Chapter 02. Group Theory

1.Groups

Definition1.1:- A **binary operator** is an operator on a set $S\ (\neq \emptyset)$ which takes two elements from S as inputs and returns a single element. If the output element also belongs to S then we say that S is closed under the defined binary operator.

A non-empty set S, together with a binary operator defined on it is called a binary structure.

Example:- i) Addition and multiplication are Binary operators on $\mathbb{R}$

ii) Square root ($\sqrt{\ }$) is not a binary operator on $\mathbb{R}$

iii) $\mathbb{Q}$ with the binary operator $\oplus$ defined as $a \oplus b = \frac{ab-a}{2}$ is closed but not on $\mathbb{Z}$.

Definition1.2:- Let S be a $(\neq \emptyset)$set and $\oplus$ be a binary operator defined on S s.t S is **closed** under $\oplus$. Then $\oplus$ is called

i) Associative

if for each $a, b, c \in S$, $(a \oplus b) \oplus c = a \oplus (\ b \oplus c)$

A binary structure whose binary operation is associative called a **semi group**.

ii) Commutative

if for each $a, b \in S$, $\ a \oplus b = b \oplus a$

Example:- i) $+$ is associative and commutative on $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ since $(a+b)+c = a+(b+c)$, $a+b = b+a$ for each $a, b, c \in \mathbb{R}, \mathbb{Q}, \mathbb{Z}$.

ii) The binary operator $\oplus$ defined as $a \oplus b = \frac{ab-a}{2}$ is not associative on $\mathbb{Q}$ since $(1\oplus 1)\oplus 2 \neq 1\oplus(1\oplus 2)$ and not commutative since $(1\oplus 2) \neq (2\oplus 1)$

iii) Let $M_{2\times 2}$ be the set of all 2×2 real matrices. Then $M_{2\times 2}$ is associative under metrics multiplication but not commutative since

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

Definition 1.3 :- Let S $(\neq \emptyset)$ be a set and $\oplus$ be a binary operator defined on S. If there exists $e \in S$ s.t for each $a \in G$, $a \oplus e = e \oplus a = a$, then e is called the **identity** element of S for the operator $\oplus$.

A semi group that has an identity is called a **monoid**.

Example:- i) 0 is the identity element of $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ for the Addition.

ii) 1 is the identity element of $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ for the Multiplication.

iii) The binary operator $\oplus$ defined by $a \oplus b = \frac{ab-a}{2}$ has no identity element in $\mathbb{R}$.

iv) $\frac{1}{2}$ is the identity element in $\mathbb{R}, \mathbb{Q}$ for the binary operator $\oplus$ defined by

$$a \oplus b = a - \frac{1}{2} + b.$$

Definition 1.4:- Let S be a $(\neq \emptyset)$set and $\oplus$ be a binary operator defined on S s.t S is closed under $\oplus$ and e be the identity element of S.Let $a \in S$. If there exist $b \in S$ s.t $a \oplus b = b \oplus a = e$ then b is called the **inverse** of a. Also a is called the inverse of b and denote $b = a^{-1}$ and $a = b^{-1}$

Example:- i) $\left(-\frac{1}{2}\right)^{-1} = \frac{1}{2}$ ($\left(\frac{1}{2}\right)^{-1} = -\frac{1}{2}$) under addition on $\mathbb{R}, \mathbb{Q}$.

ii) $\frac{1}{2}$ is the inverse of 2 (or 2 is the inverse of $\frac{1}{2}$) under multiplication on $\mathbb{R}, \mathbb{Q}$

iii) 1 is the inverse of 0 (or 0 is the inverse of 1) under the binary operator $\oplus$ defined as $a \oplus b = a - \frac{1}{2} + b$ on $\mathbb{R}, \mathbb{Q}$.

Problems

1) Which of the following sets is closed under the given binary operator ?

i) [0,1] with the binary operator $\oplus$ defined by $a \oplus b = \frac{a+b}{2}$

ii) $\mathbb{Z}$ with the binary operator $\oplus$ defined by $a \oplus b = 2a + 3b$

iii) $\mathbb{Z}$with the binary operator $\oplus$ defined by $a \oplus b = a^b$

iv) $\mathbb{Q}$ with the binary operator $\oplus$ defined by $a \oplus b = ab + a + b$

vi) $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, ad - bc \neq 0 \right\}$ with matrix multiplication.

2) i) Show that the binary operator $\oplus$ defined by $a \oplus b = 2a + 3b$ is neither associative nor commutative in $\mathbb{R}$

ii) Show that the binary operator $\oplus$ defined by $a \oplus b = \frac{a+b}{2}$ is commutative but not associative in [0,1]

iii) Show that the binary operator $\oplus$ defined by $(a, b) \oplus (c, d) = (ac, ad + b)$ is associative but not commutative in $\mathbb{R} \times \mathbb{R}$.

iv) Show that the binary operator $\oplus$ defined by $a \oplus b = ab + a + b$ is commutative and associative in $\mathbb{Q}$.

3) Let $G = \{x \in \mathbb{R} \mid x > 1\}$. Define a binary operator $\bullet$ on G by $x \bullet y = xy - x - y + 2$ for all $x, y \in G$.

i) Show that G is closed under $\bullet$

ii) Prove that $\bullet$ is associative.

iii) Is $\bullet$ commutative in G?

iv) Find the identity element of G

v) Let $x \in G$. Find the inverse element of x and hence find 2^{-1}.

