taken in any order will be the same.

(ii) For any $a \in N$, to P.T. $\exists$ an element $e \in N$ such that $a*e = e*a = a$.

Let $a \in N$. Consider $a*e = a$

$\Rightarrow \max(a,e) = a$

$\Rightarrow e = 1 \in N$ is the identity element.

DEFINITION – SEMIGROUP

Let $*$ be a binary operation defined on a nonempty set S. Then S is said to be a semigroup if $*$ satisfies CLOSURE & ASSOCIATIVE PROPERTIES. We denote the semigroup by $(S, *)$

DEFINITION – MONOID

Let $*$ be a binary operation defined on a nonempty set S. Then S is said to be a monoid if $*$ satisfies CLOSURE, ASSOCIATIVE PROPERTY and IDENTITY ELEMENT exists.

ie. A semigroup with identity property is a monoid.

EXAMPLES

1. $(N, \times)$ is a monoid with identity element '1' but $(N, +)$ is not a monoid since the additive identity '0' is not a natural number.
2. Let $E = \{2,4,6,8,\ldots\}$. Then $(E,+)$ and $(E,\times)$ are semigroups but not monoids.
3. Let S be a nonempty set and P(S) be it's power set. Then $(P(S), \cup)$ and $(P(S), \cap)$ are monoids with identity elements ϕ and S respectively.
4. Let Z_n be the set of all congruence classes modulo n. Define $+_n$ by $[a] +_n [b] = (a+b) \bmod n$, where $[a], [b] \in Z_n$ and $\times_n$ by $[a] \times_n [b] = (ab) \bmod n$. Then $(Z_n, +_n)$ and $(Z_n, \times_n)$ are monoids.

For eg., when $n=5$ consider the Cayley's table for $+_5$ and $\times_5$. (For convenience, we denote $[a]$ by a itself)

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

We see that associative property is satisfied and $[0]$ and $[1]$ are the identities w.r.t $+_n$ and $\times_n$ respectively.

DEFINITION – ABELIAN MONOID

A monoid $(S,*)$ is said to be abelian if it satisfies commutative property i.e. if $a*b=b*a \ \forall a,b \in S$

Eg.
$\mathbb{Z}, \mathbb{R}$ and $\mathbb{C}$ are abelian monoids under usual addition and multiplication.

DEFINITION – CYCLIC MONOID

A monoid $(S,*)$ is said to be cyclic if there exists an element $a \in S$ such that for any $x \in S$, $x=a^n$ (Here $a^n = a*a*a \ldots$ n times) where n is an integer. Then S is said to be generated by the element 'a' and 'a' is called the GENERATOR of S.

Egs.
① Let $\mathbb{Z}_+ = \{0,1,2,\ldots\}$ be the set of all non-ve integers. Then $(\mathbb{Z}_+, +)$ is an infinite cyclic monoid since $1 \in \mathbb{Z}_+$ is the generator of $\mathbb{Z}_+$.

$1^0 = 0$ (write 1 no number of times)

$1^1 = 1$, $1^2 = 1+1 = 2$, $1^3 = 1+1+1 = 3 \ldots$

② $G = \{1, -1, i, -i\}$ is a cyclic monoid under multiplication. Here i is a generator since $1 = i^4, -1 = i^2, i = i^1$ and $-i = i^3$

Note that $-i$ is also a generator of $(G, \times)$, since $1 = (-i)^4$, $-1 = (-i)^2$, $i = (-i)^3$ and $-i = (-i)^1$.

GROUP

DEFINITION – GROUP

Let G be a nonempty set with binary operation $*$. Then $(G, *)$ will be called a group if the following properties are satisfied.

(i) CLOSURE PROPERTY

for any $a, b \in G$, $a * b \in G$.

