Introduction to Linear Algebra
- Gilbert Strang

15

Linear Transformations

↓

Complex Vectors & Matrices

↓

Linear Algebra for Cryptography

Note Book

soorajss1729@gmail.com

+91-9400635788

15

INDEX

Name : SOORAJ S. Subject : ....

Std. : .... Div. : .... Roll No. : ....

School / College : ....

S. No.	Date	Title	Page No.	Teacher's Sign / Remarks
		INTRODUCTION TO		
		LINEAR ALGEBRA		
		— Gilbert Strang, MIT		
		(5th Edition)		

8.1

1. A linear transformation must leave the zero vector fixed: $T(0)=0$. Prove this from $T(v+w)=T(v)+T(w)$ by choosing $w=$ _____.

Prove it also from $T(cv)=cT(v)$ by choosing $c=$ _____

Ans: Take $w=0$,

$$T(v+0)=T(v)+T(0)=T(v)$$

$$\Longrightarrow \underline{\underline{T(0)=0}}$$

(OR)

$c=0$,

$$T(0v)=\underline{\underline{T(0)=0}}$$

4. If S & T are linear transformations, is $T(S(v))$ linear or quadratic

(a) (Special case) If $S(v)=v$ and $T(v)=v$, then $T(S(v))=v$ or v^2?

Ans: $T(S(v))=v$

(b) (General case)

$S(v_1+v_2) = S(v_1)+S(v_2)$ and $T(v_1+v_2) = T(v_1)+T(v_2)$

Ans.

$$T\Big(S(v_1+v_2)\Big) = T\Big(S(v_1)+S(v_2)\Big)$$

$$= T\Big(S(v_1)\Big) + T\Big(S(v_2)\Big)$$

(10) A linear transformation from V to W has an inverse from W to V when the range is all of W and the kernel contains only $v=0$. Then $T(v)=w$ has one solution v for each w in W. Why are these T's not invertible?

(a) $T(v_1, v_2) = (v_2, v_2)$, $W = \mathbb{R}^2$

Ans: $T(1, 0) = (0, 0) = 0$

(b) $T(v_1, v_2) = (v_1, v_2, v_1 + v_2)$ $\quad W = \mathbb{R}^3$

Ans: $(0, 1, 2)$ is not in the range.

(c) $T(v_1, v_2) = v_1$ $\quad W = \mathbb{R}^1$

Ans. $T(0, 1) = 0$

12. A linear transformation transforms $\underline{(1,1)}$ to $(2,2)$ and $\underline{(2,0)}$ to $(0,0)$. Find $T(v)$

Ans (a) $v = (2, 2)$

Ans: $v = (2, 2) = 2(1, 1)$

$T(v) = 2T(1, 1) = 2(2, 2) = (4, 4)$

(d) $v = (a, b)$

Ans: $v = (a, b) = b(1, 1) + \frac{a-b}{2}(2, 0)$

$T(v) = T(a, b) = b(2, 2) + \frac{a-b}{2}(0, 0) = b(2, 2) + (0, 0)$

16. $A = \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}$. Show that the identity matrix I is not in the range of T. Find a non-zero matrix M such that $T(M) = AM$ is zero.

Ans:

A is not invertible

$\Rightarrow AM = I$ is impossible.

$$\cancel{A' \begin{bmatrix} 1 & 2 \\ 3 & 6 \end{bmatrix}}$$

$$\begin{bmatrix} (1 \ \ 2) \\ (3 \ \ 6) \end{bmatrix} M = \begin{bmatrix} (1 \ \ 2)\, M \\ (3 \ \ 6)\, M \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$M = \begin{bmatrix} 2 & 2 \\ -1 & -1 \end{bmatrix}$$

ILA (11) 8.2(A)

16. T transposes every 2×2 matrix M. Try to find a matrix A which gives $AM = M^T$. Show that no matrix A will do it.

Is this a linear transformation that doesn't come from a matrix?

The matrix should be 4×4

Ans: Let $M = \left[\begin{array}{c|c} 0 & 1 \\ 0 & 0 \end{array}\right]$, $M^T = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

$$AM = A\left[\begin{array}{c|c} 0 & 1 \\ 0 & 0 \end{array}\right] = \left[A\begin{bmatrix} 0 \\ 0 \end{bmatrix} \;\; A\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right] = \left[\begin{array}{c|c} 0 & 0 \\ 1 & 0 \end{array}\right]$$

$$A\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

No matrix A gives $A\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

We have the linear transformation

$$T : M_{2\times 2}(\mathbb{R}) \longrightarrow M_{2\times 2}(\mathbb{R})$$

$$A \longrightarrow A^T$$

ILA (14) Back side

You have to go thro' an isomorphism b/w $M_{2\times 2}(\mathbb{R})$ and $\mathbb{R}^{2^2} = \mathbb{R}^4$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{R}) \xrightarrow{\;\sim\;} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \in \mathbb{R}^{2\times 2} = \mathbb{R}^4$$

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \xrightarrow{T} \begin{bmatrix}1\\0\\0\\0\end{bmatrix} ; \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \xrightarrow{T} \begin{bmatrix}0\\0\\1\\0\end{bmatrix} ; \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \xrightarrow{T} \begin{bmatrix}0\\1\\0\\0\end{bmatrix} ; \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \xrightarrow{T} \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

We can represent the linear transformation T with the representation matrix,

$$M_T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

* The vector space of $n \times n$ matrices is n^2-dimensional. Hence, the matrix representation of the linear map $A \to A^T$ would have to be $n^2 \times n^2$.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} a \\ c \\ b \\ d \end{bmatrix}$$

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} = A^T$$

18. $T(M) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} [M] \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. Find a matrix with $T(M) \neq 0$. Describe all matrices with $T(M) = 0$ (the kernel) and all op matrices $T(M)$ (the range).

Ans: $T(M) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$

Every $M = \begin{bmatrix} a & 0 \\ c & d \end{bmatrix}$ is in the kernel.

$M = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$ fill the range.

dim(range) + dim (kernel) $= 1 + 3 = 4 =$ dim of i/p space of 2×2 M's.

19. If A & B are invertible and $T(M) = AMB$, find $T^{-1}(M)$ in the form $(\ )M(\ )$

Ans: $T(T^{-1}(M)) = M$

$T^{-1}(M) = A^{-1} M B^{-1}$

(20.) How can you tell from the picture of T(house) that 'A' is ______

$T(H)=AH$

ⓐ diagonal matrix

Ans: Horizontal lines stay horizontal, vertical lines stay vertical.

ⓑ rank-one matrix

Ans: House squashes onto a line

ⓒ lower triangular matrix

Ans: Vertical lines stay vertical

(house)

22. What are the conditions on $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to ensure that T(house) will

(a) sit straight up.

Ans: $A = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$, $d > 0$

(b) expand the house by 3 in all directions?

Ans: $A = 3I$

29. What conditioned on $\det(A) = ad-bc$ ensure that the output house AH will

ⓐ be squashed onto a line

Ans: $ad-bc=0$

ⓑ keep its endpoints in clockwise order (not reflected)?

Ans: $$Ref(\theta) = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos^2 2\theta \end{bmatrix}$$

$$|Ref(\theta)| = -[\cos^2 2\theta + \sin^2 2\theta] = -1$$

$$ad-bc > 0$$

ⓒ have the same area as the original house?

Ans: $$Area(T(R)) = |\det(A)| \cdot Area(R)$$

$$|ad-bc| = 1$$

30) Why does every linear transformation T from $\mathbb{R}^2$ to $\mathbb{R}^2$ take squares to ||elograms?

Rectangles also goes to ||elograms. (squashed if T is not invertible)

Ans:

Linear transformations keep straight lines straight. !

$$\vec{u} = \frac{a\vec{v} + b\vec{w}}{a+b} \Rightarrow T(\vec{u}) = \frac{a\,T(\vec{v}) + b\,T(\vec{w})}{a+b}$$

And 2 ||el edges of a square (edges differing by a fixed v) go to two ||el edges (edges differing by $T(v)$).

$\therefore$ O/p is a ||elogram.

$\boxed{8.2}$

1. The transformation S takes the 2^{nd} derivative. Keep $1, x, x^2, x^3$ as the i/p basis v_1, v_2, v_3, v_4 and also as o/p basis w_1, w_2, w_3, w_4. Write $S(v_1), S(v_2), S(v_3), S(v_4)$ in terms of the w's. Find the 4x4 matrix A_2 for S.

Ans.

$$Sv = \frac{d^2 v}{dx^2}$$

$$v_1, v_2, v_3, v_4 = 1, x, x^2, x^3$$

$$S(v_1) = S(v_2) = 0, \quad S(v_3) = 2 = 2v_1$$

$$S(v_4) = 6x = 6v_2$$

Matrix for S is,

$$B = \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

2. What functions have $S(v) = 0$?

i.e., kernel of the 2nd derivative S.

What are the vectors in the $N(A)$?

Ans: $S(v) = \frac{d^2 v}{dx^2} = 0$ for linear functions

$$v(x) = \cancel{ax+b}$$
$$a + bx$$

Then $\begin{bmatrix} a \\ b \\ 0 \\ 0 \end{bmatrix}$ are in $N(B)$.

3. The 2nd derivative $A_2 = \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

is not the square of a rectangular 1st derivative matrix $A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$ does not allow $A_1^2 = A_2$

Add a zero row 4 to A_1 so that o/p space = i/p space. Compare A_1^2 with A_2.

Conclusion: we want o/p basis = ____ basis. Then $m = n$.

Ans:

$$A_1^2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = A_2$$

o/p basis $=\!=$ i/p basis

4. (a) The product TS of 1st and 2nd derivatives produces the 3rd derivative. Add zeros to make 4×4 matrices, then compute $A_1 A_2 = A_3$

Ans:

$$A_3 = A_1 A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = A_3$$

$A_2^2 = A_4 = 0$ since 4th derivative of cubic is zero.

same transformation

5. With bases v_1, v_2, v_3 and w_1, w_2, w_3

Suppose $T(v_1) = w_2$ and $T(v_2) = T(v_3) = w_1 + w_3$.

T is a linear transformation. Find the matrix A and multiply by the vector $(1,1,1)$. What's the o/p from T when the i/p is $v_1+v_2+v_3$?

Ans: $\cancel{A}(v_1+v_2+v_3) = w_2 + (w_1+w_3) + (w_1+w_3)$

$$= 2w_1 + w_2 + 2w_3$$

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$A\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 2 \end{bmatrix}$$

6. Since $T(v_2) = T(v_3)$, the solutions to $T(v) = 0$ are

$v =$ ______________.

