Algebra, Geometry, Topology and Algorithm

Thesis submitted to
unknown University

in partial fulfilment my dream

Doctor of Philosophy
in some crazy subject

By
XXX Department of Subject

Address line – 2
Address line – 4

April 2016

1 Introduction

The Latex doc will have many random stuff on it, there is no particular content or theme on the document. I will write whatever I would like to write based on my mood. The main objective of the document is to help me to learn some Latex. Latex is a program language used for typesetting technical documents. Latex is free program package created in 1985 by the American computer scientist Leslis Lamport as an addition to the Tex typesetting system. Latex is created to make it easier to product general-purpose books and articles within Tex

2 Power series

Proof. **The power series** $exp(A) = \sum_{k=0}^{n} \frac{A^k}{k!}$ **is convegent when A is nxn matrix**

$$\exp(X) = \sum_{k=0}^{n} \frac{X^k}{k!}$$

$$\sin(X) = \sum_{k=0}^{n} (-1)^k \frac{X^{2k}}{2k!}$$

$$\cos(X) = \sum_{k=0}^{n} (-1)^k \frac{X^{2k+1}}{(2k+1)!}$$

$$\cosh(X) = \sum_{k=0}^{n} \frac{X^{2k}}{(2k)!}$$

$$\sinh(X) = \sum_{k=0}^{n} \frac{X^{2k+1}}{(2k+1)!}$$

$$\text{Let } X = \begin{bmatrix} 0 & -\beta \\ \beta & 0 \end{bmatrix}$$

$$\exp(X) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & -\beta \\ \beta & 0 \end{bmatrix} + \frac{1}{2!} \begin{bmatrix} -\beta^2 & 0 \\ 0 & \beta^2 \end{bmatrix}$$

$$+ \frac{1}{3!} \begin{bmatrix} 0 & \beta^3 \\ -\beta^3 & 0 \end{bmatrix} + \frac{1}{4!} \begin{bmatrix} \beta^4 & 0 \\ 0 & \beta^4 \end{bmatrix} + \frac{1}{5!} \begin{bmatrix} 0 & -\beta^5 \\ \beta^5 & 0 \end{bmatrix}$$

$$\exp(X) = \begin{bmatrix} 1 + \frac{1}{2!}(-\beta^2) + \frac{1}{4!}\beta^4 + ... & -\beta + \frac{1}{3!}\beta^3 + ... \\ \beta + \frac{1}{3!} - \beta^3 + ... & 1 + \frac{1}{2!}\beta^2 + \frac{1}{4!}\beta^4 + ... \end{bmatrix}$$

$$\exp(X) = \begin{bmatrix} \sin(\beta) & -\cos(\beta) \\ \cos(\beta) & \sin(\beta) \end{bmatrix}$$

$\square$

3 Given real a symmetric matrix A, prove that all the eigenvalues of A are real numbers

Definition 1. *Given an real $n \times n$ matrix A, $\lambda \in \mathbb{K} \quad \vec{v} \in \mathbb{R}^n$ if*

$$\mathbf{A}\vec{v} = \lambda\vec{v}$$

then λ is the eigenvalue and $\vec{v}$ is the eigenvector such as $\vec{v} \neq \vec{0}$

Example 1. ***Find the eigenvalue and eigenvector of the following matrix***

$$\mathbf{A}_{2\times 2}(\mathbb{R}) = \begin{bmatrix} 1 & 2 \\ 5 & 4 \end{bmatrix}$$

From the definition, we have $\lambda \in \mathbb{C}$ and $\vec{v} \in \mathbb{R}^n$

$$\begin{aligned}
\det \mathbf{A} - \lambda\vec{I} &= 0 \\
\det\left(\begin{bmatrix} 1 & 2 \\ 5 & 4 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) &= 0 \\
\det\left(\begin{bmatrix} 1-\lambda & 2 \\ 5 & 4-\lambda \end{bmatrix}\right) &= 0 \\
(1-\lambda)(4-\lambda) - 2\times 5 &= 0 \\
\lambda^2 - 5\lambda + 4 - 10 &= 0 \\
\lambda^2 - 5\lambda - 6 &= 0 \\
(\lambda - 6)(\lambda + 1) &= 0 \\
\Rightarrow \lambda = 6 \text{ or } \lambda &= -1
\end{aligned}$$