(ii) ASSOCIATIVE PROPERTY

For any $a, b, c \in G$, $a * (b * c) = (a * b) * c$

(iii) EXISTENCE OF IDENTITY

For any $a \in G$, there exists an element $e \in G$ such that $a * e = e * a = a$

(iv) EXISTENCE OF INVERSE

For any $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Here $(G, *)$ represents a group G with $*$ as the binary operati

DEFINITION – ABELIAN GROUP

A group $(G, *)$ is said to be abelian if it satisfies commutative property. i.e. $a * b = b * a \quad \forall a, b \in G$.

EXAMPLES

1. $(Z, +)$ is a group but $(Z, \times)$ is not a group since inverse does not exist (For eg. $2 \in Z$ but $\frac{1}{2} \notin Z$)
2. $(I, +)$ and $(R, +)$ are abelian groups.
3. The set of all 3×3 matices is an abelian group under addition. It is also a group under multiplication but is not abelian, since matrix multiplication is not commutative.

DEFINITION – ORDER OF A GROUP

The order of a group $(G, *)$ denoted by $O(G)$ or $|G|$ is the number of elements in G.

If $O(G)$ is a finite number, then the group G is called a finite group. Otherwise it is called an infinite group.

Eg. $G=\{1,-1,i,-i\}$ under multiplication is a finite group of order 4 whereas $(Z,+)$ is an infinite abelian group.

PROBLEMS

1) Prove that $G=\{1,-1,i,-i\}$ is a group under usual multiplication.

Solution

Cayley's Table

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

From the table, we find the operation is closed and is associative. Identity element is 1.
Inverse of 1 is 1
Inverse of −1 is −1
Inverse of i is $-i$
Inverse of $-i$ is i
∴ G forms a group under multiplical

2) Prove that $A=\{1,\omega,\omega^2\}$ is an abelian group under multiplication where $1,\omega,\omega^2$ are cube roots of unity and $\omega^3=1$.

Solution

Cayley's Table

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

From Cayley's table, we find that $*$ is closed, associative and commutative. Identity element is 1.
Inverse of 1 is 1
Inverse of ω is ω^2
Inverse of ω^2 is ω
∴ $(A,\times)$ forms an abelian group.

3) Write down the composition table for $(Z_3,+_3)$ and prove that it is an abelian group.

Solution

$Z_3 = \{0, 1, 2\}$

Composition Table

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

From the table, we see that $+_3$ satisfies closure, associative and commutative properties. Identity is 0.
Inverse of 0 is 0
Inverse of 1 is 2
Inverse of 2 is 1
$\therefore (Z_3, +_3)$ is an abelian group.

4) Prove that the set of matrices $\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}$ forms a group under multiplication.

Solution

Let $A = \begin{pmatrix}1&0\\0&1\end{pmatrix}$ and $B = \begin{pmatrix}0&1\\1&0\end{pmatrix}$ and let $G = \{A, B\}$

To prove that $(G, \times)$ is a group.

Now $A \times A = \begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix} = A$

Similarly we find that $AB = B$, $BA = B$ and $BB = A$.

$\times$	A	B
A	A	B
B	B	A

From the table, we find that $\times$ is closed, associative. Identity element is $A = \begin{pmatrix}1&0\\0&1\end{pmatrix}$.
Inverse of A is A and inverse of B is B.
$\therefore (G, \times)$ is a group.

5) Prove that the set of all non zero real numbers forms an infinite abelian group under the operation $*$ defined by $a * b = \frac{ab}{2}$ $\forall\, a, b \in R - \{0\}$

Solution

① CLOSURE PROPERTY

Let $a, b \in R - \{0\}$

$a * b = \frac{ab}{2} \in R - \{0\}$ since $a \neq 0$ and $b \neq 0$

$\therefore *$ satisfies closure property.

② ASSOCIATIVE PROPERTY

Let $a, b, c \in R - \{0\}$

To P.T. $a * (b * c) = (a * b) * c$.