What vectors are in the $N(A)$?

Find all solutions to $T(v) = w_2$.

Ans: $T(v_2) - T(v_3) = T(v_2 - v_3) = 0$.

$v = c(v_2 - v_3)$ gives $T(v) = 0$.

$$N(A) = c\begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix}$$

$$T(v_1) = w_2 \quad \downarrow \quad v_p = v_1$$

Solutions to $T(v) = w_2$ are

Nice

$$v_p + v_n = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + c\begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix}$$

7. Find a vector that is not in the $C(A)$.
Find a combination of w's that is not in the range of the transformation T.

Hack 5/1/2021

Ans: $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \notin C(A)$

$T(v_1) = W_2 = 0W_1 + 1W_2 + 0W_3$

$T(v_2) = W_1 + W_3 = 1W_1 + 0W_2 + 1W_3$

$T(v_3) = W_1 + W_3 = 1W_1 + 0W_2 + 1W_3$

$T : V \longrightarrow W$

The matrix for the linear transformation w.r.t bases V and W is:

$$A_{vw} = \left[[T(v_1)]_W, [T(v_2)]_W, [T(v_3)]_W \right]$$

$$\cancel{= \left[[W_2], [W_1 + W_3], [W_1 + W_3] \right]}$$

$$= \left\{ [T(v_1)]_W = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, [T(v_2)]_W = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = [T(v_3)]_W \right.$$

$$A_{VW} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$\cancel{(0, 1, 0)}$

$$A_{VW}[x]_V = [x]_W$$

$$A^T = \begin{bmatrix}0 & 1 & 0\\ 1 & 0 & 1\\ 1 & 0 & 1\end{bmatrix} \Rightarrow \begin{matrix} b = 0 \\ a+c = 0 \end{matrix}$$

$$\begin{bmatrix}a\\ b\\ c\end{bmatrix} = t\begin{bmatrix}1\\ 0\\ -1\end{bmatrix}$$

$\begin{bmatrix}1\\ 0\\ 0\end{bmatrix} \notin C(A)$ since $\begin{vmatrix}0 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{vmatrix} = -1\begin{vmatrix}1 & 1\\ 1 & 0\end{vmatrix} = 1 \neq 0$

$[T(V_3)]_W$

$$\begin{bmatrix}1\\ 0\\ 0\end{bmatrix} = 1W_1 + 0W_2 + 0W_3 = W_1$$

$W \notin \text{range}(T)$

Let $v = av_1 + bv_2 + cv_3 \in V$

$$T(v) = w_1$$

$$aT(v_1) + bT(v_2) + cT(v_3) = w_1$$

$$aw_2 + b(w_1 + w_3) + c(w_1 + w_3) = w_1$$

$$w_1(b+c-1) + aw_2 + w_3(b+c) = 0.$$

$b + c = 1$ & $b + c = 0$

Not possible

$\therefore$ $w_1 \notin \text{range}(T)$.

8. You don't have enough information to determine T^2.?
Why is its matrix not necessarily A^2?
What more information do you need?

Ans:
We don't know $T(W)$ unless the W's are the same as the V's.

In that case, the matrix is A^2.

10. Suppose, $T(v_1) = w_1 + w_2 + w_3$ and $T(v_2) = w_2 + w_3$ and $T(v_3) = w_3$. Find the matrix A for T using these basis vectors.
What i/p vector v gives $T(v) = w_1$?

Ans:
$$T(v_1) = 1w_1 + 1w_2 + 1w_3 \Rightarrow [T(v_1)]_W = (1,1,1)$$
$$T(v_2) = 0w_1 + 1w_2 + 1w_3 \Rightarrow [T(v_2)]_W = (0,1,1)$$
$$T(v_3) = 0w_1 + 0w_2 + 1w_3 \Rightarrow [T(v_3)]_W = (0,0,1)$$

The matrix for T is

$$A_{VW} = \begin{bmatrix} [T(v_1)]_W & [T(v_2)]_W & [T(v_3)]_W \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$\cancel{A^{-1}V_W A}$ $\quad \cancel{T(v) = Av = (1,1,1)}$

$$\cancel{V = A^{-1}\begin{bmatrix}1\\1\\1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\-1 & 1 & 0\\0 & -1 & 1\end{bmatrix}\begin{bmatrix}1\\1\\1\end{bmatrix} = \begin{bmatrix}1\\0\\0\end{bmatrix}}$$

$$T(v) = W_1 = T(v_1) - T(v_2) = \begin{bmatrix}1\\0\\0\end{bmatrix}$$

$\cancel{A^{-1}} =$

$$V = A^{-1}\begin{bmatrix}1\\0\\0\end{bmatrix} = \begin{bmatrix}1 & 0 & 0\\-1 & 1 & 0\\0 & -1 & 1\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix} = \begin{bmatrix}1\\-1\\0\end{bmatrix} = v_1 - v_2$$

11. Invert the matrix A in problem (10).
Also invert the transformation T — what are $T^{-1}(w_1)$, $T^{-1}(w_2)$ & $T^{-1}(w_3)$?

Ans:

$$A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}$$

$$T^{-1}(w_1) = V_1 - \cancel{W}_2 = V_1 - \cancel{W}_2 + 0\cancel{W}_3$$

$$T^{-1}(w_2) = V_2 - \cancel{W}_3 = 0V_1 + V_2 - V_3$$

$$T^{-1}(w_3) = V_3 = 0V_1 + 0V_2 + V_3$$

$$T^{-1} : W \longrightarrow V$$

$$A_{WV} = \begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} = A_{VW}^{-1}$$

13. Suppose the spaces V and W have the same basis v_1, v_2.

(a) Describe a transformation T (not I) that is its own inverse

Ans: $T^2 = I$

$$\left.\begin{aligned} T(v_1) &= v_2 \\ T(v_2) &= v_1 \end{aligned}\right\} A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

(b) Describe a transformation T (not I) that equals T^2

Ans: $T^2 = T$

$$\left.\begin{aligned} T(v_1) &= v_1 \\ T(v_2) &= 0 \end{aligned}\right\} A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

(c) Why can't the same T be used for both (a) and (b)?

Ans: T must be I

$T^2 = T = I$

14. (a) What matrix B transforms $(1,0)$ to $(2,5)$ and transforms $(0,1)$ to $(1,3)$?

Ans:

$$B = \begin{bmatrix} T(1,0) & T(0,1) \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$$

(b) What matrix C transforms $(2,5)$ to $(1,0)$ and $(1,3)$ to $(0,1)$?

Ans: $\cancel{C = \begin{bmatrix} T(2,5) & T(1,3) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}$

$$C = B^{-1} = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}^{T} = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$$

(c) Why does no matrix transform $(2,6)$ to $(1,0)$ and $(1,3)$ to $(0,1)$?

Ans: $A\begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$$\hookrightarrow A\begin{bmatrix} 2 \\ 6 \end{bmatrix} = 2A\begin{bmatrix} 1 \\ 3 \end{bmatrix} = 2\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix} \neq \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

15.

(a) What matrix M transforms (1,0) and (0,1) to (r,t) and (s,u)?

Ans:

$$M = \begin{bmatrix} T(0,1) & T(1,0) \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

(b) What matrix N transforms (a,c) and (b,d) to (1,0) and (0,1)?

Ans:

$$N = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} =$$

(c) What condition on a, b, c, d will make part (b) impossible?

Ans: $ad - bc = 0$

(1,0)

16. (a) How does M & N yield the matrix that transforms (a,c) to (r,t) and (b,d) to (s,u)?

Ans: ~~NM~~ MN

(b) What matrix transforms (2,5) to (1,1) and (1,3) to (0,2) ?

Ans: $\cancel{\begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}}$ $\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}^{-1}$

$$\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}^{T} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} = \begin{bmatrix} 3 & -1 \\ -7 & 3 \end{bmatrix}$$

17. If you keep the same basis vectors but put them in different order, the change of basis matrix B is a permutation matrix.

If you keep the basis vectors in order but change their lengths, B is a positive diagonal matrix.

Prof

18. The matrix that rotates the axis vectors $(1,0)$ and $(0,1)$ thro' an angle θ is Q. What are the coordinates (a,b) of the original $(1,0)$ using the new (rotated) axes?

$$Q = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \quad \& \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} = a \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} + b \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}$$

$$\Longrightarrow a = \cos\theta, \; b = -\sin\theta$$

$$Q(1,0) = (\cos\theta, \sin\theta) \quad \& \quad Q(0,1) = (-\sin\theta, \cos\theta)$$

Ans:

$$[(a,b)]_{new} = P_{new \leftarrow old} \, [(a,b)]_{old}$$

$$= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{T} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\theta \\ -\sin\theta \end{bmatrix}$$

19. The matrix that transforms (1,0) & (0,1) to
(a) (1,4) & (1,5) is B = ______.

~~The~~

Ans: $B = \begin{bmatrix} 1 & 1 \\ 4 & 5 \end{bmatrix}$

(b) The combinations $a(1,4)+b(1,5)$ that equals (1,0) has (a,b) = ______

Ans: (1,0) in the basis of {(1,4) & (1,5)}

$$[(1,0)]_{new} = P_{new \leftarrow old} \, [(1,0)]_{old} = B^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 \\ 4 & 5 \end{bmatrix}^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 & -4 \\ -1 & 1 \end{bmatrix}^{T} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & -1 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 \\ -4 \end{bmatrix}$$

20. The parabola $\omega_1 = \frac{1}{2}(x^2+x)$ equals 1 at $x=1$, and 0 at $x=0$ and $x=-1$. Find the parabolas ω_2, ω_3 and find $y(x)$ by linearity.

ⓐ $\omega_2 = 1$ at $x=0$ and $\omega_2 = 0$ at $x=1$ & $x=-1$

Ans: $\omega = ax^2+bx+c$

$\omega_2(0) = c = 1$; $\omega_2(1) = a+b+1 = 0$; $\omega_2(-1) = a-b+1 = 0$

$$\begin{array}{r} a-b+1=0 \\ \hline 2a+2=0 \end{array} \Rightarrow a=-1,\ b=0.$$

$\underline{\underline{\omega_2 = -x^2+1}}$

ⓑ $\omega_3 = 1$ at $x=-1$ and $\omega_3 = 0$ at $x=0$ & $x=1$

Ans: $\omega_3(-1) = a-b+c = 1$; $\omega_3(0) = c = 0$; $\omega_3(1) = a+b = 0$

$$\begin{array}{r} a-b=1 \\ a+b=0 \\ \hline 2a=1 \end{array} \Rightarrow a = \tfrac{1}{2};\ b = -\tfrac{1}{2};\ c=0$$

$\omega_3 = \frac{1}{2}(x^2-x)$

(c) $y(x) = 4$ at $x = 1$ & $y(x) = 5$ at $x = 0$ & $y(x) = 6$ at $x = -1$.