4)Show that $(\mathbb{Z}, \times)$ is a monoid but not a group.

Definition 1.5:- Let G be a group and $\oplus$ binary operator on G. We called the pair $(G, \oplus)$ is a **Group** if the following properties satisfied.

i) For each $a, b \in G$, $a \oplus b \in G$. (i.e. G is closed under $\oplus$)

ii) For each $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ ($\oplus$ is associative)

iii) There exist $e \in S$ s.t for each $a \in G$, $a \oplus e = e \oplus a = a$ (identity)

iv) For each $a \in G$, there exist $a^{-1} \in S$ s.t $a \oplus a^{-1} = a^{-1} \oplus a = e$ (inverse element)

We use the notation $(G, \oplus)$or just G if the context is clear, for above defined group.

Definition 1.6:- A group G is said to be **abelian** (commutative) if for each $a, b \in S$, $a \oplus b = b \oplus a$

A group which is not abelian is called **non-abelian**.

Examples:-

i) $(\mathbb{R}, +), (\mathbb{Q}, +)$ & $(\mathbb{Z}, +)$ are abelian groups.

ii) $(\mathbb{R}^*, \times)$ and $(\mathbb{Q}^*, \times)$ are abelian groups. ($\mathbb{R}^* = \mathbb{R} \backslash \{0\}$ & $\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}$)

iii) $(\mathbb{Q}^*, +)$ and $(\mathbb{Q}, \times)$ are not groups.

iv) Let $M_{2\times2}$ be the set of all 2×2 real matrices. Then $M_{2\times2}$ is a group under metrices multiplication but is not abelian.

v) Let $G = \{x \in \mathbb{R} \mid x > 1\}$. Define a binary operator $\bullet$ on G by $x \bullet y = xy - x - y + 2$ for all $x, y \in G$. Then $(G, \bullet)$ is a group.

Problem:- Prove the above examples.

Definition1.7:- The number of element in a group G is called the **order** of the group and denoted by $O(G)$. G is said to be a finite group if $O(G)$ is finite.

Notation:-

For $a \in G$ we define $a^0 = e, a^1 = a$, and $a^k = a.a^{k-1}$ inductively for k a natural number greater than 1. We also define $a^{-k} = (a^{-1})^k$, where k is a natural number.

Then for each $m, n \in \mathbb{Z}$,

$$a^m.a^n = a^{m+n} \quad \text{and} \quad (a^m)^n = a^{mn}$$

Definition 1.8:- Let G be a group and let $a \in G$. Then the **order** of a is the least positive integer m s.t $a^m = e$. This is denoted by $O(a)$. If no such integer exists, we say that a is of infinite order.

Example:- i) 2 is of infinite order in $(\mathbb{R}, +)$

ii) $O(-1) = 2$ in $(\mathbb{R}, \times)$ since $(-1)^2 = 1$

Theorem 1.1:- Let $(G, \bullet)$ be a group, then

(i) The identity element of G is unique.

(ii) Every $a \in G$ has a unique inverse in G.

(iii) For every $a \in G$, $(a^{-1})^{-1} = a$

(iv) For every $a, b \in G$, $(a \bullet b)^{-1} = b^{-1} \bullet a^{-1}$

Proof:- (i) Let us assume there exists 2 identity element e_1 and e_2. Then,

$e_1 \bullet e_2 = e_1$ since e_2 is a identity.

$e_1 \bullet e_2 = e_2$ since e_1 is a identity.

Hence $e_1 = e_2$.

Thus the identity element is unique.

(ii) Let assume that there exists two inverse b_1 and b_2 for some $a \in G$.

Then $a \bullet b_1 = b_1 \bullet a = e$ and $a \bullet b_2 = b_2 \bullet a = e$.

Observe that,

$$b_1 \bullet (a \bullet b_2) = (b_1 \bullet a) \bullet b_2 \quad \text{(since } \bullet \text{ is associative)}$$

$$b_1 \bullet e = e \bullet b_2$$

$$b_1 = b_2$$

Thus every $a \in G$ has a unique inverse in G.

(iii) Let $a \in G$ and a^{-1} be its inverse. Then

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

Since $(a^{-1})^{-1}$ is the inverse of a^{-1}, we have

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

But we have already prove that inverse should be unique for every $a \in G$.

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

(iv) Notice that,

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

$$= b^{-1} \bullet e \bullet b$$

$$= b^{-1} \bullet b$$

$$= e$$

Also notice that,

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

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

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

$$= e$$

Thus $(b^{-1} \bullet a^{-1}) \bullet (a \bullet b) = (a \bullet b) \bullet (b^{-1} \bullet a^{-1}) = e$

Since the inverse is unique, it follows that

$$(a \bullet b)^{-1} = b^{-1} \bullet a^{-1}.$$

Problems

1) Let $(G, \bullet)$ be a group and let $a \in G$. Define a binary operation $\oplus$on G s.t

$x \oplus y = x \bullet a^{-1} \bullet y$. Show that $(G, \oplus)$ is a group.

