Week - 1

Topics:
- Set Theory
- Set operations
- Set of sets
- Binary relation

- **Definition of Set:** A set is a well defined collection of distinct objects of our perception or of our thought, to be conceived as a whole.

Commonly we shall use capital letters $A, B, C, \ldots$ to denote sets and small letters $a, b, c, \ldots$ to denote objects (or elements) of a set.

(i) A set S is a collection of objects (or elements) which is to be regarded as a single entity.

(ii) A sets is comprised of distinct objects (elements) and if a be an objects of, we denote this by $a \in S$ (read as 'a belongs to S')

(iii) A set is well defined, meaning that if S be a set and a be an object, then either a is definitely in S ($a \in S$) or a is definitely not in S, denoted by $a \notin S$ (read as 'a does not belong to S')

Example :

1. Let A be the set of first four natural number. Then

$$A = \{1, 2, 3, 4\}.$$

Then, $2 \in A$, but $5 \notin A$.

2. Let B be the set of all primes less than 15. Then

$$B = \{2, 3, 5, 7, 11, 13\}.$$

Then, say $5 \in B$, but $17 \notin B$.

Representation of a set :

Every set is defined by some property P (say).

Like, in example 1, the property P can be written as —

P : first four natural number.

So, $A = \{ x \mid x \text{ follows } P \}$

$= \{ 1, 2, 3, 4 \}$.

In example 2, P: prime numbers less than 15.

So, $B = \{ x \mid x \text{ follows } P \}$

$= \{ 2, 3, 5, 7, 11, 13 \}$

Similarly, let

$C = \{ x \mid x \text{ is an even number and positive.} \}$

$= \{ 2, 4, 6, \ldots \}$

- **Some useful accepted notations of sets:**

$\mathbb{N}$ = the set of all natural numbers

$\mathbb{Z}$ = the set of all integers

$\mathbb{Z}^+$ = the set of all positive integers

$\mathbb{Q}$ = the set of all rational numbers

$\mathbb{Q}^+$ = the set of all ~~rational~~ positive rational numbers

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

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

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

ϕ = the empty set / Null set
= the set containing no element.

$\mathcal{U}$ = universal set.

- **Subset**: Let S be a set. A set T is said to be a subset of S if $x \in T \Rightarrow x \in S$.

Notation:- $T \subseteq S$

- **Proper Subset :** If $T \subseteq S$ and there exists an element $x \in S$, but $x \notin T$ then T is called a proper subset of S.

- **Super Set :** If $T \subseteq S$ then we call S is a super set of T.

Note : (i) If S is a non-empty set (i.e., S contains at least one element) then $\phi \subset S$, i.e., ϕ is a proper subset of S.

(ii) Every set is a subset of the universal set.

- **Example :** $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{R}$, $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{R} \subset \mathbb{C}$

Note that these are all proper subsets.

For example, $0 \in \mathbb{Z}$ but $0 \notin \mathbb{N}$.

Similar for the others.

- **Equal Set:** Two sets S and T are said to be equal ($S = T$) if $S \subseteq T$ and $T \subseteq S$.

Therefore if $\forall x \in S, x \in T$ and $\forall y \in T, y \in S$

then $S = T$.

- **Set Operations:**

(I) **Union:** Let A and B be two sets. Then denote union of A and B by $A \cup B$ and is defined by

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

Note that $A \subseteq A \cup B$, $B \subseteq A \cup B$

Example: Let $A = \{1, 2, 3\}$
$B = \{2, 3, 4\}$

$$\Rightarrow A \cup B = \{1, 2, 3, 4\}.$$

(II) **Intersection:** Let A and B be two sets. Then denote intersection of A and B by $A \cap B$ and is defined by

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

Example: Let $A = \{1, 2, 3\}$
$B = \{2, 3, 4\}$

$\Rightarrow A \cap B = \{2, 3\}$.

Note: Two sets A, B are called disjoint if A and B have no common element, we write $A \cap B = \phi$.

Properties of Set operations:

(I) $B \subseteq A \Rightarrow A \cup B = A$
$A \cap B = B$

To show $A \cup B = A$:
Take $A \cup B = X$. We show that $X \subseteq A$ and $A \subseteq X$. Then it will imply $X = A$.

See, $A \subseteq A \cup B \Rightarrow A \subseteq X$.

Again, $x \in X \Rightarrow x \in A \cup B$
$\Rightarrow x \in A$ or $x \in B$
$\Rightarrow x \in A$ or $x \in A$ $[\because B \subseteq A]$
$\Rightarrow x \in A$.

So, $X \subseteq A$.

Hence, $A = X$.

Similarly show, $A \cap B = B$ if $B \subseteq A$.

(II) $A \cup \phi = A$, $A \cap \phi = \phi$

(III) $A \cup \mathcal{U} = \mathcal{U}$, $A \cap \mathcal{U} = A$.

(IV) $A \cup A = A$, $A \cap A = A$

(V) $A \cup B = B \cup A$, (commutative)
$A \cap B = B \cap A$

(VI) $A \cup (B \cup C) = (A \cup B) \cup C$ (associativity)
$A \cap (B \cap C) = (A \cap B) \cap C$

(VII) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Lets prove (VII). Take $X = A \cup (B \cap C)$
$Y = (A \cup B) \cap (A \cup C)$

<u>$X \subseteq Y$</u> : $x \in X \Rightarrow x \in A \cup (B \cap C)$

$\Rightarrow x \in A$ or $x \in (B \cap C)$

$\Rightarrow x \in A$ or $(x \in B$ and $x \in C)$

$\Rightarrow (x \in A$ or $x \in B)$ and $(x \in A$ or $x \in C)$

$\Rightarrow x \in A \cup B$ and $x \in A \cup C$

$\Rightarrow x \in (A \cup B) \cap (A \cup C)$

$\Rightarrow x \in Y$

So, $X \subseteq Y$.

$\underline{Y \subseteq X:}$ $y \in Y \Rightarrow y \in (A \cup B) \cap (A \cup C)$

$\Rightarrow y \in (A \cup B)$ and $y \in (A \cup C)$

$\Rightarrow (y \in A$ or $y \in B)$ and $(y \in A$ or $y \in C)$

$\Rightarrow y \in A$ or $(y \in B$ and $y \in C)$

$\Rightarrow y \in A \cup (B \cap C)$

$\Rightarrow y \in X.$

Hence $Y \subseteq X.$

Therefore $Y = X.$

- Complementation : The complement of a subset A is a subset of $\mathcal{U}$ denoted by A' (or A^c) and is defined by $A' = \{x \in \mathcal{U} : x \notin A\}$

Example : Let $\mathcal{U} = \{1, 2, 3, 4, 5\}$ and $A = \{2, 4\}$. Then $A' = \{1, 3, 5\}$.

Properties : (I) $(A^c)^c = A$

(II) $A \cup A^c = \mathcal{U}$

(III) $A \cap A^c = \phi$

(IV) De Morgan's laws : (i) $(A \cup B)^c = A^c \cap B^c$ and (ii) $(A \cap B)^c = A^c \cup B^c$

Proof of De Morgan's law :-

(i) Let $X = (A \cup B)^c$ and $Y = A^c \cap B^c$

<u>$X \subseteq Y$</u> :

$x \in X \Rightarrow x \notin (A \cup B)$

$\Rightarrow x \notin A$ and $x \notin B$

$\Rightarrow x \in A^c$ and $x \in B^c$

$\Rightarrow x \in (A^c \cap B^c) = Y$

$\Rightarrow x \in Y$

$\Rightarrow X \subseteq Y$

<u>$Y \subseteq X$</u> :

$y \in Y \Rightarrow y \in A^c \cap B^c$

$\Rightarrow y \in A^c$ and $y \in B^c$

$\Rightarrow y \notin A$ and $y \notin B$

$\Rightarrow y \notin (A \cup B)$

$\Rightarrow y \in (A \cup B)^c = X$

$\Rightarrow Y \subseteq X$.

Therefore $Y = X$.

(ii) To show $(A \cap B)^c = A^c \cup B^c$

$(A \cup B)^c \subseteq A^c \cup B^c$:

Let $a \in (A \cup B)^c \Rightarrow a \notin (A \cup B)$

$\Rightarrow a \notin A$ and $a \notin B$

$\Rightarrow a \in A^c$ and $a \in B^c$

$\Rightarrow a \in (A^c \cap B^c)$

$\Rightarrow (A \cup B)^c \subseteq A^c \cap B^c$.

$A^c \cup B^c \subseteq (A \cup B)^c$:

Let $b \in A^c \cup B^c \Rightarrow b \in A^c$ or $b \in B^c$

$\Rightarrow b \notin A$ and $b \notin B$

$\cancel{\Rightarrow b \notin (A \cap B)}$

$\Rightarrow b \notin (A \cup B)$

$\Rightarrow b \in (A \cup B)^c$

$\Rightarrow A^c \cup B^c \subseteq (A \cup B)^c$

Therefore, $(A \cup B)^c = A^c \cap B^c$.

- **Set Difference:** For any two sets A, B, we have

$$A - B = \{x \in A \mid x \notin B\}$$

= set of all elements which are in A but not in B.

Note that, $A - B = A \cap B^c$.

- **Theorem:** $A - (B \cap C) = (A - B) \cup (A - C)$

Proof: $a \in A - (B \cap C)$

$\Rightarrow a \in A$ and $a \notin (B \cap C)$

$\Rightarrow a \in A$ and $(a \notin B$ or $a \notin C)$

$\Rightarrow (a \in A$ and $a \notin B)$ or $(a \in A$ and $a \notin C)$

$\Rightarrow a \in (A - B)$ or $a \in (A - C)$

$\Rightarrow a \in (A - B) \cup (A - C)$

Therefore, $A - (B \cap C) \subseteq (A - B) \cup (A - C)$

In similar way, show that $(A - B) \cup (A - C) \subseteq A - (B \cap C)$.

Combining we get the result.

- **Theorem** : $A-(B\cup C) = (A-B)\cap(A-C)$

Proof : $a \in A-(B\cup C)$

$\Rightarrow a \in A$ and $a \notin (B\cup C)$

$\Rightarrow a \in A$ and $(a \notin B$ and $a \notin C)$

$\Rightarrow (a \in A$ and $a \notin B)$ and $(a \in A$ and $a \notin C)$

$\Rightarrow a \in (A-B)$ and $a \in A-C$

$\Rightarrow a \in (A-B)\cap(A-C)$

Therefore $A-(B\cup C) \subseteq (A-B)\cap(A-C)$

Similarly show that

$(A-B)\cap(A-C) \subseteq A-(B\cup C)$.

Combining we get,

$A-(B\cup C) = (A-B)\cap(A-C)$.

- **Symmetric Difference:**

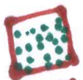
$A \Delta B = (A-B)\cup(B-A)$

= the set of all elements which belong either to A or to B but not in both.

Note that, $A \Delta B = (A \cup B) - (A \cap B)$.

Venn diagram :

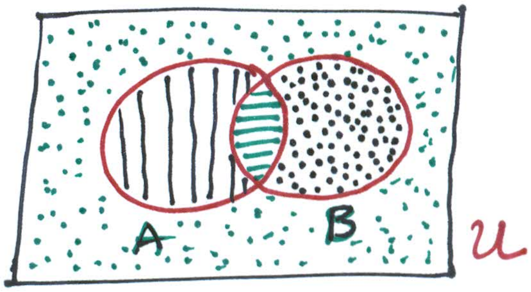
Consider two sets A, B.

 $\rightarrow (A \cup B)^c = A^c \cap B^c$

 $\rightarrow A \cap B$

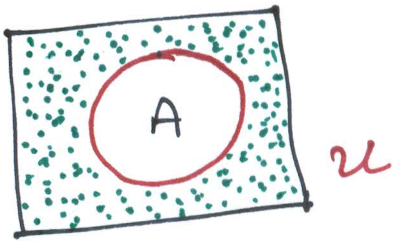
 $\rightarrow A \cap B^c$

 $\rightarrow B \cap A^c$

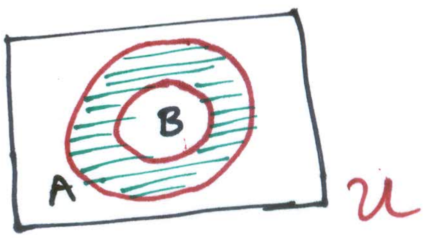


$A \cup B = (A \cap B) \cup (A \cap B^c) \cup (B \cap A^c)$

 $\rightarrow A^c$



 $\rightarrow (A - B)$
$= A \cap B^c$



Set of Sets :

Let S be a set. Then set of sets is the collection of all subsets of S. It is also called the power set of S.

Example: $S = \{1, 2, 3\}$.

Then all the set of sets for S is ϕ, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, $\{1, 2, 3\}$.

This collection is called power set of S and is denoted by $Pow(S)$.

Cardinality of a set :

Let S be a finite set. Then cardinality of S is the number of elements in S. It is denoted by $|S|$.

Example: $S = \{1, 2, 3\}$

$$\Rightarrow |S| = 3$$

Note: If S contains infinitely many elements then we call S is an infinite set.

- **Remark:** Let $S = \{a_1, \ldots, a_n\}$. Then
$|Pow(S)| = 2^n$.

We see, that
$$Pow(S) = \{\{x_1 a_1\} \cup \{x_2 a_2\} \cup \cdots \cup \{x_n a_n\} \mid x_i = 0 \text{ or } 1\}.$$

where we denote $\{x_i a_i\} = \begin{cases} \{a_i\}, & \text{if } x_i = 1 \\ \phi, & \text{if } x_i = 0 \end{cases}$

Now, number of distinct binary string of length n is 2^n.

Therefore $|Pow(S)| = 2^n$.

- **Partition of a Set:**

Let A be a non-empty set. Then a collection of sets $\mathcal{F} = \{A_i \mid i \in I\}$, where I is an index set, forms a partition of A if

(i) $\bigcup_{i \in I} A_i = A$

(ii) $A_i \cap A_j = \phi$ if $i \neq j$

Cartesian Product :

Let A and B be two non-empty sets. Then cartesian product of A and B is denoted by $A \times B$ and is defined by

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

Example : $A = \{1, 2, 3\}$
$B = \{2, 5\}$

Then $A \times B = \{ (1, 2), (1, 5), (2, 2), (2, 5), (3, 2), (3, 5) \}$.

Note : If $|A| = n$ and $|B| = m$ then,
$|A \times B| = nm$.

Relation :

Let S and T be two non-empty sets. A relation ρ is a subset of $S \times T$.

Therefore, a relation ρ between S and T is the rule that associate some or all the elements of S with elements of T.

Example: $S = \{2, 3, 4, 5\}$
$T = \{11, 12, 13, 14\}$

Define a relation ρ between S and T by :
$(s, t) \in \rho$ or we write $s \rho t$
iff s is a divisor of t.

$\Rightarrow \rho = \{(2, 12), (2, 14), (3, 12), (4, 12)\}$
$\subseteq S \times T$.

- Binary relation :

If ρ is a relation between S and S i.e, $\rho \subseteq S \times S$ then ρ is a binary relation on S.

Example: let $S = \{1, 2, 3\}$.

Define a binary relation '$<$' on S by $(a, b) \in <$ or $a < b$ iff a is less than b.

Therefore $< = \{(1,2), (1,3), (2,3)\}$.

Example: Consider the set $\mathbb{R}$.

Define a binary relation '$=$' on $\mathbb{R}$ by $(a, b) \in =$ or $a = b$ iff a is equal to b.

Therefore, see, $(1,1) \in =$,
$(\sqrt{2}, \sqrt{2}) \in =$

Also, $= \subseteq \mathbb{R} \times \mathbb{R}$

Example: Consider the set $\mathbb{Z}$.

Define a binary relation ℓ on $\mathbb{Z}$ by,

$$\ell = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b \text{ is even}\}$$

For example, $(1,1)$, $(1,3)$, $(0,4) \in \ell$.

Note that ℓ is an infinite set.

Types of binary relations : let $S \neq \phi$ and $\rho \subseteq S \times S$.

1) Reflexive relation :

ρ is reflexive relation on S if $(a,a) \in \rho \quad \forall a \in S$. (i.e. $a \rho a \ \forall a \in S$)

Example : Let $S = \mathbb{Z}$ and
$\rho = \{(a,b) : a+b \text{ is even}\}$.
Then $(a,a) \in \rho \quad \forall a \in \mathbb{Z}$ as
$a + a = 2a$ is even.
So, ρ is reflexive.

2) Symmetric relation :

ρ is symmetric relation on S if $(a,b) \in \rho \Rightarrow (b,a) \in \rho$.
(i.e. $a \rho b \Rightarrow b \rho a$).

Example : Let $S = \mathbb{R}$ and
$\rho = \{(a,b) : a = b\}$.

Then $(a,b) \in \rho \Rightarrow a = b \Rightarrow b = a$
$\Rightarrow b \rho a$
$\Rightarrow (b,a) \in \rho$

So, ρ is symmetric.

Example: Let $S = \mathbb{R}$ and

$\rho = \{(a,b) : a < b\}$

Then $(1,3) \in \rho$ but $(3,1) \notin \rho$

$\Rightarrow \rho$ is not symmetric.

3) **Transitive relation :**

ρ is transitive relation on S

if $(a,b) \in \rho$ and $(b,c) \in \rho \Rightarrow$
$(a,c) \in \rho$. (i.e., $a \rho b$ and $b \rho c$
$\Rightarrow a \rho c$)

Example: Let $S = \mathbb{R}$ and

$\rho = \{(a,b) : a < b\}$.

Then $(a,b) \in \rho$, $(b,c) \in \rho$

$\Rightarrow a < b$ and $b < c$

$\Rightarrow a < b < c \Rightarrow a < c$

$\Rightarrow (a,c) \in \rho$

So, ρ is transitive

• Equivalence Relation :

A relation ρ is called an equivalence relation if ρ is:

(i) refelxive

(ii) symmetric

(ii) transitive.

Example : Let $S = \mathbb{Z}$. Define a relation $\rho = \{ (a,b) \in S \times S \mid a-b \text{ is divisible by } 5 \}$.

(i) reflexive: $(a,a) \in \rho \; \forall a \in \mathbb{Z}$

as $a-a=0$ is divisible by 5.

(ii) Symmetric : Let $(a,b) \in \rho$. Then

$(a-b)$ is divisible by 5

$\Rightarrow \; a-b = 5k$ for some $k \in \mathbb{Z}$

$\Rightarrow \; b-a = 5(-k)$

$\Rightarrow \; b-a$ is divisible by 5

$\Rightarrow \; (b,a) \in \rho$.

(iii) Transitive : let $(a,b) \in \rho$, $(b,c) \in \rho$

$\Rightarrow$ $(a-b)$ is divisible by 5 and $(b-c)$ is divisible by 5

$\Rightarrow$ $a-b = 5k_1$ and $b-c = 5k_2$ for some integers $k_1, k_2 \in \mathbb{Z}$

$\Rightarrow$ $(a-b) + (b-c) = 5(k_1+k_2)$

$\Rightarrow$ $a-c = 5(k_1+k_2)$

$\Rightarrow$ $(a-c)$ is divisible by 5.

So, $(a,c) \in \rho$.

Hence ρ is an equivalence relation on $\mathbb{Z}$.

Example : Let $S = \mathbb{Z}$.
Let $\rho = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a+b$ is even $\}$

Then (i) $(a,a) \in \rho$ as $a+a = 2a$ is even

(ii) $(a,b) \in \rho \Rightarrow (b,a) \in \rho$

(iii) $(a,b) \in \rho$, $(b,c) \in \rho \Rightarrow$ $(a,c) \in \rho$

WEEK-2 LECTURE NOTE

Topics : Equivalence relation
Mapping
Permutation
Binary Composition
Groupoid

Equivalence class :

Let ρ be an equivalence relation on a set $S \neq \phi$. Let $a \in S$. Let $cl(a)$ be a subset of S defined by

$$[a] = cl(a) = \{ b \in S : (a,b) \in \rho \}.$$

Therefore $cl(a)$ is the set of those elements x of S such that $(a,x) \in \rho$.

Note that $cl(a)$ is a non-empty subset of S since $a \in cl(a)$.
$cl(a)$ is said to be the ρ-equivalence class of a.

Theorem: Let ρ be an equivalence relation on a set S and $a, b \in S$. Then $cl(a) = cl(b)$ or $cl(a) \cap cl(b) = \phi$.

Proof: **Case 1**: $(a, b) \in \rho$ then $cl(a) = cl(b)$.

$cl(a) \subseteq cl(b)$: Let $x \in cl(a)$

$\Rightarrow (a, x) \in \rho$ and by hypothesis $(a, b) \in \rho$

$\Rightarrow (a, x) \in \rho$ and $(b, a) \in \rho$ (Symmetry)

$\Rightarrow (b, x) \in \rho$ (transitivity)

$\Rightarrow x \in cl(\cancel{a})\ cl(b)$.

Therefore, $cl(a) \subseteq cl(b)$.

Similarly, show that $cl(b) \subseteq cl(a)$

Hence $cl(a) = cl(b)$.

Case 2: $(a, b) \notin \rho$ then $cl(a) \cap cl(b) = \phi$.

Suppose, $cl(a) \cap cl(b) \neq \phi$.

Let $x \in cl(a) \cap cl(b)$

$\Rightarrow x \in cl(a)$ and $x \in cl(b)$

$\Rightarrow (a, x) \in \rho$ and $(b, x) \in \rho$

$\Rightarrow (a, x) \in \rho$ and $(x, b) \in \rho$

(symmetry)

$\Rightarrow (a, b) \in \rho$ (transitivity)

So, we arrive at a contradiction that $(a, b) \in \rho$.

Hence, $cl(a) \cap cl(b) = \phi$.

$\blacksquare$

- Theorem: An equivalence relation ρ on a set S determines a partition of S. Conversely, each partition of S yields an equivalence relation on S.

We will see this by an example. Then the proof follows.

Example: Let $\mathbb{Z}$ = the set of integers.

Let $n \in \mathbb{N}$. Define,

$\rho = \{ (a,b) \in \mathbb{Z} \times \mathbb{Z} : (a-b)$ is divisible by n, i.e., $n \mid (a-b) \}$

Equivalently, we write

$a \bmod n = b \bmod n$.

, i.e., $a \equiv b \pmod{n}$, '$\equiv$' is called congruent.

$[0] = cl(0) = \{$ the set of integers divisible by $n \}$

$= \{ 0, \pm n, \pm 2n, \cdots \}$

$[1] = cl(1) = \{$ the set of integers which have remainder 1 when divisible by n, i.e., all $x \in \mathbb{Z}$ s.t. $n \mid (x-1) \}$

$= \{ 1, 1 \pm n, 1 \pm 2n, \cdots \}$

$\vdots$

$[n-1] = cl(n-1) = \{$ the set of integers which have remainder $(n-1)$ when divisible by $n \}$

$= \{ (n-1), (n-1) \pm n, (n-1) \pm 2n, \dots \}$

Note that, $cl(0) \cup cl(1) \cup \dots \cup cl(n-1) = \mathbb{Z}$.

We denote, $\mathbb{Z}_n$ by

$$\mathbb{Z}_n = \{ cl(0), cl(1), \dots, cl(n-1) \}$$

$$= \{ [0], [1], \dots, [n-1] \}$$

= collection of all disjoint equivalence classes of the relation ρ.

We also, call this relation as '$\equiv$ mod n' (congruent modulo n).

For $n = 5$ we have,

$$\mathbb{Z}_5 = \{ [0], [1], \dots, [4] \}$$

= collection of all disjoint equivalence classes of the relation "congruent modulo n".

Proof: Let ρ be an equivalence relation on S. Then for any $a, b \in S$ we have $cl(a) \cap cl(b) = \phi$ or $cl(a) = cl(b)$.

Also, $cl(a) = cl(b)$ if and only if $(a, b) \in \rho$.

Therefore, $\bigcup_{\text{disjoint}} cl(a) = S$

$\Rightarrow$ ρ - equivalence classes (distinct) forms a partition of S.

Conversely, let P be a partition on S.

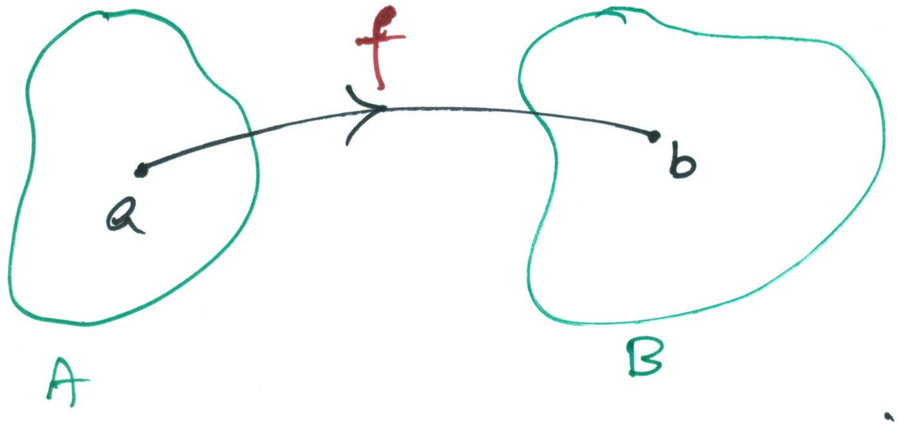
Consider the relation ρ on S such that $(a, b) \in \rho$ if and only if a, b belong to one and the same subset of partition P.

Then it is easy to verify that ρ is an equivalence relation on S.

Hence proved. $\boxed{///}$

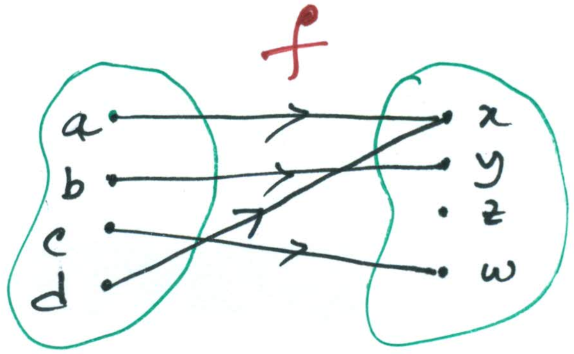
Mapping: Let A and B be two non-empty sets. A mapping f from A to B is a rule that assigns to each element x of A a definite element y in B.

Definition: Suppose that to each element in a set A is assigned by some manner or rule, a unique element of a set B. We call such assignment a mapping (function)



each element of A is assigned by some definite element of B by the rule "f". We write it as $\boxed{f : A \to B}$ in short.

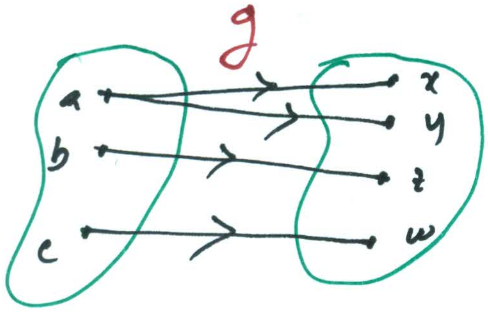
Example : (i)



$A = \{a, b, c, d\}$ $\quad B = \{x, y, z, w\}$

This is a mapping.

