Module 1

What is a Set?

A set is an unordered collection of objects, called elements or members of the set.
We write $a \in A$ to denote that a is an element of the set A. The notation $a \notin A$ denotes that a is not an element of the set A.

Example

The set O of odd positive integers less than 10 can be expressed by $O = \{1, 3, 5, 7, 9\}$.

Some existing notations of sets

$\mathbb{N} = \{1, 2, 3, \cdots\}$, the set of natural numbers

$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\} =$ the set of integers

$\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$, the set of positive integers

$\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}$= the set of rational numbers

$\mathbb{R} =$ the set of real numbers

$\mathbb{R}^+ =$ the set of positive real numbers

$\mathbb{C} =$ the set of complex numbers.

Some definitions

- A set $\mathcal{A}$ is a subset of another set $\mathcal{B}$ if every element of $\mathcal{A}$ is also an element of $\mathcal{B}$. We use the notation $\mathcal{A} \subseteq \mathcal{B}$ to indicate that $\mathcal{A}$ is a subset of the set $\mathcal{B}$.
- Two sets A and B are equal $\iff$ $A \subseteq B$ and $B \subseteq A$.
- Let S be a set. If there are exactly n distinct elements in S where n is a nonnegative integer, we say that S is a finite set and that n is the cardinality of S. The cardinality of S is denoted by $|S|$.

Cartesian Product

Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. Hence,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

For example, if $A = \{1, 2\}$ and $B = \{a, b\}$, then

$$A \times B = \{(1, a), (1, b), (2, a), (2, b)\}$$

Note that $A \times B \neq B \times A$.

Operations

Let A and B be sets.

Union

The union of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both.

Intersection

The intersection of the sets A and B, denoted by $A \cap B$, is the set that contains those elements that are in both A and B.

- Two sets are called disjoint if their intersection is the empty set.
- $|A \cup B| = |A| + |B| - |A \cap B|$

Operations

Difference of sets

The difference of A and B, denoted by $A - B$, is the set containing those elements that are in A but not in B. The difference of A and B is also called the complement of B with respect to A.

Complement

Let U be the universal set. The complement of the set A, denoted by $\bar{A}$ or A^c, is the complement of A with respect to U. Therefore, the complement of the set A is $U - A$.

Multiset

It is a modification of the concept of a set that, unlike a set, allows for multiple instances for each of its elements. In the multiset $\{a, a, b\}$, the element a has multiplicity 2, and b has multiplicity 1.

Set identities

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

What is function?

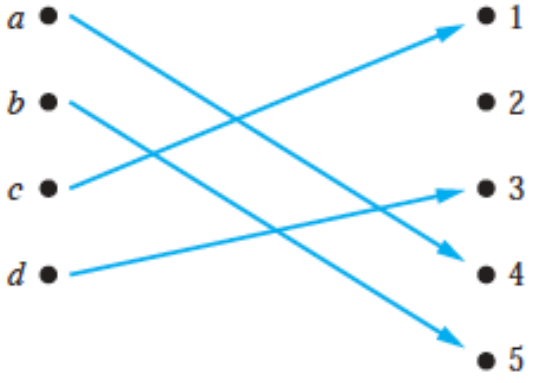
Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f : A \to B$.

Domain and Co-domain

If f is a function from A to B, we say that A is the domain of f and B is the codomain of f. If $f(a) = b$, we say that b is the image of a and a is a preimage of b. The range, or image, of f is the set of all images of elements of A. Also, if f is a function from A to B, we say that f maps A to B.

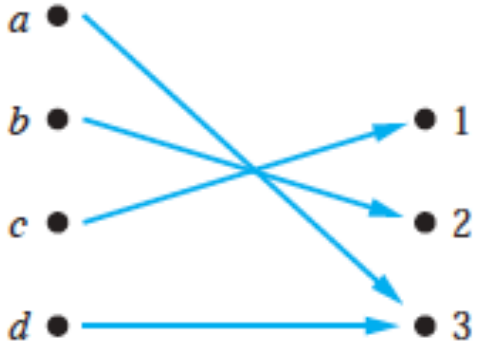
One-one function

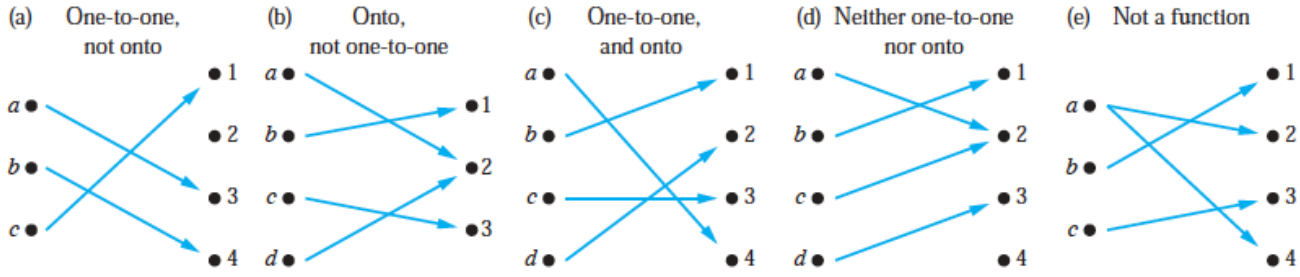
A function f is said to be one-to-one, or an injunction, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. A function is said to be injective if it is one-to-one.