2) Let G be a group s.t $(a \bullet b)^2 = a^2 b^2$ for each $a, b \in G$. Show that G is a abelian group.

3) Show that if for each $a \in G$, $a^{-1} = a$,then G is abelian.

So far we have discuss about infinite groups.(i.e. $O(G)$ is infinite). Now we will discuss some special groups which are finite.

Residue class of n or Congruence modulo n ($\mathbb{Z}_n$)

Let $n \in \mathbb{N}$ be fixed.

Now let $a \in \mathbb{Z}$. Then there exists $q_1, r_1 \in \mathbb{Z}$ s.t $a = q_1 n + r_1$.

Suppose $r_1 \geq n$. Then there exist $r_2 \in \mathbb{Z}$ s.t $r_1 = n + r_2$.

Then $a = q_1 n + n + r_2$. Then we get $a = n(q_1 + 1) + r_2$ and $(q_1 + 1), r_2 \in \mathbb{Z}$

Again if $r_2 \geq n$ we can find $r_3 \in \mathbb{Z}$ s.t $a = n(q_1 + 2) + r_3$ and $(q_1 + 2), r_3 \in \mathbb{Z}$

So eventually we will have for some $k \in \mathbb{N}$, $r_k < n$.

Hence for any $a \in \mathbb{Z}$ we can find $q, r \in \mathbb{Z}$ s.t $a = qn + r$ with $0 \leq r < n$.

q is called the quotient and the r is called the remainder.

So any $a \in \mathbb{Z}$, the remainder (r) can be $0,1,2, \dots, n-1$.

Now suppose $a, b \in \mathbb{Z}$ have the same remainder r. Then there exists $q_1, q_2 \in \mathbb{Z}$ s.t

$a = nq_1 + r$ and $b = nq_2 + r$

Notice that,

$$a - b = nq_1 + r - nq_2 - r = n(q_1 - q_2) \Rightarrow \frac{a-b}{n} = (q_1 - q_2) \in \mathbb{Z}$$

Thus two integers a, b have the same reminder iff $a - b$ is divisible by n.

Definition2.2: Let $n \in \mathbb{N}$ and let $x \in \mathbb{Z}$. We will denote the set $\{y \in \mathbb{Z} \mid x \textit{ and } y \textit{ have the same reminder}\}$ by $[x]$. Where $[x]$ is called a residue class of n.

From the above definition we have

$$[x] = \{y \in \mathbb{Z} \mid x \textit{ and } y \textit{ have the same reminder}\} = \{y \in \mathbb{Z} \mid x - y \textit{ is divisible by } n\}$$

Theorem 2.2:- Let $n \in \mathbb{N}$ be fixed. Then for any $a, b \in \mathbb{Z}$.

$[a] = [b]$ iff a, b have the same remainder when divided by n.

Proof:- obvious.

Observe that if $a = nq_1 + r$ $(q \in \mathbb{Z}$ and $0 \leq r \leq n-1)$ then $[a] = [r]$ because they give the same remainder when divided by n which is r.

We know that every integer has exactly one of integers $0,1,2, \dots, n-1$ as its remainder

Hence by the above theorem all the residue classes of n can written as

$$[0], [1], [2], \dots, [n-1]$$

We will use the symbol $\mathbb{Z}_n$ to represent all the residue class of n.

i.e. $\mathbb{Z}_n = \{ [0], [1], [2], \dots, [n-1] \}$

Now let $[r_1]$ and $[r_2]$ be two residue classes of n and suppose $a \in [r_1]$ and $b \in [r_2]$.

Then $a = nq_1 + r_1$ and $b = nq_2 + r_2$ for some $q_1, q_2 \in \mathbb{Z}$.

Notice that,

$$a + b = nq_1 + r_1 + nq_2 + r_2 = n(q_1 + q_2) + (r_1 + r_2)$$

And

$$ab = (nq_1 + r_1)(nq_2 + r_2) = n\{nq_1q_2 + q_1r_2 + q_2r_1\} + r_1r_2$$

Therefore we have,

$$[a + b] = [r_1 + r_2] \text{ and } [a.b] = [r_1.r_2]$$

Now we define two binary operators addition (denoted by $\oplus$) and multiplication (denoted by $\otimes$) on $\mathbb{Z}_n$ as follows.

Let $[x], [y] \in \mathbb{Z}_n$. Then

$$[x] \oplus [y] = [x + y]$$

$$[x] \otimes [y] = [x.y]$$

Clearly both addition and multiplication are closed on $\mathbb{Z}_n$.

From the above definition what can you say about $[-1]$?

Let $a \in [-1]$. Then there exists $q \in \mathbb{Z}$ s.t $a = nq + (-1)$

Then $a = n(q-1) + (n-1)$. So $a \in [n-1]$.

Similarly $a \in [-r]$ iff $a \in [n-r]$

Theorem 2.3:- Two binary operators addition (denoted by $\oplus$) and multiplication (denoted by $\otimes$) on $\mathbb{Z}_n$ are both commutative and associative.