Let $\lambda = 6$ and $\vec{v} = \begin{bmatrix} x \\ y \end{bmatrix}$ we have following

$$\begin{aligned}
\begin{bmatrix} 1 & 2 \\ 5 & 4 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} &= 6\begin{bmatrix} x \\ y \end{bmatrix} \\
\begin{bmatrix} x + 2y - 6x \\ 5x + 4y - 6y \end{bmatrix} &= \vec{0} \\
\begin{bmatrix} -5x + 2y \\ 5x - 2y \end{bmatrix} &= \vec{0} \\
\begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 5 \\ 2 \end{bmatrix} \\
E_{\lambda=6} &= \text{Span}\left\{\begin{bmatrix} 5 \\ 2 \end{bmatrix}\right\}
\end{aligned}$$

Let $\lambda = -1$ we have following

$$\begin{bmatrix}1 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} = -1\begin{bmatrix}x\\y\end{bmatrix}$$
$$\begin{bmatrix}x+2y+x\\5x+4y+y\end{bmatrix} = \vec{0}$$
$$\begin{bmatrix}2x+2y\\5x+5y\end{bmatrix} = \vec{0}$$
$$\begin{bmatrix}x\\y\end{bmatrix} = \begin{bmatrix}1\\-1\end{bmatrix}$$
$$E_{\lambda=-1} = \text{Span}\left\{\begin{bmatrix}1\\-1\end{bmatrix}\right\}$$

Proof. Let A is real and symmetric matrix, prove all the eigenvalues of A are real, We have following

$$A = A^T$$

Let $\lambda \in \mathbb{C}$ to be eigenvalue, $\vec{v} \in \mathbb{R}^n$ to be the eigenvector of A such as $\vec{v} \neq \vec{0}$. From the definition, we have following

$$A\vec{v} = \lambda\vec{v}$$
$$(A\vec{v})^* = (\lambda\vec{v})^*$$
$$(\vec{v})^* A^* = (\vec{v})^*\lambda^*$$

Since A is real and $\vec{v} \in \mathbb{R}^n$

$$(\vec{v})^T A = (\vec{v})^T\lambda^* \qquad \because (\vec{v})^* = (\vec{v})^T \text{ and } A = A^*$$

Multiply both side by $\vec{v}$

$$(\vec{v})^T A\vec{v} = (\vec{v})^T\lambda^*\vec{v}$$
$$\vec{v}\,, A\vec{v} = \langle\vec{v}\,, \lambda^*\vec{v}\rangle$$
$$\langle\vec{v}\,, \lambda\vec{v}\rangle = \langle\vec{v}\,, \lambda^*\vec{v}\rangle \quad \because A\vec{v} = \lambda\vec{v}$$
$$\overline{\lambda}\,\langle\vec{u}\,, \vec{u}\rangle = \lambda\,\langle\vec{u}\,, \vec{u}\rangle \quad \because \lambda^* = \overline{\lambda} \text{ and } \langle\vec{v}\,, a\vec{u}\rangle = \overline{a}\,\langle\vec{v}\,, \vec{u}\rangle$$
$$\Rightarrow \overline{\lambda} = \lambda$$
$$\Rightarrow \lambda \in \mathbb{R}$$

□

Group

Let a, b, c $\in \mathbb{G}$
There is binary operation * and satisfies

Closure Law
$a * b \in \mathbb{G}$

Associative Law
$a * b * c = a * (b * c)$

Identity
$\exists e \in \mathbb{G}$ such that $e * a = a * e \in \mathbb{G}$

Inverse
If a $\in \mathbb{G}, \exists a^{-1} \in \mathbb{G}$ such that $a * a^{-1} = e$

XOR over $\mathbb{Z}/\mathbb{Z}_2$ forms a group
1. $a \oplus b = a \oplus b$ commutative
2. $a \oplus b \oplus c = a \oplus (b \oplus c)$ associative
3. $0 \oplus a = a$ identity
4. $a \oplus a = 0$ own inverse

Semigroup

Semigroup is a set S and a binary operator $\otimes$: $S \times S \to S$ that satisfies associative property

$$\forall \text{ a, b, c} \in S \text{ such as } a \otimes b \otimes c = a \otimes (b \otimes c)$$

Monoid

A monoid is a triple $(S, \otimes, \overline{1})$
1. $\otimes$ is closed associative binary operator on the set S
2. $\overline{1}$ is identity element for $\otimes$

$\forall \quad a, b, c \in S$ such as

$$a \otimes b \otimes c = a \otimes (b \otimes c)$$

$$a \otimes \overline{1} = \overline{1} \otimes a = a$$

Category is an algebraic structure comprises "objects" that are linked by arrows

Category

A category is collection of objects and collection of arrow[morphism, map] which have following structure each arrow has domain and codomain which are object

$$f\colon X \to Y \text{ or } X \xrightarrow{f} Y$$

Composition

$$f\colon X \to Y \text{ and } g\colon Y \to Z \quad g \circ f\colon X \to Z$$

Composition Identity

$$f\colon X \to Y \text{ and } g\colon Y \to Z \quad \exists id_y\colon Y \to Y \mid id_y \circ f = f \text{ and } g \circ id_y = g$$

