- last time — calculating powers of a matrix.

  - symmetric matrix.

  - symmetric $\Rightarrow$ all eigenvalues real

    $\Rightarrow$ eigenvectors corresponding to different eigenvalues are orthogonal

- orthogonal $\Leftrightarrow$ orthonormal columns.

- diagonalizable. $P^{-1}AP = D$, D diagonal.

- $n \times n$ A diagonalizable $\Leftrightarrow$ n linearly indep. eigenvectors.

  If so, let P have these eigenvectors as its columns.

  Then P is invertible, $P^{-1}AP = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$

  λ_i eigenvalues.

If A is $n \times n$, n different eigenvalues, then it is diagonalizable.

if there are fewer than n different eigenvalues, ???

e.g. $A=\begin{pmatrix}1&3\\0&1\end{pmatrix}$. Eigenvalue: 1.

$\lambda=1$: $A-1I=\begin{pmatrix}0&3\\0&0\end{pmatrix}$.

$\left(\begin{array}{cc|c}0&3&0\\0&0&0\end{array}\right)\xrightarrow[r_1\cdot\frac{1}{3}]{\text{mult }(1)}\left(\begin{array}{cc|c}0&1&0\\0&0&0\end{array}\right)$. Let $x_1=t$, $x_2=0$. Basis: $\left\{\begin{pmatrix}1\\0\end{pmatrix}\right\}$.

Not enough vectors, not diagonalizable.

e.g. $A=\begin{pmatrix}1&3&0\\-1&5&0\\0&0&2\end{pmatrix}$. $0=\det\begin{pmatrix}1-\lambda&3&0\\-1&5-\lambda&0\\0&0&2-\lambda\end{pmatrix}=(2-\lambda)\det\begin{pmatrix}1-\lambda&3\\-1&5-\lambda\end{pmatrix}$

$=(2-\lambda)(\lambda^2-6\lambda+8)$

$=(2-\lambda)(\lambda-2)(\lambda-4)$.

$\lambda=2,4$.

$\lambda=2$: $A-2I=\begin{pmatrix}-1&3&0\\-1&3&0\\0&0&0\end{pmatrix}$.

$\left(\begin{array}{ccc|c}-1&3&0&0\\-1&3&0&0\\0&0&0&0\end{array}\right)\xrightarrow[r_1\cdot -1]{\text{mult }(1)}\left(\begin{array}{ccc|c}1&-3&0&0\\-1&3&0&0\\0&0&0&0\end{array}\right)\xrightarrow[\text{to }(2)]{\text{add }(1)}\left(\begin{array}{ccc|c}1&-3&0&0\\0&0&0&0\\0&0&0&0\end{array}\right)$.

Let $x_2=t$, $x_3=u$, $x_1=3t$. Basis: $\left\{\begin{pmatrix}3\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\end{pmatrix}\right\}$.

$\lambda=4$: $A-4I=\begin{pmatrix}-3&3&0\\-1&1&0\\0&0&-2\end{pmatrix}$.

$\left(\begin{array}{ccc|c}-3&3&0&0\\-1&1&0&0\\0&0&-2&0\end{array}\right)\xrightarrow[r_1\cdot -\frac{1}{3}]{\text{mult }(1)}\left(\begin{array}{ccc|c}1&-1&0&0\\-1&1&0&0\\0&0&-2&0\end{array}\right)\xrightarrow[\text{to }(2)]{\text{add }(1)}\left(\begin{array}{ccc|c}1&-1&0&0\\0&0&0&0\\0&0&-2&0\end{array}\right)\xrightarrow{\text{swap }(2),(3)}$

$\left(\begin{array}{ccc|c}1&-1&0&0\\0&0&-2&0\\0&0&0&0\end{array}\right)\xrightarrow[r_2\cdot -\frac{1}{2}]{\text{mult }(2)}\left(\begin{array}{ccc|c}1&-1&0&0\\0&0&1&0\\0&0&0&0\end{array}\right)$. Let $x_2=t$, $x_1=t$, $x_3=0$.

Basis: $\left\{\begin{pmatrix}1\\1\\0\end{pmatrix}\right\}$.

A is diagonalizable. Let $P=\begin{pmatrix}3&0&1\\1&0&1\\0&1&0\end{pmatrix}$.