Onto function

A function f from A to B is called onto, or a surjection, if and only if for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A function f is called surjective if it is onto.





• The function f is a one-to-one correspondence, or a bijection, if it is both one-to-one and onto.We also say that such a function is bijective.

Composition of functions

Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The composition of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(a) = f(g(a))$ for all $a \in A$

Inverse of a function

The inverse of a function f is another function g if $f \circ g = g \circ f = \mathit{identity}$, In this case we write $g = f^{-1}$.

Computer Representation of Sets.

If we store the elements of a set in an unordered fashion, the operations such as union, intersection, or difference of two sets would be time-consuming, as it requires a large amount of searching.

We can do storing of elements using an arbitrary ordering of the elements of the universal set.

Let $a_1, a_2, \ldots a_n$ be the arbitrary ordering of the elements of U. Define:

$$f: \mathbb{N} \longrightarrow U \text{ by}$$

$$f(i) = a_i.$$

Now, to represent a subset A of U with the bit string of length n, we follow:

→ i^{th} bit in this string is 1 if a_i belongs of A and 0 if a_i does not belong to A.

For example:

Let $U = \{1, 2, 3, \ldots 10\}$, and the arbitrary order is in increasing order ie

$f(i) = a_i = i$: $f(1) = 1$,
$f(2) = 2$
etc

Q: What bit string represent the subset of all integers in U, the subset of all even integers in U and the subset of integers not exceeding 5 in U.

Sol:

The bit string that represent the set of odd integers in U, ie $\{1,3,5,7,9\}$, has one bit in first, third, fifth, seventh, and ninth positions, and zero elsewhere.

It is: 1010101010.

Similarly, the bit string representation of set of ~~odd~~ even integers in U is:

0101010101.

And the bit string representation of set of integers not exceeding 5 in U, is:

1111100000

Using this string representation, it is easy of find complement, union, intersection, difference of set or sets.

For example

$U = \{1,2,\ldots,10\}$: 1111111111

$A = \{1,3,5,7,9\}$: 1010101010

$B = \{2,4,6,8,10\}$: 0101010101

$C = \{1,2,3,4,5\}$: 1111100000

Then $A^c = 0101010101 = \{2,4,6,8,10\}$

↳ replace 1 with 0 and 0 with 1.

$A \cup B$: $\{1,3,5,7,9\}$ $\cup$ (cup) $\{2,4,6,8,10\}$

$1010101010 \vee 0101010101$

(wedge/join)

$= 1111111111$

$\{1, 3, \ldots 10\}$.

$1 \vee 0 = 1$
$1 \vee 1 = 1$
$0 \vee 0 = 0$
$0 \wedge 0 = 0$
$0 \wedge 1 = 0$
$1 \wedge 1 = 1$

(iii)

$A \cap B$: $A = \{1,3,5,7,9\}$ $\cap$ (cap.) $C = \{1,2,3,4,5\}$

$1010101010 \wedge 1111100000$

(meet)

$= 1010100000$

$\{1, 3, 5\}$.

Graphs of functions

A function f from A to B can be represented as a subset of $A \times B$.

if $f: A \longrightarrow B$, then

$f = \{ (a, b) : a \in A : b = f(a) \}$.

Eg: Let $A = \{1,2,3,4,5\}$

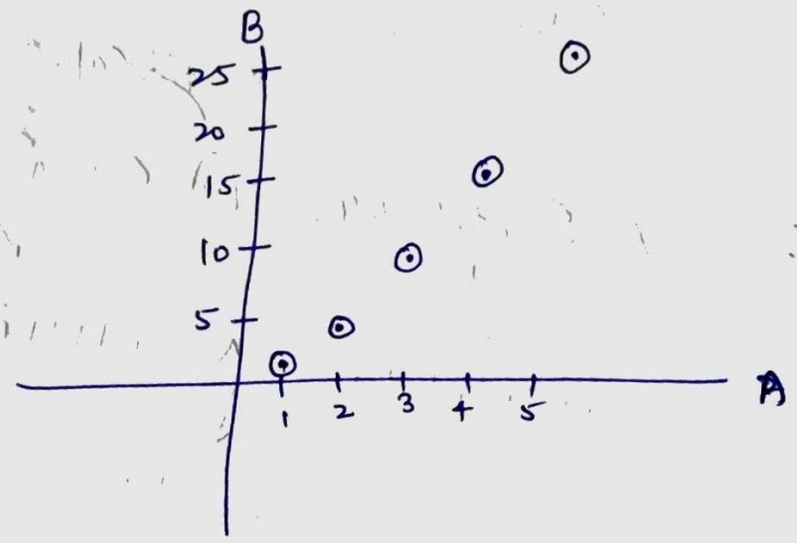
$B = \{1,2,3,\ldots,50\}$.

define $f: A \to B$ by $f(x) = x^2$

$\therefore f = \{(1,1), (2,4), (3,9), (4,16), (5,25)\}$

→ ordered pairs have two diff namely A and B.

Graph of f:



Ceiling and Floor functions:

Floor function assigns to the real no x the largest integer that is less than or equal to x.