Associative

$$f\colon X \to Y \quad g\colon Y \to Z \quad h\colon Z \to W \mid h \circ g \circ f = h \circ (g \circ f)$$

Functor

Functor can be formally defined by a pair of functions f_1 and f_0 so that $f_0 : Ob(Hask) \to Ob(Hask)$ and $f_1 : Hom(Hask) \to Hom(Hask)$ where $Hom(Hask)$ refers to the union of all sets $a \to b$ where $a, b \in Ob(Hask)$ so that the following holds

0. $id :: a \to a$
1. If $g :: a \to b$ then $f_1(g) :: f_0(a) \to f_0(b)$
2. For all $a \in \text{Ob(Hask)}, \quad f_1(id_a) = id_{f_0(a)}$
3. If $g, h \in \text{Hom(Hask)}$ then $\quad f_1(g \circ h) = f_1(g) \circ f_1(h)$

Given $f_0(a) = \text{List } a \quad f_1(g) = \text{ map } g$ Prove f_0 and f_1 is a Functor

Ring

Let a, b, c $\in \mathbb{R}$ There are addition and multiplication operations and satisfy associative and distributive laws

Associative Law
$a \times b \times c = a \times (b \times c)$

Distritutive Law
$a \times (b + c) = a \times b + a \times c$

Additive inverse
For all a in $\mathbb{R}$, there exists -a such that
$a + (-a) = 0$

Multiplicative identity
For all a in $\mathbb{R}$, there exist 1 such that
$1a = a$

Division Ring

Division Ring is a set F, together with two operations $+$ and $\times$ 1. F is abelian group under $+$ 2. The non-zero elements of F form group under $\times$ (not necessary commutative)

Group homomorphism(operation preserving)

Given group $(G1, +)$ and $(G2, *)$,for all $a_1, a_2 \in G1$ and $b_1, b_2 \in G2$,
if $\phi(a_1 + a_2) = \phi(b_1) * \phi(b_2)$, then ϕ is group homomorphism

Given $G(\mathbb{R}, +)$ and $(\mathbb{R}, *)$, then $\phi(x) = e^x$ is homomorphism
Let $a_1, b_1 \in \mathbb{R}$ and $a_2, b_2 \in \mathbb{R}$
$\phi(a_1 + b_1) = e^{a_1+b_1}$ and $\phi(a_2) * \phi(b_2) = e^{a_2} * e^{b_2} = e^{a_2+b_2}$
$\Rightarrow \phi(a_1 + b_1) = \phi(a_2) * \phi(b_2)$
$\Rightarrow \phi(x) = e^x$ is homomorphism for $G(\mathbb{R}, +)$ and $G(\mathbb{R}, *)$

Normal Group

if N is subgroup of G, and if $gH = Hg \quad \forall g \in G$, then H is normal

Coset

if N is subgroup of G, and if $gH = \{gh : \forall g \in G\}$, then gH is left coset of H in G with repsect to g.
Similarly, if $Hg = \{hg : \forall g \in G\}$, then Hg is right coset of H in G with repsect to g.

Ring homomorphism(operation preserving) Let ϕ is a function between two rings R, then ϕ is a *ring* homomorphism if for all $a \in R$ and $b \in R$

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

$$\phi(ab) = \phi(a)\phi(b)$$

and

$$\phi(1) = 1$$

e.g. $G(\mathbb{N},+)$ and $G(\mathbb{Z}/\mathbb{Z}_5,+)$

Let $\phi : \mathbb{C} \to \mathbb{C}$ be the map send a complex number to its complex conjugate. Then ϕ is an automorphism of $\mathbb{C}$. ϕ is its own inverse.

$$\begin{aligned} \phi(z) &= \overline{z} \\ \phi(z_1 + z_2) &= \overline{z_1 + z_2} \\ \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_2} \\ \phi(z_1 z_2) &= \overline{z_1 z_2} \\ \overline{z_1 z_2} &= \overline{z_1} \cdot \overline{z_2} \\ \phi(\phi(z)) &= z \end{aligned}$$

Let $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ be the map that send $f(x)$ to $f(x+1)$. Then ϕ is an automorphism of $\mathbb{R}[x]$. The inverse map sends $f(x)$ to $f(x-1)$

Ideal

Let R be a ring and let I is additive subgroup of R, then I is called an ideal of R and write $I \triangleleft R \quad$ if $\forall a \in I$ and $\forall r \in R$, and $ar \in I$ and $ra \in I$

