

Vector space - Let V be a non-empty set of elements called vectors and k, m are scalars. If the set V satisfies the following axioms then it is called a vector space.

1. Closure axiom -

- c₁ - if u and v are any 2 elements in V then $u+v$ is also in V . Therefore, V is closed under addition.
- c₂ - if k is any scalar then $k \cdot u$ is in V . Therefore, V is closed under scalar multiplication.

2. Addition axiom -

a. A₁ - $u + v = v + u$ (commutativity)

b. A₂ - $u + (v+w) = (u+v) + w$ (Associativity)

- c. A₃ - There is an element called zero in V such that $u + 0 = u$ for every u in V .

(Existence of additive identity)

- d. A₄ - There is an element $-u$ in V corresponding to every u in V such that

$$u + (-u) = 0$$

(Existence of additive inverse.)

3. Scalar multiplication axiom

a. M₁ - $k(u+v) = ku + kv$ (Distributivity)

b. M₂ - $(k+l)u = ku + lu$

c. M₃ - $(kl)u = k(lu)$ (Associativity)

- d. M₄ - There is an element 1 in V such that

$$u \cdot 1 = u \text{ for all } u \text{ in } V$$

(Existence of multiplicative identity)

e.g. if V is a vector space then show that

(i) Additive identity 0 is unique

(ii) Additive inverse of a vector u is unique.

→ if possible let there be 2 distinct additive identities 0 and $0'$
 then $u + 0 = u$ — (1)

$$u + 0' = u \quad \text{--- (2)}$$

Substituting $u = 0'$, in (1)

$$0' + 0 = 0' \quad \text{--- (3)}$$

Substituting $u = 0$ in (2)

$$0 + 0' = 0 \quad \text{--- (4)}$$

from (3) and (4),

$$0 = 0'$$

This shows that two identities are unique.

If possible let u_1 and u_2 be two additive inverses of u .

then by the definition of inverse

$$u + u_1 = 0 \quad \text{--- (1)}$$

$$u + u_2 = 0 \quad \text{--- (2)}$$

Adding u_2 in (1),

$$u + u_2 + u_1 = u_2$$

$$u + u_1 = u_2$$

This shows that the additive inverse of a vector u is unique

Yuk!

success	
done	/ /

y Check whether the set of all pairs of real numbers of the form $(1, n)$ with the operations $(1,y) + (1,y') = (1,y+y')$ and $k(1,y) = (1,ky)$ is a vector space.

→ given operations -

$$(1,y) + (1,y') = (1,y+y')$$
$$k(1,y) = (1,ky)$$

1 closure axiom

a₁- if $u = (1,n)$ and $v = (1,y)$
 $u \cdot v = (1, n+y)$

i. V is closed under addition.

B. a₂- if k is a any. scalar and $u = (1,n)$
 $ku = k(1,n)$
 $= (1,kn)$

i. V is closed under scalar multiplication.

B. addition axiom

a₁- $u+v = (1,n) + (1,y)$
 $= (1,n+y)$
 $= (1,y+n)$
 $= v+u$

a₂- $(u+v)+w = [(1,n)+(1,y)] + (1,z)$
 $= (1,n+y) + (1,z)$
 $= (1,n+y+z)$
 $= (1,n) + (1,y+z)$
 $= u + (v+w)$

a₃- $u+0 = (1,n) + (1,0)$

$$= (1,n) = u \quad (\text{Existence of addition identity})$$

a₄- $u+(-u) = (1,n) + (1,-n) = (1,0) = n$

c. Scalar multiplication

$$M_1 = k(u+v)$$

$$= k[(1, u) + (1, v)]$$

$$= k(1, u+v)$$

$$= (1, ku+kv)$$

$$= (1, ku) + (1, kv)$$

$$= ku + kv \quad (1 + (p))$$

$$M_2 = (k+l)u = (k+l)(1, u)$$

$$= (1, (k+l)u)$$

$$= (1, ku+lu)$$

$$= (1, ku) + (1, lu)$$

$$= ku + lu$$

Hence, all axioms are satisfied.

$\therefore V$ is a vector space.

Subspace

A subset W of a vector space V is called a subspace of V if W is also a vector space under addition and scalar multiplication defined on V .