$P^{-1}AP=\begin{pmatrix}2&0&0\\0&2&0\\0&0&4\end{pmatrix}$.

An $n\times n$ matrix A is orthogonally diagonalizable if there exists an orthogonal matrix P so that $P^{-1}AP$ is diagonal.

$$P^{-1}AP = P^TAP.$$

A is orthogonally diagonalizable if and only if it is symmetric.

We need an orthonormal basis for each eigenspace.

e.g. $A = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$. $0 = \det\begin{pmatrix} 1-\lambda & 3 \\ 3 & 1-\lambda \end{pmatrix} = \lambda^2 - 2\lambda - 8$

$= (\lambda-4)(\lambda+2)$

$\lambda = 4, -2.$

$\lambda = 4$: $A - 4I = \begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix}$.

$\left(\begin{array}{cc|c} -3 & 3 & 0 \\ 3 & -3 & 0 \end{array}\right) \xrightarrow[r_1 \cdot -1/3]{\text{mult } (1)} \left(\begin{array}{cc|c} 1 & -1 & 0 \\ 3 & -3 & 0 \end{array}\right) \xrightarrow[\text{to } (2)]{\text{add } -3(1)} \left(\begin{array}{cc|c} 1 & -1 & 0 \\ 0 & 0 & 0 \end{array}\right)$.

Let $x_2 = t$, $x_1 = t$. Basis: $\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\}$. Normalize: $\left\{\begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}\right\}$.

$\lambda = -2$: $A + 2I = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$

$\left(\begin{array}{cc|c} 3 & 3 & 0 \\ 3 & 3 & 0 \end{array}\right) \xrightarrow[r_1 \cdot 1/3]{\text{mult } (1)} \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 3 & 3 & 0 \end{array}\right) \xrightarrow[\text{to } (2)]{\text{add } -3(1)} \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right)$.

Let $x_2 = t$, $x_1 = -t$. Basis: $\left\{\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right\}$. Normalize: $\left\{\begin{pmatrix} -1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}\right\}$.

$P = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$, $P^{-1}AP = P^TAP = \begin{pmatrix} 4 & 0 \\ 0 & -2 \end{pmatrix}$.

e.g. $A=\begin{pmatrix}3&3&3\\3&3&3\\3&3&3\end{pmatrix}$. $0=\det\begin{pmatrix}3-\lambda&3&3\\3&3-\lambda&3\\3&3&3-\lambda\end{pmatrix}=(3-\lambda)\det\begin{pmatrix}3-\lambda&3\\3&3-\lambda\end{pmatrix}-3\det\begin{pmatrix}3&3\\3&3-\lambda\end{pmatrix}+3\det\begin{pmatrix}3&3-\lambda\\3&3\end{pmatrix}$

$0=(3-\lambda)(\lambda^2-6\lambda)-3(-3\lambda)+3(3\lambda)$

$=-\lambda^3+9\lambda^2=\lambda^2(-\lambda+9)$, $\lambda=0, 9$

$\lambda=0$: $A-0I=A$.

$\left(\begin{array}{ccc|c}3&3&3&0\\3&3&3&0\\3&3&3&0\end{array}\right)\xrightarrow[1/3]{\text{mult }(1)}\left(\begin{array}{ccc|c}1&1&1&0\\\boxed{3}&3&3&0\\\boxed{3}&3&3&0\end{array}\right)\begin{array}{c}\text{add }-3(1)\text{ to }(2)\\\text{add }-3(1)\text{ to }(3)\end{array}\left(\begin{array}{ccc|c}1&1&1&0\\0&0&0&0\\0&0&0&0\end{array}\right)$.

Let $x_2=t$, $x_3=u$. Basis: $\left\{\begin{pmatrix}-1\\1\\0\end{pmatrix},\begin{pmatrix}-1\\0\\1\end{pmatrix}\right\}$.
$x_1=-t-u$.

Apply Gram-Schmidt. $\vec{u}_1=\begin{pmatrix}-1\\1\\0\end{pmatrix}$, $\vec{u}_2=\begin{pmatrix}-1\\0\\1\end{pmatrix}$.