It is denoted by $\lfloor x \rfloor$.

Ceiling function assigns to the real no 'x' the smallest integer that is greater than or equal to x.

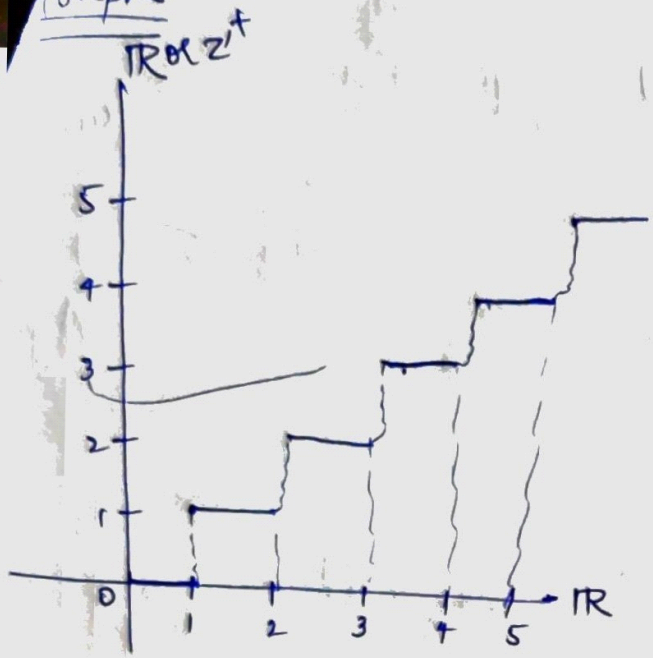
It is denoted by $\lceil x \rceil$

ie Let x be a real no. and n integer. Then

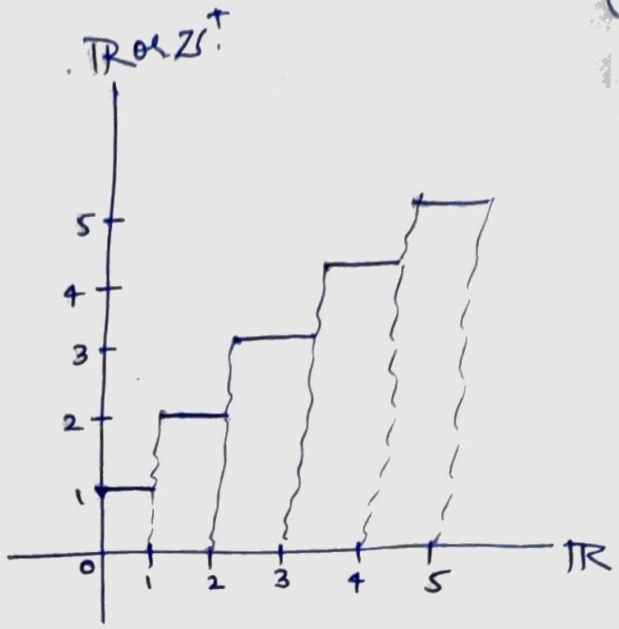
$\lceil x \rceil = n$ iff $n-1 < x \leq n$

$\lfloor x \rfloor = n$ iff $n \leq x < n+1$

Graphs:

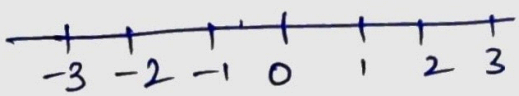


(Floor function)



(Ceiling function)

Properties:



(i) $\lceil -x \rceil = -\lfloor x \rfloor$

(ii) $\lfloor -x \rfloor = -\lceil x \rceil$

(iii) $\lfloor x+n \rfloor = \lfloor x \rfloor + n$

(iv) $\lceil x+n \rceil = \lceil x \rceil + n$

Ex:

$\lceil -3.1 \rceil = -\lfloor 3.1 \rfloor = -(3) = -3$ (Smallest)

$\lfloor -3.1 \rfloor = -\lceil 3.1 \rceil = -(4) = -4.$ (greatest)

X ——————— X.

Module - 3.

Algebraic Structures.

→ Semi groups and Monoids
→ Groups
→ Subgroups
→ Lagrange's Theorem
→ Homomorphism, properties
→ Group Codes.

Def: [Binary operation]

A binary operation $*$ in a set A is a function* from $A \times A$ to A.

Eg1: Addition is a binary operation on $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ but negation is not a binary operation.

Eg2: Union, intersection, difference are binary operations in $P(A)$; power set of A.

Recall: A function* is a rule which associate the each element of a set (called domain) to the unique element of another set (called Co-domain).

General properties of a binary operation.

Def: Let A be a set. A binary operation $*$ on A: ie $* : A \times A \longrightarrow A$ is said to be Commutative if for $\forall\ a, b \in A$,

$$a * b = b * a.$$

Eg: Addition is a Commutative operation on $\mathbb{N}, \mathbb{Z}, \mathbb{R}$.

(2) Associativity:

If $\forall\ a, b, c \in A$

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

(3) Neutral Element (Identity)

If $\exists\ a \in A$ s.t

$$b * a = a * b = b. \quad \forall\ b \in A$$

For Convenience, write this 'a' as 'e'.