(ii)



$A = \{a, b, c\}$ $\quad B = \{x, y, z, w\}$

This is not a mapping as the element $a \in A$ has two assignment x and $y \in B$.

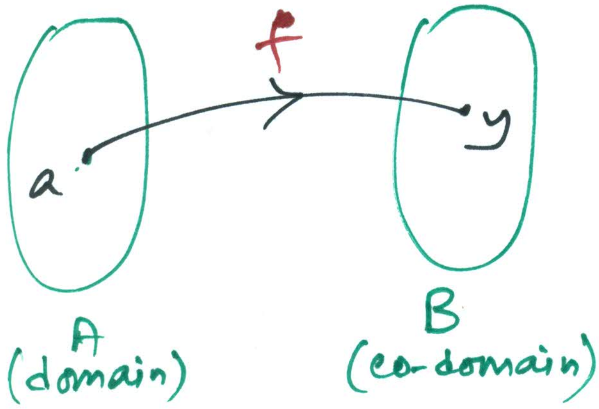
Range, Domain : Let $f : A \to B$ be a mapping then A is called the domain of f and the range of f is defined as

$$\text{Range}(f) = R(f) = \{ b \in B : \exists\, a \in A \text{ such that } f(a) = b \}.$$

Therefore, $R(f) \subseteq B$.

Therefore in Example (i), domain of f is $A = \{a, b, c, d\}$ and $R(f) = \{x, y, w\} \subset B$.

We call B as the <u>co-domain</u> of f.



We write, $y = f(a)$
We call,
y = image of 'a'
a = pre-image of 'y'

<u>$f : A \to B.$</u>

We note that, $\text{Range}(f) \subseteq$ co-domain.

- <u>Example</u>: Let $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$.

So, $f(1) = f(-1) = 1$
$f(2) = f(-2) = 4$

So, domain = co-domain = $\mathbb{R}$

$$\text{Range}(f) = \{x \in \mathbb{R} : x \geq 0\}$$
$$= \mathbb{R}^+.$$

One-to-One (injective) mapping :

A function or mapping $f : A \to B$ is said to be injective (or one-to-one) if each pair of ~~dis~~ distinct elements of A, their f-images are distinct.

That is, if $x_1 \neq x_2$ in A then $f(x_1) \neq f(x_2)$ in B.

Example : (i) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x$. Then f is one to one.

(ii) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. Then f is not one to one.

Since 2 and -2 have same image 4.

Onto (surjective) mapping :

A mapping $f : A \to B$ is said to be surjective or onto if $f(A) = B$ i.e., Range $(f) = R(f) =$ co-domain $= B$.

That is, for every $b \in B$, there exists an element $a \in f$ such that $f(a) = b$.

Example: (i) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$. Then f is onto. Because for every $y \in \mathbb{R}$ (co-domain) we have $\frac{y}{2} \in \mathbb{R}$ (domain) such that $f(\frac{y}{2}) = y$. So, $R(f) = \mathbb{R}$.

(ii) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. Then f is not onto. As, for $(-2) \in \mathbb{R}$ (co-domain), there is no $x \in \mathbb{R}$ (domain) such that $f(x) = -2$. So, $R(f) = \mathbb{R}^+ \subset \mathbb{R}$.

- ## Bijective function or mapping :

If $f: A \to B$ is both one-to-one and onto then f is a bijective mapping.

Thatis, for every pre-image there is a unique image and vice versa.

- **Example :** (i) $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$. Then we saw that f is onto. Again if $x_1 \neq x_2 \Rightarrow 2x_1 \neq 2x_2 \Rightarrow f(x_1) \neq f(x_2)$. Therefore f is one-to one. Hence f is a bijective mapping.

(ii) $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x$. Then f is a bijective mapping.

Inverse mapping :

If $f : A \to B$ be a bijection, then for every $x \in A$, $\exists$ unique $y \in B$ such that $f(x) = y$.

Let g be a mapping such that $g : B \to A$ and $g(y) = x$ iff $f(x) = y$.

Then we call g is the inverse mapping of f and denote it by f^{-1}.

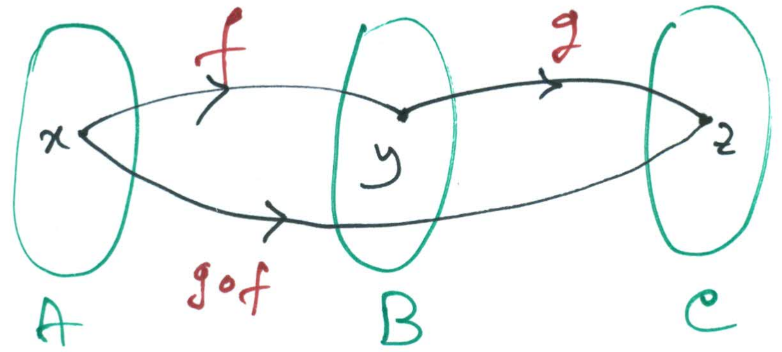
Example: (i) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x$. Then $f^{-1} : \mathbb{R} \to \mathbb{R}$ is defined as $f^{-1}(x) = \frac{x}{2}$.

We note that, $f^{-1}(f(x)) = x$ for all $x \in \mathbb{R}$, i.e.

$$f^{-1}(2x) = x \text{ for all } x \in \mathbb{R}.$$

Composition of mappings :

Let $f : A \to B$ and $g : B \to C$ be two mappings. Then the composite mapping $g \circ f : A \to C$ is defined as $g \circ f(a) = g(f(a))$ for all $a \in A$.



So, $z = g(y)$, $y = f(x)$

$\Rightarrow$ $z = g(f(x)) = g \circ f(x)$.

- We show $g \circ f = h : A \to C$ is one to one if g and f are both one to one.

Let $h(x_1) = h(x_2) \Rightarrow g(f(x_1)) = g(f(x_2))$

$\Rightarrow$ $f(x_1) = f(x_2)$ as g is one-to-one

$\Rightarrow$ $x_1 = x_2$ as f is one-to-one

So, $h(x_1) = h(x_2) \Rightarrow x_1 = x_2$

Hence $h = g \circ f$ is one-to-one.

Permutation :-

Let S be a non-empty finite set. Any bijective mapping $f: S \to S$ is called a permutation.

Suppose $S = \{a_1, \ldots, a_n\}$.

Define $f: S \to S$ by,

$a_1 \to f(a_1)$, $a_2 \to f(a_2), \ldots, a_n \to f(a_n)$

a bijection. This permutation f is denoted as

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$$

We note that $S = \{a_1, \ldots, a_n\}$
$= \{f(a_1), \ldots, f(a_n)\}$

as f is a bijection.

Example: Let $S = \{1, 2, 3, 4\}$. Define $f: S \to S$ by $f(2) = 1$, $f(1) = 3$, $f(3) = 4$, $f(4) = 2$. Then we write it as

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

Inverse permutation :-

Consider a permutation $f : S \to S$

by $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$

then $f^{-1} = \begin{pmatrix} f(a_1) & f(a_2) & \cdots & f(a_n) \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$

Example : let $f : S \to S$ with

$S = \{1, 2, 3, 4\}$ by

$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ then

$f^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

Composition of permutations :-

Consider two permutations $f : S \to S$

by $f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$ and

$g : S \to S$ by $g = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(a_1) & g(a_2) & \cdots & g(a_n) \end{pmatrix}$

then $f \circ g : S \to S$ is defined by,

$f \circ g = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(g(a_1)) & f(g(a_2)) & \cdots & f(g(a_2)) \end{pmatrix}$

and $g \circ f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(f(a_1)) & g(f(a_2)) & \cdots & g(f(a_n)) \end{pmatrix}$.

We note that $f \circ g$, $g \circ f$ are both bijective.

- **Example:** Let $S = \{1, 2, 3, 4\}$. Define

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Note that $g \circ f \neq f \circ g$.

Thus '$\circ$' (composition) operation is not commutative.

- **Cycle:** Let $S = \{a_1, \ldots, a_n\}$. A permutation $f : S \to S$ is said to be a cycle of length r, or an r-cycle if there are r elements $a_{i_1}, a_{i_2}, \ldots, a_{i_r}$ in S such that $f(a_{i_1}) = a_{i_2}$, $f(a_{i_2}) = a_{i_3}, \ldots, f(a_{i_{r-1}}) = a_{i_r}$, $f(a_{i_r}) = a_{i_1}$ and $f(a_j) = a_j$ for all $j \neq i_1, i_2, \ldots, i_r$. The cycle is denoted by $(a_{i_1}, a_{i_2}, \ldots, a_{i_r})$.

• **Example:** Let $S = \{1, 2, 3, 4\}$.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

Then $f = (2, 3, 4)$. So, f is a cycle of length 3.

• **Transposition:** A cycle of length 2 is called a transposition.

• **Example:** (i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$

$= (3, 4)$ is a transposition

(ii) $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4)$

where (a_1) is a 1-length cycle can be written as

$$(a_1) = (a_1, a_2)(a_2, a_1).$$

(iii) (a_1, a_2, a_3)

$= (a_1, a_3)(a_1, a_2)$. (composition of permutations)

(iv) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix}$

$= (1,2,3,5)\,(4,6)$

$= (1,5)\,(1,3)\,(1,2)\,(4,6)$

So, can be written as composition of transpositions.

Definition: A permutation is said to be <u>even</u> if it can be written as the product of an even number of transpositions, and <u>odd</u> if it can be written as the product of an odd number of transpositions.

Equipotent sets :-

Let A and B be two sets. Then A and B are said to be equipotent ~~Aken~~ if and only if $\exists$ a bijective mapping $f : A \to B$.

Define a relation '$\sim$' over all sets such that $A \sim B$ iff $\exists\, f : A \to B$ is a bijective mapping.

(i) <u>reflexive</u>: Define $f : A \to A$ by $f(x) = x \quad \forall x \in A$.
Then f is a bijection. Therefore $A \sim A$.

(ii) <u>Symmetric</u>: Let $A \sim B$. Then $\exists\, f : A \to B$ such that f is a bijection. Then $f^{-1} : B \to A$ exists. Also, f^{-1} is a bijection. Hence $B \sim A$.

(iii) <u>transitive</u>: Let $A \sim B$ and $B \sim C$. Then $\exists$ bijective functions $f : A \to B$ and $g : B \to C$. Then the composition function $g \circ f : A \to C$ is also a bijection. Thus $A \sim C$.

Therefore '$\sim$' is an equivalence relation.

Enumerable (Denumerable):

A set A is enumerable if $\exists$ a bijection $f : A \to \mathbb{N}$, i.e., $A \sim \mathbb{N}$, where $\mathbb{N}$ = set of all ~~naturable~~ natural numbers.

Countable sets:

A set A is countable if A is either finite or A is ~~an~~ enumerable. That is, if $A = \{a_1, \ldots, a_n\}$ or $A \sim \mathbb{N}$ then A is countable.

Example: (i) The $\mathbb{Z}$ is enumerable, as $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{1-n}{2} & \text{if } n \text{ is odd} \end{cases}$$

is a bijection.

(ii) The set $\mathbb{Q}$ is countable. (Exercise).

- **Binary Composition :-**

Let A be a non-empty set. A binary composition (or a binary operation) on A is a mapping $f : A \times A \to A$.

The commonly used symbols for binary composition are $*, +, \cdot, \oplus, \odot$.

- **Example :** Let $A = \mathbb{Z}$, then define $+ : A \times A \to \mathbb{Z}$ by $a+b = a+b$ where $a, b \in \mathbb{Z}$.

So, $2+3 = 5$.

- **Closure property of binary composition :**

Consider a binary composition $* : A \times A \to A$. Then $a*b \in A$ for any $a, b \in A$. This is called the closure property of $*$.

- **Commutative :** Consider $* : A \times A \to A$ be a binary composition.

If $a*b = b*a$ for all $a, b \in A$ then $*$ is called commutative.

- **Example**: (i) Let $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $a * b = (a+b)$ for all $a, b \in \mathbb{Z}$. Then $a * b = b * a$ as $a+b = b+a$ for all $a, b \in \mathbb{Z}$. (commutative)

  (ii) Let $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $a * b = a - b$ for all $a, b \in \mathbb{Z}$. Then $a * b \neq b * a$ for every $a, b \in \mathbb{Z}$ (not commutative)

- **Note**: Commutativity is also called abelian.

~~Assoc~~

- **Associative**: Let $* : A \times A \to A$ be a binary composition. Then $*$ is called associative if $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$.

- **Example**: (i) Let $\odot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be defined as $a \odot b = a \cdot b$, $\forall a, b \in \mathbb{R}$. Then $\odot$ is commutative and associative (check)

(ii) $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, b, c, d \in \mathbb{R} \right\}$

Define, $+ : M_2(\mathbb{R}) \times M_2(\mathbb{R}) \to M_2(\mathbb{R})$

by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a+x & b+y \\ c+z & d+w \end{pmatrix}$.

Then $+$ is associative, ~~but not~~ and commutative. (check).

Define, $\odot : M_2(\mathbb{R}) \times M_2(\mathbb{R}) \to M_2(\mathbb{R})$

by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \odot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix}$

Then $\odot$ is associative, but not commutative (check).

(iii) Consider a set $S \neq \phi$.

Let $\mathcal{P}(S) = \{$ all possible subsets of $S \}$

Define, $\cup : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S)$

by $A \cup B$ = the union of A and B

and $\cap : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S)$

by $A \cap B$ = the intersection of A and B.

Then, $A \cup B = B \cup A \Rightarrow$ '$\cup$' is commutative.

$(A \cup B) \cup C = A \cup (B \cup C)$ for all $A, B, C \in \mathcal{P}(S)$.

$\Rightarrow$ '$\cup$' is associative.

'$\cap$' is also commutative and associative. (check).

(iv) Consider $n = 5$ and

$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$,

where $[0] = \{5n : n \in \mathbb{Z}\}$

$[1] = \{5n+1 : n \in \mathbb{Z}\}$

$[2] = \{5n+2 : n \in \mathbb{Z}\}$

$[3] = \{5n+3 : n \in \mathbb{Z}\}$

$[4] = \{5n+4 : n \in \mathbb{Z}\}$

are the equivalence classes of the relation '$\equiv$' defined by

$(a, b) \in \equiv$ iff $a \equiv b \pmod 5$, i.e.,

$5 \mid (a-b)$.

Define a binary composition '+' over $\mathbb{Z}_5$ by

$$[a] + [b] \cancel{= [a+b]} = [(a+b) \bmod 5].$$

<u>Composition table</u> :

+	[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]

The composition of 'addition modulo 5' is commutative and associative.

Define '×' over $\mathbb{Z}_5$ by

$$[a] \times [b] = [a \cdot b \bmod 5]$$

×	[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]

seer '×' is commutative.

Is it associative?
(check)

Groupoid :-

Let G be a non-empty set on which a binary composition (operator) $*$ is defined, i.e., $*: G \times G \rightarrow G$ is a mapping. Then the algebraic system $(G, *)$ is said to be a groupoid.

Example : (i) $(\mathbb{Z}, +)$ is a groupoid where '+' is the addition operation on $\mathbb{Z}$.

(ii) $(\mathbb{Z}, -)$ is a groupoid where '−' is the substraction operation on $\mathbb{Z}$.

(iii) $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$ are all groupoid.

Commutative Groupoid :

Let $(G, *)$ be a groupoid. It is called a commutative groupoid if $a * b = b * a$ for all $a, b \in G$.

Let $(G, *)$ be a groupoid.

(i) We call an element 'e' $\in G$ identity element if and only if

$$\boxed{a * e = e * a = a \quad \forall a \in G.}$$

(ii) If $\boxed{a * e = a}$ for all $a \in G$ then e is called right identity in $(G, *)$.

(iii) If $\boxed{e * a = a}$ for all $a \in G$ then e is called left identity in $(G, *)$.

(iv) Let $e \in G$ be an identity element of $(G, *)$. A element a in G is said to be invertible if there exists an element a' in G such that

$$\boxed{a' * a = a * a' = e.}$$

Then a' is said to be an inverse of a in the group.

Semigroup :

Let $(G, *)$ be a groupoid. Then it is a semigroup iff

(closser property i.e, groupoid) (i) $a * b \in G \quad \forall a, b \in G$

(associativity property) (ii) $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$.

Monoid :

Let $(G, *)$ be a groupoid. Then it is a monoid iff

(closser prop. i.e, groupoid) (i) $a * b \in G \quad \forall a, b \in G$

(associativity prop. i.e, semigroup) (ii) $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$

(existence of identity element) (iii) $\exists$ an element $e \in G$ s.t. $e * a = a * e$ for all $a \in G$.

Example : (i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ are all semigroup as well as monoid.

(ii) $(\mathbb{Z}, -)$ is not a semigroup.

- **Quasigroup:**

A groupoid $(G, *)$ is said to be a quasigroup if for any two elements $a, b \in G$, each equation $a * x = b$ and $y * a = b$ has a unique solution.

- **Example:** $(\mathbb{R}, +)$ is a quasigroup, as $a + x = b$ and $y + a = b$ has a unique solution which is $(b - a) \in \mathbb{R}$.

- **Group:**

Let G be a non-empty set and $*$ be a binary operation on G. Then $(G, *)$ is called a group iff

(closure) (i) $a * b \in G$ $\forall a, b \in G$ (Groupoid)

(associativity) (ii) $a * (b * c) = (a * b) * c$ $\forall a, b, c \in G$ (Semigroup)

(identity) (iii) $\exists e \in G$ such that $e * a = a * e = a$ $\forall a \in G$. (Monoid)

(inverse) (iv) For every $a \in G$, $\exists a' \in G$ such that $a * a' = a' * a = e$.

Abelian Group :

Let $(G, *)$ be a group. Then it is called a commutative group or an abelian group if

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

Example :

(i) $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}, +)$ are all abelian group.

(ii) $(M_2(\mathbb{R}), \cdot)$ is group but not a commutative or abelian group.

Week-3

Topics:
- Group
- Order of an element
- Subgroups
- Cyclic group
- Subgroup operations

Group: A non-empty set G is said to form a group with respect to a binary composition $*$, if following properties is satisfied.

(i) Closure property:- $a*b \in G \quad \forall\, a,b \in G$.

(ii) Associative property:-

$$a*(b*c) = (a*b)*c \quad \forall\, a,b,c \in G$$

(iii) Existence of identity:-

$$\exists\, e \in G \text{ s.t. } e*a = a*e = a \quad \forall\, a \in G$$

(iv) Existence of inverse:-

$$\forall\, a \in G,\ \exists\, b \in G \text{ s.t. } a*b = b*a = e.$$

The element b is said to be an inverse of a.

The group is denoted by the symbol $(G, *)$

Abelian group or Commutative group

A group $(G, *)$ is said to be an abelian group if $a * b = b * a \quad \forall\, a, b \in G$.

Examples.

1) $(\mathbb{Z}, +)$ is a group

(i) $a + b \in \mathbb{Z} \quad \forall\, a, b \in \mathbb{Z}$

(ii) $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in \mathbb{Z}$

(iii) $0 \in \mathbb{Z}$ and $0 + a = a + 0 = a \quad \forall\, a \in \mathbb{Z}$

(iv) $\forall\, a \in \mathbb{Z} \ \exists\, -a \in \mathbb{Z}$ s.t.

$$a + (-a) = (-a) + a = 0$$

$(\mathbb{Z}, +)$ is abelian group since

$a + b = b + a \quad \forall\, a, b \in \mathbb{Z}$

2) $(\mathbb{Q}, +)$ is an abelian group

3) $(\mathbb{R}, +)$ is an abelian group

Finite group: A group $(G, *)$ is said to be finite group if $|G| =$ finite.

Examples:

1) Let $S = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$.
The S is an abelian group with respect

to multiplication.

The composition table for the set is

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

(i) From table the set S is closed under multiplication.

(ii) Multiplication is associative on $\mathbb{C}$ and $S \subseteq \mathbb{C}$. Hence multiplication is associative on S.

(iii) 1 is the identity ele

(iv) The inverse of 1 is 1, the inverse of ω is ω^2, the inverse of ω^2 is ω.

(V) The table is symmetric about the principal diagonal. Therefore multiplication is commutative on S.

$|S| = 3$ therefore S is a finite abelian group.

2: Let $S = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$, $i^4 = 1$

Then $(S, \cdot)$ is an abelian group.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

composition table

(i) S is closed under multiplication

(ii) Multiplication is associative on $\mathbb{C}$ and $S \subseteq \mathbb{C}$. Therefore multiplication is associative on S.

(iii) 1 is the identity element.

(iv) Inverse of $1, -1, i, -i$ are $1, -1, -i, i$ respectively

(v) The table is symmetric about the principal diagonal. Therefore multiplication is commutative on S.

Permutation group or Symmetric group S_n

Let $S = \{a_1, a_2, \ldots, a_n\}$

A permutation on S is a bijective map $f : S \to S$.

If f is a permutation on S then

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$$

For simplicity let us take $S = \{1, 2, \ldots, n\}$

Let P be the set of all permutations on the set S.

Let 'o' be composition of function.

Now we show that (P, o) is a group.

(i) Let $f, g \in P$ then fog is also a permutation on S because composition of two bijective function is a bijective function. Therefore $fog \in P$

(ii) Since composition of mapping

is associative therefore

$g\circ(f\circ h) = (g\circ f)\circ h \quad \forall\, f, g, h \in P$

(iii) The identity permutation

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in P$$ and it is

the identity element because

$e\circ f = f\circ e = f \quad \forall f \in P.$

(iv) Let $f = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \in P$, where

$i_k = f(k)$, $k = 1, 2, \ldots, n.$

Then $f^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix} \in P$ and

f^{-1} is the inverse of f since

$f^{-1}\circ f = f\circ f^{-1} = e.$

Properties of group

Theorem: Identity element in a group $(G, *)$ is unique.

Proof: Let e_1 and e_2 be two identity element in G.

Then $a * e_1 = e_1 * a = a \quad \forall a \in G$

$a * e_2 = e_2 * a = a \quad \forall a \in G$

$e_2 * e_1 = e_2$ (by property of e_1) —(1)

$e_2 * e_1 = e_1$ (by property of e_2) —(2)

By equations (1) and (2) $e_2 = e_1$.

Theorem: In a group $(G, *)$ each element has only one inverse.

Proof: If possible let b, c be two inverse of a.

Then $a * b = b * a = e$ —(1)

and $a * c = c * a = e$ —(2)

By equation (1) $c * (a * b) = c$

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

$\Rightarrow e * b = c$

$\Rightarrow \quad b = c.$

Hence inverse is unique.

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

Proof: Let $d = a*b$ and $d' = b^{-1}*a^{-1}$

$$d*d' = (a*b)*(b^{-1}*a^{-1})$$
$$= a*(b*b^{-1})*a^{-1}$$
$$= a*e*a^{-1} = a*a^{-1} = e \quad -(1)$$

Similarly

$$d'*d = e \quad -(2)$$

By equation (1) and (2)

$$d*d' = d'*d = e$$

$\Rightarrow b^{-1}*a^{-1}$ is the inverse of $a*b$

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

Order of an element: Let $(G, *)$ be a group and let $a \in G$.

Define $a^n = a*a*a*\cdots*a$ (n factors)

$a^{-n} = a^{-1}*a^{-1}*a^{-1}*\cdots*a^{-1}$ (n factors) a is said to be of finite order if $\exists\, n \in \mathbb{N}$ such that $a^n = e$.

The order of a is the least positive integer n such that $a^n = e$ and is denoted by $o(a)$ or $|a|$.

Theorem: Let a be an element of a group $(G, *)$. Then for integers m, n

(i) $a^m * a^n = a^{m+n}$

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

Proof: (i)

$$a^m * a^n = \underbrace{(a * a * \cdots * a)}_{m\text{-times}} * \underbrace{(a * a * \cdots * a)}_{n\text{-times}}$$

$$= a^{m+n}$$

(ii)

$$(a^n)^{-1} = (a * a * \cdots * a)^{-1}$$

$$= a^{-1} * a^{-1} * \cdots * a^{-1}$$

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

Theorem: Let a be an element of a group $(G, *)$. Then

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

(ii) If $o(a) = n$ then $a, a^2, \ldots, a^n (= e)$ are distinct element of G.

(iii) If $o(a) = n$ and $a^m = e$, then n is a divisor of m.

(iv) If $o(a) = n$ then $o(a^m) = \frac{n}{\gcd(m,n)}$

Proof: (i) Let $o(a) = n$. Then $a^n = e$, where n is the least positive integer.

Therefore $(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$

If possible, let $\exists\, m \in \mathbb{N}$ s.t. $m < n$ and $(a^{-1})^m = e$. Then $a^{-m} = e$.

$a^n = e$ and $a^{-m} = e \Rightarrow a^{n-m} = e$

Since $n-m < n$, this contradicts that $o(a) = n$. Therefore $o(a^{-1}) = e$.

(ii) If possible, let $a^r = a^s$ for some positive integers r, s such that $r < s \leq n$. Then $a^s * a^{-r} = e$

$\Rightarrow a^{s-r} = e$

Since $s-r < n$, this contradicts the assumption that $o(a) = n$.

$\Rightarrow a, a^2, a^3, \ldots, a^n$ are all distinct.

(iii) Since $o(a) = n$, n is the least positive integer such that $a^n = e$.

$\Rightarrow m \geq n$.

By division algorithm $\exists\ q, r \in \mathbb{Z}$ s.t. $m = qn + r$, where $0 \leq r < n$.

Then $e = a^m = a^{qn+r} = (a^n)^q * a^r$

$= e * a^r = a^r$

$\Rightarrow a^r = e$

This relation holds only when $r = 0$,

otherwise it will contradict that $o(a) = n$

$\Rightarrow m = qn$

$\Rightarrow n \mid m$.

(iv) Left as an exercise.

Subgroups

Let $(G, *)$ be a group and $H \subseteq G$. H is said to be stable under $*$ if $a * b \in H \ \forall \ a, b \in H$.

If H is stable under $*$ then the restriction of $*$ to $H \times H$ is a mapping from $H \times H$ to H.

This restriction, say $\circ$, is a composition on H and is defined by $a \circ b = a * b \ \forall \ a, b \in H$. $*$ is called the induced composition on H.

Definition: Let $(G, *)$ be a group and H be a non-empty subset of G. If $(H, *)$ is a group where $*$ is the induced composition, then $(H, *)$ is said to be a subgroup of $(G, *)$.

Examples:

(1) Let $(G, *)$ be a group and e be the identity element. $G \subseteq G$, $(G, *)$ is a subgroup of $(G, *)$

This subgroup $(G, *)$ is said to be the improper subgroup of $(G, *)$.

Let $H = \{e\}$ then $(H, *)$ is also a subgroup of $(G, *)$.

(2) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.

(3) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$.

(4) Let $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ and $\mathbb{R}^* = \mathbb{R} - \{0\}$.
Then $(\mathbb{Q}^*, \cdot)$ is a subgroup of $(\mathbb{R}^*, \cdot)$.

Properties of subgroups

Theorem: Subgroup of a abelian group is abelian.

