

# Linear Algebra

vector:

(1)  $\vec{\phantom{x}}$  something with magnitude & direction

(2)  $\begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$  a column of numbers

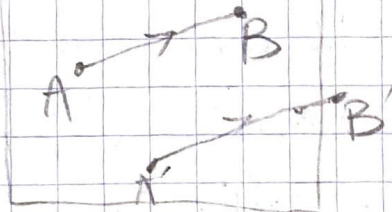
(3) an element of a vector space

(4) an ordered collection of magnitudes

\* directed segment:  $\vec{AB}$

\* translation: move the endpoints without changing the length & direction

plane  $\mathbb{R}^2$   
 $\vec{AB}$ , directed seg.  
 $[\vec{AB}]$  the vector it represents

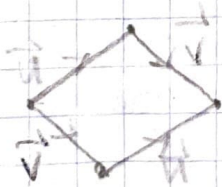
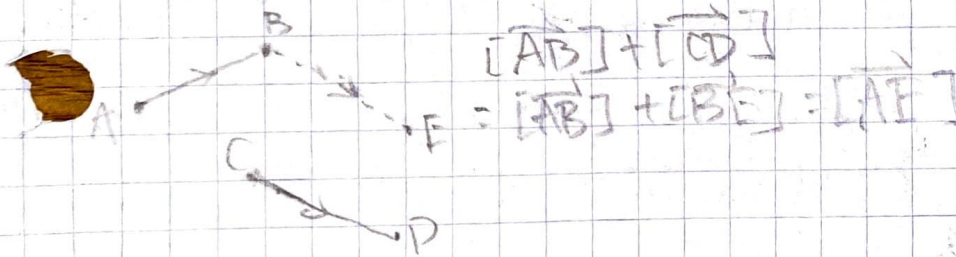


vector is an equivalence class of directed segments modulo translation. if 2 dir seg differ by a translation, they represent the same vector

$\vec{AB}$  &  $\vec{A'B'}$  are different dir seg. but the same vector

addition:  $[\vec{AB}] + [\vec{CD}]$  two vectors

\*  $\vec{MA} = \vec{OA} - \vec{OM}$



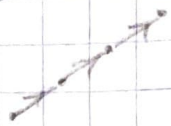
$\vec{u} + \vec{v} = \vec{v} + \vec{u}$

One can do linear combination of 2 vectors.

scalar multiplication

if  $\vec{v}, \vec{w}$  are vectors and  $a, b \in \mathbb{R}$

$3 \cdot \vec{v}$   
 $= \vec{v} + \vec{v} + \vec{v}$



then  $a \cdot \vec{v} + b \cdot \vec{w}$  is well defined

inner product (dot product): given 2 vectors,  $\vec{v}, \vec{w}$ , we define  $\langle \vec{v}, \vec{w} \rangle \in \mathbb{R}$

$\langle \vec{v}, \vec{w} \rangle = |\vec{v}| \cdot |\vec{w}| \cdot \cos \theta$



inner product is a linear operation

linear means the structure of scalar multiplication & addition

\*  $\langle \vec{v}_1 + \vec{v}_2, \vec{w} \rangle = \langle \vec{v}_1, \vec{w} \rangle + \langle \vec{v}_2, \vec{w} \rangle$

& addition

\*  $\langle 3\vec{v}, \vec{w} \rangle = 3 \cdot \langle \vec{v}, \vec{w} \rangle$

vector space: solution to  $f''(x) = f(x)$

$$\langle u, u \rangle = |u|^2$$

$$\cos \theta = \frac{\langle u, v \rangle}{\sqrt{\langle u, u \rangle} \sqrt{\langle v, v \rangle}}$$

$$\langle u_1 + u_2, v_1 + v_2 \rangle$$

$$= \langle u_1, v_1 \rangle + \langle u_2, v_1 \rangle + \langle u_1, v_2 \rangle + \langle u_2, v_2 \rangle$$

Basis Vector:

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



$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

then any other vector in  $\mathbb{R}^2$  can be written as linear combination

$$v = a_1 e_1 + a_2 e_2$$

$e_1, e_2$  forms an orthonormal basis

(orthogonal),  $\langle e_1, e_2 \rangle = 0$

normal,  $|e_1| = 1, |e_2| = 1$

claim:  $v = \langle v, e_1 \rangle e_1 + \langle v, e_2 \rangle e_2$

proof: suppose  $v = a_1 e_1 + a_2 e_2$ , then we apply  $\langle \cdot, e_1 \rangle$  to both sides

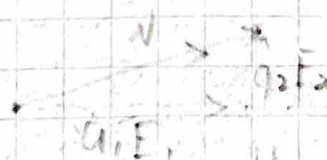
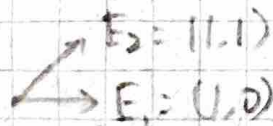
$$\begin{aligned} \langle v, e_1 \rangle &= \langle a_1 e_1 + a_2 e_2, e_1 \rangle = a_1 \langle e_1, e_1 \rangle + a_2 \langle e_2, e_1 \rangle \\ &= a_1 \cdot 1 + a_2 \cdot 0 = a_1 \end{aligned}$$

"skewed" basis on  $\mathbb{R}^2$   
↑ not orthonormal

In general, if two vectors  $E_1, E_2$  in  $\mathbb{R}^2$  satisfies the property that, any vector  $v \in \mathbb{R}^2$  can be written as

$$v = a_1 E_1 + a_2 E_2$$

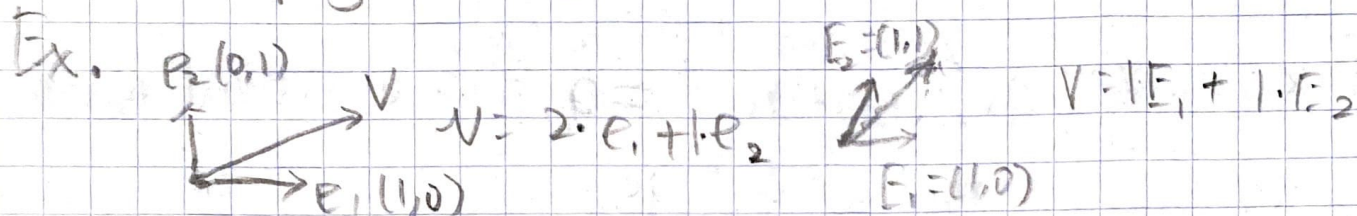
then we say  $(E_1, E_2)$  is a basis



## Coordinates:

Given a basis  $E_1, E_2$ , we say a vector  $v$  has coordinate  $(a_1, a_2)$  if  $v = a_1 E_1 + a_2 E_2$

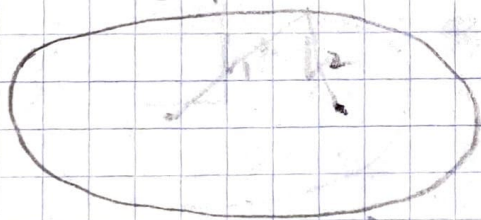
Note: if you change basis, the coordinate will change



## Conic Sections

As the "slope" of the plane increases, we get ellipse  $\rightarrow$  parabola, hyperbola

ellipse



focal points fixed



ellipse - points on  $\mathbb{R}^2$  such that  $|d_1 - d_2| = L$

A cone in  $\mathbb{R}^3$ :  $x_1^2 + x_2^2 = x_3^2$

a line in  $\mathbb{R}^2$  can be described

by an equation  $a_1 x_1 + a_2 x_2 = a_3$

A plane in  $\mathbb{R}^3$ :  $a_1 x_1 + a_2 x_2 + a_3 x_3 = a_0$

A conic section is given by  $\sum_{i=1}^2 (x_i, x_i, x_3)$   $\left. \begin{array}{l} x_1^2 + x_2^2 = x_3^2 \\ a_1 x_1 + a_2 x_2 + a_3 x_3 = a_0 \end{array} \right\}$   
 if  $a_3 \neq 0$ , then  $x_3 = \frac{a_0 - a_1 x_1 - a_2 x_2}{a_3}$

plug in  $x_3 = \dots$  to the first eq.

$$x_1^2 + x_2^2 = \left( \frac{a_0 - a_1 x_1 - a_2 x_2}{a_3} \right)^2$$

$$\Leftrightarrow Ax_1^2 + Bx_1x_2 + Cx_2^2 + Dx_1 + Ex_2 + F = 0 \quad (\text{projected to a plane})$$

$\{(x_1, x_2, x_3) \mid a_1x_1 + a_2x_2 + a_3x_3 = a_0\}$  is a vertical plane

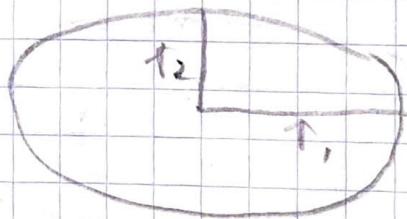
Def: a conic curve in  $\mathbb{R}^2$  is

$$\{(x_1, x_2) \in \mathbb{R}^2 \mid Ax_1^2 + Bx_1x_2 + Cx_2^2 + Dx_1 + Ex_2 + F = 0\} \quad \begin{matrix} A, B, C \text{ aren't} \\ \text{simultaneously} \end{matrix}$$

Ex.: (1)  $x_1^2 + x_2^2 = 1$  unit circle

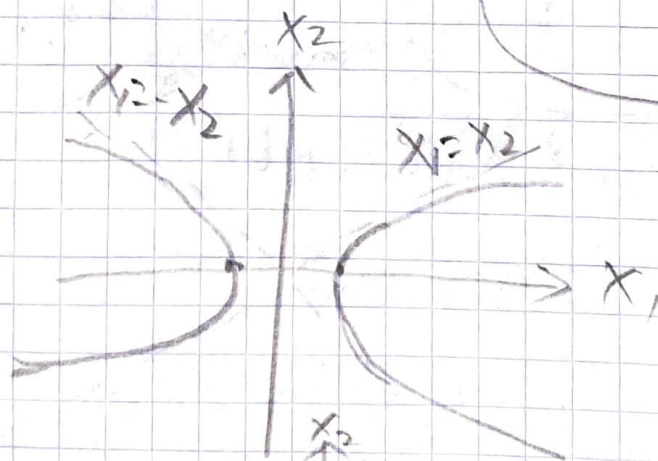
$$x_1^2 + x_2^2 = r^2 \Leftrightarrow \left(\frac{x_1}{r}\right)^2 + \left(\frac{x_2}{r}\right)^2 = 1$$

(2)  $\left(\frac{x_1}{r_1}\right)^2 + \left(\frac{x_2}{r_2}\right)^2 = 1$  ellipse