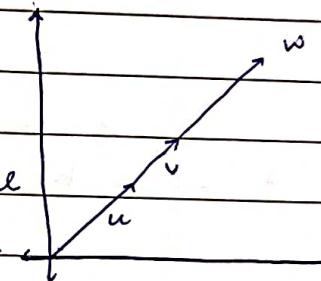
Criterion - if W is a non-empty subset of vector space V then

W is a subspace of V if

1. for all u and v in W , $u + v$ is also in W .
2. for any scalar k and any vector u in W , the ku is also in W .

q) Show that the line through the origin in \mathbb{R}^3 is a subspace of \mathbb{R}^3 .

→ Consider a line through the origin: if
 u and v are two vectors with origin as the initial point. Then $u + v$ is also lies on this line.
 Thus $u + v$ is closed under addition.



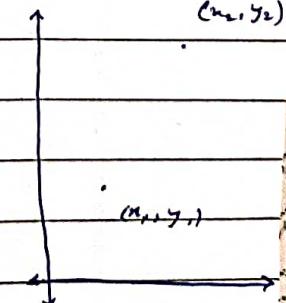
If k is any scalar, the ku is also a vector on this line.
 Thus W is closed under scalar multiplication.

This means that a line through the origin in \mathbb{R}^3 is a subspace of \mathbb{R}^3 .

q) If W is a set of all points (x, y) in \mathbb{R}^2 such that $x > 0$, $y > 0$. Then W is not a subspace of \mathbb{R}^2 .

if $(x_1, y_1), (x_2, y_2)$ are any two points on W .
 in the first quadrant then $(x_1, y_1) + (x_2, y_2)$
 $= (x_1 + x_2, y_1 + y_2)$ is also a point on W in
 the first quadrant but

$$k(x, y) \notin (kx, ky)$$



for instance, $k = -2 \rightarrow k(x, y)$ is not in the first quadrant.
 Hence, W is not closed under scalar multiplication.

(Ex V)

e.g. let W be the set of all functions of the form $p(n) = a_0 + a_1 n + \dots + a_m n^m$, where n is a non-negative integer and a_0, a_1, \dots, a_m are real numbers. Then W is a subspace of all real valued functions.

→ Similarly,

$$q(n) = b_0 + b_1 n + b_2 n^2 + \dots + b_m n^m$$

$$p(n) + q(n) = (a_0 + b_0) + (a_1 + b_1)n + \dots + (a_m + b_m)n^m$$

is also of the given form.
 ∴ $p(n) + q(n)$ is in W .

for any scalar k ,

$$k p(n) = k a_0 + k a_1 n + \dots + k a_m n^m$$

is also of the given form.
 ∴ $k p(n)$ is in W
 ∴ W is a ~~subset~~^{subspace} of all real valued functions V .

e.g. Show that any plane through the origin is a subspace of \mathbb{R}^3 .

Span Spanned by a Vector

If W be a ~~top~~ subspace of V consisting of all linear combinations v_1, v_2, \dots, v_n of s in W is called Space Spanned by s . We also say that the vectors v_1, v_2, \dots, v_n spans W .

To span means to furnish with something that extends / spreads over. "loosely speaking", to span means to generate or to create.

$$W = \text{Span}(s)$$

$$= \text{Span}(v_1, v_2, \dots, v_n)$$

$$= L(s)$$

e.g. Show that the vectors $v_1 = (1, 0, 1)$, $v_2 = (2, 1, 4)$ and $v_3 = (1, 1, 3)$ do not span the vector space in \mathbb{R}^3 .

→ if v_1, v_2, v_3 span the vector space in \mathbb{R}^3 then any vector in \mathbb{R}^3 should be expressible in terms of v_1, v_2, v_3 .

Let w_1, w_2 and w_3 be vectors in \mathbb{R}^3 , then we try to find scalars k_1, k_2, k_3 such that

$$w = k_1 v_1 + k_2 v_2 + k_3 v_3$$

$$\begin{aligned} w &= k_1(1, 0, 1) + k_2(2, 1, 4) + k_3(1, 1, 3) \\ &= [(k_1 + 2k_2 + k_3), (k_2 + k_3), (k_1 + 4k_2 + 3k_3)] \end{aligned}$$

$$\Rightarrow w_1 = k_1 + 2k_2 + k_3$$

$$w_2 = 0k_1 + k_2 + k_3$$

$$w_3 = k_1 + 4k_2 + 3k_3$$

NOTE - the system is consistent if

$$\begin{array}{|ccc|c|} \hline & 1 & 2 & 1 & | \\ & 0 & 1 & 1 & | \\ \hline & 0 & 1 & 4 & | \\ \hline \end{array} \neq 0$$

Hence, the given system is non-consistent.

This means there are no scalars k_1, k_2, k_3 satisfying the equation.