(4) Inverse:

$\forall\ a \in A$, if $\exists\ b \in A$ s.t

$a * b = b * a = e$; e is neutral element.

x ——— x

Closure: $\forall\ a, b \in A$;

$$a * b \in A.$$

All binary functions are closed under binary operation as $* : A \times A \longrightarrow A$.

Groupoid: A non-empty set 'A', together with a binary operation $*$; ie $(A, *)$ - a pair is called Groupoid.

Eg: Let E be a set of even numbers. Then $(E, +)$ is a Groupoid.

Semi-group: Let 'A' be a non-empty set. Then the algebraic structure $(A, *)$; where $*$ is a binary operation on A, is called Semi-group if the operation $*$ is associative.

= In other words, 'A' a groupoid is a semi-group if

$\forall\ a, b, c \in A$:

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

Eg: $\mathbb{N}$, the set of natural number, with addition and multiplication is a semi-group.

Monoid: A semi-group $(M, *)$ is a monoid if it has the neutral (identity) element.

ie A set M with binary operation $*$, s.t $*$ is associative and there is $e \in M$; st $a * e = a = e * a\ \forall\ a \in M$.

Eg: $\mathbb{Z}$; the set of integers, is a monoid under addition. as $\exists\ 0 \in \mathbb{Z}$ s.t $a+0 = a = 0+a$ $\forall\ a \in \mathbb{Z}$.

Note: The set of natural no's is not a monoid under addition., but under multiplication.

Group

Def: A group is an algebraic structure $(G, *)$; in which the binary operation $*$ on G satisfies:

G-1: $\forall\ a, b, c \in G$

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

G-2: $\exists\ e \in G$ s.t

$a*e = a = e*a$ (identity existence)

G-3: $\forall\ a \in G$; $\exists\ b \in G$.

s.t $a*b = e = b*a$ (inverse existence).

Note: To check, $*$ is a binary operation: you need to check, closure property.

ie if $\forall\ a, b \in G$

$a*b \in G$, then $*$ is a binary operation.

Whole proving group: this also needs to be checked.

Examples:

1) $(\mathbb{Z}, +)$ is a group.
2) $(\mathbb{R}, +)$ is a group.
3) $(\mathbb{R} - \{0\}, \times)$ is a group.
4) $(\mathbb{R}, \times)$ is not a group.
5) $(\mathbb{Z}, \times)$ is not a group.

Commutative Group:

Let $(G, *)$ be a group. Then $(G, *)$ is called a Commutative group OR an Abelian group if $*$ is a commutative operation.

Eg: $(\mathbb{Z}, +)$ is an abelian group.

A group G is said to be finite if no. of elements in G are finite.
Otherwise G is an infinite group.

Eg: $G = \{1, -1\}$ is a finite group under multiplication.

Order of a Finite Group:

The order of a finite group G means the number of elements in the set G, denoted as $O(G)$ or $|G|$.

In $G = \{1, -1\}$; $O(G) = 2$.

Eg: Show that the set $G = \{1, -1, i, -i\}$; where $i^2 = -1$; is an abelian group w.r.t multiplication.

Sol:

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1.

Multiplication table

by the above table, it is clear that $(G, \times)$ is closed under multiplication, ie $\times$ is a binary operation on G.

Associativity: clearly $\forall\ a, b, c \in G$:

$$a \times (b \times c) = (a \times b) \times c.$$

Identity: $\exists\ 1 \in G$ s.t $1 \cdot a = a \cdot 1 = a\ \forall\ a \in G$.

Inverse: inverse of $1 = 1$ as $1 \cdot 1 = 1$

" " $i = -i$ as $i \times (-i) = 1$

" " $-i = i$ as $-i \times (i) = 1$

" " $-1 = -1$ as $(-1) \times (-1) = 1$

Hence inverse of all elements exist in G itself.

Also $a \times b = b \times a\ \forall\ a, b \in G$.

Hence $(G, \times)$ is an abelian group.

$G = \{1, w, w^2, \ldots w^{n-1}\}$; where $w^n = 1$. Then show that G is a group under multiplication. Moreover G is an abelian group.

Let Z' be a set of integers. Let us divide Z' into n equivalence classes as:

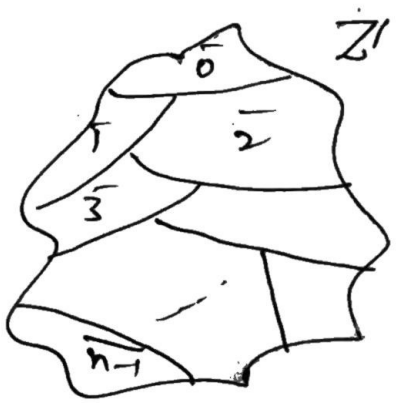
$\bar{0} = \{ m \in Z' \text{ s.t } m = nl_1 : \text{for some integer } l_1 \}$

$\bar{1} = \{ m \in Z' \text{ s.t } m = nl_2 + 1 : \text{for some integer } l_2 \}$

— — — — — — — — —

$\overline{n-1} = \{ m \in Z' : m = nl_n + (n-1) : \text{for some integer } l_n \}$.