$\vec{v}_1=\vec{u}_1=\begin{pmatrix}-1\\1\\0\end{pmatrix}$, $\vec{v}_2=\vec{u}_2-\frac{\vec{u}_2\cdot\vec{v}_1}{\vec{v}_1\cdot\vec{v}_1}\vec{v}_1$

$=\begin{pmatrix}-1\\0\\1\end{pmatrix}-\frac{1}{2}\begin{pmatrix}-1\\1\\0\end{pmatrix}$.

Double $\vec{v}_2$, $\vec{v}_2=2\begin{pmatrix}-1\\0\\1\end{pmatrix}-\begin{pmatrix}-1\\1\\0\end{pmatrix}=\begin{pmatrix}-1\\-1\\2\end{pmatrix}$.

Normalize: $\left\{\begin{pmatrix}-1/\sqrt{2}\\1/\sqrt{2}\\0\end{pmatrix},\begin{pmatrix}-1/\sqrt{6}\\-1/\sqrt{6}\\2/\sqrt{6}\end{pmatrix}\right\}$.

$\lambda=9$: $A-9I=\begin{pmatrix}-6&3&3\\3&-6&3\\3&3&-6\end{pmatrix}$.

$\left(\begin{array}{ccc|c}-6&3&3&0\\3&-6&3&0\\3&3&-6&0\end{array}\right)\xrightarrow[(1),(2)]{\text{swap}}\left(\begin{array}{ccc|c}3&-6&3&0\\-6&3&3&0\\3&3&-6&0\end{array}\right)\xrightarrow[1/3]{\text{mult }(1)}\left(\begin{array}{ccc|c}1&-2&1&0\\\boxed{-6}&3&3&0\\\boxed{3}&3&-6&0\end{array}\right)\begin{array}{c}\text{add }6(1)\text{ to }(2)\\\text{add }-3(1)\text{ to }(3)\end{array}$

$\left(\begin{array}{ccc|c}1&-2&1&0\\0&-9&9&0\\0&9&-9&0\end{array}\right)\xrightarrow[-1/9]{\text{mult }(2)}\left(\begin{array}{ccc|c}1&\boxed{-2}&1&0\\0&1&-1&0\\0&\boxed{9}&-9&0\end{array}\right)\begin{array}{c}\text{add }2(2)\text{ to }(1)\\\text{add }-9(2)\text{ to }(3)\end{array}\left(\begin{array}{ccc|c}1&0&-1&0\\0&1&-1&0\\0&0&0&0\end{array}\right)$.

Let $x_3 = t$ $\begin{matrix} x_1 = t \\ x_2 = t. \end{matrix}$ Basis: $\left\{\begin{pmatrix}1\\1\\1\end{pmatrix}\right\}$. Normalize: $\left\{\begin{pmatrix}1/\sqrt{3}\\1/\sqrt{3}\\1/\sqrt{3}\end{pmatrix}\right\}$.

Let $P = \begin{pmatrix} -1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ 1/\sqrt{2} & -1/\sqrt{6} & 1/\sqrt{3} \\ 0 & 2/\sqrt{6} & 1/\sqrt{3} \end{pmatrix}$. $P^{-1}AP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 9 \end{pmatrix}$.

Cryptography: send a secret message

Select a key, an $n \times n$ matrix A so that $\det(A) = \pm 1$, so that A and A^{-1} have integer entries.

We will then convert our message to numbers:

$A = 1, B = 2, \ldots, Z = 26, \_ = 0$. We will arrange our message in an $n \times k$ matrix, where k is determined by the message size (Pad out any blanks at the end with zeroes).

Suppose our message is M. To encrypt, calculate $B = AM$, and send B. To decrypt, calculate

$A^{-1}B = A^{-1}AM = IM = M.$

- e.g. $A = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$. XENA_RULES.
24, 5, 14, 1, 0, 18, 21, 12, 5, 19.

$M = \begin{pmatrix} 24 & 5 & 14 & 1 & 0 \\ 18 & 21 & 12 & 5 & 19 \end{pmatrix}$.

$$B = AM = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}\begin{pmatrix} 24 & 5 & 14 & 1 & 0 \\ 18 & 21 & 12 & 5 & 19 \end{pmatrix}$$

$$= \begin{pmatrix} 102 & 73 & 64 & 17 & 57 \\ 162 & 120 & 102 & 28 & 95 \end{pmatrix} \leftarrow \text{send.}$$

$$A^{-1} = \frac{1}{\det(A)}\begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}$$

$$M = A^{-1}B = \begin{pmatrix} 5 & -3 \\ -3 & 2 \end{pmatrix}\begin{pmatrix} 102 & 73 & 64 & 17 & 57 \\ 162 & 120 & 102 & 28 & 95 \end{pmatrix}$$

$$= \begin{pmatrix} 24 & 5 & 14 & 1 & 0 \\ 18 & 21 & 12 & 5 & 19 \end{pmatrix}. \quad \begin{matrix} \text{X E N A -} \\ \text{R U L E S.} \end{matrix}$$

- last time - diagonalizing.