Proof: Let $(H, *)$ be a subgroup of $(G, *)$, where G is abelian group.
Let $a, b \in H$ then $a, b \in G$ because $H \leq G$.
Since G is abelian $\Rightarrow a * b = b * a$

$\Rightarrow a * b = b * a \quad \forall a, b \in H$

$\Rightarrow H$ is an abelian subgroup.

Theorem: Let $(H, *)$ be a subgroup of $(G, *)$. Then the identity element e_H of $(H, *)$ is the identity element ~~e_G~~ e_G of $(G,*)$.

Proof: $e_H * h = h * e_H \quad \forall h \in H$

Also $e_G * h = h * e_G$ since $h \in H \subseteq G$.

$\Rightarrow h * e_H = h * e_G$ in G

$\Rightarrow e_H = e_G$ (by left cancellation law in G)

Theorem: Let $(G, *)$ be a group. A non-empty subset H of G is a subgroup of $(G,*)$ if and only if (i) $a \in H, b \in H \Rightarrow a*b \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$.

Proof: Let $(H,*)$ be a subgroup of $(G,*)$.

Since $(H,*)$ is a group. (i) and (ii) are satisfied.

Conversely, let H be a non-empty subset of G satisfying (i) and (ii).

Since (i) holds, H is closed under $*$.

Since $H \subseteq G$ and $*$ is associative on G, therefore $*$ is associative on H.

Let $a \in H$, Then by (ii) $a^{-1} \in H$.

Since $a, a^{-1} \in H$, (i) $\Rightarrow a \circ a^{-1} = e \in H$.

Since $e \in H$, a^{-1} is also the inverse of a in H. Therefore $a \in H$ implies the inverse of a in H belongs to H.

Therefore $(H, *)$ is a group and hence $(H, *)$ is a subgroup of $(G, *)$.

Theorem: Let $(G, *)$ be a group. A non-empty subset H of G forms a subgroup of $(G, *)$ if and only if $a \in H, b \in H \Rightarrow a * b^{-1} \in H$.

Proof: Let $(H, *)$ be a subgroup of $(G, *)$

$b \in H \Rightarrow b^{-1} \in H$ (Since $(H, *)$ is a group)

$a \in H, b^{-1} \in H \Rightarrow a * b^{-1} \in H$

Conversely, let H be a non-empty subset of G such that
$a \in H,\ b \in H \Rightarrow a * b^{-1} \in H$.

Let $a \in H$. Then $a \in H, a \in H \Rightarrow a * a^{-1} \in H$
$\Rightarrow e \in H$.

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

Let $a \in H, b \in H$. Then $a \in H$ and $b^{-1} \in H$.
By given condition $a * (b^{-1})^{-1} = a * b \in H$.

Since H is a non-empty subset of G and $*$ is associative on G therefore $*$ is associative on H.
Therefore $(H, *)$ is a group and hence $(H, *)$ is a subgroup of $(G, *)$.

Centre of a group :- Let $(G, *)$ be a group.

Define $H = \{x \in G \mid x * g = g * x \ \ \forall g \in G\}$

$(H, *)$ is a subgroup of $(G, *)$ and H is called the centre of the group G and denoted by $Z(G)$.

Now we will prove $(H, *)$ is a subgroup of $(G, *)$.

It is clear that $H \neq \phi$ because $e \in H$.

Let $p, q \in H$.

Then, $p * g = g * p$, $q * g = g * q$ $\forall g \in G$.

Now $(p * q) * g = p * (q * g) = p * (g * q)$

$= (p * g) * q = (g * p) * q$

$= g * (p * q)$

$\Rightarrow (p * q) * g = g * (p * q)$ $\forall g \in G$

$\Rightarrow p * q \in H$. — (i)

Let $p \in H$. Then $p * g = g * p$ $\forall g \in G$.

$\Rightarrow p^{-1} * (p * g) * p^{-1} = p^{-1} * (g * p) * p^{-1}$

$\Rightarrow g * p^{-1} = p^{-1} * g \quad \forall g \in G$

$\Rightarrow p^{-1} \in H$. — (ii)

By (i) and (ii) $(H, *)$ is a subgroup of $(G, *)$.

Note! If G is a commutative group then $H = Z(G) = G$.

Centraliser of an element in a group

Let $(G,*)$ be a group and let $a \in G$.
Define $H = \{x \in G \mid x*a = a*x\}$.
Now we prove that $(H,*)$ is a subgroup of $(G,*)$.

$H \neq \phi$ since $e \in H$.

Let $p, q \in H$. Then $p*a = a*p$
and $q*a = a*q$.

Now $(p*q)*a = p*(q*a)$

$$= p*(a*q) = (p*a)*q$$

$$= (a*p)*q = a*(p*q)$$

$\Rightarrow p*q \in H$ — (i)

Let $p \in H$. Then $p*a = a*p$.

$\Rightarrow p^{-1}*(p*a)*p^{-1} = p^{-1}*(a*p)*p^{-1}$

$\Rightarrow a * p^{-1} = p^{-1} * a$ (Since $p^{-1} * p = e$)

$\Rightarrow p^{-1} \in H$ — (ii)

From (i) and (ii) it follows that $(H, *)$ is a subgroup of $(G, *)$.

Note: This subgroup is called the centraliser of the element a and is denoted by $C(a)$.

Cyclic groups: A group $(G, *)$ is said to be cyclic group if there exist an element $a \in G$ such that $G = \{a^n : n \in \mathbb{Z}\}$ i.e. $G = \langle a \rangle$. a is said to be a generator of the cyclic group.

Examples: (i) Let $G = \{1, -1, i, -i\}$. Then $(G, \cdot)$ is a group. $G = \{i^n : n \in \mathbb{Z}\}$ i.e. $G = \langle i \rangle \Rightarrow (G, \cdot)$ is cyclic group.

(ii) $(\mathbb{Z}, +)$ is a cyclic group generated by 1 i.e. $\mathbb{Z} = \langle 1 \rangle$. $(\mathbb{Z}, +)$ is also generated by -1 i.e. $\mathbb{Z} = \langle -1 \rangle$.

Theorem: Let $(G, *)$ be a cyclic group generated by a. Then a^{-1} is also a generator.

Proof: $G = \{ a^n : n \in \mathbb{Z} \}$

Let $H = \{ (a^{-1})^n : n \in \mathbb{Z} \} = \langle a^{-1} \rangle$.

Let $p \in G$ then $p = a^r$ for some $r \in \mathbb{Z}$.

$p = a^r = (a^{-1})^{-r}$.

$-r \in \mathbb{Z} \Rightarrow p \in H \Rightarrow G \subset H$ — (i)

$a \in G \Rightarrow a^{-1} \in G \Rightarrow (a^{-1})^n \in G \quad \forall n \in \mathbb{Z}$

$\Rightarrow H \subset G$ — (ii)

by (i) and (ii) $G = H = \langle a^{-1} \rangle$

Theorem: Every cyclic group is abelian.

Proof: Let G be a cyclic group and $G = \langle a \rangle$.

Let $p, q \in G$. Then $p = a^r$, $q = a^s$ for some ~~...~~ $r, s \in \mathbb{Z}$.

$$p * q = a^r * a^s = a^{r+s}$$

$$= a^{s+r} \quad (\text{since } r+s = s+r)$$

$$= a^s * a^r$$

$$= q * p$$

$\Rightarrow p * q = q * p$

$\Rightarrow G$ is abelian.

Theorem: Let $(G, *)$ be a group and $(H, *)$, $(K, *)$ be two subgroup of G. Then $H \cap K$ is also a subgroup of G.

Proof: $e \in H \cap K$ (Since $e \in H$ and $e \in K$)

Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$.

Since $a, b \in H$ and H is a subgroup therefore $a * b^{-1} \in H$.

Since $a, b \in K$ and K is a subgroup therefore $a * b^{-1} \in K$.

$a * b^{-1} \in H$, $a * b^{-1} \in K \Rightarrow a * b^{-1} \in H \cap K$

i.e. $a, b \in H \cap K \Rightarrow a * b^{-1} \in H \cap K$

$\Rightarrow H \cap K$ is a subgroup of G.

Note: The union of two subgroups of a group G is not necessarily a subgroup of G.

Let $G = (\mathbb{Z}, +)$, $H = (2\mathbb{Z}, +)$ and $K = (3\mathbb{Z}, +)$. H, K are subgroup of G

but $H \cup K$ is not a subgroup of G because $2 \in H \cup K$, $3 \in H \cup K$ but $2+3 \notin H \cup K$.

Definition: Let H, K be two subgroup of a group $(G, *)$.

Define $HK = \{h * k : h \in H, k \in K\}$

For simplicity $HK = \{hk \mid h \in H, k \in K\}$

HK may not form a subgroup of $(G, *)$.

Example: Let $G = S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$

where $\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$

$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$

$\rho_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$

$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$$

$$\rho_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$$

Let $H = \{\rho_0, \rho_3\}$, $K = \{\rho_0, \rho_4\}$

Then $HK = \{\rho_0, \rho_0\rho_4, \rho_3, \rho_3\rho_4\}$

$= \{\rho_0, \rho_1, \rho_3, \rho_4\}$ is not a subgroup of $G = S_3$.

Theorem: Let H and K be two subgroups of a group $(G, *)$. Then HK is a subgroup of G if and only if $HK = KH$.

Proof: Let HK be a subgroup of G.

Let $x \in HK$. Since HK is a subgroup $x^{-1} \in HK$.

Let $x^{-1} = h_1 k_1$. Then $x = (x^{-1})^{-1} = k_1^{-1} h_1^{-1} \in KH$.

Thus $x \in HK \Rightarrow x \in KH$. Therefore

$HK \subset KH$. — (i)

Let $k_2 h_2 \in KH$. Then $k_2 \in K$, $h_2 \in H$ and

$h_2^{-1} k_2^{-1} \in HK$, since $h_2^{-1} \in H$, $k_2^{-1} \in K$.

Since HK is a subgroup,

$(h_2^{-1} k_2^{-1})^{-1} \in HK \Rightarrow k_2 h_2 \in HK$.

Therefore $KH \subset HK$ — (ii)

From (i) and (ii), $HK = KH$.

Conversely, let $HK = KH$.

Let $p \in HK$, $q \in HK$ and $p = h_3 k_3$,

$q = h_4 k_4$, say

Then $pq = (h_3 k_3)(h_4 k_4)$

$= h_3 (k_3 h_4) k_4$

$= h_3 (h_5 k_5) k_4$ Since $KH = HK$

$= (h_3 h_5)(k_5 k_4) \in HK$.

Therefore $p \in HK$, $q \in HK \Rightarrow pq \in HK$ — (iii)

Also $p^{-1} = (h_3 k_3)^{-1} = k_3^{-1} h_3^{-1} \in KH = HK$

Therefore $p \in HK \Rightarrow p^{-1} \in HK$ — (iv)

From (iii) and (iv), HK is a subgroup.

Cosets

Left Coset: Let $(G, *)$ be a group and H be a subgroup of G.

Let $a \in G$. $\forall h \in H$, $a * h \in G$.

Define $aH = \{ah : h \in H\}$. aH is called a left coset of H in G.

In an additive group, a left coset of H is denoted by $a + H$.

Examples: Let $G = (\mathbb{Z}, +)$ and

$H = (3\mathbb{Z}, +)$.

$0 + H = \{3n : n \in \mathbb{Z}\} = H$

$1 + H = \{1 + 3n : n \in \mathbb{Z}\}$

$2 + H = \{2 + 3n : n \in \mathbb{Z}\}$

There are three distinct left cosets of H.

Theorem: Let G be a group and H be a subgroup of G. Let $h \in H$. Then $hH = H$.

Proof: Let $p \in hH$. Then $p = hh_1$ for some $h_1 \in H$.

Since H is a subgroup $h, h_1 \in H$

$\Rightarrow p = hh_1 \in H$.

Therefore $hH \subset H$ —(i)

Let $q \in H$. Since $h, q \in H$, there exist a unique x in H such that $hx = q$.

Therefore $q \in H \Rightarrow q = hx$ for some $x \in H$
$\Rightarrow q \in hH$.

$\Rightarrow H \subset hH$ —(ii)

From (i) and (ii), $hH = H$

Week-4

Topics:

- Left Cosets
- Right Cosets
- Normal Subgroups
- Rings
- Field

Theorem: Let G be a group and H be a subgroup of G. Let $a \in G \setminus H$. Then $aH \cap H = \phi$.

Proof: Suppose, if possible $p \in aH \cap H$.

Then $p \in aH$ and $p \in H$.

Hence $p = a h_1$ for some $h_1 \in H$ and $p = h_2$ for some $h_2 \in H$.

$\Rightarrow h_2 = a h_1 \Rightarrow a = h_2 h_1^{-1} \in H$ (Since H is a subgroup)

This contradicts that $a \in G \setminus H$.

So $aH \cap H = \phi$.

Theorem: Let G be a group and H be a subgroup of G. If $a, b \in G$, then either $aH = bH$ or $aH \cap bH = \phi$.

Proof: Let $aH \cap bH \neq \phi$ and let $p \in aH \cap bH$. Then $p \in aH$ and $p \in bH$.

$p \in aH \Rightarrow p = ah_1$ for some $h_1 \in H$.

$p \in bH \Rightarrow p = bh_2$ for some $h_2 \in H$.

Hence $ah_1 = bh_2$.

$\Rightarrow a = bh_2h_1^{-1}$ and $b = ah_1h_2^{-1}$.

Let $x \in aH$. Then $x = ah_3$ for some $h_3 \in H$

$x = bh_2h_1^{-1}h_3 = bh_4$ for some $h_4 \in H$.

Thus $x \in aH \Rightarrow x \in bH$ and therefore

$aH \subset bH$ ...(i)

Let $y \in bH$. Then $y = bh_5$ for some $h_5 \in H$

$y = ah_1h_2^{-1}h_5 = ah_6$ for some $h_6 \in H$

Thus $y \in bH \Rightarrow y \in aH \Rightarrow bH \subset aH$ ...(ii)

From (i) and (ii) $aH = bH$.

Therefore either $aH = bH$ or $aH \cap bH = \phi$.

Theorem: Let G be a group and H be a subgroup of G. Let $a, b \in G$. Then $aH = bH$ if and only if $a^{-1}b \in H$.

Proof: Let $aH = bH$. Then $ah_1 = bh_2$ for some $h_1, h_2 \in H$. Therefore $a^{-1}b = h_1 h_2^{-1} \in H$, Since H is a subgroup.

Conversely, let $a^{-1}b \in H$. Then $a^{-1}b = h_3$ for some $h_3 \in H$.

Therefore $b = ah_3$ and this implies $b \in aH$.

But $b \in bH$.

Thus the left cosets aH and bH have a common element b and therefore by above theorem $aH = bH$.

Theorem: Let H be a subgroup of a group G. The relation ρ defined on G by "$a \rho b$" if and only if $a^{-1}b \in H$ for $a, b \in G$ is an equivalence relation on G.

Proof: Reflexive:

$\forall a \in G$, $a \rho a$ holds because $a^{-1}a = e \in H$. Therefore ρ is reflexive.

Symmetric: For $a, b \in G$,

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

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

$\Rightarrow b^{-1}a \in H \Rightarrow b \rho a$.

Therefore ρ is symmetric.

Transitive: For $a, b, c \in G$,

$a \rho b$ and $b \rho c \Rightarrow a^{-1}b \in H$ and $b^{-1}c \in H$

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

$\Rightarrow a^{-1}c \in H \Rightarrow a \rho c.$

Therefore ρ is transitive.

Since ρ is reflexive, symmetric and transitive, it is an equivalence relation on G.

The set G is partitioned into equivalence classes and each class is a left coset of H, because

$$cl(a) = \{x \in G : a \rho x\}$$
$$= \{x \in G : a^{-1}x \in H\}$$
$$= \{x \in G : x \in aH\} = aH.$$

Theorem: Any two left cosets of H in a group G have the same cardinality.

Proof: Let aH, bH be two left cosets in G. Let us define a mapping $f : aH \longrightarrow bH$ by $f(ah) = bh \ \forall\, h \in H$

Now we prove that f is injective.

$$f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2 \text{ (For some } h_1, h_2 \in H)$$
$$\Rightarrow h_1 = h_2$$
$$\Rightarrow ah_1 = ah_2$$

Therefore $f(ah_1) = f(ah_2) \Rightarrow ah_1 = ah_2$

$\Rightarrow f$ is injective.

Now we prove that f is surjective

Let $bh \in bH$.

$f(ah) = bh \Rightarrow f$ is surjective

Therefore f is bijective $\Rightarrow aH$ and bH have the same cardinality.

Theorem: (Lagrange) The order of every subgroup of a finite group G is a divisor of the order of G.

Proof: Let H be a subgroup of a finite group G. Let $o(G) = n$. Let us consider the set of all distinct left cosets of H in G. Since G contains a finite number of elements, the number of distinct left cosets of H is finite. Then there exist elements $x_1, x_2, \dots, x_m$ in G such that $x_1H, x_2H, \dots, x_mH$ is a complete list of distinct left cosets of H in G. Since left cosets are distinct, they are disjoint.

Therefore $G = \bigcup_{i=1}^{m} (x_i H)$, since G is partitioned into distinct left cosets of H.

$o(x_iH) = o(eH) = o(H)$ — (i)

$$G = \bigcup_{i=1}^{m} (x_i H)$$

$$\Rightarrow O(G) = o(x_1 H) + o(x_2 H) + \cdots + o(x_m H)$$

$$= o(H) + o(H) + \cdots \cdots + o(H) \quad (m \text{ times})$$

$$o(G) = m \cdot o(H)$$

$$\Rightarrow o(H) \mid o(G).$$

Note: $o(x_i H) = |x_i H|$ = Number of elements in $x_i H$.

Right Cosets: Let G be group and H be a subgroup of G. Let $a \in G$.

Define $Ha = \{h * a \mid h \in H\} = \{ha \mid h \in H\}$.

Ha is called a right coset of H in G.

Example: Let $G = (\mathbb{Z}, +)$ and $H = (3\mathbb{Z}, +)$

$H+0 = \{3n \mid n \in \mathbb{Z}\} = H$

$H+1 = \{3n+1 \mid n \in \mathbb{Z}\}$

$H+2 = \{3n+2 \mid n \in \mathbb{Z}\}$

Just as in the case of left cosets there are some theorems concerning right cosets.

Theorem: Let G be a group and H be a subgroup of G. Then $Hh = H$ $\forall\, h \in H$.

Theorem: Let G be a group and H be a subgroup of G. Then for any $a \in G \setminus H$, $Ha \cap H = \phi$.

Theorem: Let G be a group and H be a subgroup of G. Then either $Ha = Hb$ or $Ha \cap Hb = \phi$ for $a, b \in G$.

Theorem: Let H be a subgroup of a group G and $a, b \in G$. Then $b \in Ha$ if and only if $ba^{-1} \in H$.

Theorem: Let H be a subgroup of a group G. Then the set of all left cosets of H in G and the set of all right cosets in G have the same cardinality.

Proof: Let L be the set of all left cosets and R be the set of all right cosets of H in G.

Let $a \in G$. Define $f : L \longrightarrow R$ by

$f(aH) = Ha^{-1}$.

Now we show that f is well defined in the sense that if $xH = aH$ then $Hx^{-1} = Ha^{-1}$.

$xH = aH \iff x \in aH \iff a^{-1}x \in H$

$\iff a^{-1}(x^{-1})^{-1} \in H \iff a^{-1} \in Hx^{-1} \iff Ha^{-1} = Hx^{-1}$.

Therefore f assigns a unique coset

in R to a coset in L.

Let us take two distinct elements $aH, bH \in L$.

$Ha^{-1} = Hb^{-1} \Rightarrow aH = bH$.

So $aH \neq bH \Rightarrow f(aH) \neq f(bH)$.

$\Rightarrow f$ is injective.

Let us take an element $Ha \in R$. The pre-image of Ha is $a^{-1}H$ in L, since $f(a^{-1}H) = H(a^{-1})^{-1} = Ha$. Therefore f is surjective.

Therefore f is bijective and the sets L and R have the same cardinality.

Note! $[G:H]$ denotes the number of distinct left and right cosets of H in G.

i.e. $|L| = |R| = [G:H]$

$$O(G) = O(H) \cdot [G:H]$$

$$[G:H] = \frac{O(G)}{O(H)}.$$

Normal Subgroups: Let $(G,*)$ be a group and $(H,*)$ be a subgroup of G. Then $(H,*)$ is a normal subgroup if $aH = Ha \;\; \forall a \in G$.

The standard natation for "H is a normal subgroup of G" is $H \Delta G$.

Theorem: Let $(G,*)$ be a group and $(H,*)$ is a subgroup of G. Then $(H,*)$ is a normal subgroup if and only if $xhx^{-1} \in H \;\; \forall\, h \in H$ and $x \in G$.

Proof: Suppose $(H,*)$ is a normal subgroup of G.

Let $x \in G$ and $h \in H$.

Then $xh \in xH = Hx$ (by definition of normal subgroup)

$\Rightarrow xh \in Hx \Rightarrow xh = h_1 x$ for some $h_1 \in H$.

$\Rightarrow xhx^{-1} = h_1 \in H$

$\Rightarrow xhx^{-1} \in H \quad \forall h \in H$ and $\forall x \in G$.

Conversely, let $xhx^{-1} \in H \ \forall h \in H$ and $\forall x \in G$.

Now we prove that $xH = Hx \quad \forall x \in G$.

Let $p \in xH$. Then $p = xh_2$ for some $h_2 \in H$

$p = (xh_2x^{-1})x = h_3 x$, since $xh_2x^{-1} = h_3 \in H$

$\Rightarrow p \in Hx \Rightarrow xH \subset Hx$. —(i)

Now let $q \in Hx$.

Then $q = h_4 x$ for some $h_4 \in H$.

$= x(x^{-1}h_4 x)$

$= x\left(x^{-1}h_4 (x^{-1})^{-1}\right)$

$= xh_5$ for some $h_5 = x^{-1}h_4(x^{-1})^{-1} \in H$

Hence $q \in xH$

$\Rightarrow Hx \subset xH$ —(ii)

By (i) and (ii) $Hx = xH \quad \forall x \in G$.

Therefore H is a normal subgroup in G.

Theorem: Let $(H, *)$ and $(K, *)$ be two normal subgroup of a group $(G, *)$. Then $(H \cap K, *)$ is a normal subgroup.
i.e. The intersection of two normal subgroups of a group is a normal subgroup.

Proof: Let $W = H \cap K$. Then W is a subgroup of G, since the intersection of two subgroup is a subgroup.

Let $w \in W$ and $x \in G$.

Then $w \in H$ and $w \in K$.

$xwx^{-1} \in H$ (Since H is a normal subgroup)

$xwx^{-1} \in K$ (Since K is a normal subgroup

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

Therefore, $xwx^{-1} \in W \quad \forall w \in W$ and $\forall x \in G$.

$\Rightarrow H \cap K$ is a normal subgroup of G.

Quotient group / Factor group

Let H be a normal subgroup of a group $(G, *)$. Let S be the set of all distinct cosets of H in G.

Define a binary operation 'o' on S by $aH \circ bH = (a*b)H \quad \forall a, b \in G$.

Now, we prove that $(S, \circ)$ is a group.

(i) $aH \circ bH = (a*b)H \in S \quad \forall aH, bH \in S$.

(ii) $aH \circ (bH \circ cH) = aH \circ (b*c)H$

$$= a*(b*c)H$$
$$= (a*b)*cH$$
$$= (a*b)H \circ cH$$
$$= (aH \circ bH) \circ cH$$

$\Rightarrow *$ is associative.

(iii) $eH = H$ is the identity element because $eH \circ aH = aH \circ eH = (e * a)H$
$= aH$

(iv) The inverse of aH is $a^{-1}H$, because

$$aH \circ a^{-1}H = (a * a^{-1})H = eH = H$$

and $a^{-1}H \circ aH = (a^{-1} * a)H = eH = H$

All group property have been satisfied therefore $(S, \circ)$ is a group.

This group is said to be the quotient group of G by H and is denoted by G/H.

Homomorphism: Let $(G_1, *)$ and $(G_2, \circ)$ be two groups.

A mapping $\phi : G_1 \rightarrow G_2$ is said to be a homomorphism if $\phi(a * b) = \phi(a) \circ \phi(b)$ $\forall\ a, b \in G_1$.

Example: Let $\phi : G_1 \to G_2$ be defined by

$$\phi(a) = e_{G_2}.$$

$$\phi(a * b) = e_{G_2}$$
$$= e_{G_2} \circ e_{G_2} = \phi(a) \circ \phi(b).$$

Example: Let $G_1 = (\mathbb{Z}, +)$ and $G_2 = (2\mathbb{Z}, +)$

Define $\phi : G_1 \to G_2$ by $\phi(a) = 2a$ for $a \in \mathbb{Z}$

$$\phi(a+b) = 2(a+b) = 2a + 2b = \phi(a) + \phi(b)$$

$\Rightarrow \phi$ is a homomorphism.

Note: A homomorphism $\phi : G_1 \to G_2$ is said to be isomorphism if ϕ is one-one and onto.

If $\phi : G_1 \to G_2$ is an isomorphism then G_1 and G_2 are called isomorphic group.

Ring: A non-empty set R is said to form a ring with respect to two binary compositions, addition $(+)$ and multiplication $(\cdot)$ defined on it, if the following conditions are satisfied.

(1) $(R,+)$ is an abelian group,

(2) $(R,\cdot)$ is a semigroup,

(3) $a\cdot(b+c) = a\cdot b + a\cdot c$

$(b+c)\cdot a = b\cdot a + c\cdot a \quad \forall a,b,c \in R.$

The ring is denoted by $(R,+,\cdot)$.

R is said to be a commutative ring if $a\cdot b = b\cdot a \quad \forall a,b \in R$.

A ring $(R,+,\cdot)$ is said to be ring with unity if there exist multiplicative identity '1' in R s.t. $a\cdot 1 = 1\cdot a = a \quad \forall a \in R$

Example: $(\mathbb{Z}, +, \cdot)$ is a ring.

(1) $(\mathbb{Z}, +)$ is an abelian group

(2) $(\mathbb{Z}, \cdot)$ is semigroup

(3) $a \cdot (b+c) = a \cdot b + a \cdot c$

$(b+c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in \mathbb{Z}$.

Also $a \cdot b = b \cdot a \quad \forall a, b \in \mathbb{Z}$ therefore

$(\mathbb{Z}, +, \cdot)$ is commutative ring.

$\exists\, 1 \in \mathbb{Z}$ s.t. $a \cdot 1 = 1 \cdot a = a \quad \forall a \in \mathbb{Z}$

Therefore $(\mathbb{Z}, +, \cdot)$ is a

Commutative ring with unity.

Example: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and

$(\mathbb{C}, +, \cdot)$ all are

Commutative ring with unity.

Example: $(2\mathbb{Z}, +, \cdot)$ is a commutative

ring without identity.

Example! $M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; a, b, c, d \in \mathbb{R} \right\}$

$(M_2(\mathbb{R}), +)$ is an abelian group where $+$ denotes matrix addition

$(M_2(\mathbb{R}), \cdot)$ is a semigroup, where $\cdot$ denotes matrix multiplication

Therefore $(M_2(\mathbb{R}), +, \cdot)$ is a ring with unity.