$a * (b * c) = a * \frac{bc}{2} = \frac{abc}{2 \times 2} = \frac{abc}{4}$

$(a*b)*c = \left(\frac{ab}{2}\right)*c = \frac{abc}{2\times 2} = \frac{abc}{4}$

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

③ IDENTITY ELEMENT

For any $a \in R-\{0\}$, to prove that there exists an element $e \in R-\{0\}$ such that $a*e = e*a = a$.

Let $a \in R-\{0\}$

Consider $a*e = a$

$\Rightarrow \frac{ae}{2} = a$

$\Rightarrow e = 2 \in R-\{0\}$

$\therefore 2$ is the identity element

④ INVERSE ELEMENT

For any $a \in R-\{0\}$, to prove that there exists an element $a^{-1} \in R-\{0\}$ such that $a*a^{-1} = a^{-1}*a = e$

Let $a \in R-\{0\}$

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

$\Rightarrow \frac{aa^{-1}}{2} = 2$

$\Rightarrow a^{-1} = \frac{4}{a} \in R-\{0\}$

$\therefore a^{-1} = \frac{4}{a}$ is the inverse of a. $\therefore$ Inverse exists.

⑤ COMMUTATIVE PROPERTY

For any $a, b \in R-\{0\}$, to prove that $a*b = b*a$

$a*b = \frac{ab}{2} = \frac{ba}{2} = b*a$

$\therefore R-\{0\}$ forms an abelian group.

6) In z, define $*$ by $a*b = a+b+1$. Show that $*$ satisfies all the properties of a group.

Solution

① CLOSURE PROPERTY

Let $a, b \in z$

$a*b = a+b+1 \in z$ ($\because$ a, b are integers, a+b+1 will also be an integer)

$\therefore *$ satisfies closure property.

② ASSOCIATIVE PROPERTY

Let $a, b, c \in z$

$a*(b*c) = a*(b+c+1) = a+b+c+1+1 = a+b+c+2$

$(a*b)*c = (a+b+1)*c = a+b+1+c+1 = a+b+c+2$

③ IDENTITY ELEMENT

To find an element $e \in z$ such that $a*e = e*a = a \ \forall a \in z$

Let $a \in z$. Consider $a*e = a$

$\Rightarrow a+e+1 = a$

$\Rightarrow e = -1 \in z$

$\therefore$ Identity element is -1

④ INVERSE ELEMENT

For any $a \in z$, to find an element $a^{-1} \in z$ such that $a*a^{-1} = a^{-1}*a = e$.

Let $a \in z$. Consider $a*a^{-1} = e$

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

$\Rightarrow a^{-1} = -a-2 \in z$ since $a \in z$.

$\therefore$ for any $a \in z$, $-a-2$ is its inverse

$\therefore z$ forms a group under $*$.

PROPERTIES OF GROUPS

PROPERTY ①

If every element in a group is its own inverse, then the group must be abelian (OR) if $a^2 = e$ with $a \neq e$, then G is abelian.

Proof:

Let $(G, *)$ be a group. Let $a, b \in G$.

Since every element of G is its own inverse,

$a = a^{-1}$ —① and $b = b^{-1}$ —②

Since $a, b \in G$, $a*b \in G$ ($\because$ G satisfies closure property)

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

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

$= b*a$ (from ① and ②)

$\therefore$ for any $a, b \in G$, $a*b = b*a$

$\therefore G$ is abelian.

Note:

For any $a, b \in G$ where $(G, *)$ is a group,

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

Proof:

Since $a, b \in G$, $a*b \in G$ ($\because$ G satisfies closure)

To prove $(a*b)^{-1} = b^{-1}*a^{-1}$ (inverse of $a*b$ is $b^{-1}*a^{-1}$)

we need to prove $(a*b)*(b^{-1}*a^{-1}) = e$.

$$\text{LHS} = (a*b)*(b^{-1}*a^{-1})$$
$$= a*(b*b^{-1})*a^{-1} \quad \text{(Associative property)}$$
$$= a*e*a^{-1}$$
$$= a*a^{-1}$$
$$= e = \text{RHS}.$$

PROPERTY ②

If G is a group of even order, then it has an element $a \neq e$ such that $a^2 = e$.