Proof:- Observe that,

$$[x] \oplus [y] = [x + y] = [y + x] = [y] \oplus [x]$$

$$[x] \otimes [y] = [x.y] = [y.x] = [y] \otimes [x]$$

Also,

$$([x] \oplus [y]) \oplus [z] = [x + y] \oplus [z] = [(x + y) + z] = [x + (y + z)]$$

$$= [x] \oplus [y + z] = [x] \oplus ([y] \oplus [z])$$

$$([x] \otimes [y]) \otimes [z] = [x.y] \otimes [z] = [(x.y).z] = [x.(y.z)] = [x] \otimes [y.z] = [x] \otimes ([y] \otimes [z])$$

Theorem 2.4:- For each $n \in \mathbb{N}$, $(\mathbb{Z}_n, \oplus)$ is a group and $O(\mathbb{Z}_n) = n$

Proof:- Let $n \in \mathbb{N}$.

We have already proved that $\oplus$ is closed and associative.

Observe that for each $[a] \in \mathbb{Z}_n$,

$[a] \oplus [0] = [a+0] = [a]$ and $[0] \oplus [a] = [0+a] = [a]$

Hence [0] is the identity element.

Now let $[b] \in \mathbb{Z}_n$. Then $0 < b < n$. Hence there exist $c \in \mathbb{Z}$ s.t $b + c = n$ and $0 < c < n$.

Then $[b] \oplus [c] = [b+c] = [n] = [0]$ and $[c] \oplus [b] = [c+b] = [n] = [0]$

Also for $[0] \in \mathbb{Z}_n$, $[0] \oplus [0] = [0+0] = [0]$

Thus for each $[a] \in \mathbb{Z}_n$, there exist $[a]^{-1} \in \mathbb{Z}_n$, s.t

$[a] \oplus [a]^{-1} = [0]$ and $[a]^{-1} \oplus [a] = [0]$ ($[a]^{-1}$ is called the additive inverse)

Therefore $(\mathbb{Z}_n, \oplus)$ is a group and $O(\mathbb{Z}_n) = n$.

Now we will discuss $\mathbb{Z}_n$ with the multiplication. If $[a] \in \mathbb{Z}_n$, then we have

$[a] \otimes [1] = [a.1] = [a]$ and $[1] \otimes [a] = [1.a] = [a]$

Except when $a = 0$.

$\mathbb{Z}_n$ cannot form a group with multiplication since $[0] \in \mathbb{Z}_n$

Because $[a] \otimes [0] = [a.0] = [0]$ for any $[a] \in \mathbb{Z}_n$.

So we define a new set $\mathbb{Z}_n^*$ which means all the residue classes of n except [0]

i.e. $\mathbb{Z}_n^* = \mathbb{Z}_n \backslash \{[0]\} = \{[1], [2], \ldots, [n-1]\}$

Unfortunately $(\mathbb{Z}_n^*, \otimes)$ does not form a group for every $n \in \mathbb{N}$.

Consider the set $\mathbb{Z}_6^*$. Clearly $[3], [2] \in \mathbb{Z}_6^*$. Then $[3] \otimes [2] = [3.2] = [6] = [0]$

Hence $\mathbb{Z}_6^*$ is not closed under $\otimes$, since $[0] \notin \mathbb{Z}_6^*$.

We get this problem since 6 is a multiple of 2 and 3.

So if n is a product of 2 integers, $\otimes$ is not closed on $\mathbb{Z}_n^*$.

Theorem 2.5:- $(\mathbb{Z}_n^*, \otimes)$ is a group iff n is a prime number.

Proof:- We have already proved that $(\mathbb{Z}_n^*, \otimes)$ not a group if n is product of two integers.

Now suppose n is prime.

Clearly $\otimes$ closed on $\mathbb{Z}_n^*$ since n is a prime.

Also $\otimes$ is associative.

$[1]$ is the identity element since for each $[b] \in \mathbb{Z}_n^*$,

$[b]\otimes[1] = [b.1] = [b]$ and $[1]\otimes[b] = [1.b] = [b]$

Let $[a] \in \mathbb{Z}_n^*$. Suppose $[a]$ does not have an inverse.

Then $[a]\otimes[b] \neq [1]$ for each $[b] \in \mathbb{Z}_n^*$. Also $[a]\otimes[b] \neq [0]$ for each $[b] \in \mathbb{Z}_n^*$ since n is prime. So $[a]\otimes[b] = [c]$ where $[c] \in \{[2], [3], \dots, [n-1]\}$

But $[b] \in \{[1], [2], \dots, [n-1]\}$. So we have $n-1$ values for $[b]$ and $n-2$ values for $[c]$

Hence there exists $k_1, k_2 \in \mathbb{Z}_n^*$ s.t $[a]\otimes[k_1] = [a]\otimes[k_2]$ and $k_1 \neq k_2$

Let $b \in [a]\otimes[k_1] = [a.k_1]$. Then $b \in [a]\otimes[k_2] = [a.k_2]$.

Hence there exists $q \in \mathbb{Z}$ s.t $b = nq + ak_1$ and $b = nq + ak_2$

Then $a(k_1 - k_2) = 0 \Rightarrow a = 0$ or $k_1 = k_2$

This is a contradiction.