Since $A \cdot B \neq B \cdot A$ for some $A, B \in M_2(\mathbb{R})$ therefore $(M_2(\mathbb{R}), +, \cdot)$ is a non-commutative ring.

Polynomial Ring! Let $(R, +, \cdot)$ be a ring. and x an indeterminate.

$R[x] = \{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \in \mathbb{N} \cup \{0\}$ and $a_i \in R \; \forall i = 0$ to $n \}$

Equality of two polynomials

Two polynomials $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n \in R[x]$ are said to be equal if $a_0 = b_0$, $a_1 = b_1, \ldots, a_n = b_n$.

Addition of two polynomials

Let $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in R[x]$

and

$q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m \in R[x]$.

Case 1: $m = n$

$$p(x) + q(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

Case 2: $n < m$

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1) x + \cdots + (a_n + b_n) x^n + b_{n+1} x^{n+1} + \cdots + b_m x^m$$

Case 3: $n > m$

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1) x + \cdots + (a_m + b_m) x^m + a_{m+1} x^{m+1} + \cdots + a_n x^n.$$

Multiplication of two polynomials

$p(x)\cdot q(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n}$

where $c_j = a_0 b_j + a_1 b_{j-1} + \cdots + a_j b_0$ taking

$a_{n+1} = a_{n+2} = \cdots = a_{m+n} = 0$

$b_{m+1} = b_{m+2} = \cdots = b_{m+n} = 0$.

Then $(R[x], +, \cdot)$ is a ring. It is called the polynomial ring over R.

If R be a ring with unity then the ring $(R[x], +, \cdot)$ is also a ring with unity.

The identity element of the ring $(R[x], +, \cdot)$ is the constant polynomial $p(x) = 1 \in R[x]$.

Divisor of Zero: Let $(R, +, \cdot)$ be a ring. A non-zero element $a \in R$ is said to be a divisor of zero if there exists a non-zero element b in R s.t. $a \cdot b = 0$ or $b \cdot a = 0$.

In the first case, a is said to be left divisor and in the second case $(b \cdot a = 0)$ a is said to be a right divisor of zero.

Example: In the ring $(\mathbb{Z}_6, +, \cdot)$ $\bar{2}$ is a divisor of zero because $\exists\ \bar{3} \in \mathbb{Z}_6$ s.t. $\bar{2} \cdot \bar{3} = \bar{0}$.

The ring $(\mathbb{Z}_5, +, \cdot)$ contains no divisor of zero. Also $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$ contains no divisor of zero.

Integral domain: A non-trivial ring R with unity is said to be an integral domain if it is commutative and contains no divisor of zero.

Example: (i) The rings $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$ and $(\mathbb{R},+,\cdot)$ are integral domains.

(ii) The ring $(\mathbb{Z}_5,+,\cdot)$ is a commutative ring with unity and the ring contains no divisor of zero. Therefore it is an integral domain.

(iii) The ring $(\mathbb{Z}_6,+,\cdot)$ is a commutative ring with unity. It contains divisor of zero. Therefore it is not an integral domain

Field: $(F, +, \cdot)$ is a field if

(i) $(F, +, \cdot)$ is an integral domain.

(ii) For every non-zero element has a multiplicative inverse

Therefore a non-empty set F forms a field with respect to two binary compositions $+$ and $\cdot$, if

(i) $a+b \in F \quad \forall a, b \in F$

(ii) $a+(b+c) = (a+b)+c \quad \forall a, b, c \in F$

(iii) there exists an element, called the zero element and denoted by 0, in F such that $a+0=0 \; \forall a \in F$.

(iv) $\forall a \in F, \exists -a \in F$ s.t. $a+(-a)=0$

(v) $a+b = b+a \quad \forall a, b \in F$

(vi) $a \cdot b \in F \quad \forall a, b \in F$.

(vii) $a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \forall a,b,c \in F$

(viii) $\exists\ 1 \in F$ s.t. $a\cdot 1 = 1\cdot a = a \quad \forall a \in F$

(ix) For every $a \neq 0$, $\exists\ a^{-1} \in F$ s.t. $a\cdot a^{-1} = 1$

(x) $a\cdot b = b\cdot a \quad \forall a,b \in F$

(xi) $a\cdot(b+c) = a\cdot b + a\cdot c \quad \forall a,b,c \in F$

Example: (i) The rings $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ are field. $(\mathbb{C},+,\cdot)$ is also a field.

(ii) The ring $(\mathbb{Z}_5,+,\cdot)$ is a commutative ring with unity and each non-zero element of the ring is a unit. Therefore the ring $(\mathbb{Z}_5,+,\cdot)$ is a field.

Week - 5

Topics:
- Vector Spaces
- Subspaces
- Linear Span
- Basis of a Vector space
- Dimension of a Vector space

External Composition: Let F and V be two non-empty sets. A mapping $f: F \times V \longrightarrow V$ is said to be an external composition of F with V.

$$f(a, x) \in V \quad \forall a \in F \text{ and } x \in V.$$

Example: Let $F = \mathbb{R}$ and $V = \mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$

Define $\odot : F \times V \longrightarrow V$ by

$$\odot(a, (x, y, z)) = a \odot (x, y, z) = (ax, ay, az)$$

Then $\odot$ is an external composition

of F with V.

Vector space over a Field

Let V be a non-empty set and ~~$\oplus : V \times V \to V$~~ $\oplus : V \times V \to V$ be a binary composition on V. Let $(F, +, \cdot)$ be a field and let $\odot$ be an external composition of F with V. V is said to be a Vector space over the field F.

(i) $(V, \oplus)$ is an abelian group

(a) $x \oplus y \in V \quad \forall\, x, y \in V$

(b) $x \oplus y = y \oplus x \quad \forall\, x, y \in V$

(c) $x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad \forall\, x, y, z \in V$

(d) $\exists$ an element 0 in V s.t.

$x \oplus 0 = x \quad \forall\, x \in V.$

(e) For each x in V $\exists\; -x \in V$ s.t.

$x \oplus (-x) = 0.$

(ii) $a \odot x \in V$, $\forall a \in F$ and $\forall x \in V$

(iii) $a \odot (b \odot x) = (a \cdot b) \odot x \; \forall a, b \in F$ and $x \in V$

(iv) $a \odot (x \oplus y) = a \odot x \oplus a \odot y \; \forall a \in F$ and $\forall x, y \in V$

(v) $(a+b) \odot \bar{x} = a \odot x \oplus b \odot x \; \forall a, b \in F$ and $x \in V$

$1 \odot x = x \quad \forall x \in V$ (where 1 is the identity element in F)

The vector space is denoted by $(V, \oplus, \odot, F, +, \cdot)$.

Example:

(1) Let $V = \mathbb{R}^n = \{(x_1, x_2, \dots, x_n) \mid x_1, x_2, \dots, x_n \in \mathbb{R}\}$

and $F = (\mathbb{R}, +, \cdot)$

Define $\oplus$ on V by

$(x_1, x_2, \dots, x_n) \oplus (y_1, y_2, \dots, y_n)$

$= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$

Define external composition $\odot$ of $\mathbb{R}$ with V by

$$a \odot (x_1, x_2, \ldots, x_n) = (a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n)$$

$\forall a \in F$ and $(x_1, x_2, \ldots, x_n) \in V$.

Now we will show that V is a vector space over F.

(i) $(V, \oplus)$ is an abelian group

(a) Let $x = (x_1, x_2, \ldots, x_n) \in V$

and $y = (y_1, y_2, \ldots, y_n) \in V$.

Then

$$x \oplus y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \in V$$

(b) $x \oplus y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$

$= (y_1 + x_1, y_2 + x_2, \ldots, y_n + x_n)$

$= y \oplus x \quad \forall\ x, y \in V$.

(c) $x \oplus (y \oplus z) = (x \oplus y) \oplus z \quad \forall\ x, y, z \in V$

(d) $\exists\ \underline{0} = (0, 0, \dots, 0) \in V$ s.t.

$$x \oplus \underline{0} = (x_1 + 0, x_2 + 0, \dots, x_n + 0)$$
$$= x \quad \forall\ x \in V$$

(e) $\forall\ x = (x_1, x_2, \dots, x_n) \in V$ there exist $-x = (-x_1, -x_2, \dots, -x_n) \in V$ s.t.

$$x \oplus (-x) = (x_1 + (-x_1), x_2 + (-x_2), \dots, x_n + (-x_n))$$
$$= (0, 0, \dots, 0)$$

(ii) Let $a \in F$ and $x \in V$ then

$$a \odot x = (a \cdot x_1, a \cdot x_2, \dots, a x_n) \in V$$
(because $a \cdot x_i \in \mathbb{R}\ \forall i$)

(iii) Let $a \in F$, $b \in F$ and $x \in V$, then

$$a \odot (b \odot x) = a \odot (b \cdot x_1, b \cdot x_2, \dots, b \cdot x_n)$$
$$= (a \cdot b \cdot x_1, a \cdot b \cdot x_2, \dots, a \cdot b \cdot x_n)$$
$$= (a \cdot b) \odot (x)$$
$$= (a \cdot b) \odot x$$

(iv) Let $a \in F$ and $x, y \in V$

$$a \odot (x \oplus y) = a \odot (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$= \left(a \cdot (x_1 + y_1), a \cdot (x_2 + y_2), \ldots, a \cdot (x_n + y_n) \right)$$

$$= \left(a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n \right)$$

$$+ \left(a \cdot y_1, a \cdot y_2, \ldots, a \cdot y_n \right)$$

$$= a \odot x + a \odot y$$

(v) Let $a, b \in F$ and $x \in V$

$$(a+b) \odot x = \left((a+b) \cdot x_1, (a+b) \cdot x_2, \ldots, (a+b) \cdot x_n \right)$$

$$= \left(a \cdot x_1, a \cdot x_2, \ldots, a \cdot x_n \right)$$

$$+ \left(b \cdot x_1, b \cdot x_2, \ldots, b \cdot x_n \right)$$

$$= a \odot x \oplus b \odot x$$

Example: Let $V = \{ a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid a_i \in \mathbb{R}, i = 0, 1, \ldots, n \}$

and $F = (\mathbb{R}, +, \cdot)$

Let $\oplus$ be a composition on V, defined by
$$p(x) \oplus q(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

where $p(x) = \sum_{i=0}^{n} a_i x^i \in V$

and $q(x) = \sum_{i=0}^{n} b_i x^i \in V$

Define external composition $\odot$ of F with V by
$$a \odot p(x) = \sum_{i=0}^{n} (a \cdot a_i) x^i$$

where $p(x) = \sum_{i=0}^{n} a_i x^i \in V$

Then V is a vector space over F.

Example: Let $V = M_n(\mathbb{R})$ be the set of all $m \times n$ matrices over $\mathbb{R}$ and $F = (\mathbb{R}, +, \cdot)$.

Let $A = (a_{ij})$ and $B = (b_{ij})$ in V.

Let $\oplus$ be a composition on V, defined by $A \oplus B = (a_{ij} + b_{ij})$.

Define external composition $\odot$ of F with V by $a \odot A = (a \cdot a_{ij})$

Then V is a vector space over F.

Theorem: (i) In a vector space V over a field F,

$0 \odot \bar{x} = \bar{0} \quad \forall \; \bar{x} \in V$, where 0 is the zero element in F.

Proof: $(0+0) \odot \bar{x} = 0 \odot \bar{x}$ (because $0+0=0$ in F)

$\Rightarrow (0 \odot \bar{x}) \oplus (0 \odot \bar{x}) = 0 \odot \bar{x}$

$\Rightarrow -0 \odot \bar{x} \oplus (0 \odot \bar{x} \oplus 0 \odot \bar{x}) = -0 \odot \bar{x} \oplus 0 \odot \bar{x}$

$\Rightarrow (-0 \odot \bar{x} \oplus 0 \odot \bar{x}) \oplus (0 \odot \bar{x}) = \bar{0}$

$\Rightarrow \bar{0} \oplus (0 \odot \bar{x}) = \bar{0}$

$\Rightarrow 0 \odot \bar{x} = \bar{0}$

(ii) $a \odot \bar{0} = \bar{0} \quad \forall\, a \in F$

(iii) $-1 \odot \bar{x} = -\bar{x} \quad \forall\, \bar{x} \in V$, 1 is the identity element in F.

(iv) $a \odot \bar{x} = 0 \Rightarrow$ either $a = 0$ or $\bar{x} = 0$

Subspace: Let $(V, \oplus, \odot)$ be a vector space over a field F with respect to addition (+) and multiplication by elements of F. Let W be a non-empty subset of V. If W forms a vector space over F w.r.t. $\oplus$ and $\odot$ then W is said to be a subspace of V.

Theorem: Let $(V, \oplus, \odot, F, +, \cdot)$ be a vector space over the field $(F, +, \cdot)$ and $W \subseteq V$ is a non-empty subset of V. Then W will be a subspace of V if and only if

(i) $\forall\, x, y \in W \Rightarrow x \oplus y \in W$

(ii) $\forall\, a \in F, \forall\, w \in W \Rightarrow a \odot w \in W$

Proof: Suppose conditions (i) and (ii) holds in W

Let $x, y \in W$. Since F is a field $-1 \in F$ where 1 is the identity element in F.

By (ii) $-1 \odot y \in W$ i.e. $-y \in W$

Then by (i) $x \oplus (-y) = x - y \in W$

This proves that W is a subspace of the additive group V. Since V is a commutative group, W is also a commutative group.

Other conditions of a vector space is also satisfied in W.

Conversely, suppose W is a subspace of V. Then conditions (i) and (ii) follows from the definition of a vector space.

Note: A non-empty subset W of a vector space V over a field F is a subspace of V if and only if $(a \odot x) \oplus (b \odot y) \in W$, $\forall\, a, b \in F$ and $\forall\, x, y \in W$.

Examples: 1: Let $V = \mathbb{R}^3$

$$W = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 1\}$$

$(0,0,0) \notin W$ because $0+0+0 \neq 1$

$\Rightarrow$ W is not a subspace of V.

2) Let $V = \mathbb{R}^3$

$$W = \{(x, y, z) \in \mathbb{R}^3 \mid y = z = 0\}$$

Then W is a non-empty subset of $\mathbb{R}^3$, since $(0,0,0) \in W$.

Let $x = (x_1, 0, 0)$ and $y = (y_1, 0, 0) \in W$.

Let $a, b \in \mathbb{R}$.

Then $a \odot x \oplus b \odot y = (ax_1 + by_1, 0, 0) \in W$

$\Rightarrow$ W is a subspace of V.

Theorem: The intersection of two subspaces of a vector space V over a field F is a subspace of V.

Proof: Let W_1 and W_2 be two subspaces of $(V, \oplus, \odot, F, +, \cdot)$. $W_1 \cap W_2 \neq \phi$

because $\bar{0} \in W_1 \cap W_2$.

Let $x, y \in W_1 \cap W_2 \Rightarrow x, y \in W_1$ and $x, y \in W_2$

$x, y \in W_1 \Rightarrow a \odot x \oplus b \odot y \in W_1$ for all $a, b \in F$ -(i)

$x, y \in W_2 \Rightarrow a \odot x \oplus b \odot y \in W_2$ for all $a, b \in F$ -(ii)

by (i) and (ii) $a \odot x \oplus b \odot y \in W_1 \cap W_2$ $\forall a, b \in F$

$\Rightarrow W_1 \cap W_2$ is a subspace of V.

Note: The union of two subspaces of V need not be a subspace of V.

Counter example: Let $V = \mathbb{R}^3$

$W_1 = \{(x, y, z) \in \mathbb{R}^3 \mid y = 0, z = 0\}$

$W_2 = \{(x, y, z) \in \mathbb{R}^3 \mid x = 0, z = 0\}$

Let $x = (1,0,0) \in W_1$ and $y = (0,1,0) \in W_2$

then $x \oplus y = (1,1,0) \notin W_1 \cup W_2$

Hence $W_1 \cup W_2$ is not a subspace of $\mathbb{R}^3$.

Linear sum of two subspaces

Let U and W be two subspaces of a vector space $(V, \oplus, \odot, F, +, \cdot)$.

Define $U + W = \{u \oplus v \mid u \in U, v \in W\}$, then the set $U+W$ is said to be the linear sum of the subspaces U and W.

Theorem: Let U and W be two subspaces of a vector space $(V, \oplus, \odot, F, +, \cdot)$.

Then the linear sum $U+W$ is a subspace of V.

15

Proof:- Let $x, y \in U+W$, then

$x = u_1 \oplus w_1$ for some $u_1 \in U$, $w_1 \in W$

$y = u_2 \oplus w_2$ for some $u_2 \in U$, $w_2 \in W$

Let $a, b \in F$, then

$a \odot x \oplus b \odot y = a \odot (u_1 \oplus w_1) \oplus b \odot (u_2 \oplus w_2)$

$= (a \odot u_1 \oplus b \odot u_2) \oplus (a \odot w_1 \oplus b \odot w_2)$

$a \odot u_1 \oplus b \odot u_2 \in U$ because U is a subspace

$a \odot w_1 \oplus b \odot w_2 \in W$ because W is a subspace

$\Rightarrow a \odot x \oplus b \odot y \in U+W$

$\Rightarrow U+W$ is a subspace of V.

Definition: Let V be a vector space over a field F. Let $\alpha_1, \alpha_2, \ldots, \alpha_r \in V$.

A vector β in V is said to be a linear combination of the vectors $\alpha_1, \alpha_2, \ldots, \alpha_r$ if β can be expressed as

$\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r$ for some scalars $c_1, c_2, \ldots, c_r$ in F.

Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_r\} \subseteq V$.

Define $L(S) = \{c_1\alpha_1 + c_2\alpha_2 + \cdots + c_R\alpha_R \mid \forall\, c_1, c_2, \ldots, c_R \in F\}$

$L(S)$ is called linear span of S.

Theorem: Let V be a vector space over a field F and let $S \subseteq V$, where S is finite. Then linear span $L(S)$ is a subspace of V.

Proof: Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\} \subseteq V$.

$$L(S) = \left\{ \sum_{i=1}^{k} c_i \alpha_i \;\middle|\; c_i \in F \quad \forall\, i = 1, 2, \ldots, k \right\}$$

Let $x, y \in L(S)$, then $\exists\, c_1, c_2, \ldots, c_k \in F$

s.t. $x = \sum_{i=1}^{k} c_i \alpha_i$

and $\exists\, d_1, d_2, \ldots, d_k \in F$ s.t.

$$y = \sum_{i=1}^{k} d_i \alpha_i .$$

Let $a, b \in F$ then

$$ax + by = \sum_{i=1}^{k} (a c_i + b d_i) \alpha_i , \quad a c_i + b d_i \in F$$

$\Rightarrow ax + by \in L(S) \quad \forall\, a, b \in F$

$\Rightarrow L(S)$ is a subspace of V.

Theorem: Let V be a vector space over F. Let S and T be two finite subsets of V. Then,

(i) $L(L(S)) = L(S)$

(ii) $L(S \cup T) = L(S) + L(T)$

Linear dependence and Linear independence

Let V be a vector space over F. Let $S = \{\alpha_1, \alpha_2, \dots, \alpha_k\} \subseteq V$. Then S is linearly dependent if

$$c_1\alpha_1 + c_2\alpha_2 + \dots + c_k\alpha_k = \bar{0}$$

for some non-zero $c_i \in F$.

S is linearly independent if

$$c_1\alpha_1 + c_2\alpha_2 + \dots + c_k\alpha_k = 0 \Rightarrow c_i = 0 \ \forall i$$

Example: The set of vectors

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

is linearly dependent in $\mathbb{R}^3$.

Let $c_1, c_2, c_3 \in \mathbb{R}$ s.t.

$$c_1(2,1,1) + c_2(1,2,2) + c_3(1,1,1) = (0,0,0)$$

Therefore,
$$2c_1 + c_2 + c_3 = 0 \quad \text{—(i)}$$
$$c_1 + 2c_2 + c_3 = 0 \quad \text{—(ii)}$$
$$c_1 + 2c_2 + c_3 = 0 \quad \text{—(iii)}$$

By equation (i) and (ii)

$$\frac{c_1}{-1} = \frac{c_2}{-1} = \frac{c_3}{3} = k \text{ (say)}$$

$$\Rightarrow c_1 = -k,\ c_2 = -k,\ c_3 = 3k$$

equation (iii) is also satisfied by c_1, c_2, c_3.

Let $k=1$ then c_1, c_2, c_3 all are non-zero

Therefore the given set of vectors is linearly dependent.

Example: The set of vectors $\{(1,2,2), (2,1,2), (2,2,1)\}$ is linearly independent in $\mathbb{R}^3$.

Let $c_1, c_2, c_3 \in \mathbb{R}$ s.t.

$$c_1(1,2,2) + c_2(2,1,2) + c_3(2,2,1) = (0,0,0)$$

$\Rightarrow$

$$c_1 + 2c_2 + 2c_3 = 0 \quad \text{--- (i)}$$

$$2c_1 + c_2 + 2c_3 = 0 \quad \text{--- (ii)}$$

$$2c_1 + 2c_2 + c_3 = 0 \quad \text{--- (iii)}$$

$$\begin{vmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{vmatrix} = 5 \neq 0$$

By Cramer's rule, there exists a unique solution $c_1 = 0, c_2 = 0, c_3 = 0$

$\Rightarrow$ The given set of vectors is linearly independent.

Theorem: If the set of vectors $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ in a vector space V over a field F be linearly dependent, then at least one of the vectors of the set can be expressed as a linear combination of the remaining others.

Proof: Since the set $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ is linearly dependent, there exist scalars $c_1, c_2, \ldots, c_n$ in F s.t. atleast one $c_j \neq 0$ and

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_j\alpha_j + \cdots + c_n\alpha_n = 0$$

$$\Rightarrow c_j\alpha_j = -c_1\alpha_1 - c_2\alpha_2 - \cdots - c_n\alpha_n$$

$$\alpha_j = c_j^{-1}(-c_1\alpha_1 - c_2\alpha_2 - \cdots - c_n\alpha_n)$$

$$\alpha_j = -c_j^{-1}c_1\alpha_1 - c_j^{-1}c_2\alpha_2 - \cdots - c_j^{-1}c_n\alpha_n$$

Let $d_i = -c_j^{-1}c_i$ where $i = 1, 2, \ldots, j-1, j+1, \ldots n$.

$$\alpha_j = d_1\alpha_1 + d_2\alpha_2 + \cdots + d_n\alpha_n$$

$\Rightarrow \alpha_j$ is a linear combination of the vectors $\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n$.

Basis of a vector space

Let V be a vector space over a field F. Then V is said to be finitely generated or finite dimensional if $\exists$ a finite set of vectors $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq V$ s.t. $L(S) = V$. Otherwise V is infinite dimensional vector space.

Basis: Let V be a vector space over a field F. A set S of vectors in V is said to be a basis of V if

(i) S is linearly independent in V

(ii) S generates V i.e. $L(S) = V$.

Example: let $V = \mathbb{R}^3$

$S = \{(1,0,0), (0,1,0), (0,0,1)\} \subseteq \mathbb{R}^3$

let $c_1, c_2, c_3 \in \mathbb{R}$ s.t.

$c_1(1,0,0) + c_2(0,1,0) + c_3(0,0,1) = (0,0,0)$

$\Rightarrow (c_1, c_2, c_3) = (0,0,0)$

$\Rightarrow c_1 = c_2 = c_3 = 0$

$\Rightarrow$ S is linearly independent in V.

let $(a,b,c) \in \mathbb{R}^3$ then

$(a,b,c) = a(1,0,0) + b(0,1,0) + c(0,0,1)$

$\Rightarrow L(S) = V$.

Therefore S is a basis of V

Example: Let $V = \mathbb{R}^3$ and

$S = \{(1,0,1), (0,1,1), (1,1,0)\}$.

Let $\alpha_1 = (1,0,1)$, $\alpha_2 = (0,1,1)$, $\alpha_3 = (1,1,0)$

Now we show that S is a basis of V.

Let $c_1, c_2, c_3 \in F = \mathbb{R}$ s.t.

$$c_1(1,0,1) + c_2(0,1,1) + c_3(1,1,0) = (0,0,0)$$

$$\Rightarrow (c_1+c_3, c_2+c_3, c_1+c_2) = (0,0,0)$$

$$\Rightarrow \left.\begin{array}{l} c_1+c_3=0 \\ c_2+c_3=0 \\ c_1+c_2=0 \end{array}\right\}$$ By solving these equations we get $c_1 = c_2 = c_3 = 0$

Therefore S is linearly independent.

Let $\xi = (a,b,c) \in \mathbb{R}^3$. Let us examine if $(a,b,c) \in L(S)$.

If possible, let $\xi = d_1\alpha_1 + d_2\alpha_2 + d_3\alpha_3$ for $d_1, d_2, d_3 \in \mathbb{R}$.

Then,

$(a,b,c) = d_1(1,0,1) + d_2(0,1,1) + d_3(1,1,0)$

$(a,b,c) = (d_1+d_3,\ d_2+d_3,\ d_1+d_2)$

$\Rightarrow \quad d_1 + d_3 = a$

$d_2 + d_3 = b$

$d_1 + d_2 = c$

This is a non-homogeneous system of three equations in d_1, d_2, d_3.

The co-efficient determinant

$$\begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{vmatrix} = -2 \neq 0$$

By Cramer's rule, $\exists$ a unique solution for d_1, d_2, d_3.

This proves that $\xi = (a,b,c) \in L(S)$.

$\Rightarrow V = L(S)$

$\Rightarrow S$ is a basis of V.

Replacement theorem: If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of a vector space V over a field F and a non-zero vector β of V is expressed as

$\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$, $c_i \in F$,

then if $c_j \neq 0$, $\{\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_n\}$ is a new basis of V.

Proof: $\beta = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_{j-1}\alpha_{j-1} + c_j\alpha_j + \cdots + c_n\alpha_n$

or,

$$c_j\alpha_j = \beta - c_1\alpha_1 - c_2\alpha_2 - \cdots - c_{j-1}\alpha_{j-1} - c_{j+1}\alpha_{j+1} - \cdots - c_n\alpha_n.$$

$$\Rightarrow \alpha_j = c_j^{-1}\beta - c_j^{-1}c_1\alpha_1 - c_j^{-1}c_2\alpha_2 - \cdots - c_j^{-1}c_{j-1}\alpha_{j-1} - c_j^{-1}c_{j+1}\alpha_{j+1} - \cdots - c_j^{-1}c_n\alpha_n$$

(since $c_j \neq 0$ therefore $c_j^{-1} \in F$)

$\Rightarrow \alpha_j$ is a linear combination of the vectors $\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_n$.

Now we prove that the set $\{\alpha_1, \alpha_2, \dots, \alpha_{j-1}, \beta, \alpha_{j+1}, \dots, \alpha_n\}$ is linearly independent.

Let $d_1\alpha_1 + d_2\alpha_2 + \dots + d_{j-1}\alpha_{j-1} + d_j\beta + d_{j+1}\alpha_{j+1} + \dots + d_n\alpha_n = 0$, for some scalar $d_i \in F$, $i = 1, 2, \dots, n$.