⇒ No vector can be expressed as a linear combination of v_1, v_2, v_3 .

Hence, v_1, v_2, v_3 do not span the vector space in \mathbb{R}^3 .

e.g. determine whether the following vectors span P_2 (P_2 means vector space consisting of all polynomials of second order).

$$v_1 = 1 - n + 2n^2$$

$$v_2 = 3 - n + 4n^2$$

$$v_3 = -2 - 2n + 2n^2$$

Convert an orthonormal basis by applying Gram Schmidt to
the set $S = \{(3, 1), (4, 2)\}$

Given $u_1 = (3, 1)$ $u_2 = (4, 2)$
—① $\quad \quad \quad$ —②

Let $v_1 = u_1 = (3, 1)$ —③

$v_2 = u_2 - \text{proj}_{v_1} u_2$

$$= u_2 - \frac{(u_2 \cdot v_1)}{\|v_1\|^2} v_1$$

first find $(u_2 \cdot v_1)$ and $\|v_1\|^2$

$$(u_2 \cdot v_1) = 3(4, 2) \cdot (3, 1) = 14$$

$$\|v_1\|^2 = (\sqrt{3^2 + 1^2})^2 = 10$$

$$v_2 = (4, 2) - \frac{14}{10} (3, 1)$$

$$= \left(-\frac{1}{5}, \frac{3}{5}\right)$$

Hence, $v_1 = (3, 1)$

$v_2 = \left(-\frac{1}{5}, \frac{3}{5}\right)$ form an orthogonal basis for \mathbb{R}^2 .

Now the norms of this vectors are

$$\|v_1\| = \sqrt{\left(\frac{-1}{5}\right)^2 + \left(\frac{3}{5}\right)^2} = \sqrt{\frac{2}{5}}$$

$$q_1 = \frac{v_1}{\|v_1\|} = \frac{(3, 1)}{\sqrt{10}} = \left(\frac{3}{\sqrt{10}}, \frac{1}{\sqrt{10}}\right)$$

$$q_2 = \frac{v_2}{\|v_2\|} = \frac{\left(-\frac{1}{5}, \frac{3}{5}\right)}{\sqrt{\frac{2}{5}}} = \left(\frac{-1}{\sqrt{10}}, \frac{3}{\sqrt{10}}\right)$$

19. Construct an orthonormal basis for the subspace of \mathbb{R}^3 by applying Gram-Schmidt process where $S = \{(1, 2, 0), (0, 3, 1)\}$

$$\rightarrow u_1 = (1, 2, 0), u_2 = (0, 3, 1)$$

Step 1.

$$u - v_1 = u_1 = (1, 2, 0)$$

Step 2.

$$\begin{aligned} u - v_2 &= u_2 - \text{proj } u_2 \\ &= (0, 3, 1) - \frac{(u_2, v_1)}{\|v_1\|^2} \cdot v_1 \end{aligned}$$

$$u_2 \cdot v_1 = (0, 3, 1) \cdot (1, 2, 0) = 6$$

$$\|v_1\|^2 = 5$$

$$\begin{aligned} v_2 &= (0, 3, 1) - \frac{6}{5} \cdot (1, 2, 0) \\ &= \left(-\frac{6}{5}, \frac{3}{5}, 1\right) \end{aligned}$$

Norms -

$$\|v_1\| = \sqrt{5}$$

$$q_1 = \left(\frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}}, 0\right)$$

$$\|v_2\| = \sqrt{\frac{14}{5}}$$

$$q_2 = \left(\frac{-6}{\sqrt{14}}, \frac{3}{\sqrt{14}}, \frac{\sqrt{5}}{\sqrt{14}}\right)$$

~~Ans~~

====

PROBLEM	
DATE	/ /

Euclidean Inner product

If $u = u_1, u_2, \dots, u_n$ and $v = v_1, v_2, \dots, v_n$

are any two vectors of \mathbb{R}^n then the Euclidean inner product of u, v is denoted by $u \cdot v$

$$u \cdot v = u_1v_1 + u_2v_2 + \dots + u_nv_n$$

In \mathbb{R}^3 have the Euclidean Inner product. Use the Gram-Schmidt's process to transform the basis (u_1, u_2, u_3) into the orthonormal basis where