Ans: $y(x) = ax^2 + bx + c$

$y(1) = a + b + c = 4$; $y(0) = c = 5$

$y(-1) = a - b + c = 6$

$2a + 10 = 10 \Rightarrow a = 0$

$b = a + c - 6 = 5 - 6 = -1$

$a = 0,\ b = -1,\ c = 5$

$\boxed{y(x) = -x + 5} \rightarrow [0, -1, 5]$

$w_1 = \frac{1}{2}(x^2 + x) = \frac{1}{2}x^2 + \frac{1}{2}x + 0 \rightarrow [\frac{1}{2}, \frac{1}{2}, 0]$

$w_2 = -x^2 + 1 = -x^2 + 0x^2 + 1 \rightarrow [-1, 0, 1]$

$w_3 = \frac{1}{2}(x^2 - x) = \frac{1}{2}x^2 - \frac{1}{2}x + 0 \rightarrow [\frac{1}{2}, -\frac{1}{2}, 0]$

$$[0, -1, 1]_B = P_{B \leftarrow E}\ [(0, -1, 5)]$$

$$= \begin{bmatrix} \frac{1}{2} & -1 & \frac{1}{2} \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ -1 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ -1 \\ 5 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \\ 6 \end{bmatrix}$$

$$y(x) = -x+5 = \underline{4\omega_1 + 5\omega_2 + 6\omega_3}.$$

Q3. Under what conditions on the numbers $m_1, m_2, \ldots, m_9$ do these 3 parabolas give a basis for the space of all parabolas $a+bx+cx^2$?

$v_1 = m_1 + m_2 x + m_3 x^2$

$v_2 = m_4 + m_5 x + m_6 x^2$

$v_3 = m_7 + m_8 x + m_9 x^2$

Ans :

The change of basis matrix is invertible

$$M = \begin{bmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{bmatrix} \text{ is invertible.}$$

24. The Gram-Schmidt process changes a basis a_1, a_2, a_3 to an orthonormal basis q_1, q_2, q_3. These are the columns in $A = QR$. Show that R is the change of basis matrix from the a's to the q's.

Ans: $A = QR$

$$\begin{bmatrix} a_1 & a_2 & a_3 \end{bmatrix} = \begin{bmatrix} q_1 & q_2 & q_3 \end{bmatrix} \begin{bmatrix} a_1^T q_1 & a_2^T q_1 & a_3^T q_1 \\ 0 & a_2^T q_2 & a_3^T q_2 \\ 0 & 0 & a_3^T q_3 \end{bmatrix}$$

$$a_1 = (a_1^T q_1)\, q_1$$

$$a_2 = (a_2^T q_1)\, q_1 + (a_2^T q_2)\, q_2$$

$$a_3 = (a_3^T q_1)\, q_1 + (a_3^T q_2)\, q_2 + (a_3^T q_3)\, q_3$$

$\Rightarrow$ a_i as a combination of q_i

$\therefore$ R is a change of basis matrix.

GR.

25. Elimination changes the rows of A to the rows of U with $A = LU$. Row 2 of A is what combination of the rows of U? Writing $A^T = U^T L^T$ to work with columns. The change of basis matrix is $B = L^T$. We have bases if the matrices are ______

Ans. Row 2 of $A = l_{21}$ (row 1 of U) $+ l_{22}$ (row 2 of U)

The change of basis matrix is always invertible.

26. Suppose, v_1, v_2, v_3 are eigenvectors for T. This means $T(v_i) = \lambda_i v_i$ for $i = 1, 2, 3$. What is the matrix for T when the i/p and o/p bases are the v's. ?

Ans:

$$A v_1 = \lambda_1 v_1 + 0 v_2 + 0 v_3$$

$$A v_2 = 0 v_1 + \lambda_2 v_2 + 0 v_3$$

$$A v_3 = 0 v_1 + 0 v_2 + \lambda_3 v_3$$

$$A = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} = \mathrm{diag}(\lambda_1, \lambda_2, \lambda_3)$$

27. Every invertible linear transformation can have I as its matrix! Choose any i/p basis $v_1, v_2, \ldots, v_n$. For o/p basis choose $w_i = T(v_i)$. Why must T be invertible ?

Ans: If T is not invertible, $T(v_1) \ldots T(v_n)$ is not a basis.

We couldn't choose $w_i = T(v_i)$

2c. Using $v_1 = w_1$ & $v_2 = w_2$ find the standard matrix for these T's:

ⓐ $T(v_1) = 0$ & $T(v_2) = 3v_1$

Ans: $$[T] = \begin{bmatrix} 0 & 3 \\ 0 & 0 \end{bmatrix}$$

ⓑ $T(v_1) = v_1$ and $T(v_1 + v_2) = v_1$

Ans: $\cancel{[T] = \begin{bmatrix} 1 & \\ 0 & 2 \end{bmatrix}}$

$$\left.\begin{aligned} T(v_1) &= v_1 \\ T(v_2) &= 0 \end{aligned}\right\} \begin{aligned} T(v_1+v_2) &= T(v_1) + T(v_2) \\ &= v_1 + 0 = v_1 \end{aligned}$$

$$[T] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

29. Suppose T reflects the xy-plane across the x-axis & S is reflection across the y-axis. If $v = (x, y)$, what is $S(T(v))$? Find a simpler description of the product ST?

Ans:
$$\left.\begin{aligned} T\begin{bmatrix}1\\0\end{bmatrix} &= \begin{bmatrix}1\\0\end{bmatrix} \\ T\begin{bmatrix}0\\1\end{bmatrix} &= \begin{bmatrix}0\\-1\end{bmatrix}\end{aligned}\right\} [T] = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$$

$$T(x, y) = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} = \begin{bmatrix}x\\-y\end{bmatrix}$$

$$\left.\begin{aligned} S\begin{bmatrix}1\\0\end{bmatrix} &= \begin{bmatrix}-1\\0\end{bmatrix} \\ S\begin{bmatrix}0\\1\end{bmatrix} &= \begin{bmatrix}0\\1\end{bmatrix}\end{aligned}\right\} [S] = \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}$$

$$S(x, y) = \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} = \begin{bmatrix}-x\\y\end{bmatrix}$$

$$ST = \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} = \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix} = -I$$

31. The product of 2 reflections is a rotation.

multiply these reflection matrices to find the rotation angle

Ans: $$\operatorname{Ref}(\theta)\operatorname{Ref}(\alpha) = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}\begin{bmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{bmatrix}$$

$$= \begin{bmatrix} \cos(2\theta - 2\alpha) & \sin(2\alpha - 2\theta) \\ \sin(2\theta - 2\alpha) & \cos(2\theta - 2\alpha) \end{bmatrix}$$

$$= \begin{bmatrix} \cos[2(\theta-\alpha)] & -\sin[2(\theta-\alpha)] \\ \sin[2(\theta-\alpha)] & \cos[2(\theta-\alpha)] \end{bmatrix}$$

$$= \operatorname{Rot}[2(\theta-\alpha)]$$

32. Suppose A is a 3×4 matrix of rank $r = 2$, and $T(v) = Av$. Choose i/p basis vectors v_1, v_2 from the row space of A, and v_3, v_4 from the nullspace. Choose o/p basis vectors $w_1 = Av_1$, $w_2 = Av_2$ in the column space & w_3 from the nullspace of A^T. What speciality simple matrix represents T in these special bases?

Ans: ~~dim(row space)~~ =

$v_i \in \mathbb{R}^4$

$w_i \in \mathbb{R}^3$.

$$\left.\begin{aligned} Av_1 &= w_1 + 0w_2 + 0w_3 \\ Av_2 &= 0w_1 + w_2 \\ Av_3 &= 0 \\ Av_4 &= 0 \end{aligned}\right\} \quad A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

33. The space M of 2×2 matrices has the basis v_1, v_2, v_3, v_4. Suppose T multiplies each matrix by $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. With w's equal to v's, what 4×4 matrix A represents this transformation T on matrix space?

Ans: $T(v_1) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} = a v_1 + c v_3$

$T(v_2) = a v_2 + c v_4$

$T(v_3) = b v_1 + d v_3$

$T(v_4) = b v_2 + d v_4$

$$[T] = \begin{bmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{bmatrix}$$

8.3

Ex: 1

The Jordan matrix J has eigenvalues $\lambda = 2, 2, 3, 3$ (2 double eigenvalues). Those eigenvalues lie along the diagonal because J is triangular. There are 2 independent eigenvectors for $\lambda = 2$, but there is only one line of eigenvectors for $\lambda = 3$.

This is true for every matrix $C = BJB^{-1}$ that is similar to J.

Jordan matrix, $J = \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix} \end{bmatrix}$

2 eigenvectors for $\lambda = 2$ are $x_1 = (1, 0, 0, 0)$ and $x_2 = (0, 1, 0, 0)$. One eigenvector for $\lambda = 3$ is $x_3 = (0, 0, 1, 0)$.

The generalized eigenvector for this Jordan matrix is the 4th standard basis vector $x_4 = (0, 0, 0, 4)$

1. In Ex: 1, what is the rank of $J-3I$? What's the dimension of its null space?

Ans: $$J = \begin{bmatrix} 2 & & & \\ & 2 & & \\ & & 3 & 1 \\ & & & 3 \end{bmatrix} \longrightarrow J-3I = \begin{bmatrix} -1 & & & \\ & -1 & & \\ & & 0 & 1 \\ & & & 0 \end{bmatrix}$$

$$\text{rank}(J-3I) = 3$$

$$\Longrightarrow \underbrace{\dim(N(J-3I)) = 4-3 = 1}_{\#\text{ of independent eigenvectors for } \lambda = 3.}$$

The algebraic multiplicity is 2, because $\det(J-\lambda I)$ has the repeated factor $(\lambda-3)^2$.
The geometric multiplicity is 1, because there is only one independent eigenvector.