Note $\bar{n} = \bar{0}$



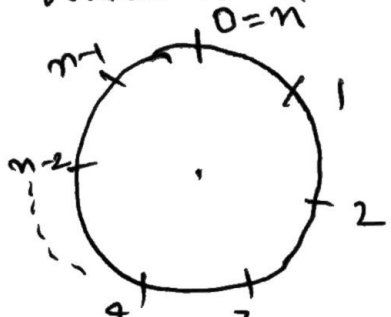
Construct a set:

$\{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\}$;

where $\bar{n} = \bar{0}$

and $\overline{n+1} = \bar{1}$ and so on.

ie denote $\{\bar{0}, \bar{1}, \bar{2}, \ldots \overline{n-1}\}$ by Z_n: which is a set of integers under modulo n



Exer: Show that Z_n is a group under addition modulo 'n'. $(+_n)$

Sol: [Two integers 'a' and 'b' are Congruent modulo 'n' iff $n \mid a-b$. we write $a \equiv b \pmod n$. Since $n \mid a-b$ $\Rightarrow a-b = nk$ for some k $\Rightarrow \boxed{a = nk+b}$]

(i) **Closure:** Let $\bar{x}, \bar{y} \in Z_n$. Then $\exists\ x, y \in Z'$ s.t

$$x = nk_1 + \bar{x}$$
$$y = nk_2 + \bar{y}$$

for some k_1, k_2 integers.

$$\Rightarrow \quad x+y = n(k_1+k_2) + \bar{x}+\bar{y}$$

Since $x+y \in Z' \Rightarrow \bar{x} +_n \bar{y} \in Z_n$

2) **Association:** exercise

3) **Identity:** $\exists\ \bar{0} \in Z_n$ s.t

$$\bar{0} +_n \bar{x} = \bar{x} = \bar{x} +_n \bar{0} \quad \forall\ \bar{x} \in Z_n \text{ (check it)}$$

4) **Inverse:** $\forall\ \bar{x} \in Z_n \ \exists\ -\bar{x} = \bar{n}-\bar{x}$ s.t $\bar{x} +_n (\bar{n}-\bar{x}) = \bar{n} = \bar{0} = (\bar{n}-\bar{x}) +_n \bar{x}$ as $\bar{n} = \bar{0}$

5) **Commutative:** $\forall\ \bar{x}, \bar{y} \in Z_n$

clearly $\bar{x} +_n \bar{y} = \bar{y} +_n \bar{x}$.

Hence $(Z_n, +_n)$ is an abelian group under addition modulo 'n'.

What about Z_n under multiplication module n, i.e $(Z, \times_n)$: $\times_n$ is defined as:

$$\bar{a} \times_n \bar{b} = \overline{ab} \quad ; \text{ where } ab = nk + \overline{ab}.$$

Will this form a group ???

If not why ?; and what Conditions we should impose on 'n' and together with any other Conditions s.t this will become a group under multiplication module 'n'.

Ex: Choose $n=4$: $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.

clearly $\bar{0}$ will not have multiplicative inverse.

what about $Z_4^* = Z_4 - \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}\}$?

Still not !!! as $\nexists$ any $\bar{a} \in Z_4^*$ s.t

$$\bar{2} \times_n \bar{a} = 1. \quad \text{instead } \bar{2} \times \bar{2} = \bar{4} = \bar{0} \notin Z_4^*$$

$\Rightarrow$ Z_4^* is also not a group under $\times_n$.

Def: Zero divisor: An element 'a' is said to be a zero-divisor in G if $\exists\ b \in G$ s.t

$$a * b = 0 \quad ; \text{ where } 0 \text{ is additive identity of } G.$$

Define: $U(n)$ = set of all positive integers less than n and relatively prime to n

For instance: $n=10$. gives

$$U(10) = \{1, 3, 7, 9\}$$

$U(10)$ is a group under multiplication

The Cayley table for $U(10)$ is:

$*_{\text{mod}10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Ex: The set $\mathbb{R}^n = \{(a_1, a_2, \ldots a_n) : a_i \in \mathbb{R}\}$.
is a group under usual addition of vectors.

The set $\{1, 2, \ldots n-1\}$ is a group under multiplication modulo n iff n is a prime.

Def: Order of an element:

Let $g \in G$. Then the order of g, denoted by $O(g)$ or $|g|$, is the smallest positive integer n s.t $g^n = e$ i.e $\underbrace{g * g * \cdots g}_{n \text{ times}} = e$

If such 'n' does not exist, 'g' has infinite order

Eg: Write order of each element of Z_{10} and $U(10)$, under addition and multiplication resp..

Sol:

$$Z_{10} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}.$$

$O(\bar{0}) = 1$ $\quad$ $O(\bar{5}) = 2$

$O(\bar{1}) = 10$ $\quad$ $O(\bar{6}) = 5$

$O(\bar{2}) = 5$ $\quad$ $O(\bar{7}) = 10$

$O(\bar{3}) = 10$ $\quad$ $O(\bar{8}) = 5$

$O(\bar{4}) = 5$ $\quad$ $O(\bar{9}) = 10$

Here we are noting that the order of each element of a group divides the order of the group.

Again $U(10) = \{1, 3, 7, 9\}$

$O(\bar{1}) = 1$

$O(3) = 4$

$O(7) = 4$

$O(9) = 2$

Def: Subgroup:

If a subset H of a group G is itself a group under the operation of G, H is a subgroup of G. we denote it as: $H \leq G$.

eg: Let $G = Z_{10}$

Then $H = \{2, 4, 6, 8, 0\}$ is a subgroup of G.