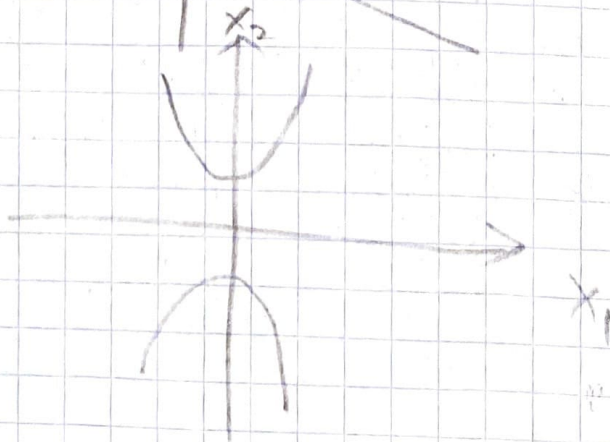


(3) hyperbola

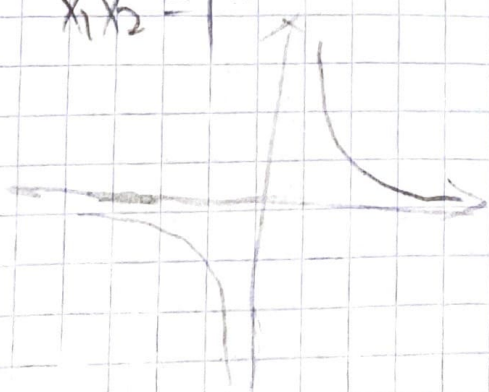
$$x_1^2 - x_2^2 = 1$$



$$-x_1^2 + x_2^2 = 1$$

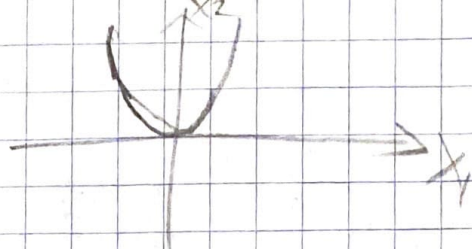


$$x_1x_2 = 1$$



(3) parabola

$$x_1^2 = x_2$$



Starting from the following 3 examples:

$$x_1^2 + x_2^2 = 1$$

$$x_1^2 - x_2^2 = 1$$

$$x_2 = x_1^2$$

Using linear transformation, we can obtain all possible conic curves

Linear Transformation

$$T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

Def 1:  
using matrix

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 \\ a_{21}x_1 + a_{22}x_2 \end{pmatrix}$$

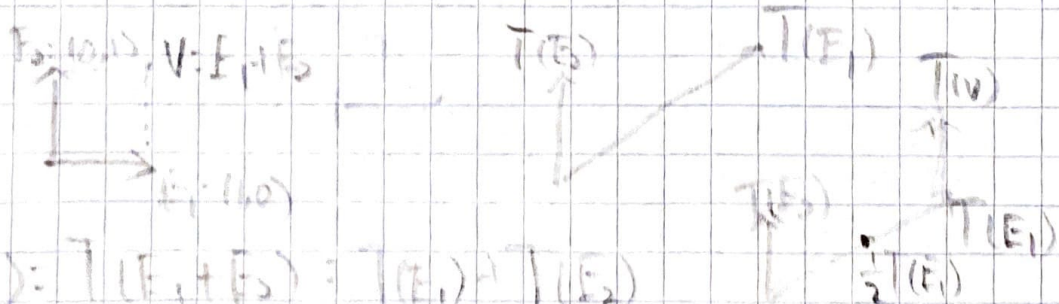
Def 2:  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  is a linear transformation

if (1)  $T(c \cdot \vec{v}) = c T(\vec{v}) \quad \forall c \in \mathbb{R}$

(2)  $T(\vec{v} + \vec{w}) = T(\vec{v}) + T(\vec{w})$

Fix a basis  $\{E_1, E_2\}$  of  $\mathbb{R}^2$  i.e.  $T$  respects / preserves the linear structure on both sides into transformation

Prop 1: A linear transformation  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  is determined by how it acts on the basis vectors



$$T(v) = T(E_1 + E_2) = T(E_1) + T(E_2)$$

$$T(w) = T(3E_1) = 3T(E_1)$$

Prop 1 pf: Any vector  $v \in \mathbb{R}^2$  can be written as

$$v = a_1 E_1 + a_2 E_2 \quad (\text{by def of the basis vectors})$$

By linearity of  $T$ ,  $T(v) = T(a_1 E_1 + a_2 E_2)$

$$= T(a_1 E_1) + T(a_2 E_2)$$

$$= a_1 T(E_1) + a_2 T(E_2)$$

Hence  $T(v)$  is determined

$$T(E_1) = a_{11} E_1 + a_{12} E_2 \quad \text{then } T(a_1 E_1 + a_2 E_2) = \underline{\quad} E_1 + \underline{\quad} E_2$$

$$T(E_2) = a_{21} E_1 + a_{22} E_2 = c_1 T(E_1) + c_2 T(E_2)$$

$$= c_1 (a_{11} E_1 + a_{12} E_2) + c_2 (a_{21} E_1 + a_{22} E_2)$$

$$= (c_1 a_{11} + c_2 a_{21}) E_1 + (c_1 a_{12} + c_2 a_{22}) E_2$$

$$= (c_1, c_2) \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}$$

$$T \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} = A \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}$$

matrix  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

$$(A \cdot B)_{ij} = \sum_k a_{ik} b_{kj}$$

$i$ th row  
 $j$ th column

$$(AB)_{11} = a_{11} b_{11} + a_{12} b_{21}$$

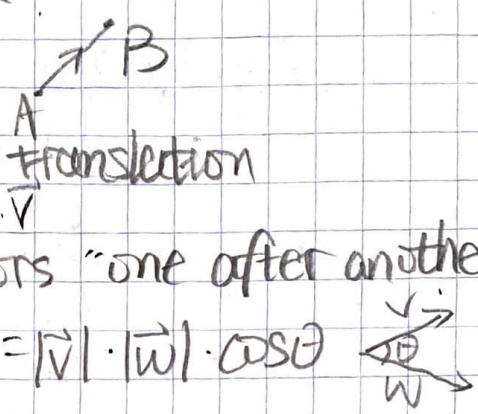
in general

$$n \times \underbrace{L}_{[A]} \cdot \underbrace{m}_{[B]} = n \times \underbrace{m}_{[AB]}$$

Recap:

(1). Geometric Def of a vector:

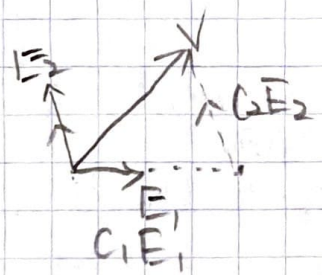
- directed segment:  $\vec{AB}$
- vectors as dir. seg. up to translation
- scalar multiplication  $3 \cdot \vec{v}$
- addition: put two vectors "one after another"
- inner product:  $\langle \vec{v}, \vec{w} \rangle = |\vec{v}| \cdot |\vec{w}| \cdot \cos \theta$



(2) basis and coordinates:

if  $\{E_1, E_2\}$  is a basis, if and only if for any  $v \in \mathbb{R}^2$ , there exist a unique way to write  $v = c_1 E_1 + c_2 E_2$

The coefficients  $(c_1, c_2)$  are called coordinate of  $v$  with respect to  $(E_1, E_2)$



$Q(\vec{x}) = ax_1^2 + bx_1x_2 + cx_2^2$   
 $\vec{x} = (x_1, x_2)$

homogeneous degree 2 polynomial in  $x_1, x_2$  variables

Given a quadratic form, we can try to solve  $Q(\vec{x}) = 1$

- $\Rightarrow$  {
- ellipse
  - hyperbola
  - empty curve

• Linear Transformation:  
 $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$

Def: linear transformation is a map from  $\mathbb{R}^2$  to  $\mathbb{R}^2$  that respect "linear structure"  $\Rightarrow$  sc. multipl. addition.

Prop:  $T(\vec{0}) = \vec{0}$

$T(c_1 E_1 + c_2 E_2) = c_1 T(E_1) + c_2 T(E_2)$

hence, if we know  $T(E_1), T(E_2)$ , we know  $T(v)$  for any  $v \in \mathbb{R}^2$

### Affine Linear Transformation

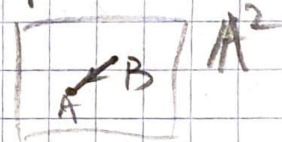


$A+B = ?$  not well-defined (no origin)

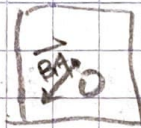
$A-B = ?$   $\vec{BA}$  a directed segment  $\rightsquigarrow$  a vector

(terminology:   
 • vector space = linear space   
 • affine space = affine linear space   
 } forget the origin   
 } choose an origin

$A^2$  to mean 2-dim affine linear space



$\mathbb{R}^2$  to mean linear space



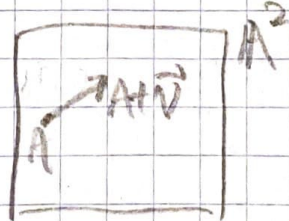
$\mathbb{R}^2$

$\therefore A^2 \times A^2 = \mathbb{R}^2$

$(A, B) \mapsto A - B = \vec{BA}$

$+ : A^2 \times \mathbb{R}^2 \rightarrow A^2$

$(A, \vec{v}) \mapsto A + \vec{v}$



notation:

• set: a collection of objects   
 if  $A, B$  are sets, a map

$f: A \rightarrow B$  is an assignment of elements in  $B$  to elements in  $A$

• Given 2 sets  $A, B$ , we can define 'Cartesian product'

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

$T: A^2 \rightarrow A^2$

$(x_1, x_2) \mapsto (\tilde{x}_1, \tilde{x}_2)$    
 $\tilde{x}_1 = a_{11}x_1 + a_{12}x_2 + a_{10}$

$\tilde{x}_2 = a_{21}x_1 + a_{22}x_2 + a_{20}$

$\begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} a_{10} \\ a_{20} \end{pmatrix}$



Prop: Any quadratic form  $Q(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$  can be written in a new coordinate  $(\tilde{x}_1, \tilde{x}_2)$  as one of the following form

①  $\tilde{x}_1^2 + \tilde{x}_2^2$       Where  $\begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

②  $\tilde{x}_1^2 - \tilde{x}_2^2$        $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix}$

③  $\tilde{x}_1^2$

④ 0      ⑤  $-\tilde{x}_1^2 - \tilde{x}_2^2$

assuming:  $a \neq 0$

$$\begin{aligned} & ax_1^2 + bx_1x_2 + cx_2^2 \\ &= a \left[ x_1^2 + \frac{b}{a} x_1x_2 \right] + cx_2^2 \\ &= a \left[ x_1^2 + 2x_1 \frac{b}{2a} x_2 + \left( \frac{b}{2a} x_2 \right)^2 - \left( \frac{b}{2a} x_2 \right)^2 \right] + cx_2^2 \\ &= a \left[ x_1 + \frac{b}{2a} x_2 \right]^2 - a \frac{b^2 x_2^2}{4a^2} + cx_2^2 \\ &= a \left[ x_1 + \frac{b}{2a} x_2 \right]^2 + \left( c - \frac{b^2}{4a} \right) x_2^2 \end{aligned}$$

① if  $a > 0, c > \frac{b^2}{4a}$ , then define  $\tilde{x}_1 = \sqrt{a} \left( x_1 + \frac{b}{2a} x_2 \right)$

$$\tilde{x}_2 = \sqrt{c - \frac{b^2}{4a}} x_2$$

$$Q = \tilde{x}_1^2 + \tilde{x}_2^2$$

② if  $a < 0, c < \frac{b^2}{4a}$ ,  $\tilde{x}_1 = \sqrt{|a|} \left( x_1 + \frac{b}{2a} x_2 \right)$

$$\tilde{x}_2 = \sqrt{|c - \frac{b^2}{4a}|} x_2$$

Prop 2:  $Q(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2 + dx_1 + ex_2 + f$

can be written in a new affine linear coordinate  $(\tilde{x}_1, \tilde{x}_2)$  as one of the following form