Then $d_1\alpha_1 + d_2\alpha_2 + \dots + d_{j-1}\alpha_{j-1} + d_j(c_1\alpha_1 + c_2\alpha_2 + \dots + c_{j-1}\alpha_{j-1} + c_j\alpha_j + c_{j+1}\alpha_{j+1} + \dots + c_n\alpha_n) + d_{j+1}\alpha_{j+1} + \dots + d_n\alpha_n = 0$

$\Rightarrow (d_1 + d_jc_1)\alpha_1 + (d_2 + d_jc_2)\alpha_2 + \dots + (d_{j-1} + d_jc_{j-1})\alpha_{j-1} + d_jc_j\alpha_j + (d_{j+1} + d_jc_{j+1})\alpha_{j+1} + \dots + (d_n + d_jc_n)\alpha_n = 0$

Since the set $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is linearly independent, we have

$d_1 + d_jc_1 = 0$, $d_2 + d_jc_2 = 0, \dots, d_{j-1} + d_jc_{j-1} = 0$,

, $d_j c_j = 0$, $d_{j+1} + d_j c_{j+1} = 0, \ldots,$

$d_n + d_j c_n = 0$.

$d_j c_j = 0 \Rightarrow d_j = 0$ and therefore

$d_i = 0$ for $i = 1, 2, \ldots, n$.

$\Rightarrow$ The set $\{\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_n\}$ is linearly independent.

Now we prove that

$L\{\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_n\} = V$.

let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \alpha_j, \alpha_{j+1}, \ldots, \alpha_n\}$ and

$T = \{\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_n\}$.

since β is a linear combination of the vectors of S, each element of T is a linear combination of the vectors of S. Therefore $L(T) \in L(S)$.

Since α_j is a linear combination of the vectors of T, each element of S is a linear combination of the vectors of T. Therefore $L(S) \subseteq L(T)$;

Consequently, $L(T) = L(S) = V$.

Hence $\{\alpha_1, \alpha_2, \ldots, \alpha_{j-1}, \beta, \alpha_{j+1}, \ldots, \alpha_n\}$ is a basis of V.

Theorem: If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of a finite dimensional vector space V over a field F, then any linearly independent set of vectors in V contains at most n vectors.

Proof: Let $\{\beta_1, \beta_2, \ldots, \beta_r\}$ be a linearly independent set of vectors in V.

None of β_i is a zero vector

Since $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of V and β_1 is a non-zero vector in V,

$\beta_1 = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$, where $c_1, c_2, \ldots, c_n \in F$ and not all are zero.

Let $c_i \neq 0$

By Replacement theorem,

$\{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, \beta_1, \alpha_{i+1}, \ldots, \alpha_n\}$ is a basis of V. Since $\beta_2 \neq 0$ and $\{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, \beta_1, \alpha_{i+1}, \ldots, \alpha_n\}$ is a basis of V,

$\beta_2 = d_1\alpha_1 + d_2\alpha_2 + \cdots + d_{i-1}\alpha_{i-1} + d_i\beta_1 + d_{i+1}\alpha_{i+1} + \cdots + d_n\alpha_n$, where d_i's are scalars, not all zero.

We assert that at least one of $d_1, d_2, \ldots, d_{i-1}, d_{i+1}, \ldots, d_n$ is non-zero.

Because, if all of them be zero, then $\beta_2 = d_i\beta_1$ and this will imply linear dependence of β_1, β_2 which is a contradiction.

Let $d_j \neq 0$, $j \neq i$. By Replacement theorem $\{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}, \beta_1, \alpha_{i+1}, \ldots, \alpha_{j-1}, \beta_2, \alpha_{j+1}, \ldots, \alpha_n\}$ is a new basis of V. Since $\beta_3 \neq 0$,

$$\beta_3 = t_1\alpha_1 + t_2\alpha_2 + \cdots + t_{i-1}\alpha_{i-1} + t_i\beta_1 + t_{i+1}\alpha_{i+1} + \cdots + t_{j-1}\alpha_{j-1} + t_j\beta_2 + t_{j+1}\alpha_{j+1} + \cdots + t_n\alpha_n,$$

where t_i's are scalars and not all zero.

We assert that at least one of $t_1, t_2, \ldots, t_{i-1}, t_{i+1}, \ldots, t_{j-1}, t_{j+1}, \ldots, t_n$ is non-zero. Because otherwise, $\beta_3 = t_i\beta_1 + t_j\beta_2$ and this will imply linear dependence of $\beta_1, \beta_2, \beta_3$, which is a contradiction.

Proceeding in this way we observe that at each step one α is replaced by any β and the resulting set remains a basis of V. The following cases may arise

(i) $\beta_1, \beta_2, \ldots, \beta_r$ all come to the new basis containing some α's. In this case $r < n$.

(ii) $\beta_1, \beta_2, \ldots, \beta_r$ exhaust all α's and form the new basis. In this case $r = n$.

It can not happen that $r > n$. Because, then by Replacement theorem, n vectors $\beta_1, \beta_2, \ldots, \beta_n$ will come to the basis replacing all α's one after another and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ becomes a new basis of V. Therefore the remaining vectors $\beta_{n+1}, \beta_{n+2}, \ldots, \beta_r$

of V will be each a linear combination of $\beta_1, \ldots, \beta_n$ showing that the set $\{\beta_1, \beta_2, \ldots, \beta_n, \beta_{n+1}, \ldots, \beta_r\}$ is linearly dependent, a contradiction.

Therefore $r \leq n$.

Theorem: Any two basis of a finite dimensional vector space V have the same number of vectors.

Proof: Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, $\{\beta_1, \beta_2, \ldots, \beta_m\}$ be two basis of a finite dimensional vector space V.

Since $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of V and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is a linearly independent set of vectors in V, $m \leq n$.

Since $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is a basis of V and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a linearly independent set of vectors in V, $n \leq m$.

$m \leq n$ and $n \leq m \Rightarrow m = n$.

Dimension of a vector space

The number of vectors in a basis of a vector space V is said to be the dimension (or rank) of V and is denoted by dim V.

Example: Let $V = \mathbb{R}^3$, then

$\mathcal{B} = \{(1,0,0), (0,1,0), (0,0,1)\}$ is a basis of V over $\mathbb{R}$.

$\Rightarrow \dim(V) = \dim(\mathbb{R}^3) = 3.$

Theorem: Let V be a vector space of dimension n over a field F. Then any linearly independent set of n vectors of V is a basis of V.

Question: Find a basis of $\mathbb{R}^3$ that contains the vectors $(1,2,0)$ and $(1,3,1)$.

$\mathbb{R}^3$ is a vector space of dimension 3. The standard basis of $\mathbb{R}^3$ is $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ where $\epsilon_1 = (1,0,0)$, $\epsilon_2 = (0,1,0)$ and $\epsilon_3 = (0,0,1)$.

Let $\alpha = (1,2,0)$, $\beta = (1,3,1)$.

Then $\alpha = 1\epsilon_1 + 2\epsilon_2 + 0\epsilon_3$.

Since the coefficient of ϵ_1 is non-zero, by Replacement theorem α can replace ϵ_1 in the basis $\{\epsilon_1, \epsilon_2, \epsilon_3\}$ and $\{\alpha, \epsilon_2, \epsilon_3\}$ can be new basis for $\mathbb{R}^3$.

Let $\beta = c_1\alpha + c_2\epsilon_2 + c_3\epsilon_3$.

Then $(1,3,1) = c_1(1,2,0) + c_2(0,1,0) + c_3(0,0,1)$

Therefore $c_1 = 1$, $2c_1 + c_2 = 3$, $c_3 = 1$.

We have $c_1 = 1$, $c_2 = 1$, $c_3 = 1$ and

$\beta = \alpha + \epsilon_2 + \epsilon_3$.

Since the coefficient of ϵ_2 is non-zero, by Replacement theorem β can replace ϵ_2 in the basis $\{\alpha, \epsilon_2, \epsilon_3\}$ and $\{\alpha, \beta, \epsilon_3\}$ can be a new basis for $\mathbb{R}^3$.

Question: Find a basis and the dimension of the subspace W of $\mathbb{R}^3$, where

$W = \{ (a,b,c) \in \mathbb{R}^3 \mid a+b+c = 0 \}$.

let $w = (a,b,c) \in W$

$$(a,b,c) = (a, b, -a-b), \text{ Since } a+b+c=0$$
$$= a(1,0,-1) + b(0,1,-1)$$

$(1,0,-1)$ and $(0,1,-1)$ are linearly independent therefore $\{(1,0,-1), (0,1,-1)\}$ is a basis of W.

$\Rightarrow \dim W = 2$.

Extension theorem: A linearly independent set of vectors in a finite dimensional vector space V over a field F is either a basis of V, or it can be extended to a basis of V.

Proof:- Let $S = \{\alpha_1, \alpha_2, \dots, \alpha_r\}$ be a linearly independent set in V.

$L(S)$ being the smallest subspace containing S, $L(S) \subset V$.

If $L(S) = V$, then S is a basis.

If $L(S)$ be a proper subspace of V, then $V - L(S) \neq \phi$. Let $\beta \in V - L(S)$. We prove the set $\{\alpha_1, \alpha_2, \dots, \alpha_r, \beta\}$ is linearly independent.

Let us consider the relation

$c_1\alpha_1 + c_2\alpha_2 + \dots + c_r\alpha_r + b\beta = 0$ where $c_1, c_2, \dots, c_r, b \in F$ — (i)

We assert that $b = 0$. Because if $b \neq 0$, then b^{-1} exists in F and β can be expressed as

$$\beta = -b^{-1}(c_1\alpha_1 + c_2\alpha_2 + \dots + c_r\alpha_r)$$
$$= d_1\alpha_1 + d_2\alpha_2 + \dots + d_r\alpha_r$$

where $d_i = -b^{-1} c_i \in F$, $i = 1, 2, \ldots, r$.

$\Rightarrow \beta \in L(S)$, a contradiction. Therefore our assertion is established.

The linear independence of the set $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ and $b = 0$ together imply $c_1 = c_2 = \cdots = c_r = b = 0$ in (i)

This proves linear independence of the set $S_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_r, \beta\}$.

Now $L(S_1) \subset V$. If $L(S_1) = V$, then S_1 is a basis of V and as S_1 is an extension of S, the theorem is proved.

If however, $L(S_1)$ is a proper subspace of V, we can take a vector $\in V - L(S_1)$ and proceed as before.

Since V is finite dimensional, after a finite number of steps we come to a finite set of vectors in V as an extension of S and also as a basis of V.

Example: Let $V = \mathbb{R}^3$

$S = \{(1,0,0), (0,1,0)\} \subseteq V$

$L(S) = \{(a,b,0) \mid a,b \in \mathbb{R}\}$

$V - L(S) \neq \phi$

Let $\beta = (0,0,2) \in V - L(S)$

Then $S = \{(1,0,0), (0,1,0), (0,0,2)\}$ is linearly independent set and has three element therefore S is a basis of V.

Theorem: Let V be a vector space over a field F. A subset $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of V is a basis of V if and only if every element of V has a unique representation as a linear combination of the vectors of B.

Proof: Let $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of V.

Let $\alpha \in V$. Then $\alpha = \sum_{i=1}^{n} c_i \alpha_i$ for some $c_i \in F$.

Let us assume $\alpha = \sum_{i=1}^{n} d_i \alpha_i$ for some $d_i \in F$.

Then $\underline{0} = \alpha - \alpha = \sum_{i=1}^{n} (c_i - d_i)\alpha_i$

Since $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is linearly independent therefore $c_i - d_i = 0 \ \forall i$

$\Rightarrow c_i = d_i \ \forall i$

$\Rightarrow \alpha$ has a unique representation

Conversely, let $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subset of V s.t. every vector of V has a unique representation as a linear combination of the vectors of B.

Clearly, $V = L\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ --- (i)

$0 \in V$, and by the condition, 0 has a unique representation as a linear combination of the vectors of B.

Let $0 = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$.

This is obviously satisfied by $c_1 = 0, c_2 = 0, \ldots, c_n = 0$ and because of uniqueness in the condition, if follows that

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$$

$\Rightarrow c_1 = 0, c_2 = 0, \ldots, c_n = 0.$

$\Rightarrow B$ is linearly independent set (ii)

From (i) and (ii) it follows that B is a basis of V.

Co-ordinate of a vector

Let $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an ordered basis of a vector space V over a field F. Then to each vector α in V $\exists\ c_1, c_2, \ldots, c_n \in F$ s.t.

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

The ordered n-tuple $(c_1, c_2, \ldots, c_n)$ is said to be the co-ordinate vector of α relative to the ordered basis B.

Example! Let $V = \mathbb{R}^3$

$B = \{(1,1,1), (1,1,0), (1,0,0)\}$

B is a basis of $\mathbb{R}^3$ over $\mathbb{R}$.

Let $\beta = (1,3,1) \in \mathbb{R}^3$ then

$\exists\ c_1, c_2, c_3 \in \mathbb{R}$ s.t.

$$(1,3,1) = c_1(1,1,1) + c_2(1,1,0) + c_3(1,0,0)$$

$$= (c_1 + c_2 + c_3,\ c_1 + c_2,\ c_1)$$

$\Rightarrow\ c_1 + c_2 + c_3 = 1,\quad c_1 + c_2 = 3,\quad c_1 = 1$

After solving we get $c_1 = 1$, $c_2 = 2$

$c_3 = -2$.

So $(1,2,-2)$ is co-ordinate vector of $\beta = (1,3,1)$ relative to ordered basis B.

WEEK-6 LECTURE NOTE

Topics : Complement of Subspace
Linear Transformation
More on Linear mapping
Linear Space

Sum of two Sub-spaces:

Let V be a vector space over a field F. Suppose $W \subseteq V$ is a subspace of V.

Theorem: $\dim(W) \leq \dim(V)$.

proof: case 1: Let $W = \{\bar{0}\}$. Then $\dim(W) = 0 \leq \dim(V) = n$ (say).

case 2: Let $V \neq \{\bar{0}\}$ and $W \subseteq V$ with $W \neq \{\bar{0}\}$.

Let $\dim(W) = m$. If possible let $m > n$. Then $\exists$ a set $\{\alpha_1, \ldots, \alpha_m\}$ $\in V$ such that $L(\{\alpha_1, \ldots, \alpha_m\}) = W$ and $\{\alpha_1, \ldots, \alpha_m\}$ is linearly independent in W.

Therefore, V contains a set $\{\alpha_1, \ldots, \alpha_m\}$ which is linearly independent $\Rightarrow$ $\dim(V) \geq m \Rightarrow n \geq m$. This is a contradiction to the fact that $m > n$.

Hence $m \leq n$, i.e., $\dim(W) \leq \dim(V)$. ▨

- Let V be a vector space over the field F. Let U and W be two sub-spaces of V. Then

$$\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W),$$

where $U + W = \{u + w : u \in U \text{ and } w \in W\}$,

and $\dim(V) < \infty$.

We note that $(U+W)$ is a sub-space of V.

Let $\alpha, \beta \in (U+W)$. Then we can write

$$\alpha = u_1 + w_1 \quad \text{for } u_1 \in U, w_1 \in W$$
$$\beta = u_2 + w_2 \quad \text{for } u_2 \in U, w_2 \in W.$$

Then for any $a, b \in F$ we have,

$$\begin{aligned} a\alpha + b\beta &= a(u_1 + w_1) + b(u_2 + w_2) \\ &= (au_1 + bu_2) + (aw_1 + bw_2) \\ &\in (U+W) \text{ as } au_1 + bu_2 \in U, \\ &\qquad aw_1 + bw_2 \in W. \end{aligned}$$

This shows that $(U+W)$ is a subspace.

Also, we have seen that $U \cap W$ is a subspace of V for any two subspaces U, W of V. (over the same field F).

Theorem: $\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

proof: Let $S = \{\alpha_1, \ldots, \alpha_p\}$ be a basis of $(U \cap W)$.

Since $\dim(U \cap W) \leq \dim(U)$ as $(U \cap W) \subseteq U$, we can extend S to $S_1 = \{\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_s\}$ such that S_1 is a basis for U.

Also, ~~Let~~ $\dim(U \cap W) \leq \dim(W)$, by similar reason, we can extent S to $S_2 = \{\alpha_1, \ldots, \alpha_p, \delta_1, \ldots, \delta_t\}$ such that S_2 is a basis for W.

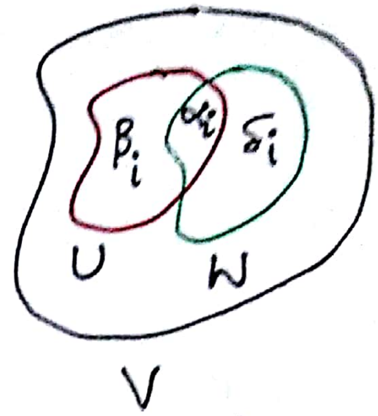
Let $B = \{\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_s, \delta_1, \ldots, \delta_t\}$.

We show that B is a basis of $(U+W)$.

We shows

(i) $L(B) = (U+W)$

(ii) B is Linearly independent in V.



$\dim(V) = n$

$\dim(U) = r+s$

$\dim(W) = r+t$

$\dim(U \cap W) = r$

(i): We see that

$$B \subseteq (U+W)$$

$$\Rightarrow L(B) \subseteq L(U+W)$$
$$= U+W \quad \text{———} \ (*)$$

Let $v \in U+W$. Then $v = u+w$ for some $u \in U$ and $w \in W$.

Now
$$v = u + w$$
$$= \left(\sum_{i=1}^{r} a_i \alpha_i + \sum_{i=1}^{s} b_i \beta_i\right) +$$
$$\left(\sum_{i=1}^{r} c_i \alpha_i + \sum_{i=1}^{t} d_i \delta_i\right)$$
$$= \sum_{i=1}^{r} (a_i + c_i)\alpha_i + \sum_{i=1}^{s} b_i \beta_i + \sum_{i=1}^{t} d_i \delta_i$$

where $a_i, b_i, c_i, d_i \in F$ for each i.

$$\Rightarrow v = u + w \in L(B)$$

$$\Rightarrow U+W \subseteq L(B) \quad \text{———} \ (**)$$

Therefore by (*) and (**) we have
$L(B) = U + W$.

(ii): Consider,

$a_1\alpha_1 + \cdots + a_r\alpha_r + b_1\beta_1 + \cdots + b_s\beta_s + c_1\delta_1 + \cdots + c_t\delta_t = \bar{0}$ for $a_i, b_i, c_i \in F$.

$$\Rightarrow \underbrace{\sum_{i=1}^{r} a_i\alpha_i + \sum_{i=1}^{s} b_i\beta_i}_{\text{belongs to } U} = -\sum_{i=1}^{t} c_i\delta_i \in W \quad \text{---} (***)$$

$$\Rightarrow -\sum_{i=1}^{t} c_i\delta_i \in U \cap W.$$

$$\Rightarrow -\sum_{i=1}^{t} c_i\delta_i = \sum_{i=1}^{r} d_i\alpha_i$$

$$\Rightarrow \sum_{i=1}^{t} c_i\delta_i + \sum_{i=1}^{r} d_i\alpha_i = \bar{0}$$

As $\{\delta_1, \ldots, \delta_t, \alpha_1, \ldots, \alpha_r\}$ is linearly independent set in W (so in V) $\Rightarrow$ $c_i = 0$ and $d_j = 0$ for $i = 1, \ldots, t$ and $j = 1, \ldots, r$

Therefore from (***) we have,

$$\sum_{i=1}^{r} a_i \alpha_i + \sum_{i=1}^{s} b_i \beta_i = \bar{0}$$

Again $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ is linearly independent set in U (so in V) we have,

$$a_i = 0, \quad \beta_j = 0 \quad \text{for } i = 1, \ldots, r \quad j = 1, \ldots, s$$

Hence, $\sum_{i=1}^{r} a_i \alpha_i + \sum_{i=1}^{s} b_i \beta_i + \sum_{i=1}^{t} c_i \delta_i = 0$

$\Rightarrow \quad a_i = 0, \quad b_j = 0, \quad c_k = 0$

for all $i = 1, \ldots, r; \; j = 1, \ldots, s;$
$k = 1, \ldots, t.$

Therefore,

$$\begin{aligned} \dim(U+W) &= r+s+t \\ &= (r+s) + (r+t) - r \\ &= \dim(U) + \dim(W) - \dim(U \cap W). \end{aligned}$$

$\blacksquare$

<u>Note</u>: If $U \cap W = \{\bar{0}\}$, then $\dim(U+W) = \dim(U) + \dim(W)$. In this case we write $U + W = U \oplus W$ if $n = r+s+t$.

Then, U and W is called complement of each other, i.e., we write $U + W = U \oplus W$ when $U \cap W = \{\bar{0}\}$

Also, $V = (U \oplus W)$ is called the direct sum of U and W if $\dim(V) = \dim(U \oplus W)$.

Linear transformation / mapping :

Let U and V be two vector spaces over the same field F. A mapping $T: U \to V$ is said to be a linear mapping or a linear transformation if it satisfies the following condition :

1. $T(\alpha + \beta) = T(\alpha) + T(\beta)$
   $\forall\ \alpha, \beta \in U$

2. $T(c\alpha) = cT(\alpha)$ $\forall\ c \in F$ and $\alpha \in U$.

These two conditions can be combined into a single condition →

$$T(a\alpha + b\beta) = aT(\alpha) + bT(\beta)$$
$\forall\ a, b \in F$ and $\alpha, \beta \in U$.

Example: $T: \mathbb{R}^3 \to \mathbb{R}^3$ be defined by $T(x_1, x_2, x_3)$

$$= (x_1+x_2+x_3,\ 2x_1+x_2+2x_3,\ x_1+2x_2+x_3)$$

Let $\alpha = (x_1, x_2, x_3)$

$\beta = (y_1, y_2, y_3)$

Then $a\alpha + b\beta = (ax_1+by_1,\ ax_2+by_2,\ ax_3+by_3)$

for $a, b \in \mathbb{R}$

Therefore $T(a\alpha + b\beta)$

$$= T(ax_1+by_1,\ ax_2+by_2,\ ax_3+by_3)$$

$$= (ax_1+by_1+ax_2+by_2+ax_3+by_3,\ 2ax_1+2by_1+ax_2+by_2+2ax_3+2by_3,\ ax_1+by_1+2ax_2+2by_2+ax_3+by_3)$$

$$= a(x_1+x_2+x_3,\ 2x_1+x_2+2x_3,\ x_1+2x_2+x_3) + b(y_1+y_2+y_3,\ 2y_1+y_2+2y_3,\ y_1+2y_2+y_3)$$

$$= aT(x_1, x_2, x_3) + bT(y_1, y_2, y_3)$$

$$= aT(\alpha) + bT(\beta)$$

$\Rightarrow$ T is a linear mapping.

Example: $T : \mathbb{R}^3 \to \mathbb{R}^3$ by

$$T(x_1, x_2, x_3) = (x_1+1, x_2+1, x_3+1).$$

Then $T(1,0,0) = (2,1,1)$

$T(0,1,0) = (1,2,1)$

$$T((1,0,0) + (0,1,0))$$

$$= T(1,1,0) = (2,2,1)$$

$$\neq T(1,0,0) + T(0,1,0)$$

Hence T is not a linear mapping.

Theorem: (i) $T(\bar{0}_U) = \bar{0}_V$ where $\bar{0}_U$, $\bar{0}_V$ are the identity element of U and V respectively, $T : U \to V$ be a linear mapping.

Proof: $\bar{0}_U + \bar{0}_U = \bar{0}_U$

$$\Rightarrow T(\bar{0}_U + \bar{0}_U) = T(\bar{0}_U)$$

$$\Rightarrow T(\bar{0}_U) + T(\bar{0}_U) = T(\bar{0}_U)$$

$$\Rightarrow T(\bar{0}_U) + T(\bar{0}_U) - T(\bar{0}_U) = T(\bar{0}_U) - T(\bar{0}_U)$$

$$\Rightarrow T(\bar{0}_U) + \bar{0}_V = \bar{0}_V$$

$$\Rightarrow T(\bar{0}_U) = \bar{0}_V.$$

(ii) $T(-\alpha) = -T(\alpha). \quad \forall \alpha \in U.$

Proof: $\alpha + (-\alpha) = \bar{0}_U$

$\Rightarrow T(\alpha + (-\alpha)) = T(\bar{0}_U)$

$\Rightarrow T(\alpha) + T(-\alpha) = \bar{0}_V$

$\Rightarrow T(-\alpha) = \bar{0}_V - T(\alpha)$

$\Rightarrow T(-\alpha) = -T(\alpha)$

Kernel of a linear mapping:

Let $T: U \to V$ be a linear mapping. We denote kernal of T as $\ker(T)$ and define it by.

$$\ker(T) = \{\alpha \in U : T(\alpha) = \bar{0}_V\}$$

See, $\ker(T) \neq \phi$ as $T(\bar{0}_U) = \bar{0}_V$

$\Rightarrow \bar{0}_U \in \ker(T)$.

Theorem: Let $T: U \to V$ be a linear mapping. Then $\ker(T)$ is a subspace of U.

Proof: Let $\alpha, \beta \in \ker(T)$.

$\Rightarrow T(\alpha) = T(\beta) = \bar{0}_V$.

Then $T(a\alpha + b\beta)$ (for any $a, b \in F$).

$= T(a\alpha) + T(b\beta)$

$= aT(\alpha) + bT(\beta)$

$= a\bar{0}_V + b\bar{0}_V = \bar{0}_V$

$\Rightarrow a\alpha + b\beta \in \ker(T)$. $\forall\ \alpha, \beta \in \ker(T)$ and $a, b \in F$.

Therefore $\ker(T)$ is a subspace of U.

(*) We call $\ker(T)$ as a <u>null space</u> of T.

• <u>Theorem</u>: $T: U \to V$ be a linear mapping. Then T is one-to-one iff $\ker(T) = \{\bar{0}_U\}$

<u>proof</u>: Suppose T is one-to-one.

$T(\bar{0}_U) = \bar{0}_V$.

Then $\alpha \in \ker(T) \Rightarrow T(\alpha) = T(\bar{0}_U) = \bar{0}_V$

Since T is one to one we have $\alpha = \bar{0}_U$.

$\Rightarrow \ker(T) = \{\bar{0}_U\}$.

Conversely, let $\ker(T) = \{\bar{0}_U\}$.

Let $\alpha, \beta \in U$ and $T(\alpha) = T(\beta)$

$\Rightarrow T(\alpha - \beta) = T(\alpha) - T(\beta) = \bar{0}_V$

$\Rightarrow \alpha - \beta \in \ker(T)$

$\Rightarrow \alpha - \beta = \bar{0}_U \Rightarrow \alpha = \beta$.

So, T is one to one. (proved)

Theorem: Let $T : U \to V$ be a linear mapping such that $\ker(T) = \{\bar{0}_V\}$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a set of linearly independent vectors then $\{T(\alpha_1), T(\alpha_2), \ldots, T(\alpha_n)\}$ is a linearly independent set of vectors in V.