2. These matrices A_1 and A_2 are similar to J. Solve $A_1 B_1 = B_1 J$ and $A_2 B_2 = B_2 J$ to find the basis matrices B_1 and B_2 with $J = B_1^{-1} A B_1$ and $J = B_2^{-1} A B_2$

$$J = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad A_1 = \begin{bmatrix} 0 & 4 \\ 0 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 4 & -8 \\ 2 & -4 \end{bmatrix}$$

Ans: $J = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is similar to all other 2×2 matrices A that have 2 zero eigenvalues but only 1 independent eigenvecto

$(A_1 - \lambda I) v_1 = 0$ & $(A_1 - \lambda I) v_2 = v_1$

$$\begin{bmatrix} 0 & 4 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = 0 \quad \& \quad \begin{bmatrix} 0 & 4 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$4d = 1 \Rightarrow d = \frac{1}{4}$

$4b = 0 \Rightarrow b = 0$

$v_1 = t \begin{bmatrix} 1 \\ 0 \end{bmatrix} \longrightarrow \quad V_2 = k \begin{bmatrix} 0 \\ \frac{1}{4} \end{bmatrix}$

$A_1 B_1 = B_1 J$.

$$\begin{bmatrix} 0 & 4 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1/4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1/4 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 4 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$(A_2 - \lambda I)\, V_1 = 0$

$$\begin{bmatrix} 4 & -8 \\ 2 & -4 \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = 0$$

$a - 2b = 0$

$a = 2b$

$$V_1 = t\begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

& $(A_2 - \lambda I)\, V_2 = V_1$

$$\begin{bmatrix} 4 & -8 \\ 2 & -4 \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

$c - 2d = \frac{1}{2}$

$d = 0, \quad c = 1/2$

$$V_2 = k\begin{bmatrix} 1/2 \\ 0 \end{bmatrix}$$

$A_2 B_2 = B_2 J$

$$\begin{bmatrix} 4 & -8 \\ 2 & -4 \end{bmatrix}\begin{bmatrix} 2 & 1/2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1/2 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 4 & -8 \\ 2 & -4 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

3. This transpose block J^T has the same triple eigenvalue 2 (with only one eigenvector) as J. Find the basis change B so that $J = B^{-1} J^T B$ ($BJ = J^T B$).

$$J = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}, \quad J^T = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix}$$

Ans: $\boxed{J^T = B J B^{-1}}$

$(J^T - \lambda I) V_1 = 0$

$$\left(\begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix} - \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} \right) \begin{bmatrix} a \\ b \\ c \end{bmatrix} = 0$$

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = 0 \longrightarrow \begin{matrix} a = 0 \\ b = 0 \end{matrix}$$

$$V_1 = t \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\left(J^T - \lambda I\right) V_2 = V_1$$

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} c \\ d \\ e \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \Longrightarrow \begin{matrix} c = 0 \\ d = 1 \end{matrix}$$

$$V_2 = k \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\left(J^T - \lambda I\right) V_3 = V_2$$

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} f \\ g \\ h \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \Longrightarrow \begin{matrix} f = 1 \\ g = 0 \end{matrix}$$

$$V_3 = l \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$BJ = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = J^T B$$

$\Longrightarrow$ Every matrix is similar to its transpose (same eigenvalues, same multiplicity, same Jordan form).

4. J & K are Jordan forms with the same
2 zero eigenvalues and the same rank 2.
But show that no invertible B solves
$BK = JB$, so K is not similar to J.

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 \\ & 0 & 0 & 0 \\ & & 0 & 1 \\ & & & 0 \end{bmatrix} \; ; \; K = \begin{bmatrix} 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 \\ & & 0 & 0 \\ & & & [0] \end{bmatrix}$$

Ans: J & K are different Jordan forms (block sizes 2, 2 versus block sizes 3, 1).

Even though J & K have the same λ's (all 0) and same rank, J and K are not similar.

$$BK = B \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & b_{11} & b_{12} & 0 \\ 0 & b_{21} & b_{22} & 0 \\ 0 & b_{31} & b_{32} & 0 \\ 0 & b_{41} & b_{42} & 0 \end{bmatrix}$$

$$JB = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} B = \begin{bmatrix} b_{21} & b_{22} & b_{23} & b_{24} \\ 0 & 0 & 0 & 0 \\ b_{41} & b_{42} & b_{43} & b_{44} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$BK = JB \Longrightarrow$

B is not invertible.

5. If $A^3 = 0$ show that all $\lambda = 0$, and all Jordan blocks with $J^3 = 0$ have size 1, 2 ~~or~~ 3.

$\Longrightarrow$ $\text{rank}(A) \leq \frac{2n}{3}$. If $A^n = 0$ why is $\text{rank}(A) < n$

Ans: $A^3 = 0$

$$Ax = \lambda x \Longrightarrow A^3 x = \lambda^3 x = 0$$

$$\Longrightarrow \underline{\underline{\lambda = 0}} \quad \text{since } x \neq 0.$$

$$A = BJB^{-1} \Longrightarrow \cancel{A^3 = BJ^3B^{-1} = 0}$$

$$J = B^{-1}AB$$

$$\Longrightarrow \underline{\underline{J^3 = B^{-1}A^3B = 0}}$$

The Jordan form J will also have $J^3 = 0$.

$$\begin{bmatrix} \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & \begin{matrix} 0 & 0 \end{matrix} & [3] \end{bmatrix}^n = \begin{bmatrix} A_1 & & \\ & A_2 & \\ & & A_3 \end{bmatrix}^n = \begin{bmatrix} A_1^n & & \\ & A_2^n & \\ & & A_3^n \end{bmatrix}$$

The Blocks of J must become zero blocks in J^3.
So these Blocks of J can be

$$[0], \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

The rank of J (and A) is largest if every block is 3×3 of rank 2.

$$\text{rank}(A) \le \left(\frac{n}{3}\right)2 = \frac{2n}{3}$$

$$A^n = 0 \Longrightarrow \lambda^n = 0 \Longrightarrow \lambda = 0 \longrightarrow |A| = 0$$

A is not invertible.

i.e., $\text{rank}(A) < n$.

J^3.

6. Show that $u(t) = \begin{bmatrix} te^{\lambda t} \\ e^{\lambda t} \end{bmatrix}$ solves $\frac{du}{dt} = Ju$

with $J = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}$ and $u(0) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

J is not diagonalizable so $te^{\lambda t}$ enters the solution.

ILA (7)

Ans: $u' = Ju$

$$\begin{bmatrix} e^{\lambda t} + t\lambda e^{\lambda t} \\ \lambda e^{\lambda t} \end{bmatrix} = \begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix} \begin{bmatrix} te^{\lambda t} \\ e^{\lambda t} \end{bmatrix} = \begin{bmatrix} t\lambda e^{\lambda t} + e^{\lambda t} \\ \lambda e^{\lambda t} \end{bmatrix}$$

At $t=0$: $u_1 = 0$ & $u_2 = 1$

$\therefore$ We have the solution & it involves $te^{\lambda t}$

7. Show that the difference equation $V_{k+2} - 2\lambda V_{k+1} + \lambda^2 V_k = 0$ is solved by $V_k = \lambda^k$ and also by $V_k = k\lambda^k$. Those correspond to $e^{\lambda t}$ and $te^{\lambda t}$ in problem (6).

Ans: The eqn. $V_{k+2} - 2\lambda V_{k+1} + \lambda^2 V_k = 0$ is solved by $u_k = \lambda^k$. But, it is a 2^{nd} order equation and there must be another solution.

In analogy with $te^{\lambda t}$ for the differential eqn. in $\boxed{8.3.6}$, the 2^{nd} solution is $u_k = k\lambda^k$.

Check:

$$(k+2)\lambda^{k+2} - 2\lambda(k+1)\lambda^{k+1} + \lambda^2 k\lambda^k =$$

$$= [k+2 - 2(k+1) + k]\lambda^{k+2} = 0$$

8. Write the 3×3 Fourier matrix F with columns $(1, \lambda, \lambda^2)$

$\lambda^3 = 1$ has 3 roots

Ans: $\omega = e^{i\frac{2\pi}{N}} = e^{i\frac{2\pi}{3}}$

$1, e^{i2\pi/3}, e^{i4\pi/3}$

$$F = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \lambda & \lambda^2 \\ 1 & \lambda^2 & \lambda^4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{i2\pi/3} & e^{i4\pi/3} \\ 1 & e^{i4\pi/3} & e^{i8\pi/3} \end{bmatrix}.$$

9. Check that any 3×3 circulant C has eigenvectors $(1, \lambda, \lambda^2)$ from problem 8
If the diagonals of your matrix C contain c_0, c_1, c_2 then its eigenvalues are in Fc.

Ans:
$$C = \begin{bmatrix} c_0 & c_1 & c_2 \\ c_2 & c_0 & c_1 \\ c_1 & c_2 & c_0 \end{bmatrix} \text{ with}$$

$$C \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = (c_0 + c_1 + c_2) \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$C \begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \end{bmatrix} = (c_0 + c_1\lambda + c_2\lambda^2) \begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \end{bmatrix}$$

$$C\begin{bmatrix}1\\ \lambda^2\\ \lambda^4\end{bmatrix}=\left(c_0+\lambda^2c_1+\lambda^4c_2\right)\begin{bmatrix}1\\ \lambda^2\\ \lambda^4\end{bmatrix}$$

$$Fc=\begin{bmatrix}1&1&1\\1&\lambda&\lambda^2\\1&\lambda^2&\lambda^4\end{bmatrix}\begin{bmatrix}c_0\\c_1\\c_2\end{bmatrix}=\begin{bmatrix}c_0+c_1+c_2\\c_0+\lambda c_1+\lambda^2c_2\\c_0+\lambda^2c_1+\lambda^4c_2\end{bmatrix}$$

9 COMPLEX VECTORS & MATRICES

The complex plane

Complex #s corresp. to points in a plane.
Real #s go along the x-axis.

Adding & subtracting complex #s is like adding and subtracting vectors in the plane. The real component stays separatate from the imaginary component.

⇒ The complex plane $\mathbb{C}^1$ is like the ordinary 2D plane $\mathbb{R}^2$, except that we multiply complex numbers & we didn't multiply vectors.

* If A is real,

$$Ax = \lambda x \longrightarrow A\bar{x} = \bar{\lambda}\bar{x}$$

* $z = a + ib$

$$|z|^2 = z\bar{z} = (a+ib)(a-ib) = a^2+b^2$$

$$\frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2} = \frac{\bar{z}}{|z|^2}$$

On the unit circle, $|z| = 1$

$$\frac{1}{z} = \bar{z}$$

* $z = a + ib = r\cos\theta + i r\sin\theta = re^{i\theta}$

Ex: Find r and θ for $z = 1+i$ and also for the conjugate $\bar{z} = 1-i$.