①  $\tilde{x}_1^2 + \tilde{x}_2^2 + \tilde{c}$       ⑤  $-\tilde{x}_1^2 - \tilde{x}_2^2 + \tilde{c}$

②  $\tilde{x}_1^2 + \tilde{x}_2^2 + \tilde{c}$

Where  $\begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} a_{10} \\ a_{20} \end{pmatrix}$

③  $\tilde{x}_1^2 + \tilde{c}$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{pmatrix} + \begin{pmatrix} b_{10} \\ b_{20} \end{pmatrix}$$

④  $\tilde{c}$

$$Q = x^2 + y^2 + 2ax + 2by + c$$

$$= (x+a)^2 - a^2 + (y+b)^2 - b^2 + c$$

$$= (x+a)^2 + (y+b)^2 + (c - a^2 - b^2)$$

$$= \tilde{x}^2 + \tilde{y}^2 + \tilde{c}$$

# Review: Linear Transformation and Matrices

$$T: \mathbb{R}^2 \rightarrow \mathbb{R}^2 \quad T(\vec{v} + \vec{w}) = T(\vec{v}) + T(\vec{w})$$

$$T(C \cdot \vec{v}) = C T(\vec{v})$$

Let  $\{\vec{E}_1, \vec{E}_2\}$  be a basis of  $\mathbb{R}^2$   
and suppose  $(T\vec{E}_1, T\vec{E}_2) = (\vec{E}_1, \vec{E}_2) \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \vec{E}_1 a_{11} + \vec{E}_2 a_{21} + \vec{E}_1 a_{12} + \vec{E}_2 a_{22}$

Let  $\vec{v} \in \mathbb{R}^2$  be any vector

Then we can write

$$\vec{v} = c_1 \vec{E}_1 + c_2 \vec{E}_2 \quad \text{for some } c_1, c_2 \in \mathbb{R}$$

$$= (\vec{E}_1, \vec{E}_2) \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

$$T\vec{v} = T(\vec{E}_1, \vec{E}_2) \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = (T\vec{E}_1, T\vec{E}_2) \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = (\vec{E}_1, \vec{E}_2) \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

$$= (\vec{E}_1, \vec{E}_2) \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

Ex: (1) stretching

$$T(\vec{E}_1) = 2\vec{E}_1$$

$$T(\vec{E}_2) = \frac{1}{3}\vec{E}_2$$

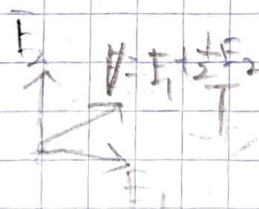
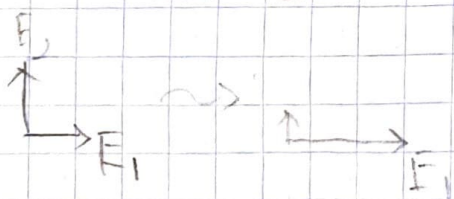
(2) projection

$$T(\vec{E}_1) = 0$$

$$T(\vec{E}_2) = \vec{E}_2$$

$$\tilde{c}_1 = a_{11}c_1 + a_{12}c_2$$

$$\tilde{c}_2 = a_{21}c_1 + a_{22}c_2$$



$$\begin{aligned} T(\vec{E}_1) &= 0 \\ T(\vec{E}_2) &= \vec{E}_2 \\ T(\vec{v}) &= T(\vec{E}_1 + \frac{1}{3}\vec{E}_2) \\ &= T(\vec{E}_1) + \frac{1}{3}T(\vec{E}_2) \\ &= 0 + \frac{1}{3}\vec{E}_2 \\ &= \frac{1}{3}\vec{E}_2 \end{aligned}$$

(3) another projection:

$$T(\vec{E}_1) = \frac{1}{2}\vec{E}_2$$

$$T(\vec{E}_2) = \vec{E}_2$$

image of  $\mathbb{R}^2$  under  $T$  is the subspace  $\mathbb{R} \cdot \vec{E}_2$

# Operations on Linear Transformations $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$

(1) addition:  $T_1: \mathbb{R}^2 \rightarrow \mathbb{R}^2$   $(c_1 T_1 + c_2 T_2)(\vec{v})$   
 scalar multiplication:  $T_2: \mathbb{R}^2 \rightarrow \mathbb{R}^2$   $= c_1 T_1(\vec{v}) + c_2 T_2(\vec{v})$

$$c_1 T_1 + c_2 T_2: \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

is still linear transformation

if  $T_1$  is represented by matrix  $[T_1] = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$

$[T_2] = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$  then  $c_1 T_1 + c_2 T_2$

$$\mathbb{R}^2 \xrightarrow{T_1} \mathbb{R}^2 \xrightarrow{T_2} \mathbb{R}^2 \quad \vec{v} \mapsto T_1(\vec{v}) \mapsto T_2(T_1(\vec{v}))$$

$$\underbrace{\hspace{10em}}_{T_2 \circ T_1}$$

Ex.  $[T_1] = \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$

$$[T_2] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$[T_2] \cdot [T_1] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{3} \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{3} \\ 2 & 0 \end{pmatrix}$$

Remarks: (1)  $[T_1] \cdot [T_2] \neq [T_2] \cdot [T_1]$

(2)  $([T_1] \cdot [T_2]) \cdot [T_3] = [T_1] \cdot ([T_2] \cdot [T_3])$

(3)  $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  identity matrix  $[I] \cdot [T] = [T]$

A linear transformation  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  is invertible, if there is an  $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$

$$S \circ T = Id$$

Lemma:

$[T] = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  then  $[T]$  is invertible, if and only if  $\det([T]) \neq 0$   
 $ad - bc$

then  $[T] \cdot [T]^{-1} = [Id]$

$$[T]^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$[T]^{-1} \cdot [T] = [Id]$$

$$T(\vec{e}_2) = \begin{pmatrix} b \\ d \end{pmatrix}$$

$$\begin{matrix} \uparrow \\ \rightarrow \end{matrix} T(\vec{e}_1) = \begin{pmatrix} a \\ c \end{pmatrix} \quad | \text{Area}(\vec{e}_1, \vec{e}_2) | = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$\vec{v}, \vec{w}$  are linear independent

if  $c_1 \vec{v} + c_2 \vec{w} = \vec{0}$  if and only if  $\iff c_1 = 0$  and  $c_2 = 0$

Recall: Let  $\mathbb{R}^2$  be equipped with the standard inner product

$$\langle \vec{u}, \vec{v} \rangle = |\vec{u}| \cdot |\vec{v}| \cdot \cos \theta$$

A basis  $\{\vec{e}_1, \vec{e}_2\}$  is orthonormal, if  $|\vec{e}_i| = 1$   
 $\langle \vec{e}_1, \vec{e}_2 \rangle = 0$

if  $\vec{v}$  has coord  $\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$   $\vec{v} = \vec{e}_1 v_1 + \vec{e}_2 v_2$

and  $\vec{w} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$

then  $\langle \vec{v}, \vec{w} \rangle = v_1 w_1 + v_2 w_2$

Def: A linear trans.  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  is an orthogonal trans. if for any  $\vec{v}, \vec{w} \in \mathbb{R}^2$   $\langle T\vec{v}, T\vec{w} \rangle = \langle \vec{v}, \vec{w} \rangle$

then  $\langle \vec{v}, \vec{w} \rangle = v_1 w_1 + v_2 w_2 = (w_1, w_2) \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = (v_1, v_2) \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$   
 $= \vec{w}^t \cdot \vec{v} = \vec{v}^t \cdot \vec{w}$

Prop: Let  $\{\vec{e}_1, \vec{e}_2\}$  be one ONB of  $\mathbb{R}^2$

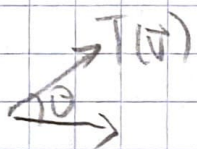
Let  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  be a linear trans.

and  $[T]$  the matrix form with respect to  $\{\vec{e}_1, \vec{e}_2\}$

Then  $T$  is an orthogonal trans.

$$\text{iff } [T^{-1}]^{-1} = [T]^t$$

$$\text{Ex: (1) } [T] = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$



$$[R_\theta]^t = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

$$[R(\theta)]^t [R_\theta] = \begin{pmatrix} c^2+s^2 & 0 \\ 0 & c^2+s^2 \end{pmatrix}$$

Recall:

vector space:  $\mathbb{R}^2$

inner product  $\langle \cdot, \cdot \rangle$

linear in each slot

$\langle u, u \rangle \geq 0$

symmetric  $\langle u, v \rangle = \langle v, u \rangle$

$T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  is an orthogonal transformation of  $\mathbb{R}^2$   $T \in O(2)$

if  $\forall u, v \in \mathbb{R}^2$   $\langle u, v \rangle = \langle Tu, Tv \rangle$

Prop: if  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  preserves length, then  $\langle u, v \rangle = \langle Tu, Tv \rangle$

Proof: By polarization, we have

$$\langle u+v, u+v \rangle = \langle T(u+v), T(u+v) \rangle$$

$$\langle u, u \rangle + \langle v, v \rangle + 2\langle u, v \rangle = \langle Tu, Tu \rangle + \langle Tv, Tv \rangle + 2\langle Tu, Tv \rangle$$

$$\Rightarrow \langle u, v \rangle = \langle Tu, Tv \rangle$$

Given an orthonormal basis  $(\vec{e}_1, \vec{e}_2)$ , then an ortho  $T \in O(2)$

can be presented as  $[T] = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

so that given a vector  $\vec{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$

$$T\vec{v} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

Prop  $[T]^{-1} = [T]^t$  ( $T \in O(2)$ ) i.e.  $[T]^t [T] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Proof: for any 2 vectors  $\vec{v}, \vec{w} \in \mathbb{R}^2$   $\vec{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$   $\vec{w} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$

$$\langle \vec{v}, \vec{w} \rangle = (v_1, v_2) \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = (v_1, v_2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$$

$$\langle T\vec{v}, T\vec{w} \rangle = ([T]\vec{v})^t \cdot ([T]\vec{w})$$

$$= \vec{v}^t \cdot [T]^t [T] \cdot \vec{w}$$

Lemma: Let  $M$  be a  $2 \times 2$  matrix

if for any  $\vec{v}, \vec{w} \in \mathbb{R}^2$

We have  $\vec{v}^t \cdot M \cdot \vec{w} = 0$

then  $M = 0$

Pf:  $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$  if  $M$  is not zero

then at least one entry of  $M$  is non zero

say  $m_{11} \neq 0$

then we can let  $\vec{v} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ,  $\vec{w} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$$0 = \vec{v}^t \cdot M \cdot \vec{w} = (1, 0) \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= (1, 0) \begin{pmatrix} m_{11} \\ m_{21} \end{pmatrix} = m_{11}$$