Two-Step Test.

Let G be a group and H a non-empty subset of G. Then H is a subgroup of G (i) if $ab \in H$ whenever $a, b \in H$ and (ii) $a^{-1} \in H$ whenever $a \in H$.

Note: If H is finite only (i) property: ie closed under operation is sufficient for proving H, a subgroup.

Intersection of Subgroups:

Let H and K are subgroups of G (Group). Then $H \cap K$ is also a subgroup of G.

Pf: Clearly H and K are subgroups $\Rightarrow e \in H$ and $e \in K$.

$\Rightarrow e \in H \cap K \neq \phi$.

Let $x, y \in H \cap K \Rightarrow x \in H \cap K,\ y \in H \cap K$

$\Rightarrow x \in H$ and $x \in K$
$y \in H$ and $y \in K$] .

$\Rightarrow y^{-1} \in H$ and $y^{-1} \in K$

$\Rightarrow xy^{-1} \in H$ and $xy^{-1} \in K$

$\Rightarrow xy^{-1} \in H \cap K$.

Union of Subgroups:

Union of two subgroups of a group needs not be a group.

Eg: Let $G = Z'$. $H = 2Z'$, $K = 3Z'$.

$2 \in H$ and $3 \in K \Rightarrow 2, 3 \in H \cup K$.

but $2 + 3 = 5 \notin H \cup K$ (not closed under addition)

Cyclic group:

A group G is called a cyclic group if there is an element $a \in G$ s.t

$G = \{ a^n : n \in Z' \}$. , denoted as $G = \langle a \rangle$

'a' is called a generator of G.

Eg: $G = Z'$. $G = \langle 1 \rangle$ or $\langle -1 \rangle$

For all $x \in G$: $x = a^n$ if $G = \langle a \rangle$.

Def: $Z_n = \{0, 1, 2, \ldots n-1\}$ is a cyclic group under addition modulo n. '1' and '-1' ($=n-1$) are generators.

Eg: In Z_8, 1, 3, 5, 7 all are generators of Z_8.

For instance;

$$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$$

$3^n = \underbrace{3 \times 3 \times \cdots \times 3}_{n \text{ times}}$

[Note $3^n = n3$ in $(Z_8, +)$]

Also

$3^1 = 3$, $3^2 = 6$,

$3^3 = 9 = 1$, $3^4 = 12 = 4$, $3^5 = 15 = 7$

$3^6 = 2$, $3^7 = 5$, $3^8 = 0$

$$Z_8 = \{3^8, 3^3, 3^6, 3^1, 3^4, 3^7, 3^2, 3^5\} = \langle 3 \rangle$$

But '2' is not a generator a Z_8.

Observation:

If $(k, n) = 1$, then 'a^k' will also be a generator of a cyclic group G, where $G = \langle a \rangle$

In Z_8; $n = 8$; $k = 1, 3, 5, 7$.

$\therefore a^k = a^1, a^3, a^5, a^7$ or $a, 3a, 5a, 7a$.

Since '1' is generator of $Z_8 \Rightarrow a = 1$

$\Rightarrow$ 3, 5, 7 are also generators of Z_8.

Order of elements of Cyclic group:

Let $G = \langle a \rangle$ be a finite cyclic group, i.e. $|G| = n$.

Then, for all $x \in G \Rightarrow x = a^n$ for some n.

$$\therefore O(a^k) = \frac{n}{(k,n)}.$$

$(1^n = 1 * 1 * \cdots * 1.)$

In Z_8: $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Since 1 is generator

$O(1) = 8$

$O(2) = \frac{8}{(2,8)} = \frac{8}{2} = 4$

$O(3) = \frac{8}{(3,8)} = 8$

$O(4) = \frac{8}{(4,8)} = 2$

$O(5) = \frac{8}{(5,8)} = 8$

$O(6) = \frac{8}{(6,8)} = 4$

$O(7) = \frac{8}{(7,8)} = 8.$

$1 = 1^1 = 1$

$2 = 1^2 = 1+1$

$3 = 1^3 = 1+1+1$

$4 = 1^4 = 1+1+1+1$

$5 = 1^5 = 1+1+1+1+1$

$6 = 1^6 = 1+1+1+1+1+1$

$7 = 1^7 = 1+1+1+1+1+1+1$

Eg: The n^{th} roots of Unity forms a Cyclic group i.e.

$G = \{1, \omega, \omega^2, \cdots \omega^{n-1}\}$; $\omega^n = 1$

Generators: ω^k such that $(k,n) = 1$.

Let $n = 10$ i.e. $G = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7, \omega^8, \omega^9\}$ $(\omega = \omega^{10})$

$\omega^{10} = 1.$

$\therefore$ $\omega^1, \omega^3, \omega^7, \omega^9$ are generators of G (check it).

Every Cyclic group is an abelian group.

If a is a generator of a Cyclic group G, then a^{-1} is also a generator of G.

Prove that the set $\{1, -1, i, -i\}$ is a cyclic group under multiplication. find generators also.

Every subgroup of a cyclic group is cyclic.

Permutation group.