$$u_1 = (1, 0, 0)$$

$$u_2 = (3, 1, -2)$$

$$u_3 = (0, 4, 1)$$

$$\text{let } v_1 = u_1 = (1, 0, 0)$$

$$v_2 = u_2 - \text{proj}_{u_2}$$

$$u_2 \cdot v_1 = 3$$

$$\|v_1\| = 1$$

$$v_2 = (3, 1, -2) - 3(1, 0, 0) \\ = (0, 1, -2)$$

$$v_3 = u_3 - \frac{(u_3 \cdot v_1)}{\|v_1\|^2} \cdot v_1 - \frac{(u_3 \cdot v_2)}{\|v_2\|^2} \cdot v_2$$

e.g. In the inner space P_2 have the inner product defined by

$$(P_f g) = \int_{-1}^1 P(n) g(n) dn$$

Use Gram Schmidt's process to transform the standard

$$\rightarrow u_1 \cdot u_1 = 1, \quad u_2 = n, \quad u_3 = n^2$$

$$\text{Step 1} \quad v_1 = u_1 = 1$$

$$\text{Step 2} \quad v_2 = u_2 - \frac{(u_2 \cdot v_1) \cdot v_1}{\|v_1\|^2}$$

$$\begin{aligned} \|v_1\|^2 &= -1 \int [v_1(n)]^2 dn \\ &= \int_{-1}^1 1^2 dn = 2 \end{aligned}$$

$$= u_2 - 0$$

$$= n - n_2$$

$$\text{Step 3} \quad v_3 = u_3 - \frac{(u_3 \cdot v_1) \cdot v_1}{\|v_1\|^2} - \frac{(u_3 \cdot v_2) \cdot v_2}{\|v_2\|^2}$$

$$= u_3 - \frac{2/3}{2} \cdot 1 - 0$$

$$= n^2 - \frac{1}{3}$$

$$\|v_3\| =$$

Let A be a $m \times n$ matrix. The subspace of \mathbb{R}^n spanned by A
 is called the Rowspace of A . The subspace of \mathbb{R}^m spanned
 by the column vectors of A is called as a Column space of
 A . Dimensions →

$$\dim(\text{Rowspan}(A)) = \dim(\text{Columnspan}(A)) = \text{rank}(A)$$

Find the basis for the Rowspace of the following matrix.

$$A = \begin{vmatrix} 1 & 1 & 4 & 1 & 2 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 \\ 1 & -1 & 0 & 0 & 2 \\ 2 & 1 & 6 & 0 & 1 \end{vmatrix}$$

→ Reduce the matrix to Row Echelon Form

$$R_4 \rightarrow R_4 - R_1$$

$$R_5 \rightarrow R_5 - 2R_1$$

$$\begin{vmatrix} 1 & 1 & 4 & 1 & 2 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & -2 & -4 & 0 & 0 \\ 0 & -1 & -2 & -2 & -3 \end{vmatrix}$$

$$R_4 \rightarrow R_4 + 2R_2$$

$$R_5 \rightarrow R_5 + R_2$$

$$\begin{vmatrix} 1 & 1 & 4 & 1 & 2 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & -1 & -2 \end{vmatrix}$$

Find the basis for the column space of the following matrix

$$A = \begin{vmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 3 & 1 & 5 \end{vmatrix}$$

Reduce to Row Echelon

$$R_3 \rightarrow R_3 - R_1$$

$$R_4 \rightarrow R_4 - 2R_1$$

$$\begin{vmatrix} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 3 & 3 \end{vmatrix}$$

$$R_3 \rightarrow R_3 - R_2$$

$$R_4 \rightarrow R_4 - 3R_2$$

$$\begin{matrix} (1) & \left| \begin{array}{cccc} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} \right| \end{matrix}$$

Check pivot columns

If any column has 1 in the diagonal positions.

(make steps) and skip if any ~~to~~ column does not have 0)

$$w_1 = [1, 0, 0, 0]$$

$$w_2 = [0, 1, 0, 0]$$

It is very clear that first and second column are pivot columns. Thus, first and ^{second} columns of the original matrix form a basis for the column space.

eg. find basis for the column space for the matrix

$$A = \left[\begin{array}{cccc} 1 & 2 & -1 & 4 \\ -2 & 1 & 7 & 2 \\ -1 & -4 & -1 & 3 \\ 3 & 2 & -7 & -1 \end{array} \right]$$

→ Reduce the matrix to Row Echelon form

We get

$$\left[\begin{array}{cccc} 1 & 2 & -1 & 4 \\ 0 & 1 & 1 & -3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array} \right]$$

column 1, 2 and 4 are the pivot columns.