Proof: Consider,

$$a_1 T(\alpha_1) + a_2 T(\alpha_2) + \cdots + a_n T(\alpha_n) = \bar{0}_V$$

$$\Rightarrow T(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) = \bar{0}_V$$

$$\Rightarrow (a_1\alpha_1 + \cdots + a_n\alpha_n) \in \ker(T)$$

$$\Rightarrow a_1\alpha_1 + \cdots + a_n\alpha_n = \bar{0}_U$$

$\Rightarrow a_1 = a_2 = \cdots = a_n = 0$ as $\{\alpha_1, \ldots, \alpha_n\}$ is linearly independent in U.

$\Rightarrow \{T(\alpha_1), \ldots, T(\alpha_n)\}$ is a linearly independent set of vectors in V.

- **Example:** $T : \mathbb{R}^3 \to \mathbb{R}^3$ by

$$T(x_1, x_2, x_3) = (x_1 + x_2 + x_3,\ 2x_1 + x_2 + 2x_3,\ x_1 + 2x_2 + x_3)$$

If $(x_1, x_2, x_3) \in \ker(T)$ then,

$T(x_1, x_2, x_3) = (0, 0, 0)$

$$\Rightarrow \left.\begin{array}{r} x_1 + x_2 + x_3 = 0 \\ 2x_1 + x_2 + 2x_3 = 0 \\ x_1 + 2x_2 + x_3 = 0 \end{array}\right\} \Rightarrow \begin{array}{l} x_1 = k,\ x_2 = 0 \\ x_3 = -k \end{array}$$

$\Rightarrow (x_1, x_2, x_3) = k(1, 0, -1)$

$\Rightarrow \ker(T) = L\{(1, 0, -1)\}.$

$\Rightarrow \dim(\ker(T)) = 1.$

- **Image of a linear mapping:**

Let $T : U \to V$ be a linear mapping over the field F.

Then image of $T = \{\beta \in V : \exists\, \alpha \in U$ such that $T(\alpha) = \beta\}$.

$= \operatorname{Im}(T)$

Theorem: $Im(T)$ is a subspace of V.

Proof: Let $\beta_1, \beta_2 \in Im(T)$.

Then $\exists$ $\alpha_1, \alpha_2 \in U$ s.t.

$T(\alpha_1) = \beta_1$, $T(\alpha_2) = \beta_2$

$$\Rightarrow T(a\alpha_1 + b\alpha_2) = aT(\alpha_1) + bT(\alpha_2)$$
$$= a\beta_1 + b\beta_2$$

for all $a, b \in F$.

$\Rightarrow a\beta_1 + b\beta_2 \in Im(T)$ $\forall a, b \in F$.

Hence $Im(T)$ is a subspace of V.

Theorem: Let $T: U \to V$ be a linear mapping over the field F. If $B = \{\alpha_1, \cdots, \alpha_n\}$ be a basis of U then $\{T(\alpha_1), \cdots, T(\alpha_n)\}$ generates $Im(T)$.

Proof: To show, $L(\{T(\alpha_1), \cdots, T(\alpha_n)\})$
$= Im(T)$

Let $\beta \in Im(T)$. Then $\exists$ $\alpha \in U$ s.t.

$T(\alpha) = \beta$.

Now, $\{\alpha_1, \cdots, \alpha_n\}$ is a basis for U.

Then $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$

$\Rightarrow T(\alpha) = a_1T(\alpha_1) + \cdots + a_nT(\alpha_n)$

$\Rightarrow \beta = a_1 T(\alpha_1) + \cdots + a_n T(\alpha_n)$

$\in L(\{T(\alpha_1), \cdots, T(\alpha_n)\})$

Hence proved.

• Example : $T: \mathbb{R}^3 \to \mathbb{R}^3$ by

$T(x_1, x_2, x_3) = (x_1+x_2+x_3,\ 2x_1+x_2+2x_3,\ x_1+2x_2+x_3)$.

Let $\varepsilon_1 = (1,0,0)$, $\varepsilon_2 = (0,1,0)$,
$\varepsilon_3 = (0,0,1)$.

Then $\operatorname{Im}(T) = L(\{T(\varepsilon_1), T(\varepsilon_2), T(\varepsilon_3)\})$

$= L(\{(1,2,1), (1,1,2), (1,2,1)\})$

$= L(\{(1,2,1), (1,1,2)\})$

$\Rightarrow \dim(\operatorname{Im}(T)) = 2$.

(*) Denote $\dim(\operatorname{Im}(T)) = \dim(R(T))$

and $\dim(\operatorname{Ker}(T)) = \dim(N(T))$

Rank Nullity Theorem :

Let $T: U \to V$ be a linear mapping over F. If U, V are finite dimensional vector spaces then

$$\text{Rank}(T) + \text{Nullity}(T) = \dim(U)$$

where $\text{Rank}(T) = \dim(R(T))$

$\text{Nullity}(T) = \dim(N(T))$.

Proof : Case I : $\ker(T) = \{\bar{0}_v\}$.

$\Rightarrow \text{Nullity}(T) = 0$.

Let $B = \{\alpha_1, \dots, \alpha_n\}$ be a basis of U.

Then $B' = \{T(\alpha_1), \dots, T(\alpha_n)\}$ generates $R(T)$. Also, B' is linearly independent in V as $\ker(T) = \{\bar{0}_v\}$.

Hence B' is a basis of $R(T)$.

$\Rightarrow \dim(R(T)) = n = \text{Rank}(T)$.

So, $\text{Rank}(T) + \text{Nullity}(T)$

$= n + 0 = n = \dim(U)$.

Case 2: $\ker(T) = U$.

$\Rightarrow$ Nullity $(T) = \dim(U)$

Rank $(T) = 0$

$\Rightarrow$ ~~Nullity~~ Rank (T) + Nullity $(T) = \dim(U)$

Case 3: $\ker(T)$ is a proper subspace of U with basis $\{\alpha_1, \dots, \alpha_k\}$ where $1 \leq k < n = \dim(U)$.

Extend $\{\alpha_1, \dots, \alpha_k\}$ to $\{\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \dots, \alpha_n\} = B$ a basis of U,

~~So~~ $\dim(U) = n$.

To show $\{T(\alpha_{k+1}), \dots, T(\alpha_n)\}$ is a basis of $R(T)$.

Now, $\{\alpha_1, \dots, \alpha_n\} = B$ is a basis of $U \Rightarrow \{T(\alpha_1), \dots, T(\alpha_n)\}$ generates $R(T)$.

$L(T(\alpha_1), \dots, T(\alpha_k), T(\alpha_{k+1}), \dots, T(\alpha_n))$

$= L(T(\alpha_{k+1}), \dots, T(\alpha_n))$

$= R(T)$ as $T(\alpha_1) = \dots = T(\alpha_k) = \overline{0}_V$.

Consider, $a_{k+1} T(\alpha_{k+1}) + \dots + a_n T(\alpha_n) = \overline{0}_V$

$\Rightarrow T(a_{k+1} \alpha_{k+1} + \dots + a_n \alpha_n) = \overline{0}_V$

$\Rightarrow \cancel{T}\,(a_{k+1}\alpha_{k+1} + \cdots + a_n\alpha_n) \in \operatorname{Ker}(T)$

$\Rightarrow \displaystyle\sum_{i=k+1}^{n} a_i\alpha_i = \sum_{j=1}^{k} (-a_j)\alpha_j$ as $\{\alpha_1, \ldots, \alpha_k\}$ is a basis of $\operatorname{Ker}(T)$, $a_i \in F$ $\forall\, i = 1, \ldots, n$

$\Rightarrow \displaystyle\sum_{i=1}^{n} a_i\alpha_i = \bar{0}_V$

$\Rightarrow a_i = 0 \quad \forall\, i = 1, \ldots, n$ as $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of V.

$\Rightarrow \{T(\alpha_{k+1}), \ldots, T(\alpha_n)\}$ is linearly independent in V.

So, $\dim(R(T)) = (n-k)$

$\dim(N(T)) = k$

$\Rightarrow$ Rank (T) + Nullity (T)

$= (n-k) + k = n = \dim(V)$.

(Proved)

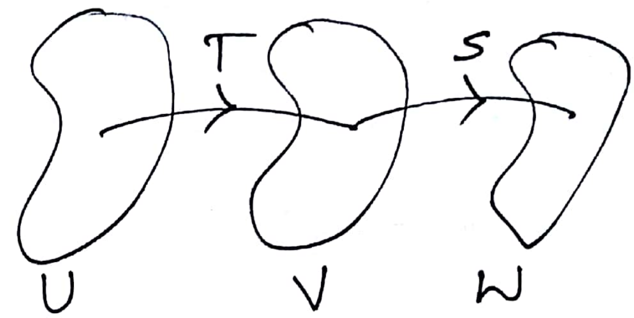
More on Linear mapping :

Let U, V, W be three vector spaces over the same field F.

$T : U \to V$

$S : V \to W$

be two linear-maps.



$\Rightarrow S \circ T : U \to W$ is also a linear mapping.

$S \circ T(a\alpha + b\beta)$ for $a, b \in F$, $\alpha, \beta \in U$

$= S\,(aT(\alpha) + bT(\beta))$

$= S(aT(\alpha)) + S\,(bT(\beta))$

$= a\,S(T(\alpha)) + b\,S(T(\beta))$

$= a\,S \circ T(\alpha) + b\,S \circ T(\beta).$

We write $ST = S \circ T$.

Inverse of a linear mapping:

Let $T : U \to V$ be a linear mapping.

Suppose T is one-to one and onto.

Then $\exists$ a map $T^{-1} : V \to U$ such that $T(\alpha) = \beta \Leftrightarrow T^{-1}(\beta) = \alpha$ for $\alpha \in U$, $\beta \in V$.

T^{-1} is a linear mapping.

Let $\beta_1, \beta_2 \in V$. Then $\exists\ \alpha_1, \alpha_2 \in U$ s.t. $T(\alpha_1) = \beta_1$, $T(\alpha_2) = \beta_2$

$\Rightarrow T(a\alpha_1 + b\alpha_2) = a\beta_1 + b\beta_2$

$T^{-1}(a\beta_1 + b\beta_2)$

$= a\alpha_1 + b\alpha_2$

Hence T^{-1} is a linear mapping.

Isomopphishm:

Let $T : U \to V$ be a linear mapping for U to V over the same field F.

Now T is called an isomorphism if T is one-to-one and onto or bijective

(*) We call two vector spaces U and V are isomorphic if there exists a bijective linear mapping $T: U \to V$ and we write $U \sim V$.

• Theorem: Let U and V be two vector space with finite dimensions. Then U and V are isomorphic iff $\dim U = \dim V$.

Proof: Let $U \sim V$. Then $\exists$ a bijective linear mapping $T: U \to V$.

T is one to one $\Rightarrow \ker(T) = \{\bar{0}_U\}$.

T is onto $\Rightarrow \operatorname{Im}(T) = V = R(T)$

By rank - nullity theorem,

$$\dim(R(T)) + \dim(\ker(T)) = \dim(U)$$

$$\Rightarrow \dim(V) + 0 = \dim(U)$$

$$\Rightarrow \dim(V) = \dim(U)$$

Conversely, let $\dim(U) = \dim(V)$.

Let $\{\alpha_1, \dots, \alpha_n\} = B_U$ be a basis of U

$\{\beta_1, \dots, \beta_n\} = B_V$ be a basis of V.

Consider a linear mapping $T: U \to V$ by $T(\alpha_1) = \beta_1, \ldots, T(\alpha_n) = \beta_n$.

So, $T(\alpha) = T\left(\sum_{i=1}^{n} a_i \alpha_i\right)$, for $\alpha \in U$

$$= \sum_{i=1}^{n} a_i T(\alpha_i)$$

$$= \sum_{i=1}^{n} a_i \beta_i \in V.$$

Let $\alpha \in \ker(T)$. Then $T(\alpha) = \bar{0}_V$

$$\Rightarrow \sum_{i=1}^{n} a_i \beta_i = \bar{0}_V$$

But B_V is a basis of V

$\Rightarrow a_i = 0 \quad \forall\, i = 1, 2, \ldots, n$

$$\Rightarrow \alpha = \sum_{i=1}^{n} a_i \alpha_i = \bar{0}_U$$

So, $\ker(T) = \{\bar{0}_U\} \Rightarrow T$ is one to one.

Also, by rank nullity theorem,

$$\dim(\operatorname{Im}(T)) + \dim(\ker(T)) = \dim(U) = \dim(V)$$

$\Rightarrow \dim(\operatorname{Im}(T)) = \dim(V)$ $[\because \dim(\ker(T)) = 0]$

Again $\operatorname{Im}(T)$ is a subspace of V.

$\Rightarrow \operatorname{Im}(T) = V \Rightarrow T$ is onto.

Hence T is a bijection $\Rightarrow U \sim V$.

Theorem: Let U be an n-dimensional vector space over the field F. Then $U \sim F^n$ where $F = \underbrace{F \times \cdots \times F}_{n\text{-times}}$.

So, $\dim_F(U) = n \Rightarrow U \sim F^n$.

Let $B = \{\alpha_1, \dots, \alpha_n\}$ be an ordered basis of U over F.

Then define, $T(\alpha) = (a_1, \dots, a_n)$

where $\alpha = \sum_{i=1}^{n} a_i \alpha_i$, $a_i \in F$ for $i = 1, \dots, n$.

Therefore $T : U \to F^n$ is a linear map.

We call $(a_1, \dots, a_n)$ as the co-ordinate of α with respect to B.

See, $T(a\alpha + b\beta)$

$= T\left(\sum_{i=1}^{n} (aa_i\alpha_i + bb_i\alpha_i)\right)$, $\alpha = \sum a_i\alpha_i$, $\beta = \sum b_i \alpha_i$

$= \sum_{i=1}^{n} T(aa_i\alpha_i + bb_i\alpha_i)$

$= a\sum_{i=1}^{n} a_i T(\alpha_i) + b\sum_{i=1}^{n} b_i T(\alpha_i)$

$= aT(\alpha) + bT(\beta)$.

So, T is a linear map.

Let $\alpha \in \ker(T)$. Then $T(\alpha) = (0, 0, \dots, 0)$

So, $\sum_{i=1}^{n} a_i \alpha_i = \alpha.$

$\Rightarrow T(\alpha) = (0, 0, \dots, 0) \Rightarrow a_1 = 0, \dots, a_n = 0$

$\Rightarrow \alpha = \bar{0}_V$

So, $\ker(T) = \{\bar{0}_V\}$. $\Rightarrow$ T is one to one.

Using rank-nullity theorem,

$$\dim(\mathrm{Im}(T)) + \dim(\ker(T)) = \dim(V) = n$$

$\Rightarrow \dim(\mathrm{Im}(T)) = n$

$\Rightarrow \mathrm{Im}(T) = F^n$.

$\Rightarrow$ T is onto.

So, $\boxed{V \sim F^n}$

Linear space of linear mappings:

Let U and V be two vector spaces over the same field F.

Let $T : U \to V$, $S : U \to V$ be two linear mappings.

We define $(T+S) : U \to V$ by,

$(T+S)(\alpha) = T(\alpha) + S(\alpha)$, $\forall \alpha \in U$.

Then $(T+S)(a\alpha + b\beta)$

$= T(a\alpha + b\beta) + S(a\alpha + b\beta)$

$= aT(\alpha) + bT(\beta) + aS(\alpha) + bS(\beta)$

$= a\big(T(\alpha) + S(\alpha)\big) + b\big(T(\beta) + S(\beta)\big)$

$= a(T+S)(\alpha) + b(T+S)(\beta)$.

Hence $(T+S)$ is linear.

Again $(cT)(\alpha+\beta)$

$= c\,T(\alpha+\beta)$

$= c\big(T(\alpha) + T(\beta)\big)$

$= (cT)(\alpha) + (cT)(\beta)$

Also, $(c\cdot T)(a\alpha) = c\cdot T(a\alpha)$

$$= c\, a T(\alpha)$$

$$= a\,(c\cdot T)(\alpha).$$

Therefore $(c\cdot T)$ is linear.

Let $L(U,V) = \{$ the set of all linear mappings with domain U and co-domain V over the same field $F \}$.

Then for all $S, T \in L(U,V)$

$$(T+S)(\alpha) = T(\alpha) + S(\alpha) \quad \forall\, \alpha \in U$$

$$(cT)(\alpha) = c\,T(\alpha) \quad \forall\, \alpha \in U, \forall\, c \in F.$$

Also we can see that

$T + 0 = T$ for all $T \in L$,

0 being the zero mapping.

Also define $-T : U \to V$ by

$$(-T)(\alpha) = -T(\alpha). \; \forall\, \alpha \in U.$$

Then $T + (-T) = 0 \quad \forall\, T \in L(U,V)$

Therefore $L(U,V)$ is a vector space over F under '+' and '$\cdot$'.

Matrix representation of linear mappings :

Let $T: U \to V$ be a linear mapping where $\dim_F(U) = n$, $\dim_F(V) = m$.

Let $B_1 = \{\alpha_1, \ldots, \alpha_n\}$, $B_2 = \{\beta_1, \ldots, \beta_m\}$ be two bases of U and V respectively

Then,

$$T(\alpha_1) = a_{11}\beta_1 + a_{21}\beta_2 + \cdots + a_{m1}\beta_m$$

$$T(\alpha_2) = a_{12}\beta_1 + a_{22}\beta_2 + \cdots + a_{m2}\beta_m$$

$$\vdots$$

$$T(\alpha_n) = a_{1n}\beta_1 + a_{2n}\beta_2 + \cdots + a_{mn}\beta_m.$$

Now for any $\alpha \in U$, $\alpha = \sum_{i=1}^{n} x_i \alpha_i$

$$T(\alpha) = \sum_{i=1}^{n} x_i T(\alpha_i)$$

$$= x_1(a_{11}\beta_1 + a_{21}\beta_2 + \cdots + a_{m1}\beta_m) + x_2(a_{12}\beta_1 + a_{22}\beta_2 + \cdots + a_{m2}\beta_m) + \cdots + x_n(a_{1n}\beta_1 + a_{2n}\beta_2 + \cdots + a_{mn}\beta_m)$$

$$= y_1\beta_1 + y_2\beta_2 + \cdots + y_m\beta_m$$

$$\Rightarrow \quad y_i = \sum_{j=1}^{n} x_j a_{ij}, \quad i = 1, \ldots, m.$$

So,
$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

$\Rightarrow \quad Ax = y \quad$ where $A = (a_{ij})_{\substack{i=1,\dots,m \\ j=1,\dots,n}}$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

A is said to be the matrix of T relative to the ordered basis B_1 and B_2.

Example: $T : \mathbb{R}^3 \to \mathbb{R}^2$ by

$$T(x_1, x_2, x_3) = (3x_1 - 2x_2 + x_3,\ x_1 - 3x_2 - 2x_3)$$

Let $B_1 = \{(1,0,0), (0,1,0), (0,0,1)\}$

$B_2 = \{(1,0), (0,1)\}$

$T(1,0,0) = (3,1) = 3\cdot(1,0) + 1\cdot(0,1)$

$T(0,1,0) = (-2,-3) = -2\cdot(1,0) + (-3)(0,1)$

$T(0,0,1) = (1,-2) = 1\cdot(1,0) + (-2)(0,1)$

Then $A = \begin{pmatrix} 3 & -2 & 1 \\ 1 & -3 & -2 \end{pmatrix}.$

See, $T(x_1, x_2, x_3) = \begin{pmatrix} 3 & -2 & 1 \\ 1 & -3 & -2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$

$= Ax.$

WEEK 7 LECTURE NOTE

Topics: - Rank of a matrix
- System of linear equations
- Row rank and Column rank
- Eigen value of a matrix.

Rank of a matrix:

Let A be a non-zero matrix of order $m \times n$. The rank of A is defined to be the greatest positive integer r such that A has at least one non-zero minor of order r.

Therefore $0 < \text{rank of } A \leq \min\{m, n\}$.

Example: Let $A = \begin{pmatrix} 2 & 3 & -1 & 1 \\ 3 & 0 & 4 & 2 \\ 6 & 9 & -3 & 3 \end{pmatrix}_{3\times 4}$

We define rank of zero matrix $= 0$

Here rank of $A \leq \min\{3, 4\} = 3$.

We can verify that every minor of order 3 is zero.

Thus, rank of $A < 3$

See a second order minor

$$\begin{vmatrix} 2 & 3 \\ 3 & 0 \end{vmatrix} = -9 \neq 0.$$

Therefore, rank of $A = 2$.

- **Square matrix:**

Let $A = (a_{ij})_{n\times n}$ be a square matrix of order n.

If rank of $A = n$ then $\det(A) = |A| \neq 0$.

In this case we say A is a non-singular matrix.

If A is non-singular then $\exists\ B = (b_{ij})_{n\times n}$ such that $AB = I_{n\times n}$ (identity matrix)

$$\Rightarrow AB = BA = I_{n\times n}$$

$$\Rightarrow B = A^{-1}$$

We know,

$$A \cdot (\operatorname{adj} A) = (\operatorname{adj} A)\cdot A = I_n |A|$$

$$\Rightarrow \quad A \cdot \frac{\operatorname{adj} A}{|A|} = I_n = \frac{\operatorname{adj} A}{|A|} \cdot A$$

$$\Rightarrow \quad A^{-1} = \frac{\operatorname{adj} A}{|A|}, \quad |A| \neq 0.$$

Example: Let $A = \begin{pmatrix} 1 & 0 & 1 \\ 3 & 4 & 5 \\ 2 & 3 & 4 \end{pmatrix}$

$$|A| = 3 \neq 0$$

$$\operatorname{adj} A = \begin{pmatrix} \begin{vmatrix} 4 & 5 \\ 3 & 4 \end{vmatrix} & -\begin{vmatrix} 0 & 1 \\ 3 & 4 \end{vmatrix} & \begin{vmatrix} 0 & 1 \\ 4 & 5 \end{vmatrix} \\ -\begin{vmatrix} 3 & 5 \\ 2 & 4 \end{vmatrix} & \begin{vmatrix} 1 & 1 \\ 2 & 4 \end{vmatrix} & -\begin{vmatrix} 1 & 1 \\ 3 & 5 \end{vmatrix} \\ \begin{vmatrix} 3 & 4 \\ 2 & 3 \end{vmatrix} & -\begin{vmatrix} 1 & 0 \\ 2 & 3 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 3 & 4 \end{vmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 3 & -4 \\ -2 & 2 & -2 \\ 1 & -3 & 4 \end{pmatrix}$$

so, $$A^{-1} = \frac{\operatorname{adj} A}{|A|} = \begin{pmatrix} 1/3 & 1 & -4/3 \\ -2/3 & 2/3 & -2/3 \\ 1/3 & -1 & 4/3 \end{pmatrix}$$

How to find the rank of A ?

- Elementary operations :

An elementary operation on a matrix A over a field F is an operation of the following three types –

1. Exchange of two rows (or columns)

Notation → $\boxed{\begin{matrix} R_i \leftrightarrow R_j \\ C_i \leftrightarrow C_j \end{matrix}}$ (for rows) (for columns)

where R_i = i^{th} row of A

C_i = i^{th} column of A

2. Multiplication of a row (or column) by a non-zero scalar α in F.

Notation → $\boxed{\begin{matrix} R_i \leftarrow \alpha R_i \\ C_i \leftarrow \alpha C_i \end{matrix}}$ (for rows) (for columns)

3. Addition of a scalar multiple of one row (or column) to another row (or column)

Notation → $\boxed{\begin{matrix} R_i \leftarrow R_i + \alpha R_j \\ C_i \leftarrow C_i + \alpha C_j \end{matrix}}$ (for rows) (for columns)

• **Example:** Let $A = \begin{pmatrix} 2 & 0 & 4 & 2 \\ 3 & 2 & 6 & 5 \\ 5 & 2 & 10 & 7 \\ 0 & 3 & 2 & 5 \end{pmatrix}_{4\times 4}$

$$\xrightarrow{R_1 \leftarrow \frac{1}{2}R_1} \begin{pmatrix} 1 & 0 & 2 & 1 \\ 3 & 2 & 6 & 5 \\ 5 & 2 & 10 & 7 \\ 0 & 3 & 2 & 5 \end{pmatrix} \xrightarrow{R_2 \leftarrow R_2 - 3R_1} \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 2 \\ 5 & 2 & 10 & 7 \\ 0 & 3 & 2 & 5 \end{pmatrix}$$

$= B$ (say)

(*) If B can be derived from A by using only row elementary operations then we say B is row equivalence to A and write it as $A \sim B$.
Similar, for the case of column equivalence matrices.

$$B \xrightarrow{R_3 - 5R_1} \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & 2 \\ 0 & 3 & 2 & 5 \end{pmatrix}$$

$$\xrightarrow{R_3 \leftarrow R_3 - R_2} \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 3 & 2 & 5 \end{pmatrix}$$

$$\xrightarrow{R_3 \leftrightarrow R_4} \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 2 \\ 0 & 3 & 2 & 5 \\ 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(using row elementary operations)

We will show that if $A \sim B$ then rank of A = rank of B.

Then, from the last matrix we see that rank of the given matrix is 3.

Elementary matrices :

An $n \times n$ matrix obtained by applying a single elementary row operation on $I_{n\times n}$ is said to be an elementary matrix of order n.

Therefore, there are three types of elementary matrices.

1. Apply $\underline{R_i \leftrightarrow R_j \text{ on } I_n}$
   Notation → $\boxed{E_{ij}}$

2. Apply $\underline{R_i \leftarrow \alpha R_i \text{ on } I_n}$
   Notation → $\boxed{E_{\alpha i} \text{ or } E_i(\alpha)}$

3. Apply $\underline{R_i \leftarrow R_i + \alpha R_j \text{ on } I_n}$
   Notation → $\boxed{E_{i+\alpha j} \text{ or } E_{ij}(\alpha)}$

We can check that applying $R_i \leftrightarrow R_j$ on A is equivalent to multiply E_{ij} with A, i.e.,

$$\boxed{R_i \leftrightarrow R_j \text{ on } A \equiv E_{ij} A}$$

Similarly,

$$\boxed{R_i \leftarrow \alpha R_i \text{ on } A \equiv E_i(\alpha) A}$$

$$\boxed{R_i \leftarrow R_i + \alpha R_j \text{ on } A \equiv E_{ij}(\alpha) A}$$

- Thus, $\boxed{A \sim B \Rightarrow B = E_1 E_2 \cdots E_l A}$

where E_i, $i = 1, \ldots, l$, are elementary matrices.

- We note that an elementary matrix of any of the three types can also be obtained by applying an elementary column operation on I.

- Also we note that elementary matrices are non-singular matrices.

So, $A \sim B \Rightarrow B = E_1 E_2 \cdots E_l A$

$$= PA$$

where $P = E_1 \cdots E_l$ is a non-singular matrix. Therefore, $\boxed{\text{rank of } B = \text{rank of } A}$

- **Row equivalent:** An $m \times n$ matrix B is row equivalent to $m \times n$ matrix A iff $B = PA$ for some non-singular matrix P of order m.

- **Column equivalent:** An $m \times n$ matrix B is column equivalent to $m \times n$ matrix A iff $B = AQ$ for some non-singular matrix Q of order n.

  As in the case of $B = PA$, we apply elementary column operations from the right of A, i.e,

$$A E_1 \cdots E_t = B \Rightarrow AQ = B$$

where $Q = E_1 \cdots E_t$.

- **Equivalent matrices:** An $m \times n$ matrix B is equivalent to an $m \times n$ matrix A iff $B = PAQ$ where P, Q are non-singular matrices.