Proof:

Since G is a group of even order, let $O(G) = 2n$.

Omitting e, there are $(2n-1)$ elements in G. If we pair off these $(2n-1)$ elements with their inverses, we will be left with only one element say $a \neq e$ which is its own inverse. i.e. $a = a^{-1}$

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

PROPERTY ③

In a group G, the left and right cancellation laws hold.

Left Cancellation Law

For any $a, b, c \in G$, $\quad a*b = a*c \Rightarrow b = c$

Proof:

Since G is a group, $a \in G \Rightarrow a^{-1} \in G$.

Consider $a*b = a*c$

Premultiply by a^{-1} on both sides,

$$a^{-1}*(a*b) = a^{-1}*(a*c)$$
$$\Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c \quad \text{(Associative property)}$$

∴ Inverse of any element is unique.

PROPERTY ⑥

A group cannot have any element which is idempotent other than the identity element.

Proof:

Let G be a group and let $a \in G$.

Let us assume that a is idempotent.

Then $a*a = a$ —①

Let e be the identity element of G.

Then $a*e = e*a = a$ —②

From ① and ②, $a*a = a*e$

$\Rightarrow a = e$ (By Left Cancellation Law)

∴ Identity element is the only idempotent element.

PROPERTY ⑦

If a is an element of a group G, then $(a^{-1})^{-1} = a$.

i.e. If inverse of a is a^{-1}, then the inverse of a^{-1} is a.

Proof:

Let $a \in G$. Then it's inverse $a^{-1} \in G$, such that

$a*a^{-1} = a^{-1}*a = e$ —①

since $a^{-1} \in G$, it's inverse $(a^{-1})^{-1} \in G$ such that

$a^{-1}*(a^{-1})^{-1} = (a^{-1})^{-1}*a^{-1} = e$ —②

From ① and ②,

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

$\Rightarrow a = (a^{-1})^{-1}$ (By right cancellation law)

PROPERTY ⑧

If a has inverse b and b has inverse c, then $a = c$.

Proof:

a has inverse b $\Rightarrow$ $a*b = b*a = e$ —①

b has inverse c $\Rightarrow$ $b*c = c*b = e$ —②

From ① and ②, $a*b = c*b$

$\Rightarrow a = c$ (By right cancellation law)

PROPERTY ⑨

A group G is abelian iff $(a*b)^2 = a^2 * b^2$.

Proof:

First we assume that G is abelian.

To P.T. $(a*b)^2 = a^2 * b^2$

Since G is abelian, $a*b = b*a$ for any $a, b \in G$

$LHS = (a*b)^2$

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

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

$= a*(a*b)*b$ ($\because$ G is abelian)

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

$= a^2 * b^2 = RHS$

Conversely, assume $(a*b)^2 = a^2 * b^2$. To P.T. G is abelian.

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

$\Rightarrow (a*b)*(a*b) = (a*a)*(b*b)$

$\Rightarrow a*(b*a)*b = a*(a*b)*b$

$\Rightarrow b*a = a*b$ (By left and right cancellation laws)

$\therefore$ G is abelian

PROPERTY ⑩

If $(G, *)$ is an abelian group, then for all $a, b \in G$

$(a*b)^n = a^n * b^n$.

Proof:

We prove this result by the method of mathematical induction

Step ①

Let $n=1$. $(a*b)^1 = a^1 * b^1$ which is true.