  - orthogonally diagonalizable $\Leftrightarrow$ symmetric.

  - cryptography. $\det(A) = \pm 1$, $M \to AM \to A^{-1}AM = M$.

<u>Mod 2 arithmetic</u>

$\cdot$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

- e.g. $1+1+0+1 = 0+0+1 = 0+1 = 1$.

A <u>binary string</u> is a list of zeroes and ones.

In a <u>parity check code</u>, we append a <u>check bit</u> to our string, being the mod 2 sum of the numbers in the string.

- e.g. (110101) $\quad 1+1+0+1+0+1 = 0$.

  We send (1101010). The recipient checks that the mod 2 sum is 0. If so, the last ~~ch~~ bit is deleted to obtain the message. If not, there is an error

- e, (101101) ✓ Message: (10110)

  (101100) error.

Advantages: easy, efficient

Disadvantages: can't fix errors.

two errors? eek!

<u>Hamming code</u>: Our message will be a binary string

of length 4, (w_1, w_2, w_3, w_4).

We have three check bits: $c_1 = w_1 + w_2 + w_4$.

$$\left.\begin{aligned} c_1 &= w_1+w_2+w_4 \\ c_2 &= w_1+w_3+w_4 \\ c_3 &= w_2+w_3+w_4 \end{aligned}\right\} \bmod 2.$$

Our encoded message is: $(c_1 c_2 w_1 c_3 w_2 w_3 w_4)$.

- e.g. $(1\,0\,0\,1)$ $c_1 = 1+0+1 = 0$, $c_2 = 1+0+1 = 0$, $c_3 = 0+0+1 = 1$.

We get $(0\,0\,1\,1\,0\,0\,1)$.

To check the message C, the recipient forms the Hamming

matrix: $H = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}$

The recipient calculates HC^T

$$\begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \\ w_1 \\ c_3 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = \begin{pmatrix} c_3+w_2+w_3+w_4 \\ c_2+w_1+w_3+w_4 \\ c_1+w_1+w_2+w_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

If we get $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, our message is correct, and we drop the check bits, to get the original message.

- e.g. we receive (1010101)

$$\begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Valid. Original message (1101).

Suppose one bit gets ~~bit~~ flipped. Our message should have been C, but instead it is $C+E$, where

$$E = (0 \cdots 0 \underset{i}{1} 0 \cdots 0)$$

$$H(C+E)^T = HC^T + HE^T = HE^T = \text{column } i \text{ of } H.$$

- e.g. we receive (1010111).

$$\begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \text{ column 6 of } H.$$

Error in bit 6, message should have been (1010101), so the original message (1101).

Advantages: can fix any 1 error.

will know there is a problem with 2 errors.

Disadvantages: less efficient, more complicated

Read Chapter 1.

Chapter 3 - Probability (3.1-3.7)

An *experiment* is any procedure leading to an *outcome*

The *sample space*, S, is the set of all possible outcomes for an experiment.

An *event* is any collection of outcomes; that is, it is a subset of the sample space.

- e.g. flip a coin 3 times, record the results.

$S = \{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT\}$

- e.g. flip a coin 3 times, count the heads

$S = \{0, 1, 2, 3\}$

- e.g. roll two dice, record the total

$S = \{2, 3, \ldots, 12\}$.

- e.g. roll 2 dice, record the results.

$S = \{11, 12, \ldots, 16, 21, 22, \ldots, 66\}$.

In <u>discrete probability</u> (chapters 3+4), we have either finitely many or countably many possible outcomes.

A <u>countable</u> set has terms that can be put in an infinite sequence.