Ans: $r = |z| = \sqrt{2} = |\bar{z}|$

$\tan\theta = -1$ & $\sin\theta = \frac{-1}{\sqrt{2}}$, $\cos\theta = \frac{1}{\sqrt{2}}$

$\theta = -\pi/4$

* $z = r\cos\theta + i r\sin\theta = re^{i\theta}$

$$z^n = r^n\left(\cos n\theta + i\sin n\theta\right) = r^n e^{in\theta}$$

$$z_1 z_2 = r_1(\cos\theta_1 + i\sin\theta_1)\cdot r_2\left(\cos\theta_2 + i\sin\theta_2\right) = r_1 e^{i\theta_1} * r_2 e^{i\theta_2}$$

$$= r_1 r_2\left[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\right]$$

$$= r_1 r_2 e^{i(\theta_1+\theta_2)}$$

* n^{th} root of unity

~~Solutions of~~ $\cancel{z^n = 1}$.

n different #s whose n^{th} powers equal 1.

Let, $\omega = e^{i 2\pi/n}$,

the n^{th} powers of $1, \omega, \omega^2, \ldots, \omega^{n-1}$ all equal 1.

Those are the n^{th} roots of 1. They solve the equation $z^n = 1$.

- These are equally spaced around the unit circle, where the full 2π is divided by n. Multiply their angles by n to take n^{th} powers.

Hermitian & Unitary matrices

$$Z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} a_1+ib_1 \\ a_2+ib_2 \\ \vdots \\ a_n+ib_n \end{bmatrix}$$

Conjugate transpose

$$z^H = \bar{z}^T = \begin{bmatrix} \bar{z}_1 & \bar{z}_2 & \cdots & \bar{z}_n \end{bmatrix} = \begin{bmatrix} a_1-ib_1 & a_2-ib_2 & \cdots & a_n-ib_n \end{bmatrix}$$

The length squared of a real vector is $x_1^2 + \cdots + x_n^2$.

The length squared of a complex vector is NOT $z_1^2 + \cdots + z_n^2$.

The length of $(1, i)$ would be $1^2 + i^2 = 0$

A non-zero vector would have zero length.

— not good.

Other vectors would have complex lengths.

Length squared

$$\begin{bmatrix} \bar{z}_1 & \bar{z}_2 & \cdots & \bar{z}_n \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = |z_1|^2 + |z_2|^2 + \cdots + |z_n|^2$$

$$\bar{z}^T z = \|z\|^2$$

$$\boxed{\|z\|^2 = \bar{z}^T z = z^H z = |z_1|^2 + |z_2|^2 + \cdots + |z_n|^2}$$

where,

$\bar{z}^T = z^H$: conjugate transpose of z

(or)

z Hermitian

Complex inner products

It'll be very desirable if $z^H z$ is the inner product of z with itself.

The inner product of real or complex vectors u and v is $u^H v$:

$$\boxed{u^H v = \begin{bmatrix} \bar{u}_1 & \cdots & \bar{u}_n \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \bar{u}_1 v_1 + \cdots + \bar{u}_n v_n}$$

$$(a+ib)(c-id) = (ac+bd) + i(bc-ad)$$

$$(c-id)(a+ib) = (ac+bd) + i(bc-ad)$$

$$v^H u = \begin{bmatrix} \bar{v}_1 & \cdots & \bar{v}_n \end{bmatrix} \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = \bar{v}_1 u_1 + \cdots + \bar{v}_n u_n$$

$$\boxed{u^H v \neq v^H u}$$

* The inner product of Au with v equals the inner product of u with $A^H v$.

$$\boxed{(Au)^H v = u^H (A^H v)}$$

A^H : adjoint of A

$$(AB)^H = B^H A^H$$

□ Hermitian matrices, $S^H = S$

* If $S^H = S$ and z is any real or complex column vector, the number $z^H S z$ is real.

Proof.

$z^H S z$ is 1×1.

$$(z^H S z)^H = z^H S^H (z^H)^H = z^H S z$$

$$\Longrightarrow \quad z^H S z \text{ is real.}$$

$z^H S z$: energy

* Every eigenvalue of a Hermitian matrix is real.

<u>Proof</u>

$Sz = \lambda z$

$z^H S z = \lambda z^H z$

$\lambda = \dfrac{z^H S z}{z^H z}$ is real

* The eigenvectors of a Hermitian matrix are orthogonal. (when they corresp. to different eigenvalues)

If $Sz = \lambda z$ and $Sy = \beta y$,

then $y^H z = 0$

Proof $Sz = \lambda z$ & $Sy = \beta y$

$$\Downarrow$$

$$y^H S^H = \beta y^H.$$

$$y^H S z = \lambda y^H z$$

$$y^H S z = \beta y^H z$$

$$\Longrightarrow \lambda y^H z = \beta y^H z \Longrightarrow y^H z = 0 \text{ since } \lambda \neq \beta$$

Unitary matrices

* A unitary matrix Q is a (complex) square matrix that has orthonormal columns.

Every matrix Q with orthonormal columns has $Q^H Q = I$.

If Q is square, it is a unitary matrix. Then $Q^H = Q^{-1}$.

Real V/s Complex

$\mathbb{R}$ = line of all real #
$-\infty < x < \infty$

$\mathbb{C}$ = plane of all complex #
$z = x + iy$

$|x|$ = absolute value of x

$|z| = \sqrt{x^2+y^2} = r$ = absolute value (or modulus) of z

1 & -1 solve $x^2 = 1$

$z = 1, \omega, \ldots, \omega^{n-1}$ solve $z^n = 1$ where $z = e^{2\pi i/n}$.

The complex conjugate of $z = x+iy$ is $\bar{z} = x - iy$
$$|z|^2 = x^2+y^2 = z\bar{z} \quad \& \quad \frac{1}{z} = \frac{\bar{z}}{|z|^2}$$

The polar form of $z = x+iy$ is $|z|e^{i\theta} = re^{i\theta}$
$= r(\cos\theta + i\sin\theta)$
$\tan\theta = y/x$

$\mathbb{R}^n$: vectors with n real components

$\mathbb{C}^n$: vectors with n complex components.

length: $\|x\|^2 = x_1^2 + \cdots + x_n^2$

length: $\|z\|^2 = |z_1|^2 + \cdots + |z_n|^2$

transpose: $(A^T)_{ij} = A_{ji}$

Conjugate transpose: $(A^H)_{ij} = \bar{A}_{ji}$

dot product: $x^Ty = x_1y_1 + \cdots + x_ny_n$

Inner product: $u^Hv = \bar{u}_1v_1 + \cdots + \bar{u}_nv_n$

reason for A^T: $(Ax)^Ty = x^T(A^Ty)$

reason for A^H: $(Au)^Hv = u^H(A^Hv)$

Orthogonality: $x^Ty = 0$

Orthogonality: $u^Hv = 0$

Symmetric matrices: $S = S^T$
$S = Q\Lambda Q^{-1} = Q\Lambda Q^T$ (real Λ)

Hermitian matrices: $S = S^H$
$S = U\Lambda U^{-1} = U\Lambda U^H$ (real Λ)

Skew-symmetric matrices

$K^T = -K$

Orthogonal matrices : $Q^T = Q^{-1}$

Orthonormal columns : $Q^T Q = I$

$(Qx)^T(Qy) = x^T y$ &

$\|Qx\| = \|x\|$

Skew-Hermitian matrices

$K^H = -K$

Unitary matrices : $U^H = U^{-1}$

Orthonormal columns : $U^H U = I$

$(Ux)^H(Uy) = x^H y$ &

$\|Ux\| = \|x\|$

$\boxed{9.1}$

4.

7. The complex multiplication $M = (a+bi)(c+di)$ is a 2×2 real multiplication

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} \quad \end{bmatrix}$$

The right side contains the real & imaginary parts of M.

Ans:

$$M = (a+bi)(c+di) = (ac-bd) + i(bc+ad)$$

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac-bd \\ bc+ad \end{bmatrix}$$

8. $A = A_1 + iA_2$ is a complex $n \times n$ matrix and $b = b_1 + ib_2$ is a complex vector.

The solution to $Ax = b$ is $x_1 + ix_2$.

Write $Ax = b$ as a real system of size $2n$:

complex $n \times n$

Real $2n \times 2n$: $\begin{bmatrix} & \\ & \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$

Ans: ~~A+iX~~

$Ax = b$

$$\boxed{\begin{gathered} (A_1 + iA_2)(x_1 + ix_2) = (b_1 + ib_2) \\[1em] \begin{bmatrix} A_1 & -A_2 \\ A_2 & A_1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \end{gathered}}$$

11. For a real matrix, the conjugate of $Ax = \lambda x$ is $A\bar{x} = \bar{\lambda}\bar{x}$.

$\longrightarrow$ $\bar{\lambda}$ is another eigenvalue &

$\bar{x}$ is its eigenvector.

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

Ans: $\det(A - \lambda I) = 0$

$$\begin{vmatrix} a-\lambda & b \\ -b & a-\lambda \end{vmatrix} = (a-\lambda)^2 + b^2 = 0$$

$$(a-\lambda)^2 - (ib)^2 = 0$$

$$(a - ib - \lambda)(a + ib - \lambda) = 0$$

$$\cancel{\lambda_1 = a - ib,\ \lambda_2 = a + ib = \bar{\lambda}}$$

$$\underline{\lambda_1 = a + ib}\ ,\ \underline{\lambda_2 = a - ib = \bar{\lambda}_1}$$

λ_1: $\begin{bmatrix} -ib & b \\ -b & -ib \end{bmatrix}\begin{bmatrix} t \\ u \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Longrightarrow \left.\begin{matrix} -it + u = 0 \\ t + iu = 0 \end{matrix}\right\}$ $\begin{matrix} -it + u = 0 \\ it - u = 0 \end{matrix}$

$u = it \Longrightarrow x_1 = \begin{bmatrix} 1 \\ i \end{bmatrix}$

λ_2: $\begin{bmatrix} ib & b \\ -b & ib \end{bmatrix}\begin{bmatrix} v \\ w \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Longrightarrow iv + w = 0$

$w = -iv \Longrightarrow x_2 = \begin{bmatrix} 1 \\ -i \end{bmatrix}$

$$x_1 = \begin{bmatrix} 1 \\ i \end{bmatrix},\ x_2 = \begin{bmatrix} 1 \\ -i \end{bmatrix} = \bar{x}_1$$

14. A real skew-symmetric matrix $(A^T = -A)$ has pure imaginary eigenvalues.

Proof

$$Ax = \lambda x$$

$$\underbrace{\begin{bmatrix} 0 & A \\ -A & 0 \end{bmatrix}}\begin{bmatrix} x \\ ix \end{bmatrix} = i\lambda \begin{bmatrix} x \\ ix \end{bmatrix}$$

symmetric
Block matrix
has real eigenvalues. $\Rightarrow i\lambda$ is real

$\therefore \lambda$ is purely imaginary

18. Cube roots of 1 ?

Cube roots of -1 ?