$\therefore$ the statement is true for $n=1$

Step ②

Assume the statement is true for $n=k$.

i.e. assume $(a*b)^k = a^k * b^k$

Step ③

To P.T. the statement is true for $n=k+1$

i.e. to P.T. $(a*b)^{k+1} = a^{k+1} * b^{k+1}$

$LHS = (a*b)^{k+1} = (a*b)^k * (a*b)$

$= (a^k * b^k) * (a*b)$ (from step ②)

$= (a^k * b^k) * (b*a)$ ($\because$ G is abelian)

$= a^k * (b^k * b) * a$ ($\because$ G satisfies associative property)
$= a^k * (b^{k+1} * a)$
$= a^k * (a * b^{k+1})$ ($\because$ G is abelian)
$= (a^k * a) * b^{k+1}$ ($\because$ G satisfies associative property)
$= a^{k+1} * b^{k+1}$
$=$ RHS.

Thus the statement is true for all n.

SUBGROUPS

DEFINITION_SUBGROUP

Let G be a group and H a nonempty subset of G. Then H is a subgroup of G if H itself is a group under the same operation in G.

i.e. Let $(G, *)$ be a group and H be a nonempty subset of G. Then $(H, *)$ is a subgroup of G if

① For any $a, b \in H$, $a * b \in H$ (closure property)
② For any $a, b, c \in H$, $a * (b * c) = (a * b) * c$ (Associative property)
③ $e \in H$ where e is the identity element of G (Existance of Identity)
④ For any $a \in H$, $a^{-1} \in H$ (Existence of Inverse)

Egs
$(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$
$(2\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$

Note:
For any group G, the subgroups G and $\{e\}$ are called improper or trivial subgroups and all other subgroups are called proper or non-trivial subgroups.

THEOREM ①

A nonempty subset H of a group G is a subgroup of G iff for any pair of elements $a, b \in H$, $a * b^{-1} \in H$

Proof:

Assume that H is a subgroup of G.

To P.T. for any $a,b \in H$, $a * b^{-1} \in H$

Let $a,b \in H \Rightarrow a, b^{-1} \in H$ ($\because$ H is a subgroup, $b \in H \Rightarrow b^{-1} \in H$)

$\Rightarrow a * b^{-1} \in H$ ($\because$ H satisfies closure property)

CONVERSELY,

Assume $a,b \in H \Rightarrow a * b^{-1} \in H$ for any $a,b \in H$ ——①

To P.T. H is a subgroup of G, we have to P.T. H itself is a group under $*$.

① **ASSOCIATIVE PROPERTY**

Since G satisfies associative property and $H \subseteq G$, H also satisfies associative property.

② **IDENTITY ELEMENT**

Since $H \neq \phi$, there exists an element $a \in H$.

$a, a \in H \Rightarrow a * a^{-1} \in H$ (from ①)

$\Rightarrow e \in H$

$\therefore$ Identity element exists in H.

③ **INVERSE ELEMENT**

We know that $e \in H$. Let $a \in H$

$e, a \in H \Rightarrow e * a^{-1} \in H$ (from ①)

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

$\therefore$ Inverse exists for every $a \in H$

④ **CLOSURE PROPERTY**

Let $a,b \in H$. Then $a, b^{-1} \in H$ (since inverse exists in H)

$\Rightarrow a * (b^{-1})^{-1} \in H$ (from ①)

$\Rightarrow a * b \in H$

$\therefore$ H satisfies closure property.

Thus H is a subgroup of G.

THEOREM ②

The intersection of any two subgroups of a group is also a subgroup of the group. i.e. If H_1 and H_2 are subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.

Proof:

since H_1 and H_2 are subgroups of G, $e \in H_1$ and $e \in H_2$

$\Rightarrow e \in H_1 \cap H_2 \quad \therefore H_1 \cap H_2 \neq \phi$

To P.T. $H_1 \cap H_2$ is a subgroup of G.