A map 'f' from S to S (where S is any set) is called a permutation if f is 1-1 and an onto map.

Let $|S| = 3$; ie $S = \{a, b, c\}$.

Then all possible 1-1 and onto maps are as follows.

$$f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad f_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \quad f_3 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

$$f_4 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \quad f_5 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad f_6 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

Then $P_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ is a group, called permutation group.

A group is a permutation group if its elements are permutations. Therefore any subgroup of permutation group is a permutation group.

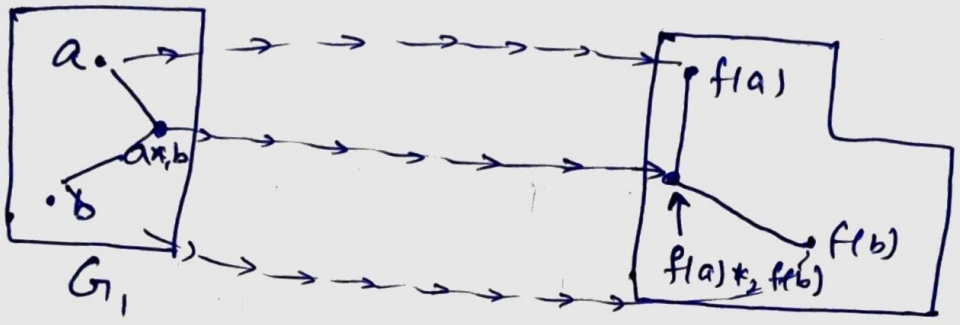
Check P_3 is a group, and find identity, order, inverse of all elements of P_3. Find possible subgroups of P_3 also.

Homomorphism

Let G and G' be two groups under $*_1$ and $*_2$. Then a map $f: (G, *_1) \longrightarrow (G, *_2)$ is called a homomorphism if:

or (Group homomorphism)

(a) $$f(a *_1 b) = f(a) *_2 f(b)$$



Isomorphism: If f is a homomorphism and f is a 1-1 and onto map.

Properties: If f is a homomorphism from G to G', then

(i) $f(e) = e'$ where e is the identity of G and e' is the identity of G'

$e *_1 e = e$ in G.

Pf: $\Rightarrow f(e *_1 e) = f(e)$.

$\Rightarrow f(e) *_2 f(e) = e' *_2 f(e)$ $\quad \left[\begin{array}{l} f(e) \in G' \\ \Rightarrow (f(e))^{-1} \in G' \end{array} \right]$

$\Rightarrow f(e) = e'$ (Multiply both sides with $(f(e))^{-1}$)

(ii) $(f(a))^{-1} = f(a^{-1})$.

Hint:

$$a *_1 a^{-1} = e = a^{-1} * a \quad \text{in } G.$$

$$\Rightarrow f(a) *_2 f(a^{-1}) = e' = f(a^{-1}) *_2 f(a)$$

$$\Rightarrow f(a^{-1}) = (f(a))^{-1}.$$

Any finite cyclic group of order n is isomorphic to Z_n, and any infinite cyclic group is isomorphic to Z.

If a is a generator of the cyclic group G, then define $f: G \longrightarrow Z$ or Z_n, according as G is infinite or finite.

$$a^k \longrightarrow k$$

$\therefore$ The map is an isomorphism and hence the result.

Cor: Any two cyclic groups of same order are isomorphic.

Note: $\phi(x) = x^3$ is a 1-1 and onto map, but not homomorphism as $\phi(x+y) = (x+y)^3 \neq x^3+y^3$, so ϕ is not an isomorphism.

$U(10) \cong Z_4$ and $U(5) \cong Z_4$, since $U(10), U(5)$ are cyclic groups of order 4.

$\Rightarrow U(10) \cong U(5)$.

But $U(10) \not\cong U(12)$: Since $U(12) = \{1, 5, 7, 11\}$

$\because 5^2 \equiv 1 = 7^2 = 11^2$

ie $U(12)$ is not cyclic.

Moreover, if $\phi: U(10) \longrightarrow U(12)$ is an isomorphism, then $\phi(9) = \phi(3)\phi(3) = (\phi(3))^2$; but $x^2 = 1 \; \forall x \in U(12)$

$\Rightarrow (\phi(3))^2 = 1$

$\Rightarrow \phi(9) = 1$

Also $\phi(1) = \phi(1).\phi(1) = 1$ $\quad (\because (\phi(1))^2 = 1)$

$\phi(9) = \phi(1)$ but $9 \neq 1$ in $U(10)$

$\Rightarrow \phi$ is not a 1-1 map. Contradiction.

Cayley's Theorem:

Every group is isomorphic to a group of permutations.

ie $\exists\ f : G \longrightarrow \overline{G}$ (group of permutations)

G: any group

s.t f is isomorphism.

we claim, $f: G \to \overline{G}$ is defined as:

[Choose $a \in G$ (fixed) and then define
$f_a : G \to G$ by $f_a(x) = ax \quad \forall\ x \in G$.
f_a is a permutation on G.]

Now define f as $f(a) = f_a \quad \forall\ a \in G$.

Exer: Check if f is an isomorphism. Hence the result.