Contradiction

In fact

$$m_{ij} = \vec{e}_i^t \cdot M \cdot \vec{e}_j \quad \text{Thus } m_{ij} = 0 \quad \forall i, j$$

$$\text{Since } 0 = \langle \vec{v}, \vec{w} \rangle = \langle T\vec{v}, T\vec{w} \rangle$$

$$= \vec{v}^t \cdot I_2 \cdot \vec{w} = \vec{v}^t [T]^t [T] \cdot \vec{w}$$

$$= \vec{v}^t \cdot (I_2 - [T]^t [T]) \cdot \vec{w}$$

By the previous lemma, we have  $I_2 - [T]^t [T] = 0$

$$R(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

$$\det R(\theta) = \cos^2 \theta - (\sin \theta)(-\sin \theta)$$

$$= \cos^2 \theta + \sin^2 \theta = 1$$

Rotation matrix

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos \theta \\ \sin \theta \end{pmatrix}$$

A B  $(2 \times 2)$

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

$$\det(A \cdot B) = (\det A) (\det B)$$

$$\det(A) = \det(B)$$



## Inverses

A is invertible iff  $\exists B$  such that  $AB = I$ . we

write  $B = A^{-1}$

1) If  $AB = I \Rightarrow BA = I$

2)  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$   
 $ad-bc \neq 0$

$x_1 = ax'_1 + bx'_2$   
 $x_2 = cx'_1 + dx'_2$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x'_1 \\ x'_2 \end{bmatrix}$$

$A^{-1} \vec{x} = \vec{x}'$

## Similarity Transformations

$\vec{y} = T \vec{x}$

$T \vec{x} = A \vec{y}'$

$A^{-1}TA$  is the matrix of the [T. that send  $\vec{x} \mapsto \vec{y}'$

$\vec{x} = A \vec{x}'$

$A^{-1}T \vec{x} = \vec{y}'$

$\vec{x} \mapsto \vec{y}'$

$\vec{y} = A \vec{y}'$

$A^{-1}TA \vec{x}' = \vec{y}'$

$A^{-1}TA$  and  $T$  are similar (related) by a similarity transformation

Prove that  $z^{-1}, \bar{z}$  are proportional -

$z = a + bi$

$\bar{z} = a - bi$

$\frac{\bar{z}}{z^{-1}} = (a-bi)(a+bi)$

$= a^2 + b^2$

$= \cos^2 \theta + \sin^2 \theta$

$z^{-1} = \frac{1}{a+bi}$

$z^{-1} = \frac{1}{(a+bi)} \bar{z} = \frac{a-bi}{a^2+b^2} \bar{z} = \frac{1}{2} \frac{1+i\sqrt{3}}{2}$

Compute  $\left(\frac{\sqrt{3} + i}{2}\right)^{100}$

$= \left(\cos \frac{\pi}{6} + i \sin \frac{\pi}{6}\right)^{100} = \left(e^{i\pi/6}\right)^{100} = e^{50i\pi/3}$

Express  $\cos(\theta_1 + \theta_2)$   
 $\cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2$   
 $e^{i(\theta_1 + \theta_2)} = (e^{i\theta_1})(e^{i\theta_2})$

in terms of  $(\cos(\theta_1), \sin(\theta_1))$   $i=1,2$   
 $\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2) = \cos \theta_1 \cos \theta_2 - \sin \theta_1 \sin \theta_2 + i(\sin \theta_1 \cos \theta_2 + \cos \theta_1 \sin \theta_2)$

$$z^3 + 8 = 0$$

$$(z+2)(z^2-2z+4)=0$$

$$z = -2, \quad z^2 - 2z + 4 = 0$$

$$z = \frac{2 \pm \sqrt{4-16}}{2} = \frac{2 \pm \sqrt{-12}}{2} = 1 \pm i\sqrt{3}$$

$$z^3 + i = 0$$

$$(z + \sqrt[3]{i})(z^2 - \sqrt[3]{i}z - 1) = 0$$

$$z = -\sqrt[3]{i}, \quad z = \frac{\sqrt[3]{i} \pm \sqrt{3}}{2}$$

$$z^4 + 4z^2 + 4 = 0$$

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

$$z^2 = -2$$

$$z = \pm \sqrt{-2}$$

$$z^4 - 2z^2 + 4 = 0$$

$$z^4 + 1 = 0$$

$$z^4 - (i)^2 = 0$$

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

$$z^2 = i \quad z^2 = -i$$

$$z = \pm \sqrt{i} \quad z = \pm \sqrt{-i}$$

# Complex Numbers

$i$  or  $\sqrt{-1}$  as the one of the solutions to  $x^2 + 1 = 0$   
the real part

a complex number:  $z = a + bi$   $a, b \in \mathbb{R}$   $\sqrt{-1}$ ,  $-\sqrt{-1}$   
the imaginary part  $\text{Re}(z) = a; \text{Im}(z) = b$

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

$$(a + bi)(c + di) = ac + bci + adi - bcd = (ac - bd) + (bc + ad)i$$

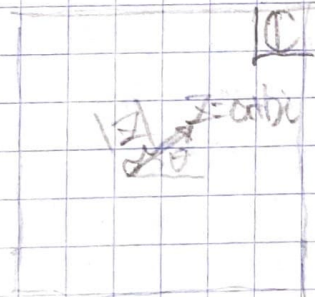
complex conjugation:

$$z = a + bi \quad \bar{z} = a + b(-i) \quad \text{change } i \text{ to } (-i)$$

if we are given a degree 2 polynomial with real coeff

$$f(x) = x^2 + Cx + C_0 \quad C, C_0 \in \mathbb{R}$$

Then the equation  $f(x) = 0$  Sometimes has 2 complex solutions  
 - they are in complex conjugate



$$|z| = \sqrt{a^2 + b^2} \quad \text{argument}$$

$$\theta = \arg(z) \quad (\text{we identify } \theta \text{ with } \theta + 2\pi k)$$

polar form

$$z = r \cdot e^{i\theta} \quad e^{i\theta} = \cos(\theta) + i \sin(\theta)$$

$$= r \cos \theta + i r \sin \theta$$

$$z_1 z_2 = (r_1 e^{i\theta_1})(r_2 e^{i\theta_2}) = (r_1 r_2) e^{i(\theta_1 + \theta_2)} \quad \bar{z} = r e^{-i\theta} \quad i = e^{i \frac{\pi}{2}}$$

Fundamental theorem of algebra:

Let  $f(z) = z^n + C_{n-1}z^{n-1} + C_{n-2}z^{n-2} + \dots + C_0$   
 be a degree  $n$  polynomial where  $C_i \in \mathbb{C}$

Then  $f(z)$  has  $n$  solutions, counted with multiplicity

$$f(z) = (z - z_1)^{m_1} \dots (z - z_r)^{m_r} \quad m_i \geq 1 \text{ integers}$$

$z_i$  are distinct roots  $m_1 + \dots + m_r = n$

# Four Theorems of Linear Algebra

- Rank Thm
- Inertia Thm
- Orthogonal Diag. Thm
- Jordan Normal Thm

Math: Classification Problem

- Transformation (Group)

• We want to define equivalence up to transformation

$$G \curvearrowright X$$

$$a: G \times X \rightarrow X$$

Two elements  $x, y \in X$  are equivalent, if there exists  $g \in G$ , such that  $g \cdot x = y$ . We denote  $x \sim y$ .

$$\Leftrightarrow x = g^{-1} \cdot y$$

For a system of linear equations:

$$y_1 = a_{11}x_1 + \dots + a_{1n}x_n$$

$$y_2 = a_{21}x_1 + \dots + a_{2n}x_n$$

$$\vdots$$

$$y_m = a_{m1}x_1 + \dots + a_{mn}x_n$$

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$$\vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

$$\vec{y} = A \cdot \vec{x}$$

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

① Describe the equivalence class

$$X/\sim$$

an equivalence class can be described by a model element  
a.k.a. representative

Ex: {conic curves}

$$= \{\text{ellipses}\} \cup \{\text{parabolas}\} \cup \{\text{hyperbolas}\}$$

mit  
circle  $\bigcirc$

$$y^2 = x \cup$$

$$x^2 - y^2 = 1$$

Rank Thm:

Any linear equation of the form  $\vec{y} \in M_{m \times 1}$   
 $\vec{y} = A \vec{x}$ , where  $\vec{x} \in M_{n \times 1}$   
 $\vec{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$   $\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

Can be simplified by a "change of variables"

$$\vec{y} = B \vec{Y}, \quad \vec{x} = C \vec{X}$$

B is  $m \times m$   
invertible

C is  $n \times n$   
invertible

so that

$$\vec{y} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \vec{X}$$

↑  
"I"

$$A \in M_{m \times n}$$

$$Y_1 = X_1$$

$$Y_2 = X_2$$

⋮

$$Y_r = X_r$$

$$Y_{r+1} = 0$$

⋮

$$Y_m = 0$$

Ex:  $T: \mathbb{R} \rightarrow \mathbb{R}^2$

$$t \mapsto (2t, 3t)$$

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \cdot (x_1)$$

$$\begin{cases} Y_1 = 2y_1 \\ Y_2 = 3y_1 - 2y_2 \end{cases} \quad \vec{X} = \vec{x}$$

$$\begin{cases} Y_1 = x_1 \\ Y_2 = 0 \end{cases}$$

$$T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$\vec{x} \mapsto \vec{y}$

$$\vec{y} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \vec{x}$$

Graph of functions

$$f_1(x, y) = x^2 + y^2$$



$$f_2(x, y) = x^2 - y^2$$

$$f_3(x, y) = -x^2 - y^2$$



Given a quadratic form

$$Q(\vec{x}) = \vec{x}^t \cdot M \cdot \vec{x}$$

$$\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad M = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

Symmetric  $a_{ij} = a_{ji}$

Up to linear transformation

$$\vec{x} = A \cdot \vec{x} \quad A \in GL(\mathbb{R}^n)$$

$$Q(\vec{x}) = \vec{x}^t \cdot A \cdot \vec{x} = (A \cdot \vec{x})^t \cdot M \cdot (A \cdot \vec{x})$$

$\uparrow$   $n \times n$  invertible matrices  
 $\uparrow$   $n \times n$  matrices

$$\Lambda = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & -1 & \\ & & & \ddots & \\ 0 & & & & 0 \\ & & & & & \ddots & \\ & & & & & & -1 \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{pmatrix} = \vec{x}^t \cdot (A^t \cdot M \cdot A) \cdot \vec{x} = \vec{x}^t \cdot \Lambda \cdot \vec{x}$$

input  $\vec{y} = A \vec{x}$

want to find

$$\begin{aligned} \vec{y} &= B \vec{Y} \\ \vec{x} &= C \vec{X} \\ B \vec{Y} &= A \cdot C \cdot \vec{X} \\ \vec{Y} &= \underbrace{B^{-1} \cdot A \cdot C}_{\Lambda} \cdot \vec{X} \end{aligned}$$

Orthogonal Diagonalization Thm

want to find:  $A \in O(\mathbb{R}^n)$

Orthogonal group

Given  $Q(\vec{x}) = \vec{x}^t \cdot M \cdot \vec{x}$

$$\begin{aligned} &= \{M \in GL(n) \mid M^t = M^{-1}\} \\ &= \{M: \mathbb{R}^n \rightarrow \mathbb{R}^n \mid \langle M u, M v \rangle = \langle u, v \rangle \forall u, v \in \mathbb{R}^n\} \end{aligned}$$

s.t. if we set  $\vec{x} = A \cdot \vec{X}$

then  $\vec{x}^t \cdot M \cdot \vec{x} = \vec{X}^t \cdot \underbrace{(A^t \cdot M \cdot A)}_{\Lambda} \cdot \vec{X}$

$$\Lambda = \begin{pmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ 0 & & \lambda_n \end{pmatrix} \quad \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$$