Thus $[a]$ should have an inverse ($[a]^{-1}$) in $\mathbb{Z}_n^*$. ($[a]^{-1}$ is called the multiplicative inverse)

Problems

1) i) Write down the all the element in $\mathbb{Z}_7$

ii) Write down the additive inverse of each element in $(\mathbb{Z}_7, \oplus)$

iii) Write down the multiplicative inverse of each element in $(\mathbb{Z}_7^*, \otimes)$

iv) Find the order of each elements in $(\mathbb{Z}_7, \oplus)$

v) Find the order of each elements in $(\mathbb{Z}_7^*, \otimes)$

2) i) Find all the element in $(\mathbb{Z}_{12}^*, \otimes)$ which does not have a multiplicative inverse

ii) Find the element in $(\mathbb{Z}_{10}, \oplus)$ which itself is the additive inverse.

n^{th} root of unity

A **complex number** is an expression of the form $a + ib$ where a, b are real numbers and $i = \sqrt{-1}$. The real part of the complex number $a + ib$ is the real number a and imaginary part is the real number b.

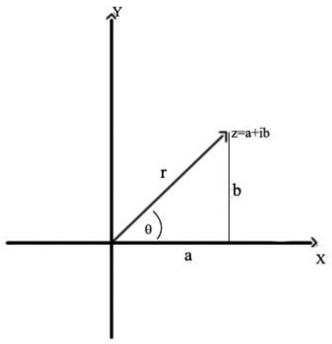
We denote by $\mathbb{C}$, the set of all complex numbers. Notice that all the real numbers are also complex numbers.

Definition 2.3:- The **absolute value** or **modulus** of the number $z = a + ib$ denoted by $|z|$ is the distance from the origin to the point z.

Let $z = a + ib$ be a complex number. Then $|z| = \sqrt{a^2 + b^2}$.

Polar Representation of a complex numbers

If r is the modulus of the complex number z and θ is the angle of inclination of z, measured positively in a counterclockwise sense from the positive real axis, we call r and θ the polar coordinates of the point z. This set of parameters reflects the interpretation of z as an object with magnitude and direction.



From the above figure, we deduce that

$$a = r\cos\theta, \quad b = r\sin\theta \text{ and } r = \sqrt{a^2 + b^2} = |z|.$$

θ which is usually given in radians is determined by the equations

$$\cos\theta = \frac{a}{|z|} \text{ and } \sin\theta = \frac{b}{|z|}.$$

Therefore the complex number $z = a + ib$ can be written in polar form

$$z = r(\cos\theta + i\sin\theta)$$

We note that one can determine θ only up to a multiple of 2π. The value of any of these equivalent angles is called the argument of z and denoted by arg z. The particular value of arg z that lies in the interval $(-\pi, \pi]$ is called the principle value of z and denoted by Arg z.

Note: If $z = 0$ then arg z is not defined. Therefore, it is understood that if a complex number is written in polar form it is non-zero

Result 2.1:- Let $z_1 = r_1(cos\theta_1 + isin\theta_1)$ and $z_2 = r_2(cos\theta_2 + isin\theta_2)$ be two complex Numbers. Then $z_1z_2 = r_1r_2[cos(\theta_1 + \theta_2) + isin(\theta_1 + \theta_2)]$

Proof:- Notice that,

$$z_1z_2 = r_1r_2(cos\theta_1 + isin\theta_1).(cos\theta_2 + isin\theta_2)$$

$$= r_1r_2[(cos\theta_1\, cos\theta_2 - sin\theta_1\, sin\theta_2) + i(cos\theta_1 sin\theta_2 + cos\theta_2 sin\theta_1)]$$

$$= r_1r_2[cos(\theta_1 + \theta_2) + isin(\theta_1 + \theta_2)]$$

<u>De Moivre's Thorem</u>

Let $z = r(cos\theta + isin\theta)$ be a complex number and $n \in \mathbb{N}$. Then,

$$z^n = r^n(cosn\theta + isinn\theta)$$

Proof:- Follows by result 2.1 and induction.

Now let us focus on our main topic the nth root of unity.

Let us solve the equation $z^n = 1$.

Let $z = r(cos\theta + isin\theta)$. Then, $z^n = r^n(cosn\theta + isinn\theta) = 1(cos0 + isin0)$

Therefore $r^n = 1$ and $\theta = \frac{0+2\pi k}{n}$, $(k = 0,1,2, \dots, n-1)$

Thus $(1)^{\frac{1}{n}} = 1\left(cos\frac{2\pi k}{n} + isin\frac{2\pi k}{n}\right)$, $(k = 0,1,2, \dots, n-1)$

Hence we have n solutions for our equation.

When $k = 1$, we obtain the root

$$\omega_n = \cos\left(\frac{2\pi}{n}\right) + isin\left(\frac{2\pi}{n}\right)$$

This ω_n is called the **primitive nth root of unity**.

Note that ω_n satisfies $\omega_n^n = 1$. But $\omega_n^n \neq 1$ for $k = 1,2, \dots, n-1$

Geometrically the n^th^ roots of unity form the vertices of a regular n-sided polygon inscribed in the circle of radius 1 about the origin.