Eg: let $G = U(12) = \{1, 5, 7, 11\}$

$$f_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}$$

$$f_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}, \quad f_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix}$$

$\therefore$ $f : U(12) \longrightarrow \{f_1, f_5, f_7, f_{11}\}$

defined as: $1 \to f_1,\ 5 \to f_5,\ 7 \to f_7,\ 11 \to f_{11}$

is an isomorphism.

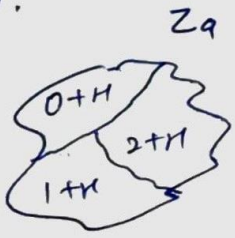
Cosets and Lagrange's Theorem

Let G be a group and H be a subset of G.

Define a set: $aH = \{ah : h \in H\}$, where $a \in G$,

When H is a subgroup of G, aH is called a left coset of H in G.

Similarly Ha is a right coset of H in G.



Eg: Let $G = Z_9$, $H = \{0, 3, 6\}$.

Then list of all left cosets of H in G:

$0+H = H$
$1+H = \{1, 4, 7\}$
$2+H = \{2, 5, 8\}$
$3+H = \{3, 6, 0\} = H$
$4+H = \{4, 7, 1\} = H$
$5+H = \{5, 8, 2\} = 2+H$
$6+H = \{6, 0, 3\} = H$
$7+11 = \{7, 1, 4\} = 1+H$
$8+11 = \{8, 2, 5\} = 2+H$.

In total, there are 3 distinct left cosets of H in G given as: $0+H = H$, $1+H$ and $2+H$.

\# Note that cosets are not subgroups in general.

\# Some properties of cosets:

(i) $aH = H$ iff $a \in H$

(ii) $aH = bH$ or $aH \cap bH = \phi$

(iii) $|aH| = |bH| \ \forall \ a, b \in G$.

(iv) aH is a subgroup of $G \iff a \in H$.

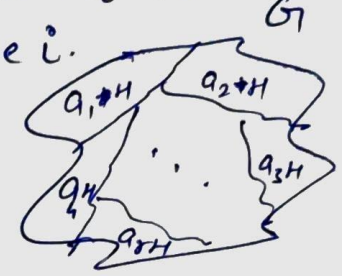
(v) $a \in aH \ \forall \ a \in G$.

Lagrange's Theorem:

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $\frac{|G|}{|H|}$.

Pf: Let $a_1H, a_2H, \dots a_rH$ denote the distinct left cosets of H in G.

Now for all $a \in G$, we have $aH = a_iH$ for some i.



Also, since $a \in aH \Rightarrow \forall\ x \in G$

$\Rightarrow x \in a_1H \cup a_2H \cup \dots \cup a_rH$

$\Rightarrow G \subseteq a_1H \cup a_2H \cup \dots a_rH$

but $a_1H \cup a_2H \cup \dots a_rH \subseteq G$, as $a_iH \subseteq G\ \forall\ a_i$.

$\Rightarrow G = a_1H \cup a_2H \cup \dots a_rH$.

Also $|aH| = |bH|\ \forall\ a, b \in G$.

and $aH \cap bH = \phi$ if $aH \neq bH$.

$\Rightarrow |G| = |a_1H| + |a_2H| + \dots |a_rH|$ $\quad [\because |a_iH| = |H|]$

$= r|H|$

$\Rightarrow r = \frac{|G|}{|H|}$.

Corollary:1) $|a| \mid |G|\ \forall\ a \in G$.

Hint $|H| = |a|$ where $H = \langle a \rangle$.

Cor:2) Every group of prime order is cyclic.

Cor:3: $a^{|G|} = e\ \forall\ a \in G$. Since $|G| = |a| \cdot k \Rightarrow a^{|G|} = a^{k|a|} = (e)^k = e$

Normal Subgroup and Quotient Group.

Def: A subgroup H of a group G is called a normal subgroup of G if $aH = Ha \ \forall a \in G$ (i.e. left coset is the right coset induced by same element) we denote it by $H \trianglelefteq G$.

[don't be confused with the property:
$ah = ha \ \forall h \in H, \ \forall a \in G$
it has more restriction than $aH = Ha$]

Actually in normal condition is:
$ah = h'a$ for some $h, h' \in H$.

A subgroup H of G is normal in G iff $xHx^{-1} \subseteq H$. i.e. $\forall h \in H, x \in G \Rightarrow xhx^{-1} \in H$.

Eg: A_n is a normal subgroup of S_n.

$A_3 = \{1, (123), (132)\}$

$S_n = \{1, (12), (13), (23), (123), (132)\}$

$(12)(123) \neq (123)(12)$

but $= (132)(12)$

Every subgroup of an abelian group is normal.

Def: Let G be a group and H a normal subgroup of G. Then set

$G/H = \{aH : a \in G\}$ is a group under the operation $*$ defined as:

$$(aH)(bH) = abH \quad \forall\ a, b \in G.$$

Let $G = \mathbb{Z}'$ and $H = 4\mathbb{Z}'$.

Then $$\frac{\mathbb{Z}'}{4\mathbb{Z}'} = \{0+4\mathbb{Z}', 1+4\mathbb{Z}', 2+4\mathbb{Z}', 3+4\mathbb{Z}'\}$$

$$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}'_4$$

Moreover $O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)}$ if G is finite.

X ——————— X