# Jordan Normal Form

$$T: \mathbb{R}^n \rightarrow \mathbb{R}^n$$

$$\vec{y} = A \cdot \vec{x}$$

Want to find change of basis of  $\mathbb{R}^n$

$$\vec{x} = B \vec{X} \quad B \in GL(n)$$

$\vec{y} = B \vec{X}$  s.t. the equation in  $\vec{X}, \vec{Y}$  simplifies

$$B \cdot \vec{Y} = A \cdot B \cdot \vec{X}$$

$$Y = \underbrace{B^{-1} \cdot A \cdot B}_{\Lambda} \vec{X}$$

$\Lambda$  consists of block diagonal matrices

each block

$$T_1 \left( \begin{array}{ccc|ccc} \lambda_1 & 1 & 0 & & & \\ 0 & \lambda_1 & 0 & & & \\ & & \ddots & & & \\ 0 & & & \lambda_2 & 1 & 0 \\ & & & 0 & \lambda_2 & 0 \\ & & & & & \ddots \\ 0 & & & & & & \lambda_n & 1 & 0 \\ & & & & & & 0 & \lambda_n & 0 \\ & & & & & & & & \ddots \end{array} \right) \text{ is } \left( \begin{array}{cccc|cccc} \lambda_1 & & & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_1 & & 0 & 0 & 0 & 0 & 0 \\ & & & & & & & \\ 0 & & & \lambda_2 & & 0 & 0 & 0 \\ & & & 0 & \lambda_2 & & 0 & 0 \\ & & & & & & & \\ 0 & & & & & & & & \lambda_n & 1 & 0 \\ & & & & & & & & 0 & \lambda_n & 0 \\ & & & & & & & & & & \ddots \end{array} \right) \leftarrow \text{Jordan Block}$$

Notation:  $A = [a_{ij}]$   $i$ : row index  $j$ : column index  
 • transpose  $A$ :  $n \times m$  matrix  $A^T = [a_{ji}]$   
 $(A^T)_{ij} = A_{ji}$

• matrix multiplication:  
 $A: n \times m$   $B: m \times l$   $A \cdot B: n \times l$   
 $(A \cdot B)_{ij} = \sum_{k=1}^m A_{ik} B_{kj}$

Definition of Determinant:

Let  $A$  be a  $n \times n$  matrix  
 •  $\det A$  is a number defined by  $\det(A) = \sum_{\sigma} \epsilon(\sigma) \cdot a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$   
permutation of  $\{1, 2, \dots, n\}$

a permutation of  $\{1, 2, \dots, n\}$   
 is a bijection

$$\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

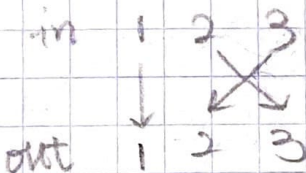
Ex:  $1 \rightarrow 1$  number of permutations of size  $n$  is  $n!$



• length of a permutation:  $L(\sigma) \geq 0$  integer

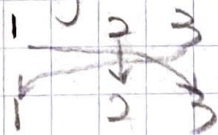
• geometrical definition

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



$L(\sigma) = \#$  of pairs  $(i, j)$  that swap ordering  $i < j$  and  $\sigma(i) > \sigma(j)$   
 = number of crossing

Ex:  $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$



Rank: there is exactly 1 element  $\sigma \in S_n$  that  $L(\sigma) = \frac{n(n-1)}{2}$

$$\epsilon(\sigma) = (-1)^{L(\sigma)} = \begin{cases} +1 & L(\sigma) \text{ even} \\ -1 & L(\sigma) \text{ odd} \end{cases}$$



$n=3$ :

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$   $S_{12}=S_1$ ,  $L(\sigma)=0, E(\sigma)=1$

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ,  $L(\sigma)=1, E(\sigma)=1$

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ,  $L(\sigma)=1, E(\sigma)=-1$

These 2 are the only length 1 permutation

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ,  $L(\sigma)=2$  +

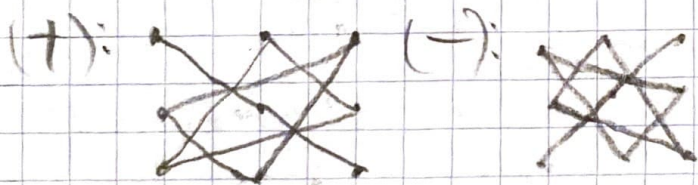
$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ ,  $L(\sigma)=2$  +

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ,  $L(\sigma)=3$  -

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$\det(A) = \sum_{\sigma \in S_3} E(\sigma) \cdot a_{1\sigma(1)} \cdot a_{2\sigma(2)} \cdot a_{3\sigma(3)}$$

$$= a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}$$



$S_n$ : permutation group  $[n] = \{1, 2, \dots, n\}$

given  $\sigma_1: [n] \rightarrow [n]$

$\sigma_2: [n] \rightarrow [n]$

I can compose them

$$\sigma_2 \circ \sigma_1: [n] \rightarrow [n]$$

$$i \mapsto \sigma(\sigma_1(i))$$

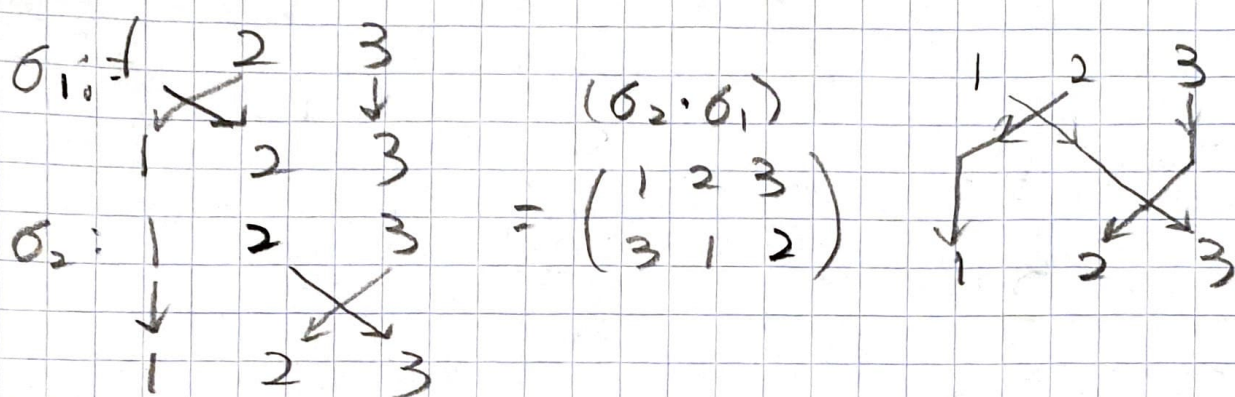
map of sets

$$f: A \rightarrow B$$

$$g: B \rightarrow C$$

$$g \circ f: A \rightarrow C$$

$$a \mapsto g(f(a))$$



Lemma: Let  $\sigma \in S_n$

Let  $S_i$  be a simple transposition

then  $L(\sigma \cdot S_i) = \begin{cases} L(\sigma) + 1 & \text{if } \sigma(i) < \sigma(i+1) \\ L(\sigma) - 1 & \text{if } \sigma(i) > \sigma(i+1) \end{cases}$

Proof: Consider any pair  $(j, k)$  with  $j < k$

• if  $(j, k) \neq (i, i+1)$ , then  $\sigma(j) < \sigma(k) \Leftrightarrow \sigma \cdot S_i(k)$

• if  $(j, k) = (i, i+1)$ , then  $\sigma(i) < \sigma(i+1) \Leftrightarrow \sigma \cdot S_i(i) > \sigma \cdot S_i(i+1)$

$S_i \cdot S_i = \text{id}$ , Prop: if  $\sigma \in S_n$  has length  $L(\sigma)$  then

$S_i$   $\sigma$  can be written as

$\sigma = S_{i_1} \dots S_{i_k}$

where  $i_1, \dots, i_k \in \{1, \dots, n-1\}$

The statement is true for  $L(\sigma) = 0$

Proof: We prove by induction. Suppose the statement

is true for all those  $\sigma$ , with  $L(\sigma) \leq k-1$

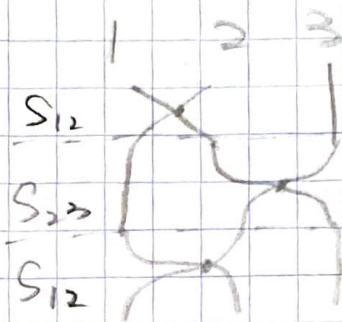
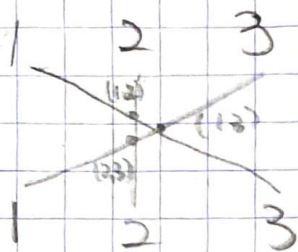
And suppose  $L(\sigma) = k$

• Find a  $S_i$ , such that  $L(\sigma \cdot S_i) = L(\sigma) - 1 = k-1$   
then by induction hypothesis

$(\sigma \cdot S_i) = S_{i_{k-1}} \dots S_i$

$\sigma = (\sigma \cdot S_i) \cdot S_i = S_{i_{k-1}} \dots S_i \cdot S_i$

• if no such  $S_i$  exists, then  $\sigma(i) < \sigma(i+1)$  then  $\sigma = \text{id}$ , which we already cover



$$\sigma = S_{12} S_{23} S_{12}$$

$$= S_{23} S_{12} S_{23}$$

$A$ :  $n \times n$  matrix with  $A_{ij}$  the entry on  $i$ th row  $j$ th col

$$\det A = \sum_{\sigma \in S_n} \epsilon(\sigma) \cdot A_{1\sigma(1)} \cdot A_{2\sigma(2)} \cdots A_{n\sigma(n)}$$

Where  $S_n$  is the group of permutation of  $n$  elements

$$\epsilon(\sigma) = (-1)^{l(\sigma)}$$

$l(\sigma)$  = minimum number of elementary swapping to obtain  $\sigma$

Ex:  $n=3$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Alternative definition

$$\begin{pmatrix} \odot & \cdot & \cdot \\ \cdot & \odot & \cdot \\ \cdot & \cdot & \odot \end{pmatrix} \quad \begin{pmatrix} \cdot & \odot & \cdot \\ \odot & \cdot & \cdot \\ \cdot & \cdot & \odot \end{pmatrix} \quad \begin{pmatrix} \cdot & \odot & \cdot \\ \cdot & \cdot & \odot \\ \odot & \cdot & \cdot \end{pmatrix}$$

$$(123) \quad +1 \quad (213) \quad -1 \quad (231) \quad +1$$

each row appears once, each column appears once

Expansion by column:

$$\text{Claim: } \det(A) = \sum_{\sigma} \epsilon(\sigma) A_{\sigma(1)1} A_{\sigma(2)2} \cdots A_{\sigma(n)n}$$

$$\text{Pf: } \text{By def. } \det(A) = \sum_{\sigma} \epsilon(\sigma) A_{\sigma^{-1}(1)1} A_{\sigma^{-1}(2)2} \cdots A_{\sigma^{-1}(n)n}$$