- e.g. the positive integers: $1, 2, 3, 4, \ldots$.
- e.g. the integers: $0, 1, -1, 2, -2, 3, -3, \ldots$
- e.g. the rational numbers are countable.
- e.g. the real numbers are uncountable.
- e.g. $[0,1)$ is uncountable.

In <u>continuous probability</u> (chapter 5+), the possible outcomes are either all real numbers, or an interval.

- ~~the~~ e.g. flip a coin until heads appears, count the flips

$S = \{1, 2, 3, \ldots\}$.

Let E and F be events. Then the <u>intersection</u> of E and F, $E \cap F$, is the event that E and F both occur. It is the set of all outcomes lying in E and F simultaneously.

- roll a die, $E = \{1, 3, 5\}$, $F = \{3, 6\}$, $G = \{2, 4, 6\}$.

$E \cap F = \{3\}$, $F \cap G = \{6\}$

$E \cap G = \phi$ "empty set".

We say that E and G are <u>mutually exclusive</u>.

$E \cap E = E$, $E \cap \phi = \phi$, $E \cap S = E$

e.g. solve $-x_1 + 3x_2 + 4x_3 = 5$
$2x_1 - 7x_2 + 3x_3 = 2$.

$$\left(\begin{array}{ccc|c} -1 & 3 & 4 & 5 \\ 2 & -7 & 3 & 2 \end{array}\right) \xrightarrow[\text{by } -1]{\text{mult } (1)} \left(\begin{array}{ccc|c} 1 & -3 & -4 & -5 \\ \boxed{2} & -7 & 3 & 2 \end{array}\right) \xrightarrow[\text{to } (2)]{\text{add } -2(1)} \left(\begin{array}{ccc|c} 1 & -3 & -4 & -5 \\ 0 & -1 & 11 & 12 \end{array}\right) \xrightarrow[\text{by } -1]{\text{mult } (2)}$$

$$\left(\begin{array}{ccc|c} 1 & \boxed{-3} & -4 & -5 \\ 0 & 1 & -11 & -12 \end{array}\right) \xrightarrow[\text{to } (1)]{\text{add } 3(2)} \left(\begin{array}{ccc|c} 1 & 0 & -37 & -41 \\ 0 & 1 & -11 & -12 \end{array}\right).$$

let $x_3 = t$, $x_1 = -41 + 37t$, $x_2 = -12 + 11t$.

e.g. find the equation of the plane passing through $\underline{(1,2,1)}$, $(2,3,4)$, $(3,1,8)$.

vectors in the plane: $\vec{a} = \langle 1,1,3 \rangle$, $\vec{b} = \langle 2,-1,7 \rangle$.

$$\vec{n} = \vec{a} \times \vec{b} = \det\begin{pmatrix} \vec{i} & \vec{j} & \vec{k} \\ 1 & 1 & 3 \\ 2 & -1 & 7 \end{pmatrix} = \begin{vmatrix} 1 & 3 \\ -1 & 7 \end{vmatrix}\vec{i} - \begin{vmatrix} 1 & 3 \\ 2 & 7 \end{vmatrix}\vec{j} + \begin{vmatrix} 1 & 1 \\ 2 & -1 \end{vmatrix}\vec{k}$$
$$= \langle 10, -1, -3 \rangle.$$

$10x - y - 3z = d$, $10(1) - 2 - 3(1) = d$, so $d = 5$.

$10x - y - 3z = 5$.

e.g. let $A = \begin{pmatrix} 0 & 1 & 3 \\ 2 & 9 & 12 \\ 1 & 3 & 2 \end{pmatrix}$. Is A invertible? If so, find A^{-1}.

$$\left(\begin{array}{ccc|ccc} 0 & 1 & 3 & 1 & 0 & 0 \\ 2 & 9 & 12 & 0 & 1 & 0 \\ 1 & 3 & 2 & 0 & 0 & 1 \end{array}\right) \xrightarrow[(1),(3)]{\text{swap}} \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 0 & 0 & 1 \\ \boxed{2} & 9 & 12 & 0 & 1 & 0 \\ 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right) \xrightarrow[\text{to }(2)]{\text{add }-2(1)} \left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 0 & 0 & 1 \\ 0 & 3 & 8 & 0 & 1 & -2 \\ 0 & 1 & 3 & 1 & 0 & 0 \end{array}\right) \xrightarrow[(2),(3)]{\text{swap}}$$