Ans: $x^3 = 1 \Rightarrow (x^3 - 1) = (x-1)(x^2 + x + 1) = 0$

$x = 1$ (or) $x = \frac{-1 \pm i\sqrt{3}}{2}$

$$1, e^{i\frac{2\pi}{3}}, e^{i\frac{4\pi}{3}} \Bigg\} \quad e^{i\frac{2\pi k}{n}}$$

$k = 0, 1, \cdots, (n-1)$

$z^3 = -1 \Rightarrow z^3 - (-1)^3 = 0$

$(z+1)(z^2 - z + 1) = 0$

$z = -1$ (or) $z = \dfrac{1 \pm i\sqrt{3}}{2}$

$-1, e^{i\frac{\pi}{3}}, e^{-i\frac{\pi}{3}}$

19. Comparing $e^{3i\theta} = \cos 3\theta + i\sin 3\theta$ with $(e^{i\theta})^3 = (\cos\theta + i\sin\theta)^3$. find the 'triple angle' formulas for $\cos 3\theta$ and $\sin 3\theta$ in terms of $\cos\theta$ and $\sin\theta$.

Ans: $(e^{i\theta})^3 = (\cos\theta + i\sin\theta)^3 = \cos^3\theta + 3\cos^2\theta(i\sin\theta) + 3\cos\theta(i\sin\theta)^2 + (i\sin\theta)^3$

$= (\cos^3\theta - 3\cos\theta\sin^2\theta) + i[3\cos^2\theta \sin\theta - \sin^3\theta]$

$= e^{3i\theta} = \cos 3\theta + i\sin 3\theta$

$\Rightarrow$

$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta$

$= \cos^3\theta - 3\cos\theta(1 - \cos^2\theta)$

$= \underline{4\cos^3\theta - 3\cos\theta}$

$\sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta = 3(1 - \sin^2\theta)\sin\theta - \sin^3\theta$

$= \underline{3\sin\theta - 4\sin^3\theta}$

21

(a) Why do e^i and i^e both have absolute value 1?

(b) In the complex plane put stars near the points e^i & i^e.

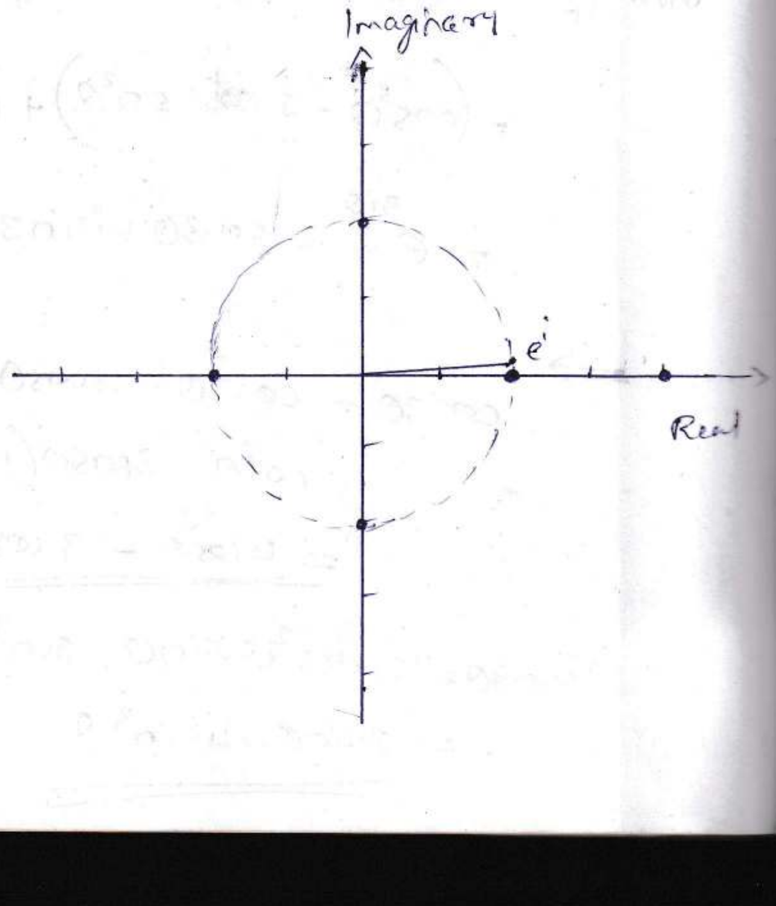
(c) The number i^e could be $\left(e^{i\pi/2}\right)^e$ or $\left(e^{5i\pi/2}\right)^e$. Are those equal?

Ans:

(a) $|e^i|^2 = e^i e^{-i} = 1$

$|i^e| = i^e \times (-i)^e = (i \times -i)^e = 1^e = 1$

(b)



$$i^e = \left(e^{i\frac{\pi}{2}}\right)^e = e^{i\frac{\pi}{2}e}$$

$$= e^{i\left(\frac{\pi}{2}+2\pi n\right)e}$$

Infinitely many i^e

22. Draw the paths of these numbers from $t=0$ to $t=2\pi$ in the complex plane

ⓐ e^{it}

Ans: unit circle

ⓑ $e^{(-1+i)t} = e^{-t}e^{it}$

Ans: Spiral in to $e^{2\pi}$

ⓒ $(-1)^t = e^{t\pi i}$

Ans: $t\pi = k$

e^{ki} ~~from to~~ $k : 0 \rightarrow 2\pi^2$

circle continuing around to angle $\theta = 2\pi^2$

9.2

Q. Compute $A^H A$ and AA^H.

$$A = \begin{bmatrix} i & 1 & i \\ 1 & i & i \end{bmatrix}$$

Ans: $$A^H A = \begin{bmatrix} 2 & 0 & 1+i \\ 0 & 2 & 1+i \\ 1-i & 1-i & 2 \end{bmatrix}$$

$$AA^H = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}$$

Heomitian matrices & share the same eigenvalues. 4, 2

3. Solve $Az=0$ to find a vector $z \in N(A)$, in problem ②. Show that z is orthogonal to the columns of A^H. Show that z is not orthogonal to the columns of A^T. The good row space is no longer $C(A^T)$. Now it is $C(A^H)$

Ans: $$\begin{bmatrix} i & 1 & i \\ 1 & i & i \end{bmatrix}\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Rightarrow \left[\begin{array}{ccc|c} 1 & i & i & 0 \\ i & 1 & i & 0 \end{array}\right] \rightarrow \left[\begin{array}{ccc|c} 1 & i & i & 0 \\ 0 & 2 & i+1 & 0 \end{array}\right]$$

$a+ib+ic=0$ & $2b+(i+1)c=0 \Rightarrow$

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = c\begin{bmatrix} -\frac{(1+i)}{2} \\ -\frac{1+i}{2} \\ 1 \end{bmatrix} = k\begin{bmatrix} 1+i \\ 1+i \\ -2 \end{bmatrix} \in N(A)$$

$a+i\left[-\frac{(i+1)c}{2}\right]+ic=0$

$$a = \frac{i(i+1)c - 2ic}{2} = \frac{c[-1+i-2i]}{2} = \frac{c[-1-i]}{2}$$

$$Az = 0 \Longrightarrow z^H A^H = 0^H$$

$$z^H \left[A_1 \; A_2 \cdots \right] = 0$$

$\therefore$ z is orthogonal to all columns of A^H.

Answer

4. The 4 fundamental subspaces are $C(A)$ and $N(A)$ & $C(A^H)$ and $N(A^H)$.

Their dimensions are still r and $n-r$ & r and $m-r$.

They are still orthogonal subspaces.

5.

If $Az=0$ then $A^H A z = 0$. ~~If $A^H A z = 0$~~,

The nullspaces of A and $A^H A$ are always the same.

$$\boxed{N(A) = N(A^H A)}$$

$\therefore$ $A^H A$ is an invertible Hermitian matrix when $N(A)$ contains only $z=0$.

Proof

If $A^H A z = 0 \Rightarrow (z^H A^H)(Az) = 0.$

$(Az)^H (Az) = \|Az\| = 0$

$\therefore$ $Az = 0$

$\Rightarrow$ The null spaces of A and $A^H A$ are always the same.

A^H.

6. True/False

(a) If A is a real matrix then $A+iI$ is invertible

Ans:

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$|A+iI| = \begin{vmatrix} i & -1 \\ 1 & i \end{vmatrix} = -1+1 = 0$$

False

(b) If S is a Hermitian matrix, then $S+iI$ is invertible.

Ans: $S^H = S \longrightarrow S = \begin{bmatrix} a & b \\ \bar{b} & c \end{bmatrix}$

$$S+iI = \begin{bmatrix} a+i & b \\ \bar{b} & c+i \end{bmatrix}$$

$$|S+iI| = ac - 1 + i(a+c) - |b|^2 \neq 0.$$

(OR)

TRUE $-i$ is not an eigenvalue when $S = S^H$.

(c) If Q is a unitary matrix, then $Q + iI$ is invertible

Ans:

False eigenvalue of Q is $e^{i\phi}$

$|\lambda| = 1$ need not have to be $-i$

$Q\vec{v} = \lambda\vec{v}$

8. $P = \begin{bmatrix} 0 & i & 0 \\ 0 & 0 & i \\ i & 0 & 0 \end{bmatrix}$

$P, P^2, P^{100} = ?$

Eigenvalues of $P = ?$

Ans: $\begin{vmatrix} -\lambda & i & 0 \\ 0 & -\lambda & i \\ i & 0 & -\lambda \end{vmatrix} = -\lambda(\lambda^2) - i(+1) = 0$

$\underline{\lambda^3 = -i}$

$= -i\lambda^3 = -1 \Rightarrow (i\lambda)^3 + 1 = 0$

$(i\lambda + 1)((i\lambda)^2 - i\lambda + 1) = 0 \Rightarrow i\lambda = \frac{1 \pm i\sqrt{3}}{2}$

$\lambda = i\left[\frac{-1 \mp i\sqrt{3}}{2}\right] = i e^{4\pi/3}$ (or) $i e^{2\pi/3}$ (or) $-i$

$\vec{x}_1 = (1,1,1)$ with $\lambda_1 = i$

$x_2 = (1, \omega, \omega^2)$

$x_3 = (1, \omega^2, \omega^4)$, $\omega = e^{i2\pi/3}$

Eigenvector matrix,

$$F_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{bmatrix}$$, Fourier matrix.