  In this case rank of A = rank of B.

- If rank of $A = r$ then we can find non-singular matrices P, Q such that $PAQ = \left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$

The inverse of a non-singular matrix can be calculated by using elementary matrices. Let $|A| \neq 0$ and A is of order n. Then A is equivalent to I_n.

So, for suitable elementary matrices E_i,

$$\boxed{E_r E_{r-1} \cdots E_2 E_1 A = I_n}$$

$$\Rightarrow \boxed{E_r E_{r-1} \cdots E_2 E_1 I_n = A^{-1}}$$

Therefore if a (finite) sequence of elementary row operations applied successively on A reduces A to I_n, the same sequence of operations applied on I_n will reduce I_n to A^{-1}.

This gives us technique for finding A^{-1} described below by an example.

Let $A = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 4 & 4 \\ 3 & 3 & 7 \end{pmatrix}$

Consider

$$(A \mid I_3) = \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 2 & 4 & 4 & 0 & 1 & 0 \\ 3 & 3 & 7 & 0 & 0 & 1 \end{array}\right)$$

$$(A \mid I_3) \xrightarrow[R_3 \leftarrow R_3 - 3R_1]{R_2 \leftarrow R_2 - 2R_1} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & -2 & 1 & 0 \\ 0 & 0 & 1 & -3 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_2 \leftarrow \frac{1}{2} R_2} \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1/2 & 0 \\ 0 & 0 & 1 & -3 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_1 \leftarrow R_1 - R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & 2 & 2 & -1/2 & 0 \\ 0 & 1 & 0 & -1 & 1/2 & 0 \\ 0 & 0 & 1 & -3 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{R_1 \leftarrow R_1 - 2R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 8 & -1/2 & -2 \\ 0 & 1 & 0 & -1 & 1/2 & 0 \\ 0 & 0 & 1 & -3 & 0 & 1 \end{array}\right)$$

$$= (I_3 \mid A^{-1})$$

Therefore $A^{-1} = \begin{pmatrix} 8 & -\frac{1}{2} & -2 \\ -1 & 1/2 & 0 \\ -3 & 0 & 1 \end{pmatrix}$

Fully Reduced Normal form :-

If ~~A~~ a matrix is in fully reduced normal form then it is in (i) row reduced echelon form, (ii) column reduced ~~echelon~~ echelon form such that,

(i) No zero row is followed by a non-zero row.

(ii) No zero column is followed by a non-zero column.

(iii) leading 1 in each row is the only non-zero ~~ele~~. element in that row

(iv) leading 1 in each column is the only non-zero element in that column.

(v) leading 1 in the k^{th} row is the leading 1 in the k^{th} column.

- **Example:** Fully reduced normal form.

$$A = \begin{pmatrix} 0 & 0 & 1 & 2 & 1 \\ 1 & 3 & 1 & 0 & 3 \\ 2 & 6 & 4 & 2 & 8 \\ 3 & 9 & 4 & 2 & 10 \end{pmatrix}$$

$$\xrightarrow{R_1 \leftrightarrow R_2} \begin{pmatrix} 1 & 3 & 1 & 0 & 3 \\ 0 & 0 & 1 & 2 & 1 \\ 2 & 6 & 4 & 2 & 8 \\ 3 & 9 & 4 & 2 & 10 \end{pmatrix} \xrightarrow[R_4 - 3R_1]{R_3 - 2R_1} \begin{pmatrix} 1 & 3 & 1 & 0 & 3 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix}$$

$$\xrightarrow[\substack{R_3 - 2R_2 \\ R_4 - R_2}]{R_1 - R_2} \begin{pmatrix} 1 & 3 & 0 & -2 & 2 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{-\frac{1}{2}R_3} \begin{pmatrix} 1 & 3 & 0 & -2 & 2 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(row reduced echelon form)

$$\xrightarrow[C_5 - 2C_1]{C_2 - 3C_1} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_5 - C_3} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\xrightarrow{C_{23}} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_{34}} \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

(row reduced normal form)

[Here we shorten the notation as →

$R_3 \leftarrow R_3 - 2R_1$ by $\underline{R_3 - 2R_1}$

$C_2 \leftrightarrow C_3$ by $\underline{C_{23}}$]

• **Example:** Reduce the matrix $A=\begin{pmatrix}2&1&2\\1&0&1\\1&1&1\end{pmatrix}$ to the fully reduced normal form and find non-singular matrices P, Q such that PAQ is the fully reduced normal form.

$$A=\begin{pmatrix}2&1&2\\1&0&1\\1&1&1\end{pmatrix}\xrightarrow{R_{12}}\begin{pmatrix}1&0&1\\2&1&2\\1&1&1\end{pmatrix}\xrightarrow[R_3-R_1]{R_2-2R_1}\begin{pmatrix}1&0&1\\0&1&0\\0&1&0\end{pmatrix}$$

$$\xrightarrow{R_3-R_2}\begin{pmatrix}1&0&1\\0&1&0\\0&0&0\end{pmatrix}\xrightarrow{C_3-C_1}\left(\begin{array}{cc|c}1&0&0\\0&1&0\\\hline 0&0&0\end{array}\right)=R \text{ (say)}$$

$\Rightarrow$ Rank $(A)=2\neq 3 \Rightarrow A$ is singular

So, $R=(C_3-C_1)(R_3-R_2)(R_3-R_1)(R_2-2R_1)(R_{12})\,A$

$$=E_{32}(-1)\,E_{31}(-1)\,E_{21}(-2)E_{12}A\,\{E_{31}(-1)\}^T$$

$$=PAQ$$

where $P=E_{32}(-1)\;E_{31}(-1)\;E_{21}(-2)\;E_{12}$

$Q=(E_{31}(-1))^T=E_{13}(-1)$

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\xrightarrow{R_3-R_2}\begin{pmatrix}1&0&0\\0&1&0\\0&-1&1\end{pmatrix}=E_{32}(-1)$$

similarly, $E_{31}(-1)=\begin{pmatrix}1&0&0\\0&1&0\\-1&0&1\end{pmatrix}$

$E_{21}(-2)=\begin{pmatrix}1&0&0\\-2&1&0\\0&0&1\end{pmatrix}$, $E_{12}=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$

$$E_{13}(-1) = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

So, $$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 1 \\ -1 & 1 & 1 \end{pmatrix}$$ (check calculation)

$$Q = E_{13}(-1) = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$ (check)

Therefore, ~~...~~ $R = PAQ$ where

$P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -2 & 1 \\ -1 & 1 & 1 \end{pmatrix}$, $Q = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ are

non-singular matrices.

• **Exercise:** Reduce A into fully reduced normal form R s.t. $PAQ = R$

where $A = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 2 & 1 & 4 & 6 \\ 3 & 0 & 7 & 9 \end{pmatrix}$, $P_{3\times 3}$, $Q_{4\times 4}$ are non-singular.

Ans: $R = (I_3 \mid 0)$, $P = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 0 & 1 \\ -2 & 1 & 0 \end{pmatrix}$,

$$Q = \begin{pmatrix} 1 & -2 & 0 & -3 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(check).

Congruence operations and Congruence of matrices :-

Let $A_{n\times n}$ symmetric matrix.

$$\left.\begin{array}{l} \text{congruence operations} \to R_{ij} / C_{ij}, \\ \qquad R_i \pm \alpha R_j / C_i \pm \alpha C_j \\ \qquad \alpha R_i / \alpha C_i \end{array}\right\}$$

$$A \xrightarrow[\text{operations}]{\text{congruence}} \text{diagonal matrix} = D = \begin{pmatrix} I_m & & \\ & -I_{r-m} & \\ O & & 0 \end{pmatrix}$$

where $\boxed{\begin{array}{l} r = \text{rank of } A \\ 2m - r = \text{signature of } A \end{array}}$

$\boxed{\begin{array}{l} A \text{ is congruent to } B \text{ if} \\ \text{rank of } A = \text{rank of } B \text{ and} \\ \text{signature of } A = \text{signature of } B. \end{array}}$

• Example: let $A = \begin{pmatrix} 2 & 4 & 3 \\ 4 & 6 & 3 \\ 3 & 3 & 1 \end{pmatrix}$ (check)

Then $A \xrightarrow[\text{operations}]{\text{congruence}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = B$ (say)

So, rank (A) = 3, signature of (A) $= 2\cdot 2 - 3 = 1$

where $m = 2$, $r = 3$.

• Exercise: $A = \begin{pmatrix} 2 & -2 & 0 \\ -2 & 1 & -2 \\ 0 & -2 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 4 & 1 \\ 4 & 9 & 4 \\ 1 & 4 & 2 \end{pmatrix}$

Show A is ~~congrgatent~~ congruent to B.

Homogeneous System :

- $Ax = 0$, $A_{m \times n}$ matrix, $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

m equations in n unknowns.

- $(0, 0, \dots, 0) \rightarrow$ trivial solution.

- Solution space of a homogeneous system $Ax = 0$ ~~forms~~ over a field F forms a subspace of F^n where $A_{m \times n}$ and $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

- $X(A)$ = sol. space of $Ax = 0$ with $(0, 0, \dots, 0)$ as a null vector.

- $\text{Rank}(A) + \text{Rank}(X(A)) = n$

where $\text{Rank}(X(A)) = \dim(X(A))$
$= \text{kernel of } A.$

- $AX = 0$, m equations in n unknowns

if $m < n$, then $AX = 0$ has non-trivial solutions (infinite solutions exist)

Example:

$$x + 2y + z - 3w = 0$$
$$2x + 4y + 3z + w = 0$$
$$3x + 6y + 4z - 2w = 0 \quad , \boxed{\begin{array}{l} m = 3 \\ n = 4 \end{array}}$$

$$A = \begin{pmatrix} 1 & 2 & 1 & -3 \\ 2 & 4 & 3 & 1 \\ 3 & 6 & 4 & -2 \end{pmatrix} \xrightarrow[R_3 - 3R_1]{R_2 - 2R_1} \begin{pmatrix} 1 & 2 & 1 & -3 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 1 & 7 \end{pmatrix}$$

$$\xrightarrow{R_3 - R_2} \begin{pmatrix} 1 & 2 & 1 & -3 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_1 - R_2} \begin{pmatrix} 1 & 2 & 0 & -10 \\ 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(row reduced echelon form)

Equivalent system

$$\left.\begin{array}{r} x + 2y - 10w = 0 \\ z + 7w = 0 \end{array}\right\} \Rightarrow \begin{array}{l} x = 10w - 2y \\ z = -7w \end{array}$$

Let $w = \alpha$, $y = \beta$ be any reals.

So, $(x, y, z, w) = (10\alpha - 2\beta, \beta, -7\alpha, \alpha)$

$= \alpha(10, 0, -7, 1) + \beta(-2, 1, 0, 0)$

$\in L(\{(10, 0, -7, 1), (-2, 1, 0, 0)\})$

$= X(A)$ = sol. space.

Rank $(X(A)) = 2$, Rank $(A) = 2$

Thus, Rank(A) + Rank $(X(A)) = 2 + 2 = 4 = n$

- Note: $A_{n\times n}$, $AX = 0$ i.e, n equations, n unknowns

It has non-zero solutions iff rank of $(A) < n$, i.e, $\boxed{\begin{array}{l} \det(A) = 0 \\ \Rightarrow A \text{ is singular} \end{array}}$

and # of solutions is infinite.

System of linear Equations:

Non-Homogeneous system: $Ax = b$, $A_{m\times n}$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $b(\neq 0) \in F^m$

Example:

$$x_1 + x_2 = 4$$
$$x_2 - x_3 = 1$$
$$2x_1 + x_2 + 4x_3 = 7$$

Then we can write this system as

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 2 & 1 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \\ 7 \end{pmatrix}$$

$$\Rightarrow \quad Ax = b$$

where $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 2 & 1 & 4 \end{pmatrix}$, $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, $b = \begin{pmatrix} 4 \\ 1 \\ 7 \end{pmatrix}$

Suppose we have $Ax = b$ where $|A| = \det(A) \neq 0$. Then x can be written as $x = A^{-1}b$ and we say that solution is unique.

Augmented matrix :

Given $Ax = b$, the augmented matrix is given by $\bar{A} = (A \mid b)$

Example :

From the above example we have

$$\bar{A} = (A \mid b) = \left(\begin{array}{ccc|c} 1 & 1 & 0 & 4 \\ 0 & 1 & -1 & 1 \\ 2 & 1 & 4 & 7 \end{array}\right)$$

Apply elementary row operations on $\bar{A}$.

$$\bar{A} \xrightarrow{R_3 \leftarrow R_3 - 2R_1} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 4 \\ 0 & 1 & -1 & 1 \\ 0 & -1 & 4 & -1 \end{array}\right)$$

$$\xrightarrow[R_3 \leftarrow R_3 + R_2]{R_1 \leftarrow R_1 - R_2} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 3 & 0 \end{array}\right)$$

$$\xrightarrow{R_3 \leftarrow \frac{1}{3}R_3} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

$$\xrightarrow{R_2 \leftarrow R_2 + R_3} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

Therefore $\text{Rank}(A) = \text{Rank}(\bar{A}) = 3$

Since, $\text{Rank}(A) = 3 \Rightarrow A^{-1}$ exists.

So, $x = A^{-1} b$

$$\Rightarrow x = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$$

i.e., $x_1 = 3, \; x_2 = 1, \; x_3 = 0$

• **Theorem:** A necessary and sufficient condition for a non-homogeneous system $Ax = b$ to be consistent (that is, it has a solution) is

$$\boxed{\text{rank of } A = \text{rank of } \bar{A}}$$

• **Remark:** If $\text{Rank}(A) \neq \text{Rank}(\bar{A})$ then the system $Ax = b$ does not have a solution.

Consider the system $Ax = b$, $A = (a_{ij})_{m \times n}$

Then the following holds $\rightarrow$

Consistent if rank of A = rank of $\bar{A}$	inconsistent
(i) <u>Unique solution</u> if (a) $m = n$ and $\text{Rank}(A) = \text{Rank}(\bar{A}) = n$ (b) $m > n$ and $\text{Rank}(A) = \text{Rank}(\bar{A}) = n$	no solution when rank of $A \neq$ rank of $\bar{A}$

(ii) <u>infinite solution</u>

if (a) $m = n$

and $\text{Rank}(A) = \text{Rank}(\bar{A}) < n$

(b) $m < n$

and $\text{Rank}(A) = \text{Rank}(\bar{A}) \leq m < n$

(c) $m > n$

and $\text{Rank}(A) = \text{Rank}(\bar{A}) < n$

Example :

Consider the system

$$x_1 + 2x_2 - x_3 = 10$$
$$-x_1 + x_2 + 2x_3 = 2$$
$$2x_1 + x_2 - 3x_3 = 2$$

So,
$$\underbrace{\begin{pmatrix} 1 & 2 & -1 \\ -1 & 1 & 2 \\ 2 & 1 & -3 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}}_{x} = \underbrace{\begin{pmatrix} 10 \\ 2 \\ 2 \end{pmatrix}}_{b}$$

$$\bar{A} = \left(\begin{array}{ccc|c} 1 & 2 & -1 & 10 \\ -1 & 1 & 2 & 2 \\ 2 & 1 & -3 & 2 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 1 & 2 & -1 & 10 \\ 0 & 3 & 1 & 12 \\ 0 & -3 & -1 & -18 \end{array}\right)$$

$$\longrightarrow \left(\begin{array}{ccc|c} 1 & 2 & -1 & 10 \\ 0 & 3 & 1 & 12 \\ 0 & 0 & 0 & -6 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & -1 & 10 \\ 0 & 1 & 1/3 & 4 \\ 0 & 0 & 0 & -6 \end{array}\right)$$

$$\rightarrow \left(\begin{array}{ccc|c} 1 & 0 & -5/3 & 2 \\ 0 & 1 & 1/3 & 4 \\ 0 & 0 & 0 & -6 \end{array}\right)$$

So, rank of $A = 2$

rank of $\bar{A} = 3 \neq$ rank of A.

Hence the system has no solution.

• Example :

Consider,
$$x + 2y + z = 1$$
$$3x + y + 2z = 3$$
$$x + 7y + 2z = 1$$

So, $\bar{A} = \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 3 & 1 & 2 & 3 \\ 1 & 7 & 2 & 1 \end{array}\right)$

$\sim \left(\begin{array}{ccc|c} 1 & 0 & 3/5 & 1 \\ 0 & 1 & 1/5 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$

The equivalent system is

$$\left.\begin{aligned} x_1 + \frac{3}{5}x_3 &= 1 \\ x_2 + \frac{1}{5}x_3 &= 0 \end{aligned}\right\} \Rightarrow \begin{aligned} x_1 &= 1 - \frac{3}{5}x_3 \\ x_2 &= -\frac{1}{5}x_3 \end{aligned}$$

For any $x_3 \in \mathbb{R}$, $\left(1 - \frac{3}{5}x_3, \frac{-1}{5}x_3, x_3\right)$

is a solution.

Hence the system has infinitely many solution.

• Example: Determine the condition for which the following system has (i) only one solution (ii) no sol., (iii) infinite sol.

$$x + y + z = 1$$
$$x + 2y - z = b$$
$$5x + 7y + az = b^2, \qquad A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & -1 \\ 5 & 7 & a \end{pmatrix}, \begin{pmatrix} 1 \\ b \\ b^2 \end{pmatrix}$$

$$\bar{A} = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & b \\ 5 & 7 & a & b^2 \end{array}\right), \quad \det(A) = a - 1 \neq 0 \text{ iff } a \neq 1$$

case 1: $(a \neq 1)$ Rank $(\bar{A})$ = Rank $(A) = 3$ if $a \neq 1$

$\boxed{\text{Unique Solution if } a \neq 1}$

case 2: $(a = 1)$

$$\bar{A} = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 2 & -1 & b \\ 5 & 7 & 1 & b^2 \end{array}\right)$$

$$\xrightarrow[R_3 - 5R_1]{R_2 - R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & -2 & b-1 \\ 0 & 2 & -4 & b^2-5 \end{array}\right) \xrightarrow[R_3 - 2R_2]{R_1 - R_2} \left(\begin{array}{ccc|c} 1 & 0 & 3 & 2-b \\ 0 & 1 & -2 & b-1 \\ 0 & 0 & 0 & b^2-2b-3 \end{array}\right)$$

case 2.1: $(b^2 - 2b - 3 \neq 0)$ Then Rank$(\bar{A}) = 3$

Rank $(A) = 2$ $\neq$ Rank $(\bar{A})$

if $b^2 - 2b - 3 \neq 0$

$\boxed{\text{No Solution if } a = 1, b \neq -1, 3}$

case 2.2: $(b^2 - 2b - 3 = 0)$ Rank$(\bar{A})$ = Rank$(A) = 2$

$\boxed{\text{Infinite solution if } b^2 - 2b - 3 = 0 \Rightarrow b = -1, 3 \text{ and } a = 1}$

Row and Column Rank :

Consider $A = (a_{ij})_{m\times n}$, $a_{ij} \in F$

where F is a field.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

So, $R_i = (a_{i1}\ a_{i2}\ \cdots\ a_{in})$ is

the i^{th} row of A, $i = 1, \ldots, m$

$c_j = (a_{1j}\ a_{2j}\ \cdots\ a_{mj})$ is

the j^{th} column of A, $j = 1, \ldots, n$

$$\Rightarrow \quad R_i \in F^n = \underbrace{F \times \cdots \times F}_{n \text{ times}}, \quad i = 1, \ldots, m$$

$$c_j \in F^m = \underbrace{F \times \cdots \times F}_{m \text{ times}}, \quad j = 1, \ldots, n$$

Let $R = \{R_1, R_2, \ldots, R_m\} \subseteq F^n$

$L(R) = L(\{R_1, \ldots, R_m\})$ is

a subspace of F^n where

$L(R)$ is the set of all vectors of F^n which are linear combin-ation of the row vectors $R_1, \dots, R_m$.

$L(R)$ is called the <u>row space</u> of A.

Similarly,

$L(C) = L(\{C_1, \dots, C_n\})$ is a subspace of F^m and $L(C)$ is called the <u>column space</u> of A.

Denote, $R(A) = L(R) \subseteq F^n$

$\Rightarrow \dim(R(A)) \le n.$

Define $\boxed{\text{Row rank of } A = \dim(R(A))}$

Denote, $C(A) = L(C) \subseteq F^m$

$\Rightarrow \dim(C(A)) \le m.$

Define, $\boxed{\begin{array}{l}\text{column rank of } A \\ = \dim(C(A))\end{array}}$

● **Example:** Let $A = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 3 & 2 & 6 & 9 \\ 1 & 1 & 2 & 6 \end{pmatrix}$

$R(A) = L(\{(2,1,4,3), (3,2,6,9), (1,1,2,6)\})$.

Apply elementary row operations on A.

$$A \xrightarrow{R_1 \leftrightarrow R_3} \begin{pmatrix} 1 & 1 & 2 & 6 \\ 3 & 2 & 6 & 9 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\xrightarrow[R_3 \leftarrow R_3 - 2R_1]{R_2 \leftarrow R_2 - 3R_1} \begin{pmatrix} 1 & 1 & 2 & 6 \\ 0 & -1 & 0 & -9 \\ 0 & -1 & 0 & -9 \end{pmatrix}$$

$$\xrightarrow{R_3 \leftarrow R_3 - R_2} \begin{pmatrix} 1 & 1 & 2 & 6 \\ 0 & -1 & 0 & -9 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & -3 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$R(A) = L(\{(1,0,2,-3), (0,1,0,9)\})$

$\dim(R(A)) = 2$

$\Rightarrow$ row rank of $A = 2$.

To get the column rank of A, consider A^t and apply elementary row operations on A^t.

$$A^t = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 1 \\ 4 & 6 & 2 \\ 3 & 9 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$C(A) = L(\{(1,0,-1), (0,1,1)\})$$

$$\Rightarrow \dim(C(A)) = 2$$

So column rank of $A = 2$

- Some results on $A = (a_{ij})_{m\times n}$

1. row rank of $A \leq n$
2. column rank of $A \leq m$
3. row rank = column rank = rank of A
4. rank of $(AB) \leq \min\{$rank of A, rank of B$\}$
5. rank of $(A+B) \leq$ rank of A + rank of B.

● Proof of result 4 :

Let $A = (a_{ij})_{m\times n}$, $B = (b_{ij})_{n\times p}$

Rows of $B = \{\beta_1, \beta_2, \dots, \beta_n\}$

Rows of $AB = \{l_1, l_2, \dots, l_m\}$

Then $l_1 = a_{11}\beta_1 + a_{12}\beta_2 + \dots + a_{1n}\beta_n$

$l_2 = a_{21}\beta_1 + a_{22}\beta_2 + \dots + a_{2n}\beta_n$

$\dots \quad \dots \quad \dots$

$l_m = a_{m1}\beta_1 + a_{m2}\beta_2 + \dots + a_{mn}\beta_n.$

$\Rightarrow L\{l_1, \dots, l_m\} \subset L\{\beta_1, \dots, \beta_n\}$

$\Rightarrow R(AB)$ is a subspace of $R(B)$.

$\Rightarrow$ row rank of $AB \le$ row rank of B.

$\Rightarrow$ rank of $AB \le$ rank of B —(i)

Consider the product $B^t A^t$.

Then, using (i), rank of $B^t A^t \le$ rank of A^t

$\Rightarrow$ rank of $(AB)^t \le$ rank of A^t

$\Rightarrow$ rank of $AB \le$ rank of A ...(ii)

Combining (i) and (ii), rank of (AB) $\le \min\{\text{rank of } A, \text{rank of } B\}$.

Proof of result 5 :

Apply the same strategy as in the proof of result 4, we can show,

row rank of $(A+B) \leq$ row rank of A + row rank of B

$\Rightarrow$ rank of $(A+B) \leq$ rank of A + rank of B.

Eigen value of a matrix :

Characteristic equation →

let $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}_{n\times n}$

$$\det(A - x I_n) = \begin{vmatrix} a_{11}-x & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-x & \cdots & a_{2n} \\ \cdots & & & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-x \end{vmatrix}$$

$$= \psi_A(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n$$

(a polynomial of degree n.)

- $\psi_A(x)$ is called the characteristic polynomial ~~equation~~ of A.

- $c_r = (-1)^{n-r}$ [sum of the principle minors of A of order r]

See, $\boxed{c_0 = (-1)^n}$

$c_1 = (-1)^{n-1}(a_{11} + a_{22} + \cdots + a_{nn})$

$\Rightarrow \boxed{c_1 = (-1)^{n-1} \text{trace}(A)}$

$$\boxed{c_n = \det(A)}$$

Example: let $A = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix}$

$$\psi_A(x) = \det(A - xI_2) = \begin{vmatrix} 2-x & 1 \\ 3 & 5-x \end{vmatrix} = 0$$

$$\Rightarrow (2-x)(5-x) - 3 = 0$$

$$\Rightarrow x^2 - (5+2)x + 10 - 3 = 0$$

$$\Rightarrow x^2 - 7x + 7 = 0 \quad (\psi_A(x) = 0)$$

See, $\operatorname{trace}(A) = c_1 = 7$

$\det(A) = c_n = 7$

$\psi_A(x) = 0$ is called the <u>characteristic equation of A.</u>

Cayley–Hamilton theorem :–

Every square matrix satisfies its own characteristic equation, i.e.;

$$\psi_A(A) = 0$$

• **Example**: $A = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix}$

Then, $\Psi_A(x) = x^2 - 7x + 7$

By Cayley-Hamilton th,

$$\boxed{A^2 - 7A + 7I_2 = 0}$$

We can get inverse using this equation.

$$A^2 - 7A + 7I_2 = 0$$

$$\Rightarrow A(A - 7I_2) = -7I_2$$

$$\Rightarrow A \cdot \frac{-1}{7}(A - 7I_2) = I_2$$

So, $A^{-1} = -\frac{1}{7}(A - 7I_2)$

$$= \begin{pmatrix} 5/7 & -1/7 \\ -3/7 & 2/7 \end{pmatrix}$$

• **Example**: Using Cayley-Hamilton th. to find A^{50}, where $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$$\Psi_A(x) = \begin{vmatrix} 1-x & 1 \\ 0 & 1-x \end{vmatrix} = x^2 - 2x + 1$$

By cayley Hamilton th.

$$A^2 - 2A + I_2 = 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow \quad A^2 - A = A - I_2$$

$$A^3 - A^2 = A^2 - A = A - I_2$$

$$A^4 - A^3 = A^3 - A^2 = A - I_2$$

$$\cdots \qquad \cdots$$

$$A^{50} - A^{49} = A^{49} - A^{48} = A - I_2$$

Adding, $\quad A^{50} - A = 49(A - I_2)$

$$\Rightarrow \quad A^{50} = 49(A - I_2) + A$$

$$= 50A - I_2$$

$$= \begin{pmatrix} 1 & 50 \\ 0 & 1 \end{pmatrix}$$

- Eigen value of a matrix →

Let $A = (a_{ij})_{n \times n}$. Then the roots of $\psi_A(x)$ are the eigen values of A.