$$\left(\begin{array}{ccc|ccc} 1 & \boxed{3} & 2 & 0 & 0 & 1 \\ 0 & 1 & 3 & 1 & 0 & 0 \\ 0 & \boxed{3} & 8 & 0 & 1 & -2 \end{array}\right) \xrightarrow[\text{add }-3(2)\text{ to }(3)]{\text{add }-3(2)\text{ to }(1)} \left(\begin{array}{ccc|ccc} 1 & 0 & -7 & -3 & 0 & 1 \\ 0 & 1 & 3 & 1 & 0 & 0 \\ 0 & 0 & -1 & -3 & 1 & -2 \end{array}\right) \xrightarrow[\text{by }-1]{\text{mult }(3)}$$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & \boxed{-7} & -3 & 0 & 1 \\ 0 & 1 & \boxed{3} & 1 & 0 & 0 \\ 0 & 0 & 1 & 3 & -1 & 2 \end{array}\right) \xrightarrow[\text{add }-3(3)\text{ to }(2)]{\text{add }7(3)\text{ to }(1)} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 18 & -7 & 15 \\ 0 & 1 & 0 & -8 & 3 & -6 \\ 0 & 0 & 1 & 3 & -1 & 2 \end{array}\right)$$

$$\begin{pmatrix} 18 & -7 & 15 \\ -8 & 3 & -6 \\ 3 & -1 & 2 \end{pmatrix} = A^{-1}$$

- e.g. find all 3 forms of the line through $(1,-3,4)$, $(3,1,7)$.

vector: $\langle x,y,z\rangle = \langle 1,-3,4\rangle + t\langle 2,-4,3\rangle$.

parametric: $x=1+2t$, $y=-3-4t$, $z=4+3t$.

symmetric: $\dfrac{x-1}{2} = \dfrac{y+3}{-4} = \dfrac{z-4}{3}$.

- e.g. are $\langle 1,3,2\rangle, \langle 2,5,1\rangle, \langle 3,8,3\rangle$ linearly dep or indep?

$$\begin{pmatrix} 1 & 3 & 2 \\ 2 & 5 & 1 \\ 3 & 8 & 3 \end{pmatrix} \xrightarrow[\text{add }-3(1)\text{ to }(3)]{\text{add }-2(1)\text{ to }(2)} \begin{pmatrix} 1 & 3 & 2 \\ 0 & -1 & -3 \\ 0 & -1 & -3 \end{pmatrix} \xrightarrow[\text{to }(3)]{\text{add }-(2)} \begin{pmatrix} 1 & 3 & 2 \\ 0 & -1 & -3 \\ 0 & 0 & 0 \end{pmatrix}.$$

Zero row, so linearly dependent.

rank $=2$.

e.g. $V = \{ \langle 2a-b, a, b \rangle : a, b \in \mathbb{R} \}$.

(i) Is $\langle 1, 3, 7 \rangle \in V$?

(ii) Is V a subspace of $\mathbb{R}^3$?

(i) Can we solve
$$\begin{aligned} 2a-b &= 1 \\ a &= 3 \\ b &= 7. \end{aligned}$$

If $a=3$, $b=7$, then $2a-b = 2(3)-7 = -1$, not 1.

$\langle 1, 3, 7 \rangle \notin V$.

(ii) Let $a=b=0$, $\langle 0, 0, 0 \rangle \in V$.

$\langle 2a_1-b_1, a_1, b_1 \rangle + \langle 2a_2-b_2, a_2, b_2 \rangle$

$= \langle 2a_1-b_1+2a_2-b_2, a_1+a_2, b_1+b_2 \rangle$

$= \langle 2(a_1+a_2)-(b_1+b_2), a_1+a_2, b_1+b_2 \rangle \in V$.

$\lambda \langle 2a-b, a, b \rangle = \langle 2\lambda a - \lambda b, \lambda a, \lambda b \rangle \in V$.

V is a subspace.

$v \in V$; $(-1)v \in V$, so $-v \in V$, and so $v + (-v) = 0 \in V$.

e.g. $A=\begin{pmatrix}2&0&0\\0&1&2\\0&-1&4\end{pmatrix}$. (i) Is it diagonalizable? (ii) Is it orthogonally diagonalizable?

(ii) No, not symmetric.