Eigenvectors of any unitary matrix are orthogonal

10. Write down the 3×3 circulant matrix $C = 2I + 5P$. It has the same eigenvectors as P in Problem 8. Find its eigenvalues.

Ans:

13. The matrix $A^H A$ is not only Hermitian but also +ve definite, when the columns of A are independent.

Proof

$$z^H S z = z^H A^H A z = (Az)^H (Az)$$
$$= \|Az\|^2 \quad \text{for any } z$$

$\|Az\| \neq 0$

$Az \neq 0$ when $z \neq 0$

$\Rightarrow z^H S z$ is the +ve number $\|Az\|^2$ and the matrix S is +ve definite.

22. ma

Ans:

S^H

U

OM (23)

Spinc

22. Describe all 1x1 and 2x2 Hermitian matrices and unitary matrices.

Ans: $[1]$, $[-1]$ Hermitian

$[e^{i\theta}]$: Unitary

$$S^H = S \Rightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix} \Longrightarrow \begin{array}{l} a^* = a,\ c^* = b \\ b^* = c,\ d^* = d. \end{array}$$

$$\boxed{\begin{bmatrix} u & v+iw \\ v-iw & z \end{bmatrix} \quad \text{is } 2\times 2 \text{ Hermitian}}$$

$$U^H = U^{-1} \Rightarrow \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix} = \frac{1}{\det(U)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{e^{i\phi}} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$d = e^{i\phi} a^*, \quad b = -c^* e^{i\phi}$$

$$\boxed{U = \begin{bmatrix} a & -e^{i\phi} c^* \\ c & e^{i\phi} a^* \end{bmatrix} \quad \text{is } 2\times 2 \text{ unitary}}$$

OM (23)

Spinors

24. If $u^H u = I$ show that $\underline{I-2uu^H}$ is Hermitian and also unitary. The rank-1 matrix uu^H is the projection onto what line in $\mathbb{C}^n$?

Ans: $(I-2uu^H)^H = I-2uu^H$

$$(I-2uu^H)^2 = I-4uu^H+4u(u^Hu)u^H$$
$$= I-4uu^H+4uIu^H = I$$

$$(uu^H)w = (u^Hw)u$$

$\Longrightarrow$ The rank-1 matrix uu^H projects onto the line thro' u.

25. If $A+iB$ is a unitary matrix (A & B are real) Show that $Q = \begin{bmatrix} A & -B \\ B & A \end{bmatrix}$ is an orthogonal matrix

Ans: $(A^T - iB^T)(A+iB) = (A^TA + B^TB) + i(A^TB - B^TA) = I$

$$\Rightarrow A^TA + B^TB = I \quad \& \quad A^TB - B^TA = 0$$

$$Q^TQ = \left[\begin{array}{c|c} A & -B \\ \hline B & A \end{array}\right]^T \left[\begin{array}{c|c} A & -B \\ \hline B & A \end{array}\right] = \left[\begin{array}{c|c} A^T & B^T \\ \hline -B^T & A^T \end{array}\right]\left[\begin{array}{c|c} A & -B \\ \hline B & A \end{array}\right]$$

$$= \begin{bmatrix} A^TA + B^TB & -(A^TB - B^TA) \\ A^TB - B^TA & B^TB + A^TA \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

✓

26. If $A+iB$ is Hermitian (A & B are real) show that $\begin{bmatrix} A & -B \\ B & A \end{bmatrix}$ is symmetric

Ans: $A^T - iB^T = A + iB \Longrightarrow A^T = A \;\&\; B^T = -B$

$$\left[\begin{array}{c|c} A & -B \\ \hline B & A \end{array}\right]^T = \left[\begin{array}{c|c} A^T & B^T \\ \hline -B^T & A^T \end{array}\right] = \left[\begin{array}{c|c} A & -B \\ \hline B & A \end{array}\right]$$

Symmetric

10.7 Linear Algebra for Cryptography

Cryptography is about encoding and decoding messages.

Finite fields and finite vector spaces.

The field for $\mathbb{R}^n$ contains all real # & there are infinitely many vectors in $\mathbb{R}^n$.

* The field for "modular arithmetic" contains only p integers $0, 1, 2, \ldots, p-1$., and there are only p^n messages of length n in message space.

$\Longrightarrow$ Linear Algebra with finite fields

$$\boxed{y \equiv x \pmod{p} \quad : \quad y - x \text{ is divisible by } p}$$

Ex:-

$27 \equiv 2 \pmod{5}$: $(27-2)$ is divisible by 5

'$\equiv$' : congruent

All the numbers $5, -5, 10, -10, \ldots$ with no remainder are congruent to $0 \pmod{5}$.

$y = 6, -4, 11, -9, \ldots$ are all congruent to $x = 1 \bmod (5)$.

☐ Modular Arithmetic

Linear algebra is based on linear combinations of vectors.

Now, our vectors $(x_1, x_2, \ldots, x_n)$ are strings of integers limited to $x = 0, 1, \ldots, p-1$.

All calculations produce these integers when we work "mod p". ie.,

$$\boxed{\begin{array}{c} y = qP + x \iff y = x \pmod{p} \\ x = y \bmod P \\ y \text{ divided by } p \text{ has remainder } x \end{array}}$$

Addition mod 3 :

$10 \equiv 1 \pmod 3$ and $16 \equiv 1 \pmod 3$

$\Longrightarrow 10+16 \equiv 1+1 \pmod 3$

Addition mod 2 :

$11 \equiv 1 \pmod 2$ and $17 \equiv 1 \pmod 2$

$2 \equiv 0 \pmod 2 \Longrightarrow 11+17 = 28 \equiv 0 \pmod 2$

~~Addition mod p~~:

Multiplication mod p

$p = 3$:

$10 \equiv 1 \pmod 3$ times $16 \equiv 1 \pmod 3 \Rightarrow 10 \times 16 = 160 \equiv 1 \pmod 3$

$5 \equiv 2 \pmod 3$ times $8 \equiv 2 \pmod 3 \Rightarrow 5 \times 8 = 40 \equiv 1 \pmod 3$

$\Rightarrow$ We can safely add & multiply modulo p.

$\therefore$ we can take linear combinations.

Division ?

In the real number field, the inverse is $1/y$ (for any # except $y=0$). ie., we can find another real # z so that $yz=1$.

Invertibility is a requirement for a field.

Is inversion always possible mod p ?

For every number $y = 1, 2, \cdots, p-1$ can we find another number $z = 1, 2, \cdots, p-1$ so that $yz \equiv 1 \mod p$?

$yz \equiv 1 \pmod p$

$\Rightarrow$ 'z' is the multiplicative inverse of 'y' modulo 'p'.

$yz \equiv 1 \pmod p$ iff $yz + tp = 1$ for some $t \in \mathbb{Z}$

Bezout's theorem : Diophantine equations

+1 (6)

Let a & b be non-zero integers and let $d = \gcd(a, b)$. Then there exists integers x and y that satisfy $ax + by = d$.

A linear equation $ax + by = d$ has an integer solution iff $\gcd(a, b)$ divides d.

ie., $\gcd(a,b) \mid d$

$yz \equiv 1 \pmod{p}$

$\Longrightarrow yz + tp = 1$ for some $t \in \mathbb{Z}$

We can find z and t such that

$yz + tp = \gcd(y, p)$.

i.e., if $\gcd(y, p) = 1$, we can find a multiplicative inverse.

Inversion of every y $(0<y<p)$ will be possible iff p is prime.

Ex:-

Find the multiplicative inverse of 27 modulo 4.

i.e., find z such that

$27z \equiv 1 \pmod 4$

$\gcd(27,4) = \gcd(4,3) = \gcd(3,1) = \gcd(1,0) = 1$

$\therefore$ inverse exists.

$$\boxed{\begin{array}{c} 27 \equiv 3 \pmod{4} \\ \hline 4 \equiv 1 \pmod 3 \end{array}}$$

$27 = 6 \times 4 + 3$

$4 = 1 \times 3 + 1$

$3 = 27 - 6 \times 4$

$1 = 4 - 1 \times 3$

$1 = 4 - 1 \times 3 = 4 - 1(27 - 6 \times 4)$

$= 4 + 6 \times 4 - 1 \times 27$

$1 = 7 \times 4 + (-1) \times 27$

$(27)(-1) - 1 = -7(4)$

$$(27)^{-1} = -1 \equiv 3 \pmod 4$$

Ex:- Inverse of $a = 27$ under modulo $b = 5$.

Ans: $27z \equiv 1 \pmod 5 \implies 27 \equiv 2 \pmod 5$

$$\left.\begin{aligned} 27 &= 5(5) + 2 \\ 5 &= 2(2) + 1 \end{aligned}\right\} \quad \begin{aligned} 2 &= 27 - 5(5) \\ 1 &= 5 - 2(2) \end{aligned}$$

$$1 = 5 - 2(2) = 5 - 2\left[27 - 5(5)\right] = 5 - 2(27) + 10(5)$$

$$1 = 11(5) - 2(27) \implies -2(27) - 1 = -11(5)$$

$$(27)^{-1} = -2 \equiv 3 \pmod 5$$

Ex:- $a = 9,\ m = 26$

Ans: $9z \equiv 1 \pmod{26} \implies 9 = 9 \bmod (26)$

$$\left.\begin{aligned} 26 &= 2(9) + 8 \\ 9 &= 1(8) + 1 \end{aligned}\right\} \quad \begin{aligned} 8 &= 26 - 2(9) \\ 1 &= 9 - 1(8) \end{aligned}$$

$$1 = 9 - 1(26 - 2(9)) = 3(9) - 1(26)$$

$$3(9) - 1 = 1(26) \implies 9^{-1} = 3 \equiv 3 \pmod{26}$$

Ex:- $a = 7$, $m = 26$. Find $a^{-1} \bmod m$

Ans: $7x \equiv 1 \pmod{26}$

$7 \equiv 7 \pmod{26}$

$7 = 0(26) + 7$

$26 = 3(7) + 5$ $5 = 26 - 3(7)$

$7 = 1(5) + 2$ $2 = 7 - 1(5)$

$5 = 2(2) + 1$ $1 = 5 - 2(2)$

$1 = 5 - 2(2) = 5 - 2[7 - 1(5)]$

$= 3(5) - 2(7)$

$= 3[26 - 3(7)] - 2(7)$

$1 = 3(26) - 11(7)$

$-11(7) - 1 = -3(26)$

$\therefore \quad 7^{-1} = (-11) = 15 \pmod{26}$

Modular Arithmetic

In mathematics, modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" when reaching a certain value, called the modulus.