Rename  $\sigma^{-1}$  to  $\sigma$

$$= \sum \epsilon(\sigma^{-1}) A_{\sigma(1)1} A_{\sigma(2)2} \cdots A_{\sigma(n)n}$$

$$= \sum \epsilon(\sigma) A_{\sigma(1)1} A_{\sigma(2)2} \cdots A_{\sigma(n)n}$$

Properties of det:

①  $\det(A^T) = \det(A)$

② Interchange any 2 columns would change the sign

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} = [\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n]$$

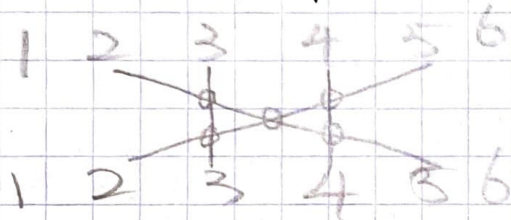
$$\det([\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n])$$

swapped  $\vec{a}_i$  and  $\vec{a}_j$

$$= (-1) \det([\vec{a}_1, \dots, \vec{a}_{i-1}, \vec{a}_j, \vec{a}_i, \dots, \vec{a}_{j+1}, \vec{a}_i, \vec{a}_{j+1}, \dots, \vec{a}_n])$$

Lemma: if  $\sigma$  is a transposition  $(ij)$ , then  $\epsilon(\sigma) = -1$

pf:



$\sigma = (ij)$

$l(\sigma)$  is odd

$$\epsilon(\sigma) = (-1)^{\text{odd}} = -1$$

③  $\det(\vec{a}_1, \vec{a}_2, \dots, \lambda \vec{a}_i, \vec{a}_{i+1}, \dots, \vec{a}_n)$

$$= \lambda \cdot \det(\vec{a}_1, \vec{a}_2, \dots, \vec{a}_{i-1}, \vec{a}_i, \vec{a}_{i+1}, \dots, \vec{a}_n)$$

for any  $\lambda \in \mathbb{R}$

④  $\det(\vec{a}_1, \vec{a}_2 + \vec{a}'_2, \vec{a}_3)$

$$= \det(\vec{a}_1, \vec{a}_2, \vec{a}_3) + \det(\vec{a}_1, \vec{a}'_2, \vec{a}_3)$$

③④  $\Leftrightarrow \det(\_, \_, \_, \_, \_, \_) is a multilinear function  $\underbrace{\mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R}}_{n \text{ factors}} = \mathbb{R}$$

⑤  $\det I = 1$

⑥  $\det(\vec{a}_1, \dots, \vec{a}_n) = 0$  if one of the  $\vec{a}_i = 0$

⑦  $\det(\vec{a}_1, \vec{a}'_2, \dots, \vec{a}_n) = 0$ , if there are  $i, j$ , such that  $\vec{a}_i = \vec{a}_j$

$$\det(A) = \sum (-1)^{\epsilon(\sigma)} \underbrace{a_{\sigma(1)1} \cdots a_{\sigma(n)n}}_{= S(\sigma)}$$

if  $a_i = a_j$ , then

$$S(\sigma) = S(\sigma(ij))$$

$$\text{but } (-1)^\sigma = -(-1)^{\sigma(ij)}$$

⑧ Fix  $i, j, \lambda \in \mathbb{R}$

$$\det(\vec{a}_1, \vec{a}_2, \dots, \vec{a}_n)$$

$$= \det(\vec{a}_1, \vec{a}_2, \dots, \vec{a}_i + \lambda \vec{a}_j, \dots, \vec{a}_n)$$

$$\text{RHS} = \det(a_1, \dots, a_n) + \lambda \det(a_1, \dots, a_j, \dots, a_j, \dots, a_n)$$

$$= \det(a_1, \dots, a_n) + 0$$

$$\textcircled{9} \det \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix} = \lambda_1 \lambda_2 \cdots \lambda_n$$

$$\text{LHS} = \lambda_1 \cdots \lambda_n \det \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = \lambda_1 \cdots \lambda_n$$

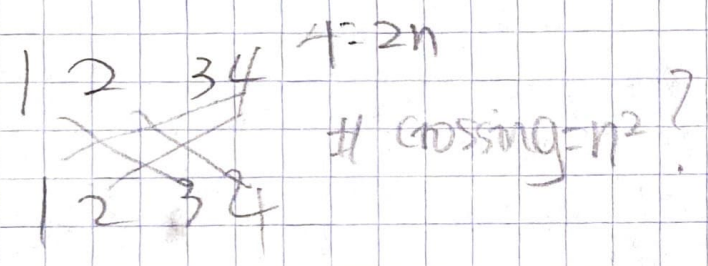
$$M = \begin{bmatrix} \overbrace{A}^{n_1} & B \\ \underbrace{C}_{n_2} & D \end{bmatrix}$$

• if  $C = 0$ , then  $\det M = (\det A) \cdot (\det D)$

Prop: if  $A, B$  are  $n \times n$  matrices  
then  $\det(A \cdot B) = (\det A) \cdot (\det B)$

$$\text{Pf: } \det(A) \cdot \det(B) = \det \left( \begin{array}{c|c} A & 0 \\ \hline -I & B \end{array} \right) \Bigg\}_{2n}$$

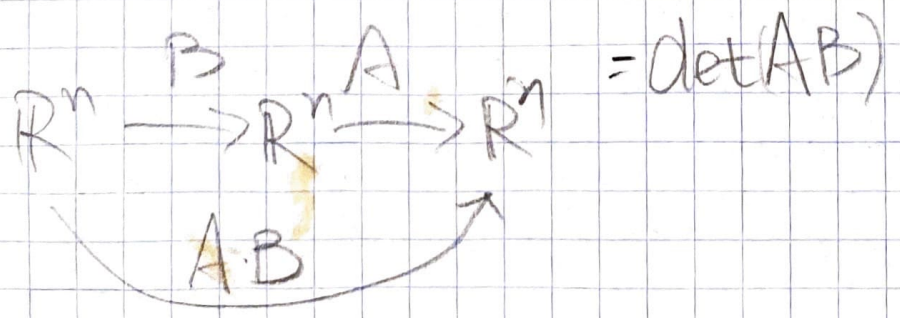
$$\begin{pmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ \hline -1 & 0 & b_{11} & b_{12} \\ 0 & -1 & b_{21} & b_{22} \end{pmatrix} \rightarrow \begin{pmatrix} a_{11} & a_{12} & b_{11} \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} + b_{21} \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} & 0 \\ a_{21} & a_{22} & b_{11} \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix} + b_{21} \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix} & 0 \\ \hline -1 & 0 & 0 & b_{12} \\ 0 & -1 & 0 & b_{22} \end{pmatrix}$$



$$= (-1)^{n^2} \left( \begin{array}{c|c} AB & A \\ \hline 0 & -I \end{array} \right)$$

$$\begin{pmatrix} A & A \cdot B \\ \hline -I & 0 \ 0 \\ & 0 \ 0 \end{pmatrix}$$

$$= (-1)^n \det(AB) \det(-I_n) = (-1)^n (-1)^n \det(AB) \det(I)$$



$$= \det(AB)$$

# Cofactor

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \det(A) = ad - bc$$

if  $\det A \neq 0$

$$\text{then } A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$A^{-1} \cdot A = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{\det A} \begin{pmatrix} ad - bc & 0 \\ 0 & -bc + ad \end{pmatrix}$$

$$A^{-1} \cdot A = \frac{1}{\det A} \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$C_{ij} = (-1)^{i+j} \det(A \text{ remove } i\text{th row } j\text{th column})$$

# Cofactor Thm:

A:  $n \times n$  matrix

$$A = \begin{bmatrix} A_{11} & \dots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \dots & A_{nn} \end{bmatrix}$$

Given  $1 \leq i \leq j \leq n$ , we form a new (sub) matrix by deleting the  $i$ th row and  $j$ th column matrix.

let  $C_{ij} = (-1)^{i+j} \cdot \det(\text{this } (n-1) \times (n-1) \text{ matrix})$   
 $\uparrow$  cofactor

Thm:  $\det(A) \stackrel{!}{=} A_{11}C_{11} + A_{12}C_{12} + \dots + A_{1n}C_{1n}$  (first row)  
 $= A_{11}C_{11} + A_{21}C_{21} + \dots + A_{n1}C_{n1}$  (first column)

• In general, for  $1 \leq i, j \leq n$ , we have  $\sum_{j=1}^n A_{ij}C_{ij} = \begin{cases} \det(A) & i_1 = i_2 \\ 0 & i_1 \neq i_2 \end{cases}$

Similarly  $\sum_{j=1}^n A_{ji}C_{ji} = (\delta_{i_1 i_2}) \det(A) = \det(A) \cdot \delta_{i_1 i_2}$

$\det(A) = \sum_{\sigma \in S_n} \epsilon(\sigma) \cdot A_{1\sigma(1)} A_{2\sigma(2)} \dots A_{n\sigma(n)}$   
 $= A_{11} \cdot \det(\text{matrix A delete 1st row 1st col}) - A_{12} \cdot \det(\text{A remaining 1st row 2nd col}) + A_{13} \det(\text{A - 1st row - 3rd col}) + \dots$   
 All the terms with  $\sigma(1)=1$       All the terms with  $\sigma(1) \neq 1$

$= A_{11}C_{11} + A_{12}C_{12} + A_{13}C_{13} + \dots + A_{1n}C_{1n}$

If  $i_1 = i_2 = i \neq 1$ ,  $A_{i1}C_{i1} + A_{i2}C_{i2} + \dots + A_{in}C_{in} = \det A$   
 build a new matrix,  $\tilde{A}$  that moves the  $i$ -th row to the top

$\det(\tilde{A}) = (-1)^{i-1} \det(A)$   
 $(\tilde{A})_{ij} = A_{ij}$   
 $C_{ij} = (-1)^{i+j} \det(\text{A delete } i\text{-th row } j\text{-th col})$   
 $= (-1)^{i+j} (-1)^{i+j} (-1)^{i+j} \det(\dots) = (-1)^{i+j} C_{ij}$



$$\det \tilde{A} = \sum_j \tilde{A}_{ij} \tilde{C}_{ij}$$

$$\rightarrow (-1)^{i+j} \det(A) = \sum_j A_{ij} C_{ij} (-1)^{i+j}$$

$$\det(A) = \sum_j A_{ij} C_{ij}$$

If  $i_1 \neq i_2$ , say  $i_1=1, i_2=2$ , we want to show

$$\sum_{j=1}^n A_{1j} C_{2j} = 0$$

$$\tilde{A} = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{i1} & A_{i2} & \dots & A_{in} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{bmatrix} \begin{array}{l} \tilde{A} \text{ copies the} \\ i\text{-th row of } A \\ \text{for } i \geq 2, \tilde{A}_{ij} = A_{ij} \end{array}$$

$$0 = \det \tilde{A} = \tilde{A}_{21} \tilde{C}_{21} + \tilde{A}_{22} \tilde{C}_{22} + \dots + \tilde{A}_{2n} \tilde{C}_{2n}$$

$$= A_{11} C_{21} + A_{12} C_{22} + \dots + A_{1n} C_{2n}$$

Corollary: if  $A$  is an  $n \times n$  matrix with  $\det A \neq 0$ , then

$$A^{-1} = \frac{1}{\det A} \cdot C^t \quad (C \text{ is the matrix of all cofactors } C_{ij})$$

$$\text{Pf: } \left[ \left( \frac{1}{\det A} C^t \right) \cdot A \right]_{ij}$$

$$= \frac{1}{\det A} \sum_{k=1}^n (C^t)_{ik} A_{kj} = \frac{1}{\det A} \sum_{k=1}^n C_{ki} A_{kj} = \frac{1}{\det A} \cdot \det A \cdot \delta_{ij} = \delta_{ij}$$

$$\left[ A \cdot \left[ \frac{1}{\det A} C^t \right] \right]_{ij} = \delta_{ij} \text{ by similar argument } \begin{array}{l} i=j \text{ only when} \\ \text{the array is on} \\ \text{the diagonal} \end{array}$$