Thus, 1st, 2nd and 3rd column of the original matrix form a basis for the column space of A.

$$w_1 = [1, -2, 1, 3]$$

$$w_2 = [2, 1, -4, 2]$$

$$w_3 = [4, 2, 3, -1]$$

eg. find a basis for nullspace of $A = \left[\begin{array}{cccc} 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 2 \\ 2 & 3 & 1 & 5 \end{array} \right]$

LEAST

if A be a $m \times n$ matrix and b be a vector in \mathbb{R}^n . To find the least square solution of $AX = b$

1. Compute the matrix $A^T A$ and $A^T b$

2. Form the augmented matrix $[A^T A | A^T b]$

3. Reduce the matrix $[A^T A | A^T b]$ to reduced row echelon form

4. This equation is always consistent and any solution
is a least square solution

Find the least square solution of $AX = B$ where

$$A = \begin{vmatrix} 2 & -1 \\ 1 & 2 \\ 1 & 1 \end{vmatrix} \text{ and } B = \begin{vmatrix} 2 \\ 1 \\ 4 \end{vmatrix}$$

Compute $A^T A$ and $A^T B$

$$A^T A = \begin{vmatrix} 2 & 1 & 1 \\ -1 & 2 & 1 \end{vmatrix} \begin{vmatrix} 2 & -1 \\ 1 & 2 \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} 6 & 1 \\ 1 & 6 \end{vmatrix}$$

$$A^T B = \begin{vmatrix} 2 & 1 & 1 \\ -1 & 2 & 1 \end{vmatrix} \begin{vmatrix} 2 \\ 1 \\ 4 \end{vmatrix} = \begin{vmatrix} 9 \\ 4 \end{vmatrix} \Rightarrow A^T A \cdot X = A^T B$$

Form the augmented matrix and now reduce

$$\left[\begin{array}{cc|c} 6 & 1 & 9 \\ 1 & 6 & 4 \end{array} \right]$$

$R_1 \leftrightarrow R_2$

$$\left| \begin{array}{cc|c} 1 & 6 & 4 \\ 6 & 1 & 9 \end{array} \right|$$

 $R_2 \rightarrow R_2 - 6R_1$

$$\left| \begin{array}{cc|c} 1 & 6 & 4 \\ 0 & -35 & -15 \end{array} \right|$$

 $R_2 \rightarrow R_2 - 35$

$$\left| \begin{array}{cc|c} 1 & 6 & 4 \\ 0 & 1 & 3/7 \end{array} \right|$$

 $R_1 \rightarrow R_1 - 6R_2$

$$\left| \begin{array}{cc|c} 1 & 0 & 10/7 \\ 0 & 1 & 3/7 \end{array} \right|$$

 \therefore The least square solution

$$\hat{x} = \begin{pmatrix} 10/7 \\ 3/7 \end{pmatrix}$$

that is a unique least square solution

e.g. find the least square solution of $AX = b$ where

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & -1 \\ 1 & 2 & -3 \end{pmatrix} \quad b = \begin{pmatrix} 6 \\ 0 \\ 0 \end{pmatrix}$$

$$\rightarrow A^T A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & -1 & -3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & -1 \\ 1 & 2 & -3 \end{pmatrix}$$

$$= \begin{pmatrix} 3 & 3 & -3 \\ 3 & 5 & -7 \\ -3 & -7 & 11 \end{pmatrix}$$

$$A^T b = \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & -1 & -3 \end{vmatrix} \begin{pmatrix} 6 \\ 0 \\ 6 \end{pmatrix} = \begin{pmatrix} 6 \\ 0 \\ 6 \end{pmatrix}$$

We form an augmented matrix

$$\left[\begin{array}{ccc|c} 3 & 3 & -3 & 6 \\ 3 & 5 & -7 & 0 \\ -3 & -7 & 11 & 6 \end{array} \right]$$

Converting to reduced row echelon form

$$\left[\begin{array}{ccc|c} 1 & 0 & 1 & 5 \\ 0 & 1 & -2 & -3 \\ 0 & 0 & 0 & 0 \end{array} \right]$$

Solving the system

$$n_1 + n_3 = 5$$

$$n_2 - 2n_3 = -3$$

Put random values and solve

$$n_3 = 0 \quad n_3 = 1$$

$$n_2 = -3 \quad n_2 = -1$$

$$n_1 = 5 \quad n_1 = 4$$

$$\tilde{n} = \begin{pmatrix} 0 \\ -3 \\ 5 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 4 \end{pmatrix}$$

Q. find the least square solution of $AX = b$ for

$$A = \begin{pmatrix} 2 & 0 \\ -1 & 1 \\ 0 & 2 \end{pmatrix} \quad B = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$$

Samaran

You decoding - $\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

Application of Matrices to Coding and Decoding

Cryptography - A study of coding and decoding a message is called as cryptography.