Familiar use:

12-hour clock, in which the day is divided into two 12-hour periods.

If the time is 7:00 now, then 8 hours later it will be 3:00. Simple addition would result in $7+8=15$, but clocks "wrap around" every 12 hours. Because the hour number starts over after it reaches 12, this is arithmetic modulo 12.

15 is congruent to 3 modulo 12.

$15 \equiv 3 \pmod{12}$ (or) $15 \bmod 12 = 3 \bmod 12$

$\therefore$

"15:00" on a 24-hour clock is displayed "3:00" on a 12-hour clock.

A number a-mod N is the equivalent of asking for the remainder of a when divided by N.

Two integers a and b are said to be congruent (or in the same equivalence class) modulo N if they have the same remainder upon division by N. In such a case, we say that,

$$a \equiv b \pmod{N}$$

$$a = xN + b$$

$$\begin{array}{r|l} & x \\ \hline N & a \\ \hline & b \end{array}$$

$$a \equiv b \pmod{N}$$

$$x = a \text{ div } N$$

$b = a \bmod N$: remainder of 'a' when divided by 'N'.

The congruence relation satisfies all the conditions of an equivalence relation:

* Reflexivity : $a \equiv a \pmod{N}$

* Symmetry : $a \equiv b \pmod{N}$ if

$b \equiv a \pmod{N}$ for all a, b, N

* Transitivity : If $a \equiv b \pmod{N}$ and $b \equiv c \pmod{N}$

~~then~~ then, $a \equiv c \pmod{N}$

Ex:-

$$9 \equiv 3 \pmod 6$$

$$23 \equiv 5 \pmod 6$$

$$-8 \equiv 4 \pmod 6$$

$$12 \equiv 0 \pmod 6$$

* If $a \equiv c \pmod{p}$ and $b \equiv d \pmod{p}$,

  then $a + b \equiv c + d \pmod{p}$

* If $a \equiv c \pmod{p}$ and $b \equiv d \pmod{p}$,

  then $a \cdot b \equiv c \cdot d \pmod{p}$

Properties of addition in modular arithmetic

* If $a+b=c$, then

$$a \pmod N + b \pmod N \equiv c \pmod N$$

* If $a \equiv b \pmod N$, then

$$a+k \equiv b+k \pmod N \text{ for any integer } k$$

* If $a \equiv b \pmod N$ and $c \equiv d \pmod N$, then

$$a+c \equiv b+d \pmod N$$

* If $a \equiv b \pmod N$, then

$$-a \equiv -b \pmod N$$

Properties of multiplication in modular arithmetic

* If $a \cdot b = c$, then

$$a \pmod N \cdot b \pmod N \equiv c \pmod N$$

* If $a \equiv b \pmod N$, then

$$ka \equiv kb \pmod N \text{ for any } k \in \mathbb{Z}$$

* If $a \equiv b \pmod N$ and $c \equiv d \pmod N$, then

$$ac \equiv bd \pmod N$$

2. Modular Arithmetic with Matrices

To multiply mod p, we can multiply the integers in A times the integers in 'x' as usual - and then replace every entry of Ax by its value mod p.

Can we solve $Ax \equiv b \pmod p$?

#

There is an inverse matrix mod p whenever the determinant of A is non-zero mod p, and p is a prime #.

~~Ex:-~~ $\cancel{A = \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix}}$ ~~mod 3 with 2×n integer matrix A~~

$$\cancel{[A\ I] = \left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right] \to \left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 \end{array}\right] \to}$$

Ex:-

Solve
$$2x + 6y = 1 \pmod 7$$
$$4x + 3y = 2 \pmod 7$$

Ans:
$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \pmod 7 = \begin{bmatrix} a \\ b \end{bmatrix}$$

$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}^{-1} = \frac{1}{-18} \begin{bmatrix} 3 & -6 \\ -4 & 2 \end{bmatrix} = (-18)^{-1} \begin{bmatrix} 3 & -6 \\ -4 & 2 \end{bmatrix}$$

$$-18 = 3 \pmod 7$$

$-18z = 1 \pmod 7$ (or) $\cancel{3 \pmod 7 \times x \pmod 7 = 1 \pmod 7}$

$\cancel{3x \pmod 7 = 1 \pmod 7}$

$$-18 = -3(7) + 3$$

$$7 = 2(3) + 1$$

$$3 = -18 + 3(7)$$

$$1 = 7 - 2(3)$$

$$1 = 7 - 2(3) = 7 - 2\left[-18 + 3(7)\right]$$

$$= 7 + 36 - 6(7)$$

$$= 43 - 6(7) = 6(7) + 1 - 6(7)$$

$$= 7 - 2(-18) - 6(7)$$

$$= -5(7) - 2(-18)$$

$$(-18)^{-1} = \left(3 \pmod{7}\right) = 5$$

$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}^{-1} = \cancel{5}(-18)^{-1} \begin{bmatrix} 3 & -6 \\ -4 & 2 \end{bmatrix} = \frac{1}{3 \pmod{7}} \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix} \pmod{7}$$

$$= 5 \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix} \pmod{7}$$

$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \pmod 7$$

$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}^{-1}\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}^{-1}\begin{bmatrix} 1 \\ 2 \end{bmatrix} \pmod 7$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = 5\begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix} \pmod 7 \begin{bmatrix} 1 \\ 2 \end{bmatrix} \pmod 7$$

$$= 5\begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix}\begin{bmatrix} 1 \\ 2 \end{bmatrix} \pmod 7$$

$$= 5\begin{bmatrix} 5 \\ 7 \end{bmatrix} \pmod 7$$

$$= \begin{bmatrix} 25 \\ 35 \end{bmatrix} \pmod 7$$

$$= \begin{bmatrix} 4 \\ 0 \end{bmatrix}$$

Ex:- $4x + 6y = 1 \pmod{7}$

$x + 5y = 2 \pmod{7}$

Ans: $\begin{bmatrix} 4 & 6 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \pmod{7}$

$\det(A) = 20 - 6 = 14 = 0 \pmod{7}$

$4(x + 5y) = 4x + 6y = 1 \pmod{7}$

$\Rightarrow$ 1st equation is 4 times the 2nd.

$\therefore$ It suffices to solve $\cancel{4x+6y}$ $x + 5y = 2 \pmod{7}$

Equivalent Diophantine equation $\longrightarrow$ $x + 5y + 7z = 2$

Ex.: $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$. mod (29)

$$AA^{-1} = I$$

Ans:

$$[A|I] = \left[\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right] \Leftrightarrow \left[\begin{array}{cc|cc} 30 & 45 & 15 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right]$$

$\left\{ \begin{array}{l} 30 \equiv 1 \pmod{29} \\ (2)^{-1} = 15 \end{array} \right.$

$$\equiv \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 4 & 5 & 0 & 1 \end{array}\right] \cancel{\text{mod } 29} \pmod{29}$$

$$\Leftrightarrow \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & -59 & -60 & 1 \end{array}\right]$$

$\{ -4 \equiv 25$

$$\equiv \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 28 & 27 & 1 \end{array}\right] \pmod{29}$$

$\{ (28)^{-1} = 28$

$$\Leftrightarrow \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 784 & 756 & 28 \end{array}\right]$$

$$\equiv \left[\begin{array}{cc|cc} 1 & 16 & 15 & 0 \\ 0 & 1 & 2 & 28 \end{array}\right] \pmod{29}$$

$$\longleftrightarrow \left[\begin{array}{cc|cc} 1 & 0 & -17 & -448 \\ 0 & 1 & 2 & 28 \end{array}\right] \qquad \left\{ -16 = 13 \right.$$

$$\equiv \left[\begin{array}{cc|cc} 1 & 0 & 12 & 16 \\ 0 & 1 & 2 & 28 \end{array}\right] \pmod{29}$$

$$A\,A^{-1} \pmod{29} = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix} = \begin{bmatrix} 30 & 116 \\ 58 & 204 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{29}$$

$$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}^{-1} = \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix} \pmod{29}$$

(OR) $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$

$$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}^{-1} = \begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} \cdot (10-12)^{-1}$$

$$= (-2)^{-1} \begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix}$$

$-2z \equiv 1 \pmod{29}$

$-2 \equiv 27 \pmod{29}$

$-2 = -1(29) + 27$ $\quad\Big\}\quad 27 = -2 + 1(29)$

$29 = 1(27) + 2$ $\quad\Big\}\quad 2 = 29 - 1(27)$

$27 = 13(2) + 1$ $\qquad 1 = 27 - 13(2)$

$2 = 29 - 1(-2 + 1(29))$

$= 29 + 1(2) - 1(29)$

$1 = 27 - 13(2) = 27 - 13[29 - 1(27)] = 14(27) - 13(29)$

$1 = 14[-2 + 1(29)] - 13(29) = 14(-2) + 1(29)$

$-2(14) - 1 = -1(29)$

$\therefore (-2)^{-1} = 14 \equiv 14 \pmod{29}$

$$\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}^{-1} = 14 \begin{bmatrix} 5 & -3 \\ -4 & 2 \end{bmatrix} (\text{mod } 29)$$

$$= \begin{bmatrix} 70 & -42 \\ -56 & 28 \end{bmatrix}$$

$$= \begin{bmatrix} 12 & 16 \\ 2 & 28 \end{bmatrix} (\text{mod } 29)$$

Ex:- $A = \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix}$

$$[A \mid I] = \left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right]$$

$$\leftrightarrow \left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 0 & 1 & -1 & 1 \end{array}\right]$$

$$\equiv \left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{array}\right] (\text{mod } 3)$$

$2z = 1 \; (\text{mod } 3)$

$2 = 2 \; (\text{mod } 3)$

$2^2 (2^{-1}) = 2 \equiv 2 \; (\text{mod } 3)$

$$\rightarrow \left[\begin{array}{cc|cc} 4 & 0 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{array}\right]$$

$$\equiv \left[\begin{array}{cc|cc} 1 & 0 & 2 & 0 \\ 0 & 1 & 2 & 1 \end{array}\right]$$

$$\begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 2 & 0 \\ 2 & 1 \end{bmatrix} \pmod 3$$