Cramer's Rule:

Let  $\vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$  be a column of unknown variables,

let  $\vec{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$  be a given vector

Let  $A$  be a  $n \times n$  matrix (invertible)  
consider equation  $A\vec{x} = \vec{a}$   
then  $\vec{x} = A^{-1} \cdot \vec{a}$

thus

$$x_1 = \frac{\det \begin{pmatrix} a_1 & A_{12} & \dots & A_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_n & A_{n2} & \dots & A_{nn} \end{pmatrix}}{\det A} = \frac{\det(\vec{a}, A_{\cdot 2}, A_{\cdot 3}, \dots, A_{\cdot n})}{\det A}$$

$$\vdots$$

$$x_i = \frac{\det(A_{\cdot 1}, \dots, \overset{\text{ith slot}}{\vec{a}}, \dots, A_{\cdot n})}{\det A}$$

$$\vdots$$

$$x_i = (A^{-1} \cdot \vec{a})_i$$

$$\vec{a} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

$$= \sum_{k=1}^n (A^{-1})_{ik} a_k$$

$$= \sum_{k=1}^n \left( \frac{1}{\det A} C^t \right)_{ik} a_k \quad (a_k \rightarrow A_{ki})$$

$$= \frac{1}{\det A} \left[ \sum_{k=1}^n C_{ki} a_k \right] = \frac{1}{\det A} \det \left( A, \text{replacing the } i\text{th column by } a \right)$$

$$A = \begin{matrix} & \begin{matrix} n_1 & n_2 \end{matrix} \\ \begin{matrix} n_1 \\ n_2 \end{matrix} & \left[ \begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right] \end{matrix}$$

$$B = \begin{matrix} & \begin{matrix} n_1 & n_2 \end{matrix} \\ \begin{matrix} n_1 \\ n_2 \end{matrix} & \left[ \begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array} \right] \end{matrix}$$

One can treat the blocks as if they're numbers

$$AB = \left[ \begin{array}{c|c} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ \hline A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{array} \right]$$

$$M = \begin{matrix} & \begin{matrix} n_1 & n_2 \end{matrix} \\ \begin{matrix} n_1 \\ n_2 \end{matrix} & \left[ \begin{array}{c|c} A & B \\ \hline C & D \end{array} \right] \end{matrix}$$

$$\det(M) = \det(D) \cdot \det(A - B D^{-1} C)$$

$$[M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}] \det M = ad - bc = d \left( a - \frac{bc}{d} \right)$$

↑  
needs  $d \neq 0$

$$\begin{aligned}
 \det \begin{pmatrix} A & B \\ C & D \end{pmatrix} &= \det \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \det \left( \begin{array}{c|c} I & 0 \\ \hline D^{-1}C & I \end{array} \right) \\
 &= \det \left[ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & 0 \\ -D^{-1}C & I \end{pmatrix} \right] \\
 &= \det \begin{bmatrix} A - BD^{-1}C & B \\ C - D^{-1}DC & D \end{bmatrix} \\
 &= \det \begin{pmatrix} A - BD^{-1}C & B \\ 0 & D \end{pmatrix} = \det(A - BD^{-1}C) \det(D)
 \end{aligned}$$

Gauss Elimination:

- row operations:
  - swap two rows, put (-) in front
  - multiple one row, add the result to another row  
 $\lambda \cdot r_i + r_j \xrightarrow{\text{put in}} r_j$
- similarly for column operation

Goal: make the matrix upper triangular

Recall: ① "Algebra-like object" Field  $K$

② "Modulo-like obj" Vector space

• What is a field?

a field is a set  $K$  with  $+$ ,  $\cdot$ ,  $0$ ,  $1$ ,  $i$  such that:

•  $(K, +, 0)$  every element in  $K$  has an inverse  
 $\forall x, \exists x' \in K, \text{ s.t. } x+x'=0$

•  $(K^* = K \setminus \{0\}, \cdot, 1)$ ,  $\forall y \in K^*, \exists y' \in K^* y \cdot y' = 1$

Ex:  $\cdot \mathbb{R}$   $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$   $\cdot \mathbb{C}$   $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$   $\cdot \mathbb{P}$  prime number

$\cdot \mathbb{Q}$   $\mathbb{F}_p = \mathbb{Z}/p \cdot \mathbb{Z} = \{0, 1, \dots, p-1\}$

Ex:  $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

Q: Does every element in  $\mathbb{F}_5$  have an "inverse"  $\cdot$ ?

$2 \cdot 3 = 0$   $1+4=0$

Q:  $1 \cdot 1 = 1$   $2 \cdot 3 = 1$   $3 \cdot 2 = 1$   $4 \cdot 4 = 1$

Q: Does  $\mathbb{Z}/6 \cdot \mathbb{Z}$  form a field under the natural  $(+, \cdot)$ ?

No.  $2 \cdot 3 = 0$

$n \geq 1$  integer  $\exists!$   $\mathbb{F}_{p^n}$  finite field with  $p^n$  many elements  
*exists unique*

Let  $p(x) \in \mathbb{F}_p[x]$

with variable  $x$  with coefficient in  $\mathbb{F}_p$

Ex:  $p=5$   $3x^2+4x-2 \in \mathbb{F}_5[x]$

Assume  $f(x)$  is irreducible in  $\mathbb{F}_p[x]$  i.e.  $f(x) \neq g(x)h(x)$

with  $h$  &  $g$  of smaller degree

Ex:  $p=5$   $f(x) = x^2+1 = (x-2)(x-3)$

$f(x) = x^2+2$

$= x^2 - 5x + 6$

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

$= x^2 + 1$

then  $\mathbb{F}_p[x]/(f(x)) \cdot \mathbb{F}_p[x]$

is a field of size  $p^{n/\text{degree}(f)}$

$\mathbb{F}_5 = \mathbb{F}_5[x]/(x^2+2)$  typical element:  $x, 3, x^3+1$

$x^2+2=0$   
 $5=0$

$x^2+3 = (x^2+2)+1=1$

$x^2 = -2, x^3 = -2x$

$$F_5[x]/(x^2+2) = \{ax+bx \mid a, b \in F_5\} \cong (F_5)^2$$

as vector space

Does every non-zero element in  $K$  has inverse  $\mathbb{C} \cong \mathbb{R}^2$

$$Q_{[x^2+1]} := Q[x]/(x^2+1) \cong Q^2$$

$$= \{ax+bx \mid a, b \in Q\}$$

$$(ax+bx)(cx+dx) = (ac+bd)(x+ad) \quad (acx^2 = ac(x^2+1-1))$$

Let  $K$  be a field

A vector space  $V$  over  $K$  is a set such that:

- ①  $(V, +, 0)$  is an abelian group
- ②  $K \curvearrowright V$  (scalar product)

a function on a set  $S$ , valued in  $K$  is an assignment to each element in  $S$ , some element in  $K$

$$\text{Map}(S, K) = K^S$$

The set of all functions from  $S$  to  $K$  is

Ex: if  $S = \{*\}$  <sup>point</sup> if  $S = \{a, b\}$

$$K^S = K \quad K^S = K^2$$

$$S = \emptyset \quad K^\emptyset = K^0 = \{*\}$$

$$f, g \in \text{Map}(\{1, 2\}, K)$$

$$f, g: \{1, 2\} \rightarrow \mathbb{R}$$

↑  
vector space

$$(f+g)(x) = f(x) + g(x)$$

$$\forall c \in K, (c \cdot f)(x) = c \cdot f(x)$$

•  $S = \{1, 2, \dots, n\}$   $K^S = K^n$  |  $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}$  field

•  $S = [n] \times [m]$

$= \{(i, j) \mid \begin{matrix} 1 \leq j \leq n \\ 1 \leq i \leq m \end{matrix}, \text{integer}\}$

$K^S = \left\{ \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & & a_{mm} \end{bmatrix} \mid a_{ij} \in K \right\}$  vector space

• Let  $V$  be a vector space over  $K$

A subspace  $W \subset V$  is a subset that is closed under  $+$  and  $K$

Ex:  $K \in \mathbb{R}$

•  $V = \mathbb{R}^{\mathbb{R}} = \text{Map}(\mathbb{R}, \mathbb{R})$  all functions on  $\mathbb{R}$   
 $W = \mathbb{R}[x] = \{a_n x^n + \dots + a_0 \mid \begin{matrix} a_i \in \mathbb{R} \\ n \in \mathbb{Z}_{\geq 0} \end{matrix}\}$

### Category Theory

- a set of objects
- morphisms between objects
- composition of morphisms

Ex 1: set: the category of sets

• objects: any set

• morphisms: Given  $S_1, S_2$  two sets,  $\text{mor}(S_1, S_2)$

• compositions:  $\text{mor}(S_1, S_2) \times \text{mor}(S_2, S_3) = \text{Map}(S_1, S_3)$

$\downarrow$   
 $f_{12}$

$\downarrow$   
 $f_{23}$

$\rightarrow \text{Mor}(S_1, S_3)$

$f_{23} \circ f_{12} = f_{23}(f_{12}(x))$

$\text{Vect}_K$ : the category of vector spaces/ $K$

- an object is a vector space over  $K$

- a morphism between  $V_1, V_2$  is a linear map

$$\text{Mor}(V_1, V_2) = \text{LinMap}(V_1, V_2) \quad ?$$

Note: the set  $\text{LinMap}(V_1, V_2)$  also forms a vector space

- Let  $f: V \rightarrow W$  be a linear map

? •  $\ker(f) = \{v \in V \mid f(v) = 0\} \subset V$

- $\text{im}(f) = \{w \in W \mid \exists v \in V, w = f(v)\} \subset W$

- $\text{coker}(f) = \frac{W}{\text{im}(f)}$

Recall: A vector space  $V$  over a field  $K$  is a Set  $V$  such that

$$\bullet \quad +: V \times V \rightarrow V$$

$$\bullet \quad \bullet \quad \cdot: K \times V \rightarrow V$$

are well-defined and compatible

Given 2 vector spaces,  $V, W$

$\text{Lin Map}(V, W)$  is the set of linear maps

We also write it as  $\text{Hom}(V, W)$

homomorphism

$\text{Hom}(V, W)$  also forms a vector space over  $K$

• Direct Sum:

$$V \oplus W = \{(v, w) \mid v \in V, w \in W\} = V \times W$$

$$(v_1, w_1), (v_2, w_2) \in V \oplus W \quad \cdot \quad c \in K$$

$$(v_1, w_1) + (v_2, w_2)$$

$$c(v, w) = (cv, cw)$$

$$= (v_1 + v_2, w_1 + w_2)$$

$$\text{Ex: } \mathbb{R} \oplus \mathbb{R} = \mathbb{R}^2$$

• Quotient space:

Let  $V$  be a vector space

and  $W \subset V$  a subspace

then  $V/W$  is the vector space consisting of equivalence class in  $V$ ,

where we say  $v_1, v_2 \in V$  are equivalent

if  $v_1 - v_2 \in W$

$$V/W = v + W, \quad v \in V$$



Ex:  $V = \mathbb{R}^2$

$W = \{(0, y) \mid y \in \mathbb{R}\}$

$v_1 = (-1, 1) \quad v_2 = (-1, -1) \quad v_1 - v_2 = (0, 2) \in W$

we say  $v_1 \sim v_2$  ?

the line  $v_1 + W = \{v_1 + w \mid w \in W\}$  is the equivalence class that  $v_1$  belongs to

Let  $v_1 + W, v_2 + W \in V/W$   
 then  $(v_1 + W) + (v_2 + W)$   
 $= (v_1 + v_2) + W$

This is well defined cuz  
 if  $\tilde{v}_1 + W = v_1 + W$  i.e.  $\tilde{v}_1 \in v_1 + W$   
 ?  $\tilde{v}_2 + W = v_2 + W$   $\tilde{v}_2 \in v_2 + W$   
 addition of two elements from equivalence class

then  $\tilde{v}_1 + \tilde{v}_2 \in v_1 + v_2 + W$

if  $v_1 - \tilde{v}_1 \in W, v_2 - \tilde{v}_2 \in W$  then

$(v_1 + v_2) - (\tilde{v}_1 + \tilde{v}_2) \in W$

$\pi_W: V \rightarrow V/W$   
 $v \mapsto v + W$  ?

If  $V$  is a  $\mathbb{R}$  vector space and has inner product  $\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{R}$

then given  $W \subset V$ , we can form  $W^\perp \subset V$

recall that, given  $\langle \cdot, \cdot \rangle \quad v_1 \perp v_2 \iff \langle v_1, v_2 \rangle = 0$

$v_1 \perp W \iff \forall w \in W, \langle v_1, w \rangle = 0$

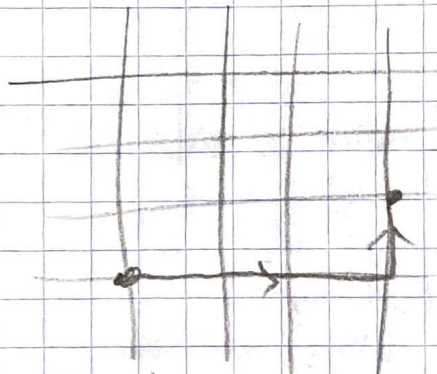
$W^\perp = \{v \in V \mid v \perp W\} \subset V$

\* definitions

$\pi_U : V \rightarrow V/W$  quotient map  
 $\pi_U$  restricted to  $W^\perp$  gives a bijection

$$\pi_U|_{W^\perp} : W^\perp \rightarrow V/W$$

Aside on distance:



$$l_1: d((x_1, x_2, \dots, x_n), (y_1, \dots, y_n))$$

$$l_2: \left[ \sum_{i=1}^n |x_i - y_i|^2 \right]^{1/2}$$

Dual space:

$$\dim V/W = \dim V - \dim W$$

$V$  vector space over  $K$

$$V^* = \text{Hom}(V, K)$$

= the set of linear functions on  $V$

Ex:  $V = \mathbb{R}^2$   $x_1, x_2$

$$V^* = \{ ax_1 + bx_2 \mid a, b \in \mathbb{R} \}$$

# Ch 3. 1. Basis,

span, linear independence

Def: a collection (possibly infinite) of vectors  $v_1, v_2, \dots$  is called a basis if any  $v \in V$  can be written uniquely as finite linear combination of  $\{v_i\}$

Ex:  $\mathbb{K}[x]$  vector space of 1-variable polynomials  
 $\{1, x, x^2, \dots\}$  forms a basis

Span: let  $v_1, v_2, \dots, v_n$  be vectors in  $V$ , then we have a map

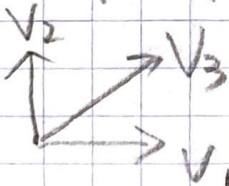
$$f: \mathbb{K}^n \rightarrow V$$

$$(a_1, \dots, a_n) \mapsto a_1 v_1 + a_2 v_2 + \dots + a_n v_n$$

$$\text{Span}\{v_1, \dots, v_n\} = \text{image of } f = \{a_1 v_1 + \dots + a_n v_n \mid a_i \in \mathbb{K}\}$$

We say  $\{v_1, \dots, v_n\}$  span  $V$

$$\text{if } \text{span}\{v_1, \dots, v_n\} = V$$

Ex:   $V = \mathbb{R}^2$   
 $\text{span}(v_1, v_2, v_3) = V$  ?  $(v_1, v_2)$

We say  $\{v_1, \dots, v_n\}$  is linearly independent, if the

map  $f: \mathbb{K}^n \rightarrow V$  is injective ?

if  $(a_1, a_2, \dots, a_n) \neq (0, 0, \dots, 0)$ , then  $a_1 v_1 + \dots + a_n v_n \neq 0$

$$V = \mathbb{R}^3$$

$$\text{span}(v_1, v_2, v_3) = XZ \text{ plane}$$

$$= \{(a, 0, b) \mid a, b \in \mathbb{R}\}$$

$$\begin{array}{l} \xrightarrow{v_1 = (1, 0, 0)} v_2 = (2, 0, 0) \\ \downarrow v_3 = (0, 0, 1) \end{array}$$

$\{v_1, v_2\}$  is not linearly independent

?

because  $2 \cdot v_1 + (-1) \cdot v_2 = 0$

$\{v_1, v_3\}$  is lin indep

$\dim_{\mathbb{R}} V = \#$  of elements in a basis

any collection of linearly indep vectors in  $V$

$$\{v_1, \dots, v_m\}$$

can be completed to a basis

Ex: Let  $v_1 = (1, 1, 0)$   $v_3 = (0, 1, 1)$

$v_2 = (1, 0, 1)$  in  $\mathbb{R}^3$

Q: are they linearly independent

$$\begin{pmatrix} v_1 & v_2 & v_3 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\det A = \begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix}$$

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

$$= -1 - 1 = -2 \neq 0$$

is  $A$  invertible  $\Leftrightarrow \det A \neq 0$

$$A \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0$$

$$A^{-1} A \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = A^{-1} (0)$$

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = 0$$

basis lin indep  $V$   
span  $V$

Let  $V_4 = (1, 1, 1)$

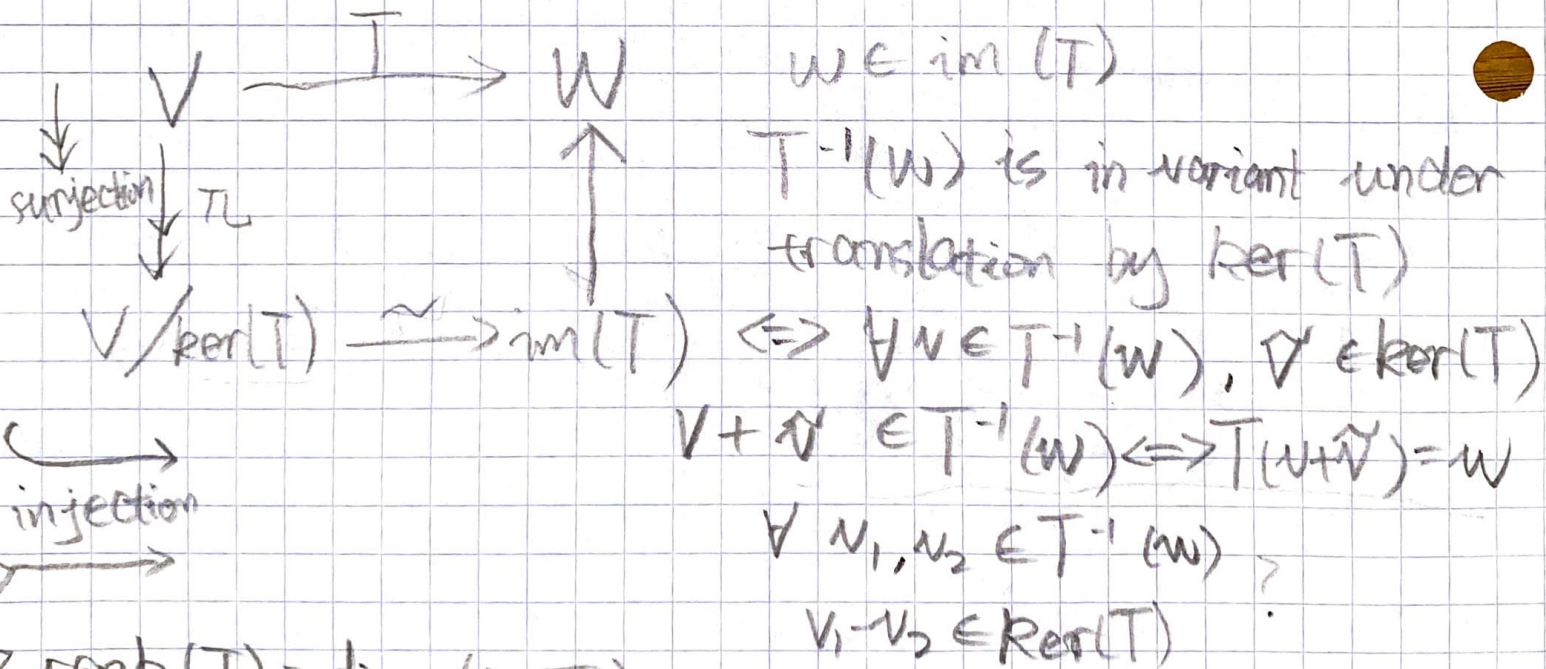
Q: are  $\{v_1, v_2, v_3, v_4\}$  linearly indep

A: No  $\{v_1, v_2, v_3\}$  forms a basis

$\therefore V_4 = a_1 v_1 + a_2 v_2 + a_3 v_3$

$T: V \rightarrow W$   $V, W$  fin. dim.

$\text{rank}(T) = \dim(\text{im } T)$   $\text{im } T = T(V)$   
 $\Rightarrow \text{rank}(T) \leq \dim W$   $\text{rank}(T) \leq \dim V$



?  $\text{rank}(T) = \dim(\text{im } T) = \dim(V/\ker T)$

Let  $T$  be a rank  $r$  map  
from  $V$  to  $W$ , then there exists bases

$v_1, \dots, v_n$  of  $V$   $w_1, \dots, w_m$  of  $W$   
s.t. w.r.t. basis  $T$  is

$$\left[ \begin{array}{c|c} \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} & 0 \\ \hline 0 & 0 \end{array} \right]$$

$$T(v_1) = w_1$$

$$T(v_i) = w_i$$

$$T(v_{r+1}) = 0$$

$$T(v_n) = 0$$