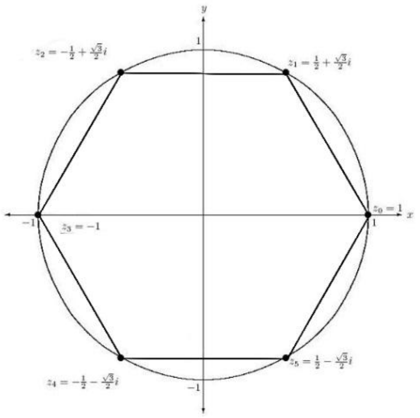
Example:- Solve $z^6 = 1$

Notice that the roots of the above equation given by

$$(1)^{\frac{1}{6}} = 1\left(cos\frac{2\pi k}{n} + isin\frac{2\pi k}{n}\right) \ , \ (k = 0,1,2,3,4,5)$$

Hence the roots are,

$\left(cos\frac{2\pi}{6} + isin\frac{2\pi}{6}\right)$,$\left(cos\frac{4\pi}{6} + isin\frac{4\pi}{6}\right)$, $\left(cos\frac{6\pi}{6} + isin\frac{6\pi}{6}\right)$, $\left(cos\frac{8\pi}{6} + isin\frac{8\pi}{6}\right)$, $\left(cos\frac{10\pi}{6} + isin\frac{10\pi}{6}\right)$ and 1.



Result 2.2:- Let $n \in \mathbb{N}$. and $\omega \neq 1$ be any root of the equation $z^n = 1$. Then,

$$1 + \omega + \omega^2 + \cdots + \omega^{n-1} = 0$$

Proof:- Observe that, $(1 - \omega)(1 + \omega + \omega^2 + \cdots + \omega^{n-1}) = 1 - \omega^n = 0$.

Clearly $\omega^n \neq 1$. Hence $(1 + \omega + \omega^2 + \cdots + \omega^{n-1}) = 0$.

Let $n \in \mathbb{N}$ and ω_n be the primitive n^th^ root of unity. Then notice that,

$$\omega_n^2 = \omega_n.\omega_n = \left(\cos\left(\frac{2\pi}{n}\right) + isin\left(\frac{2\pi}{n}\right)\right)\left(\cos\left(\frac{2\pi}{n}\right) + isin\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{4\pi}{n}\right) + isin\left(\frac{4\pi}{n}\right)$$

$$\omega_n^3 = \omega_n^2.\omega_n = \left(\cos\left(\frac{4\pi}{n}\right) + isin\left(\frac{4\pi}{n}\right)\right)\left(\cos\left(\frac{2\pi}{n}\right) + isin\left(\frac{2\pi}{n}\right)\right) = \cos\left(\frac{6\pi}{n}\right) + isin\left(\frac{6\pi}{n}\right)$$

So proceeding this manner we get all the roots for the equation $z^n = 1$.

Therefore every root can be written as the power of the primitive n^th^ root of unity.

Thus the roots of the equation $z^n = 1$ given by the set

$$U_n = \{\omega_n^k \ |\omega_n \text{ be the primitive nth root of unity and } k = 0,1,2,\dots,n-1\}$$

Or simply we can write as, $U_n = (\omega_n)$ where ω_n is the n^{th} root of unity.

So we can say that the roots of the equation $z^n = 1$ or U_n is **generated** by ω_n.

Theorem 2.6:- $(U_n,\times)$ is a finite abelian group where $\times$ is usual multiplication.

Proof:- Clearly U_n is finite.

i) Now let $\omega_n^k,\omega_n^m \in U_n$

Then, $\omega_n^k \times \omega_n^m = \left(\left(cos\frac{2\pi k}{n} + isin\frac{2\pi k}{n}\right)\right) \times \left(\left(cos\frac{2\pi m}{n} + isin\frac{2\pi m}{n}\right)\right)$

$$= \left(\left(cos\frac{2\pi(k+m)}{n} + isin\frac{2\pi(k+m)}{n}\right)\right)$$

$$= \omega_n^{k+m}$$

If $k + m \le n - 1$ then $\omega_n^{k+m} \in U_n$. If $k + m > n - 1$ then there exists $0 < r \le n - 2$ s.t $k + m = n + r$ and hence $\omega_n^{k+m} = \omega_n^{n+r} = \omega_n^n \times \omega_n^r = 1 \times \omega_n^r = \omega_n^r \in U_n$.

Therefore U_n is closed under $\times$.

ii) Let $\omega_n^k,\omega_n^l,\omega_n^m \in U_n$. then

$$(\omega_n^k \times \omega_n^l) \times \omega_n^m = \omega_n^{(k+l)} \times \omega_n^m = \omega_n^{(k+l)+m} = \omega_n^{k+(l+m)} = \omega_n^k \times \omega_n^{(l+m)}$$

$$= \omega_n^k \times (\omega_n^l \times \omega_n^m)$$

Hence $\times$ is associative.

iii) Clearly $1 \in U_n$ and 1 is the identity element.

iv) For each $\omega_n^k \in U_n$ the element $\omega_n^{n-k} \in U_n$ is the inverse element.

Problems:- i) Write down all the solutions of the equation $z^8 = 1$

ii) Find the order of the each of the elements.

iii) Find the element of U_8 which, itself is the inverse.

Now for any $n \in \mathbb{N}$, the groups $(Z_n, +), (Z_n^*, \times)$ and $(U_n, \times)$ are abelian groups. Now we discuss one more example of group which is not abelian.