Plain text - message to be sent

Codes are ciphers

Code messages are cipher codes

Encoding / Enciphering - process of converting plain text by coding

Decoding / Deciphering - process of getting plain text from cipher text

Method - consists of the following steps -

i. To convert the words / obliques to numbers by numbers

ii. To encode the message

iii. To decode the message

iv. To replace numbers by words / letters

$$\begin{array}{l} A \rightarrow 1 \\ B \rightarrow 2 \end{array}$$

$$\begin{array}{l} 2 \rightarrow 26 \\ (*) \text{Space} \rightarrow 27 \end{array}$$

NOTE - in The selected matrix is called as an encoding matrix and its inverse is called as a decoding matrix.

(ii) Encoding matrix is also known as key

v. Using a suitable 2×2 matrix encode and decode the message

WE GO (only usual)

→ i. Converting words into numbers then the transformation
is

W E G O

23 5 7 15

then we write this as a 2×1 matrix

$$\begin{bmatrix} 23 \\ 15 \end{bmatrix}, \begin{bmatrix} 7 \\ 15 \end{bmatrix}$$

ii. We now multiply each of the above column vectors by the encoding matrix.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 23 & 7 \\ 5 & 15 \end{pmatrix} = \begin{pmatrix} 28 & 22 \\ 5 & 15 \end{pmatrix}$$

The columns of this matrix give the encoding encoded message
The above message is then transmitted linearly
28 5 22 15

3. The original message is now written in a matrix
 $\begin{pmatrix} 28 & 22 \\ 5 & 15 \end{pmatrix}$

This is then premultiplied by the inverse of the coding matrix
 $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

$$\Rightarrow \begin{pmatrix} 28 & 22 \\ 5 & 15 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 28 & -6 \\ 5 & 10 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 28 & 22 \\ 5 & 15 \end{pmatrix} = \begin{pmatrix} 23 & 7 \\ 5 & 15 \end{pmatrix}$$

4. The columns of the above matrix in linear form is

$$23 \quad 5 \quad 7 \quad 15$$

it is transformed

$$23 \quad 5 \quad 7 \quad 15$$

$$W \quad E \quad G \quad O$$

Use a suitable 2×2 matrix to encode and decode the message
NOW * STUDY

For 2×2 matrix multiplication, the last number has to have a pair
 \Rightarrow NOW * STUDY *

1. Replacing letters by numbers

NOW * STUDY *

14 15 23 27 19 20 21 4 25 27

We write the sequence in a 2×1 column matrix

$$\begin{bmatrix} 14 \\ 15 \end{bmatrix}, \begin{bmatrix} 23 \\ 27 \end{bmatrix}, \begin{bmatrix} 19 \\ 20 \end{bmatrix}, \begin{bmatrix} 21 \\ 4 \end{bmatrix}, \begin{bmatrix} 25 \\ 27 \end{bmatrix}$$

2. We now premultiply each of the vectors by the encoding matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 14 & 23 & 19 & 21 & 25 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix}$$

$$\begin{bmatrix} 29 & 50 & 39 & 25 & 52 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix}$$

Columns give the encoded message. Message is transmitted as

29 15 50 27 39 20 25 4 52 27

3. The received message is then written in a sequence of 2×1 matrices

$$\begin{bmatrix} 29 \\ 15 \end{bmatrix}, \begin{bmatrix} 50 \\ 27 \end{bmatrix}, \begin{bmatrix} 39 \\ 20 \end{bmatrix}, \begin{bmatrix} 25 \\ 4 \end{bmatrix}, \begin{bmatrix} 52 \\ 27 \end{bmatrix}$$

Premultiplying the above matrix by the inverse of the coding matrix

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 29 & 50 & 39 & 25 & 52 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix}$$

$$\begin{bmatrix} 14 & 23 & 19 & 21 & 25 \\ 15 & 27 & 20 & 4 & 27 \end{bmatrix}$$

columns are written in linear form

14 15 23 27 19 20 21 4 25 27

Q. Encode and decode the given message using
2x2 matrix MOVE

1. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for shift cipher

2. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for Caesar cipher

3. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for Vigenere cipher

4. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for Hill cipher

5. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for DES cipher

6. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for AES cipher

7. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ for RSA cipher