If λ is an eigen value then we say λ has algebraic multiplicity r if $\boxed{\psi_A(x) = (x-\lambda)^r \phi(x)}$ where $\phi(\lambda) \neq 0$.

We also call λ an r-fold eigen value of A.

Example: Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$$\psi_A(x) = \begin{vmatrix} 0-x & -1 \\ 1 & 0-x \end{vmatrix} = x^2+1$$

So, $\psi_A(x) = 0 \Rightarrow x^2+1=0$
$\Rightarrow x = \pm i$ where $i = \sqrt{-1}$

So, A has complex eigenvalues $\pm i$.

Note:

1. If $A_{n\times n}$ is a real symmetric matrix then the eigenvalues of A are all real numbers.

2. Let $\psi_A(x) = c_0 x^n + c_1 x^{n-1} + \dots + c_n$
$= \det(A - x I_n)$

then $c_r = (-1)^{n-r}.$ [sum of all principle minors of order r]

Then, $c_0 = (-1)^n$

$c_1 = (-1)^{n-1} [a_{11} + \cdots + a_{nn}]$

where $A = (a_{ij})_{n \times n}$

$c_n = \det(A)$.

If $\lambda_1, \dots, \lambda_n$ are all the eigen-values of A then, these are all the roots of $\psi_A(x)$.

Therefore, $\lambda_1 \lambda_2 \cdots \lambda_n = (-1)^n \dfrac{c_n}{c_0}$

$= \dfrac{\det(A)}{(-1)^n} (-1)^n$

$= \det(A)$

So, $\boxed{\lambda_1 \lambda_2 \cdots \lambda_n = \det(A)}$

product of all eigenvalues of A $= \det(A)$.

If $\det(A) = 0 \Rightarrow \lambda_i = 0$ for some $i = 1, \dots, n$

For singular matrix ($|A| = 0$) we have some of eigen value of A must be zero.

3. If A is a diagonal matrix, let

$$A = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix}$$

then $$\varphi_A(x) = \begin{vmatrix} d_1 - x & 0 & \cdots & 0 \\ 0 & d_2 - x & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & d_n - x \end{vmatrix}$$

$$= (d_1 - x) \cdots (d_n - x).$$

So, $\varphi_A(x) = 0 \Rightarrow x = d_1, d_2, \ldots, d_n$

$\boxed{\text{Therefore, the eigen values of } A \text{ are } d_1, d_2, \ldots, d_n.}$

Week-8

Topics:

- Eigen Vector
- Geometric multiplicity
- Eigen value
- Similar matrices
- Diagonalisable

Theorem: If λ is an eigen value of a non-singular matrix A, then λ^{-1} is an eigen value of A^{-1}.

Proof: Let A be a non-singular matrix of order $n \times n$.

A is non-sigular $\Rightarrow$ A^{-1} exist and λ^{-1} exists.

$$\det(A - \lambda I_n) = 0$$

Now
$$\det(A^{-1} - \lambda^{-1} I_n) = \det(A^{-1} - \lambda^{-1} A^{-1} A)$$
$$= \det(A^{-1} - A^{-1}\lambda^{-1} A)$$
$$= \det(A^{-1}(I_n - \lambda^{-1} A))$$
$$= \det(A^{-1}) \cdot \det(I_n - \lambda^{-1} A)$$
$$= \det(A^{-1}) \cdot (\lambda^{-1})^n \det(\lambda I_n - A)$$
$$= [\det(A)]^{-1} (\lambda^{-1})^n (-1)^n \det(A - \lambda I_n)$$
$$= 0$$

$\Rightarrow \lambda^{-1}$ is an eigen value of A^{-1}.

Theorem: If A and P be both $n \times n$ matrices and P be non-singular, then A and $P^{-1}AP$ have the same eigen values.

Proof: The characteristic polynomial of $P^{-1}AP$ is $\det(P^{-1}AP - xI_n)$

$$\det(P^{-1}AP - xI_n) = \det[P^{-1}AP - P^{-1}(xI_n)P]$$

since $P^{-1}(xI_n)P = xI_n$

$$= \det[P^{-1}(A - xI_n)P]$$

$$= \det(P^{-1}) \cdot \det(A - xI_n) \cdot \det(P)$$

$$= \det(A - xI_n) \cdot \det(P^{-1}P)$$

$$= \det(A - xI_n) \cdot \det(I_n)$$

$$= \det(A - xI_n)$$

Therefore the matrix $P^{-1}AP$ and A have the same characteristic polynomial and so they have the same eigen values.

Eigen vectors of a matrix

Let A be $n \times n$ matrix over a field F. A non-null vector $X \in V_n(F)$ (i.e. n tuple) is said to be an eigen vector or a characteristic vector of A if there exist a scalar $\lambda \in F$ such that $AX = \lambda X$ holds.

Let there exist an eigen vector X of the matrix. Then for some suitably scalar λ, $AX = \lambda X$ holds. That is $(A - \lambda I_n) X = 0$.

This is a homogeneous system of n equations in n unknowns. Since there exists a non-null solution of the system, therefore $\det(A - \lambda I_n) = 0$. This implies that λ is an eigen value of A. Thus for an eigen vector, if it exists, there corresponds an eigen value of the matrix.

Theorem: Let A be an $n \times n$ matrix over a field F. To an eigen vector of A there corresponds a unique eigen value of A.

Proof: Let there be two distinct eigen values λ_1 and λ_2 of A corresponding to an eigen vector X.

Then $AX = \lambda_1 X$ and $AX = \lambda_2 X$.

Therefore $\lambda_1 X = \lambda_2 X \Rightarrow (\lambda_1 - \lambda_2) X = 0$.

But this is a contradiction, since X is a non-null vector and $\lambda_1 - \lambda_2 \neq 0$.

Therefore $\lambda_1 = \lambda_2$.

Theorem: Let A be an $n \times n$ matrix over a field F and λ be an eigen value belonging to F. To each such eigen value of A there corresponds at least one eigen vector.

Proof: Since λ is eigen value, therefore

$$\det(A - \lambda I_n) = 0.$$

$\Rightarrow (A - \lambda I_n) X = 0$ has a non-null solution, say $X = X_1$ where $X_1 \in V_n(F)$ (n-tuple)

Then $(A - \lambda I_n) X_1 = 0$ or $AX_1 = \lambda X_1$

$\Rightarrow X_1$ is an eigen vector of A corresponding to λ.

Example: Let $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$$\det(A - x I_2) = \begin{vmatrix} -x & -1 \\ 1 & -x \end{vmatrix} = x^2 + 1 = 0$$

$\Rightarrow x = \pm i$

A is a real matrix and the eigen values of A are not real numbers. Therefore the real matrix A has no eigen vector.

But if A be considered as a complex matrix, then the eigen vectors of A corresponding to the eigen values $i, -i$ can be obtained.

Let $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ be an eigen vector corresponding to i.

Then $AX = iX \Rightarrow (A - iI_2)X = 0$

$$\Rightarrow \begin{pmatrix} -i & -1 \\ 1 & -i \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\Rightarrow \left.\begin{array}{l} -ix_1 - x_2 = 0 \\ x_1 - ix_2 = 0 \end{array}\right\} \quad -(1)$$

The equivalent system is

$x_1 - ix_2 = 0$.

Let $x_2 = k$, where $k \in \mathbb{C} - \{0\}$

Then $x_1 = ik$

$$\therefore X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ik \\ k \end{pmatrix} = k \begin{pmatrix} i \\ 1 \end{pmatrix}$$

Similarly, eigen vectors corresponding to $-i$ are $c\begin{pmatrix} 1 \\ i \end{pmatrix}$, where $c \in \mathbb{C} - \{0\}$.

Theorem: Two eigen vectors of a square matrix A over a field F corresponding to two distinct eigen values of A are linearly independent.

Proof: Let X_1, X_2 be the eigen vectors of A corresponding to two distinct eigen values λ_1, λ_2 respectively.

Then $AX_1 = \lambda_1 X_1$, $AX_2 = \lambda_2 X_2$.

Let $c_1, c_2 \in F$ s.t. $c_1 X_1 + c_2 X_2 = 0$ —(1)

Then $c_1 AX_1 + c_2 AX_2 = 0$

$\Rightarrow c_1 \lambda_1 X_1 + c_2 \lambda_2 X_2 = 0$ —(2)

$c_1 \lambda_1 X_1 + c_2 \lambda_1 X_2 = 0$ —(3) (by $\lambda_1 \times$ (1))

(2) − (3) $\Rightarrow c_2(\lambda_2 - \lambda_1) X_2 = 0$

Since $\lambda_1 \neq \lambda_2$ and $X_2 \neq 0$ therefore

$c_2 = 0$.

put $c_2 = 0$ in equation (1) $\Rightarrow c_1 = 0$.

$\Rightarrow c_1 = c_2 = 0$

$\Rightarrow X_1, X_2$ are linearly independent.

Note: If $X_1, X_2, \ldots, X_r$ be r eigen vectors of an $n \times n$ matrix A corresponding to r distinct eigen values $\lambda_1, \lambda_2, \ldots, \lambda_r$ respectively, then $X_1, X_2, \ldots, X_r$ are linearly independent.

~~Proof.~~

Theorem: The eigen vectors of an $n \times n$ matrix A over a field F corresponding to an eigen value $\lambda \in F$, together with the null-vector, form a vector space, a subspace of $V_n(F) = F^n$.

Proof: To an eigen value λ, there corresponds an eigen vector of A. Let S be the set of all eigen vectors of A corresponding to λ and let $X_1, X_2 \in S$.

Then $AX_1 = \lambda X_1$ and $AX_2 = \lambda X_2$.

Therefore $A(X_1 + X_2) = \lambda(X_1 + X_2)$.

$\Rightarrow X_1 + X_2$ is an eigen vector of A corresponding to λ.

So $X_1, X_2 \in S \Rightarrow X_1 + X_2 \in S$ —(1)

Let $c \in F$. Then $A(cX_1) = \lambda(cX_1)$.

Therefore if $c \neq 0$, cX_1 is an eigen vector of A corresponding to λ.

So $X_1 \in S$ and $c(\neq 0) \in F \Rightarrow cX_1 \in S$ —(2)

By equation (1) and (2), S is a vector space.

This is a subspace of $V_n(F) = F^n$, since each element of S is an n-tuple vector belonging to F.

Definition: The non-null vector space formed by the eigen vectors of a matrix A corresponding to an eigen value λ, together with the null-vector, is said to be the characteristic subspace corresponding to λ.

Theorem: If λ be an r-fold eigen value of an $n \times n$ matrix A, then rank of $(A - \lambda I_n) \geq n - r$.

Definition: For an r-fold eigen value λ, r is called the algebraic multiplicity of λ and the rank of the characteristic subspace corresponding to λ is called the geometric multiplicity of λ.

Since the characteristic subspace is always a non-null subspace, it follows that for an eigen value λ,

$1 \leq$ geometric multiplicity $\leq$ algebraic multiplicity.

An eigen value λ is said to be regular if the geometric multiplicity of λ is equal to its algebraic multiplicity.

$\gamma = 1 \Rightarrow \lambda$ is a simple eigen value.

Example: Let $A = \begin{pmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$

The characteristic equation of A is $\det(A - x I_3) = 0$

$$\Rightarrow \begin{vmatrix} 1-x & 1 & 1 \\ -1 & -1-x & -1 \\ 0 & 0 & 1-x \end{vmatrix} = 0$$

$\Rightarrow x^2(1-x) = 0$

$\Rightarrow$ Eigen values of A are $0, 0, 1$.

0 is an eigen value of algebric multiplicity 2; and 1 is a simple eigen value of A (i.e., of algebraic multiplicity 1).

The eigen vectors corresponding to the eigen value 0.

$$\begin{pmatrix} 1-0 & 1 & 1 \\ -1 & -1-0 & -1 \\ 0 & 0 & 1-0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Rightarrow \left.\begin{aligned} x_1 + x_2 + x_3 &= 0 \\ -x_1 - x_2 - x_3 &= 0 \\ x_3 &= 0 \end{aligned}\right\}$$

let $x_2 = c$, where $c \in \mathbb{R} - \{0\}$, then

$$x_1 + x_2 + x_3 = 0 \Rightarrow x_1 + c + 0 = 0$$

$$\Rightarrow x_1 = -c$$

eigen vector $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -c \\ c \\ 0 \end{pmatrix} = c \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$

The rank of the characteristic subspace is 1.

therefore the geometric multiplicity of the eigen value 0 is 1. So in this case, the geometric multiplicity is less than the algebraic multiplicity.

<u>Eigen vector corresponding to eigen value 1.</u>

$$\begin{pmatrix} 1-1 & 1 & 1 \\ -1 & -1-1 & -1 \\ 0 & 0 & 1-1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

i.e. $\left.\begin{array}{l} x_2 + x_3 = 0 \\ -x_1 - 2x_2 - x_3 = 0 \end{array}\right\}$

let $x_3 = k$, $k \in \mathbb{R} - \{0\}$

$\Rightarrow x_2 = -k$

$x_1 = -2x_2 - x_3 = 2k - k = k$

$$\therefore\ X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} k \\ -k \\ k \end{pmatrix} = k \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}$$

The rank of the characteristic subspace is 1 and therefore the geometric multiplicity of the eigen value 1 is 1. In this case, the geometric multiplicity = the algebraic multiplicity.

Theorem: The eigen values of a real symmetric matrix are all real.

Proof: Let A be an $n \times n$ real symmetric matrix. The characteristic equation of A is an equation with real coefficients. So the eigen values of A are complex numbers, some or all of which may be purely real.

Let λ be an eigen value of A. Then $\det(A-\lambda I_n)=0$. Therefore there exist non-null solutions of the homogeneous system $(A-\lambda I_n)X=0$. Let X_1 be one such solution.

Then $(A-\lambda I_n)X_1=0$. That is, $AX_1=\lambda X_1$. Taking transpose of the conjugate, we have

$$(\overline{AX_1})^t = (\overline{\lambda X_1})^t \Rightarrow (\bar{X}_1)^t(\bar{A})^t = \bar{\lambda}(\bar{X}_1)^t$$

$$\Rightarrow (\bar{X}_1)^t A = \bar{\lambda}(\bar{X}_1)^t \quad \left(\text{since } \bar{A}^t = A^t = A\right)$$

Multiplying by X_1 from the right, we have

$$(\bar{X}_1)^t A X_1 = \bar{\lambda}(\bar{X}_1)^t X_1$$

$$\Rightarrow \bar{X}_1^t \lambda X_1 = \bar{\lambda}\, \bar{X}_1^t X_1$$

$$\Rightarrow (\lambda-\bar{\lambda})\, \bar{X}_1^t X_1 = 0$$

17

But $(\bar{X}_1)^t X_1 \neq 0$, since X_1 is non-null.

It follows that $\lambda = \bar{\lambda}$ and therefore λ is purely real.

Theorem: The eigen values of a real skew symmetric matrix are purely imaginary, or zero.

Proof: Let A be an $n \times n$ real skew symmetric matrix. Following the same argument as in the previous theorem, we have

$(\lambda + \bar{\lambda})(\bar{X}_1)^t X_1 = 0$, since $\bar{A}^t = A^t = -A$

Since X_1 is non-null, $\lambda + \bar{\lambda} = 0$ i.e. $\lambda = -\bar{\lambda}$.

$\Rightarrow \lambda$ is purely imaginary, or zero

and the theorem is proved.

Note: The eigen values of a Hermitian matrix are all real.

Theorem: The eigen vectors corresponding to two distinct eigen values of a real symmetric matrix are orthogonal.

Proof: Let A be a real symmetric matrix. Let X_1, X_2 be two eigen vectors of A corresponding to two distinct eigen values λ_1 and λ_2.

Then $AX_1 = \lambda_1 X_1$ and $AX_2 = \lambda_2 X_2$.

Now $AX_1 = \lambda_1 X_1 \Rightarrow (AX_1)^t = \lambda_1 X_1^t$, since λ is real

$\Rightarrow X_1^t A^t = \lambda_1 X_1^t$, since $A^t = A$.

Multiplying by X_2 from the right, we have $X_1^t A X_2 = \lambda_1 X_1^t X_2$

or, $X_1^t \lambda_2 X_2 = \lambda_1 X_1^t X_2$

$\Rightarrow (\lambda_2 - \lambda_1) X_1^t X_2 = 0$

$\Rightarrow X_1^t X_2 = 0$, since $\lambda_1 \neq \lambda_2$.

Since $X_1 \neq 0$ and $X_2 \neq 0$, it follows that X_1 is orthogonal to X_2.

Theorem: Each eigen value of a real orthogonal matrix has unit modulus.

Proof: Let A be an $n \times n$ real orthogonal matrix. Then $AA^t = I_n$. The eigen values of A are in general, complex numbers, some of which may be purely real.

Let λ be an eigen value of A. Then $\det(A - \lambda I_n) = 0$.

Therefore there exists a non-null solution of the homogeneous system

$(A-\lambda I_n)X=0$. Let X_1 be one such solution. Then $(A-\lambda I_n)X_1=0$. That is, $AX_1=\lambda X_1$. Note that this X_1 is not an eigen vector of A unless λ is purely real.

$$AX_1=\lambda X_1 \Rightarrow (\overline{AX_1})^t=(\overline{\lambda X_1})^t$$

$$\Rightarrow \bar{X}_1^t \bar{A}^t = \bar{\lambda}\bar{X}_1^t$$

$$\Rightarrow \bar{X}_1^t A^t = \bar{\lambda}\bar{X}_1^t, \text{ since } \bar{A}^t = A^t$$

Multiplying by AX_1 from the right, we have,

$$\bar{X}_1^t A^t (AX_1) = \bar{\lambda}\bar{X}_1^t (AX_1)$$

$$\Rightarrow \bar{X}_1^t (A^tA)X_1 = \bar{\lambda}\bar{X}_1^t \lambda X_1$$

$$\Rightarrow \bar{X}_1^t X_1 = \bar{\lambda}\lambda \bar{X}^t X_1, \text{ since } AA^t=I_n \Rightarrow A^tA=I_n$$

$$\Rightarrow \bar{X}_1^t X_1 (1-\bar{\lambda}\lambda)=0.$$

Since X_1 is non-null, $\bar{X}_1^t X_1 \neq 0$. It follows that $\bar{\lambda}\lambda=1$ i.e. $|\lambda|=1$.

Theorem: If λ be an eigen value of a real orthogonal matrix A, prove that $\frac{1}{\lambda}$ is also an eigen value of A.

Proof: Let A be an orthogonal matrix of order n. Then $AA^t = I_n$ and A is non-singular. Since A is non-singular, $\lambda \neq 0$.

Since λ is an eigen value of A,

$\det(A - \lambda I_n) = 0$.

$\Rightarrow \det(A - \lambda A A^t) = 0$

$\Rightarrow \det(A) \cdot \det(I_n - \lambda A^t) = 0$

$\Rightarrow \det(I_n - \lambda A^t) = 0$, since $\det(A) \neq 0$.

$\Rightarrow (-1)^n \lambda^n \det\left(A^t - \frac{1}{\lambda} I_n\right) = 0$

$\Rightarrow (-1)^n \lambda^n \det\left(A - \frac{1}{\lambda} I_n\right)$, since $\det\left(A^t - \frac{1}{\lambda} I_n\right)$
$= \det\left(A - \frac{1}{\lambda} I_n\right)^t$

$\Rightarrow \frac{1}{\lambda}$ is an eigen value of A.

Question: If S is a real symmetric matrix of order n then show that

(i) $I_n + S$ is non-singular

(ii) $(I_n+S)^{-1}(I_n-S)$ is orthogonal

(iii) If X be an eigen vector of S with eigen value λ then X is also an eigen vector of the matrix $(I_n+S)^{-1}(I_n-S)$ with eigen value $\frac{1-\lambda}{1+\lambda}$.

(iv) If $\bar{S} = (I_n+S)^{-1}(I_n-S)$ then $I_n+\bar{S}$ is also non-singular and $\bar{S}=S$.

Solution: (i) Since S is a real skew symmetric matrix, its eigen

values are imaginary or zero.
Therefore -1 is not an eigen value of S. So -1 is not a root of the characteristic equation $\det(S - xI_n) = 0$.

$\Rightarrow \det(S + I_n) \neq 0 \Rightarrow S + I_n$ is non-singular.

(ii) Let $P = (I_n + S)^{-1}(I_n - S)$.

Then $$PP^t = (I_n+S)^{-1}(I_n-S)\left[(I_n+S)^{-1}(I_n-S)\right]^t$$

$$= (I_n+S)^{-1}(I_n-S)(I_n-S)^t\{(I_n+S)^{-1}\}^t$$

$$= (I_n+S)^{-1}(I_n-S)(I_n+S)\{(I_n+S)^t\}^{-1}$$

$$= (I_n+S)^{-1}\{(I_n+S)(I_n-S)\}(I_n-S)^{-1}$$

$\left(\text{Since } (I_n-S)(I_n+S) = (I_n+S)(I_n-S)\right)$

$$= \{(I_n+S)^{-1}(I_n+S)\}\{(I_n-S)(I_n-S)^{-1}\}$$

$= I_n \cdot I_n = I \Rightarrow P$ is orthogonal

(iii) $SX = \lambda X$

Therefore $(I_n + S)^{-1}(I_n - S)X = (I_n+S)^{-1}(1-\lambda)X$

$= (1-\lambda)(I_n+S)^{-1}X.$

Again $(I_n+S)X = (1+\lambda)X$

$\Rightarrow X = (I_n+S)^{-1}(1+\lambda)X = (1+\lambda)(I_n+S)^{-1}X.$

So we have $\frac{1}{1+\lambda}X = (I_n+S)^{-1}X$ since $\lambda+1 \neq 0$

Therefore $(I_n+S)^{-1}(I_n-S)X = (1-\lambda)\frac{1}{1+\lambda}X = \frac{1-\lambda}{1+\lambda}X.$

$\Rightarrow X$ is an eigen vector of $(I_n+S)^{-1}(I_n-S)$ with eigen value $\frac{1-\lambda}{1+\lambda}$.

(iv) $\bar{S} = (I_n+S)^{-1}(I_n-S)$

$I_n + \bar{S} = (I_n+S)^{-1}(I_n+S) + (I_n+S)^{-1}(I_n-S)$

$= (I_n+S)^{-1}\{(I_n+S) + (I_n-S)\}$

$= 2(I_n+S)^{-1}$

Therefore $(I_n+\bar{S})^{-1} = \frac{1}{2}(I_n+S)$, proving that $I_n+\bar{S}$ is non-singular.

Also, $I_n - \bar{S} = (I_n+S)^{-1}(I_n+S) - (I_n+S)^{-1}(I_n-S)$

$$= (I_n+S)^{-1}\{(I_n+S)-(I_n-S)\}$$

$$= 2(I_n+S)^{-1}S.$$

Therefore, $\bar{S} = (I_n+\bar{S})^{-1}(I_n-\bar{S})$

$$= \frac{1}{2}(I_n+S)\cdot 2(I_n+S)^{-1}S = S.$$

Diagonalisation of matrices

Let us consider the set of all $n\times n$ matrices over a field F. An $n\times n$ matrix A is said to be similar to an $n\times n$ matrix B if there exists a non-singular $n\times n$ matrix P s.t. $B = P^{-1}AP$.

$B = P^{-1}AP \Rightarrow A = PBP^{-1} = Q^{-1}BQ$ where $Q(=P^{-1})$ is non-singular. Therefore if A is similar to B then B is similar to A and two matrices A and B are said to be similar.

Note: Two similar matrices A and B have the same eigen values

(Because A, $P^{-1}AP$ have same set of eigen values, where P is non-singular matrix).

But the matrices having the same eigen values may not be similar.

Example: let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

These matrices have the same characteristic polynomial and hence they have the same eigen values. But A being the matrix I_2 there is no matrix other than itself which is similar to it, because for any non-singular 2x2 matrix P, $P^{-1} I_2 P = I_2$. Therefore B is not similar to A.

Definition: An $n \times n$ matrix A is said to be diagonalisable if A is similar to an $n \times n$ diagonal matrix.

If A is similar to a diagonal matrix $D = diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$ then $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigen values of A.

Note: An $n \times n$ matrix A over a field F is diagonalisable if and only if there exist n eigen vectors of A which are linearly independent.

Theorem: Let A be an $n \times n$ matrix over a field F. If the eigen values of A be all distinct and belong to F, then A is diagonalisable.

Proof: Let $\lambda_1, \lambda_2, \dots, \lambda_n$ be n distinct eigen values of A and $\lambda_i \in F$.

Let X_i be an eigen vector corresponding to the eigen value λ_i. Then $X_1, X_2, \dots, X_n$ are n linearly independent eigen vectors of A. Thus A has n linearly independent eigen vectors and therefore A is diagonalisable.

Note: The condition stated in the above theorem is not necessary for a matrix A to be diagonalisable.

Example: Let $A = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

Then the characteristic equation of A is $(x-1)^2(x-5) = 0$.

$\Rightarrow$ Eigen values of A are $1, 1, 5$.

The eigen vectors corresponding to the eigen value 1 are the non-null solutions of the system of equations

$$2x_1 + 2x_2 + x_3 = 0$$
$$2x_1 + 2x_2 + x_3 = 0$$

The system is equivalent to

$$x_1 + x_2 + \frac{1}{2}x_3 = 0$$

The eigen vectors are $c\begin{pmatrix}1\\-1\\0\end{pmatrix} + d\begin{pmatrix}1\\0\\-2\end{pmatrix}$

where $(c,d) \neq (0,0)$

Two linearly independent eigen vectors corresponding to the eigen value 1 are

$\begin{pmatrix}1\\-1\\0\end{pmatrix}$ and $\begin{pmatrix}1\\0\\-2\end{pmatrix}$.

The eigen vectors corresponding to the eigen value 5 are the non-null solutions of the system of equations

$$-2x_1 + 2x_2 + x_3 = 0$$

$$2x_1 - 2x_2 + x_3 = 0$$

$$x_3 = 0$$

The system is equivalent to

$$x_1 - x_2 = 0$$

$$x_3 = 0.$$

The eigen vectors are $c\begin{pmatrix}1\\1\\0\end{pmatrix}$ where $c \neq 0$.

Thus A has three distinct eigen vectors

$\begin{pmatrix}1\\-1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\-2\end{pmatrix}, \begin{pmatrix}1\\1\\0\end{pmatrix}$ which are linearly

independent.

Therefore by the theorem A is

diagonalisable.

If $P = \begin{pmatrix}1 & 1 & 1\\-1 & 0 & 1\\0 & -2 & 0\end{pmatrix}$ then $P^{-1}AP = \text{diag}(1, 1, 5)$

The three eigen values of A are not

distinct, yet A is diagonalisable.

Note:

Diagonalise $A_{n\times n}$ → find $P_{n\times n}$ non-singular matrix s.t. $P^{-1}AP = \begin{pmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ 0 & & \lambda_n \end{pmatrix}$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are eigen values of A.

How to find such $P_{n\times n}$?

n linearly independent eigen vectors of A is taken as column of P.

Orthogonal diagonalisation of real matrices:

A square matrix A is said to be orthogonally diagonalisable if there exists an orthogonal matrix P s.t. $P^{-1}AP$ is a diagonal matrix. The matrix P is said to diagonalise A orthogonally.