Definition 2.3:- Let S be any set and f is a function s.t $f: S \to S$. If f is one to one and onto S (f is a bijection) then f is called a **permutation** of S.

A permutation, also called an "arrangement number" or "order," is a rearrangement of the elements of an ordered list S into a one to one correspondence with S itself.

The permutation on S given by $f(x) = x$ for each $x \in S$ is called the **Identity** permutation of S denoted by I.

Definition 2.4:- Let $n \in \mathbb{N}$. Then the set, $\{f : f \text{ } is\ a\ permutation\ of \text{ } \{1,2,3, \dots, n\}\}$ is denoted by S_n.

For a given $n \in \mathbb{N}$, S_n has $n!$ elements.

Example 1:- Consider the all the permutation of $\{1,2\}$ or S_2.

Then we have two $(2! = 2)$ permutations. One permutation is the identity permutation.

Other permutation f can be written as $\binom{1\ 2}{2\ 1}$ or $(1\ 2)$.

Example 2:- Consider the all the permutation of $\{1,2,3\}$ or S_3.

Then we have $3! = 6$ permutations. They are,

$I\ , (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$

Theorem 2.7:- For any $n \in \mathbb{N}$, (S_n, o) is a group where o is the composition of functions.

Proof:- Do it by yourself ☺.

We will show that (S_3, o) not abelian.

Notice that $(1\ 2) o (2\ 3) = (1\ 2\ 3)$

And $\quad (2\ 3) o (1\ 2) = (1\ 3\ 2)$

Thus (S_3, o) not abelian.

Problems

1) Consider the groups (S_3, o) and (S_4, o)..

i) Write down the inverse of all the elements in (S_3, o) and (S_4, o).

ii) Find the order of each element.

2.Sub Groups

Definition 2.1:- A non-empty subset H of a group G is said to be a **subgroup** of G, if under the same binary operator in G, H itself forms a group. If H is a subgroup of G, then we write H≤G. If H≠G then we write H<G.

Example:- G and $\{e\}$ are subgroups of the group G. These are called trivial subgroups.

Suppose there exist $a \in G$ s.t $a^{-1} = a$. Then $\{a, e\}$ is a subgroup.

Theorem 2.1:- A non-empty subset H of the group $(G,*)$ is a subgroup of G, iff

(i) for each $a, b \in H,\ \ a \bullet b \in H$.

(ii) for each $a \in H,\ \ a^{-1} \in H$.

Proof:- Let $a, b, c \in H$. Since $a, b, c \in G$ it satisfies the associative property.

for each $a \in H$ we have $a^{-1} \in H$. Hence $a \bullet a^{-1} \in H$. Thus $e \in H$. Therefore H containing the identity element.

Thus $(H, \bullet)$ is a group.

Theorem 2.2:- If H is a non-empty finite subset of a group G, and H is closed under multiplication, then $H < G$.

Proof:- Let $H \neq \emptyset$. Then $a.a \in H$ and also $a.a.a \in H$. Hence we have $a^n \in H$ for each $n \in \mathbb{N}$. Since H is finite and closed there exists $m \in \mathbb{N}$ s.t $a^n = a^m$ with $m > n$.

Then $a.a^{m-n-1} = a^{m-n-1}.a = e$. Hence it satisfying the theorem 2.1.

Thus $H \leq G$.

Examples:- i) Consider the subset $H = (3) = \{3m | m \in \mathbb{Z}\}$ in $\mathbb{Z}$.

Then H is a subgroup in $(\mathbb{Z}, +)$

In particular for any $n \in \mathbb{N}$, the subset (n) is a subgroup in $(\mathbb{Z}, +)$.

ii) Consider the group Z_6. Then it has exactly four subgroups.

$$\{0\}, \{0,3\}, \{0,2,4\} \text{ and } Z_6.$$

iii) The subgroups of Z_8 are

$$\{0\}, \{0,4\}, \{0,2,4,6\}, \text{ and } Z_8$$

iv) Z_5^* does not have any proper subspaces.

v)The subgroups of U_6 are

$$\{1\}, \{1, \omega_5^3\}, \{1, \omega_5^2, \omega_5^4\} \text{ and } U_6$$

Problems

1) Show that the sets $H_1 = \{2m | m \in \mathbb{Z}\}$ and $H_2 = \{3m | m \in \mathbb{Z}\}$ are subgroups of $(\mathbb{Z}, +)$.

Is $H_1 \cap H_2 < G$?

Is $H_1 \cup H_2 < G$?

2) Let $H_1, H_2, \dots, H_n$ be subgroups of G.Show that $(H_1 \cap H_2 \cap \dots \cap H_n)$ is also a subgroup of G.

3) Let G be a group and $a \in G$. Then prove that

$$N(a) = \{x \in G \mid xa = ax\} < G$$

This subgroup is called the normalizer or centralizer of a in G.

4) The Center $Z(G)$ is define by

$$Z(G) = \{z \in G \mid zx = xz \text{ } for \text{ } each \text{ } x \in G\}.$$ Show that $Z(G) < G$.

5) Let H be a subgroup of group G and $a \in G$. Then the subset define by

$$a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$$ is also a subgroup of G.