(i) $0=\det\begin{pmatrix}2-\lambda&0&0\\0&1-\lambda&2\\0&-1&4-\lambda\end{pmatrix}=(2-\lambda)\det\begin{pmatrix}1-\lambda&2\\-1&4-\lambda\end{pmatrix}$

$=(2-\lambda)(\lambda^2-5\lambda+6)$

$=(2-\lambda)(\lambda-2)(\lambda-3)$

$\lambda=2,3.$

$\lambda=2$. $A-2I=\begin{pmatrix}0&0&0\\0&-1&2\\0&-1&2\end{pmatrix}$.

$\left(\begin{array}{ccc|c}0&0&0&0\\0&-1&2&0\\0&-1&2&0\end{array}\right)\xrightarrow[(1),(2)]{\text{swap}}\left(\begin{array}{ccc|c}0&-1&2&0\\0&0&0&0\\0&-1&2&0\end{array}\right)\xrightarrow[\text{by } -1]{\text{mult}(1)}\left(\begin{array}{ccc|c}0&1&-2&0\\0&0&0&0\\0&-1&2&0\end{array}\right)\xrightarrow[\text{to }(3)]{\text{add}(1)}\left(\begin{array}{ccc|c}0&1&-2&0\\0&0&0&0\\0&0&0&0\end{array}\right)$

Let $x_1=t$, $x_3=u$, $x_2=2u$. $B_{(1)}=\left\{\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\2\\1\end{pmatrix}\right\}$.

$\lambda=3$: $A-3I=\begin{pmatrix}-1&0&0\\0&-2&2\\0&-1&1\end{pmatrix}$.

$\left(\begin{array}{ccc|c}-1&0&0&0\\0&-2&2&0\\0&-1&1&0\end{array}\right)\xrightarrow[\text{by } -1]{\text{mult}(1)}\left(\begin{array}{ccc|c}1&0&0&0\\0&-2&2&0\\0&-1&1&0\end{array}\right)\xrightarrow[\text{by } -\frac{1}{2}]{\text{mult}(2)}\left(\begin{array}{ccc|c}1&0&0&0\\0&1&-1&0\\0&-1&1&0\end{array}\right)\xrightarrow[\text{to }(3)]{\text{add}(2)}\left(\begin{array}{ccc|c}1&0&0&0\\0&1&-1&0\\0&0&0&0\end{array}\right)$

Let $x_3=t$. $x_1=0$, $x_2=t$. $B_{(1)}=\left\{\begin{pmatrix}0\\1\\1\end{pmatrix}\right\}$

$P=\begin{pmatrix}1&0&0\\0&2&1\\0&1&1\end{pmatrix}$. $P^{-1}AP=\begin{pmatrix}2&0&0\\0&2&0\\0&0&3\end{pmatrix}$.

- e.g. encode and decode the message HOWDY using the key $A = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}$

$$M = \begin{pmatrix} 8 & 15 & 23 \\ 4 & 25 & 0 \end{pmatrix}$$

encode: $B = AM = \begin{pmatrix} 1 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 8 & 15 & 23 \\ 4 & 25 & 0 \end{pmatrix} = \begin{pmatrix} 20 & 90 & 23 \\ 36 & 155 & 46 \end{pmatrix}$.

$$A^{-1} = \frac{1}{-1}\begin{pmatrix} 5 & -3 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -5 & 3 \\ 2 & -1 \end{pmatrix}.$$

check $A^{-1}B = \begin{pmatrix} -5 & 3 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 20 & 90 & 23 \\ 36 & 155 & 46 \end{pmatrix} = \begin{pmatrix} 8 & 15 & 23 \\ 4 & 25 & 0 \end{pmatrix}$ HOWDY_.

- e.g. using the Cayley-Hamilton method, find A^8, $A = \begin{pmatrix} -1 & 0 \\ 3 & 2 \end{pmatrix}$

$$A^8 = c_0 I + c_1 A.$$

If λ is an eigenvalue of A, $c_0 + c_1\lambda = \lambda^8$.

A is lower triangular, $\lambda = -1, 2$

$$\begin{aligned} c_0 - c_1 &= 1 \\ c_0 + 2c_1 &= 256 \\ \hline 3c_1 &= 255. \\ c_1 = 85,\ & c_0 = 86. \end{aligned}$$

$$A^8 = 86I + 85A.$$