By Theorem ①, it is enough to P.T. $a, b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

Let $a, b \in H_1 \cap H_2$

$\Rightarrow a, b \in H_1$ and $a, b \in H_2$

$\Rightarrow a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$ ($\because$ H_1 and H_2 are subgroups of G, by Theorem ①)

$\Rightarrow a * b^{-1} \in H_1 \cap H_2$

$\therefore H_1 \cap H_2$ is a subgroup of G.

NOTE:

The union of two subgroups of a group G need not be a subgroup of G.

Consider the group $(\mathbb{Z}, +)$

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

$3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$ are subgroups of $(\mathbb{Z}, +)$ but $(2\mathbb{Z} \cup 3\mathbb{Z}, +)$ is not a subgroup of $(\mathbb{Z}, +)$ since closure property is not satisfied.

$2\mathbb{Z} \cup 3\mathbb{Z} = \{\ldots -6, -4, -3, -2, 0, 2, 3, 4, 6, \ldots\}$

For eg., $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ but $2+3=5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

DEFINITION – ORDER OF AN ELEMENT

Let G be a group and let $a \in G$. If there is a least positive integer n such that $a^n = e$, then n is called the order of the element a. If no such integer exists, then a is said to be infinite order.

Egs.

① In $(\mathbb{R} - \{0\}, \times)$, the order of -1 is 2

② In $(\mathbb{C} - \{0\}, \times)$, the order of $-i$ is 4

DEFINITION – CYCLIC GROUP

Let $(G, *)$ be a group. Then G is said to be cyclic if there exists an element $a \in G$ such that every element $x \in G$ can be expressed as an integral power of a,

i.e. $x = a^n$ where n is an integer. Here a is called the generator of the group and we denote it as $G = (a)$ or $G = \langle a \rangle$

THEOREM (3)

Every cyclic group is abelian.

Proof:

Let $(G, *)$ be a cyclic group generated by an element $a \in G$. i.e. $G = (a)$

Let $x, y \in G$. Then $x = a^m$ and $y = a^n$ where m and n are integers.

Consider $x * y = a^m * a^n$

$= a^{m+n}$

$= a^{n+m}$

$= a^n * a^m$

$= y * x$ for any $x, y \in G$.

$\therefore$ G is abelian.

NOTE:

The converse is not true. i.e. Every abelian group is not cyclic.

THEOREM (4)

Every subgroup of a cyclic group is cyclic.

Proof:

Let G be a cyclic group generated by an element 'a' and let H be a subgroup of G. To P.T. H is cyclic.

Since H is a subgroup of G, every element of H is of the form a^n for some $n \in Z$.

If $a^x \in H$ then $(a^x)^{-1}$ i.e. $a^{-x} \in H$ since H is a subgroup.

Now either x or $-x$ is a positive integer. $\therefore$ H contains elements with positive indices. Let m be the least positive integer such that $a^m \in H$.

Claim: a^m is a generator of H.

Let $b \in H$. Then $b = a^n$ for some $n \in Z$.
Since m and n are integers, by division algorithm there exist integers q and r such that
$n = mq + r$ where $0 \le r < m$.

Consider $b = a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r$

$\Rightarrow a^n = (a^m)^q * a^r$

Premultiplying by $(a^m)^{-q}$ on both sides,

$(a^m)^{-q} * a^n = (a^m)^{-q} * (a^m)^q * a^r = a^r$ ——①

Since $a^m \in H$, $(a^m)^{-q} \in H$ ($\because$ H is a subgroup of G)

Also $a^n \in H$ $\therefore (a^m)^{-q} * a^n \in H$ ($\because$ H satisfies closure)

$\Rightarrow a^r \in H$ (from ①)

If $r \neq 0$, then $r < m$ and $a^r \in H$ contradicts the fact that m is the least positive integer such that $a^m \in H$. $\therefore r = 0$.

$\therefore b = a^n = a^{mq} = (a^m)^q$

$\Rightarrow$ b is an integral power of a^m.

$\Rightarrow H = (a^m)$

Hence H is a cyclic subgroup of G.