3.Cosets

Definition 3.1:-The set Ha is called a **right coset of H in G** and aH is called a **left coset of H in G**

Results:- i) $H = He = eH$. Therefore, H itself is a left and right coset.

ii) $ea \in Ha$. Therefore, $Ha \neq \emptyset$ for each $a \in G$.

Theorem 3.1:- Let H be a subgroup of G. Then for all $a \in G$, $O(H) = O(aH) = O(Ha)$

Theorem 3.2:- Any two right (left) cosets of a subgroup are either disjoint or are identical.

Theorem 3.3:- If H is a subgroup of a group G, then G is the union of all distinct right(left) cosets of H in G.

i.e. $G = \bigcup_{a\in G} Ha = \bigcup_{a\in G} aH$

Definition 3.2:- Let H be a subgroup of a group G. Then the number of distinct right cosets of H in G is called the **index of H in G** and is denoted by $i_G(H)$ or $[G: H]$

Theorem 3.4:- **Lagrange's Theorem**

If G is a finite group and H is a subgroup of G, then the order of H is a divisor of the order of G. i.e. $O(H) \mid O(G)$.

Note:- The converse of this theorem is false. If m is a divisor of $O(G)$, G need not have a subgroup of order m.((S_4, o) does not have a subgroup of order 6 but $6 \mid O(S_4)$)

Example:-

Consider the group $G = (Z_4, +)$ and the subgroup $H = \{0,2\}$ of G. Now according to definition 3.1, for each $a \in G$, we will find $b \in G$ s.t a is right congruent to b modulo H.

Now we will find the right cosets of H in G.

$H0 = \{h + 0 \mid h \in H \} = \{0 + 0, 2 + 0\} = \{0,2\} = H$

$H1 = \{h + 1 \mid h \in H \} = \{0 + 1, 2 + 1\} = \{1,3\}$

$H2 = \{h + 2 \mid h \in H \} = \{0 + 2, 2 + 2\} = \{2,0\} = H$

$H3 = \{h + 3 \mid h \in H \} = \{0 + 3, 2 + 3\} = \{3,1\}$

Now for 0 we get $\{0,2\}$, for 1 we get $\{1,3\}$

For 2 we get $\{0,2\}$, for 3 we get $\{1,3\}$

So for our H we get two distinct subsets of G where union of those sets is G.

Also notice that $O(Ha) = 2$ for each $a \in G$ and $O(H) = 2$. Therefore $O(Ha) = O(H)$ for each $a \in G$. In general we define a bijection $f: Ha \to H$ s.t $f(ha) = h$ or $f: aH \to H$ s.t $f(ah) = h$. Since it's a bijection $O(Ha) = O(H) = O(aH)$

According to definition 3.1, Ha is called a right coset of H in G.

So in our example $\{0,2\}$ and $\{1,3\}$ are right cosets of H in G.

But $\{0,2\}$ is our subgroup H. Hence we get H as one right coset of H in G. Also for each $a \in G$, we got 2 elements in its right coset hence it is non-empty.

Also any two right cosets of H are either disjoint or are identical

$$H0 = H2 = \{0,2\} \quad \text{and} \quad H1 = H3 = \{1,3\}$$

There are 2 distinct cosets of H in G, hence $[G: H] = i_G(H) = 2$

If we take the union of all the distinct right cosets of H, then its equal to G.

Hence $H0 \cup H1 = G \Rightarrow O(H0) + O(H1) = O(G)$.

Since $O(H0) = O(H1) = O(H) = 2$ we have $2. O(H) = O(G)$.

So finally we have $\frac{O(G)}{O(H)} = 2 = [G: H]$. Thus order of H is a divisor of the order of G.

Problems

1) Consider the subgroup $H = \{1, \omega_5^2, \omega_5^4\}$ in U_6. Find all the right cosets of H in G.

2) Find all the right cosets for the subgroups $H_1 = \{2m | m \in \mathbb{Z}\}$ and $H_2 = \{3m | m \in \mathbb{Z}\}$ in $(\mathbb{Z}, +)$.

   This shows that even if $O(H)$ is infinite or $O(G)$ is infinite $[G: H]$ could be finite.

3) Explain why $(Z_{11}^*, \times)$ cannot have any proper subgroups?

4.Some Theorems concerning subgroups

We will state some of important theorems for existence of subgroups without proofs.

First we will restate the Lagrange's Theorem to get things organized.

Theorem 4.1:- **Lagrange's Theorem**

If G is a finite group and H is a subgroup of G, then the order of H is a divisor of the order of G. i.e. $O(H) \mid O(G)$.

So what about the converse of the Lagrange's Theorem? Is the converse also true ?

If G is not abelian then, in general the answer is no. But if G is abelian, the answer is true.

Theorem 4.2:- Let G be a finite abelian group of order n. Then G has at least one subgroup of order m for every (positive) divisor m of n.

Theorem 4.3:- **Cauchy's theorem**

Let G be a finite group of order n, and let p be a prime that divides n. Then G has at least one subgroup of order p.

Theorem 4.4:- **Sylow's first theorem**

Let G be a finite group of order n, and let $n = p^k m$ where p is a prime and $p \nmid m$. Then G has at least one subgroup of order p^i for each $0 < i < k$.