Example
$R = (\mathbb{N},+)$ and $I = (2k,+) \quad k \in \mathbb{N}$

Let I be a kernal of ϕ, then I is an ideal of R
Let $a \in I$ and $r \in R$, then $\phi(ra) = \phi(r)\phi(a)$
I is kernal of $\phi \Rightarrow \phi(a) = 0 \therefore \phi(ra) = 0, \therefore ra \in I$

If $\gcd(a,b) = 1$ **and** $a|bc \quad \Rightarrow a|c$
Proof
$\gcd(a,b) = 1$
$\Rightarrow ma + nb = 1 \quad m,n \in \mathbb{N}$
$\Rightarrow mac + nbc = c$
$a|bc \Rightarrow ak = bc \quad k \in \mathbb{N}$
$\Rightarrow mac + n(ak) = c \quad (ak = bc)$
$\Rightarrow a(mc + nk) = c$
$\Rightarrow a|c$

If $\gcd(a,b) = 1 \Rightarrow ma + nb = 1 \quad m,n \in \mathbb{N}$
Proof

Prove there is infinite prime

Prove all the eigeivalues $\lambda \geq 0$ **if the matrix is symmetic**

If the determine of matrix $\det A > 0 \iff$ **the matrix is invertable**

Efficient Algorithm to compute Fibonacci Number
Fibonacci Sequence $F_n = F_n + F_{n-1}$ with $F_0 = 0$ $F_1 = 1$
(1) Navier algorithm with recursion in $O(2^n)$
(2) Use Dynamic Algorithm in $O(n)$
(3) Use matrix with repeated squaring to compute Fibonacci Sequence in $O(\log n)$

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}^n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

Visual proof
$(\sum_{k=1}^{n} k)^2 = \sum_{k=1}^{n} k^3$

/Users/cat/myfile/bitbucke

Show the sum of odd number are square number 1

1 + 3
1 + 3 + 5
1 + 3 + 5 + ... + (2k+1)

$S = \sum_{k=1}^{n} (2k - 1)$
$S = \sum_{k=1}^{n} 2k - \sum_{k=1}^{n} 1$
$S = 2(\sum_{k=1}^{n} k) - n$
$S = 2\frac{(1+n)n}{2} - n$
$S = (1 + n)n - n$
$S = n^2$

composition function
$g \circ f \circ h$
$g \circ f \colon A \to B$

Find the sum of sequence of squares

$$s = \sum_{k=1}^{n} k^2$$

$$\sum_{k=1}^{n}((k+1)^3 - k^3) = \sum_{k=1}^{n}(k+1)^3 - \sum_{k=1}^{n} k^3$$

$$\Rightarrow 2^3 + 3^3 + ... + n^3 + (n+1)^3 - (1 + 2^3 + 3^3 + ... + n^3) = (n+1)^3 - 1$$

$$\Rightarrow \sum_{k=1}^{n}(k+1)^3 - \sum_{k=1}^{n} k^3 = (n+1)^3 - 1$$

$$\Rightarrow (n+1)^3 - 1 = \sum_{k=1}^{n}(3k^2 + 3k + 1)$$

$$\Rightarrow (n+1)^3 - 1 = 3\sum_{k=1}^{n} k^2 + 3\sum_{k=1}^{n} k + n$$

$$\Rightarrow (n+1)^3 - 1 = 3\sum_{k=}^{n} k^2 + (n+1)n\frac{3}{2} + n$$

$$\Rightarrow (n+1)^3 - 1 - (n+1)n\frac{3}{2} - n = 3\sum_{k=1}^{n} k^2$$

$$\Rightarrow (n+1)((n+1)^2 - n\frac{3}{2}) - (n+1) = 3\sum_{k=1}^{n} k^2$$

$$\Rightarrow (n+1)((n+1)^2 - n\frac{3}{2} - 1) = 3\sum_{k=1}^{n} k^2$$

$$\Rightarrow (n+1)(n^2 + 1 + 2n - n\frac{3}{2} - 1) = 3\sum_{k=1}^{n} k^2$$

$$\Rightarrow (n+1)(n^2 + \frac{1}{2}n) = \sum_{k=1}^{n} k^2$$

$$\Rightarrow \frac{1}{2}(n+1)(2n^2 + n) = \sum_{k=1}^{n} k^2$$

$$\Rightarrow \frac{1}{6}n(n+1)(2n+1) = \sum_{k=1}^{n} k^2$$

Vector Space

Let $\vec{u}, \vec{v}, \vec{w} \in \vec{V}$ and scalars $\alpha, \beta \in \mathbb{F}$

Closure

$\vec{u} + \vec{v}$ and $\in \vec{V}$

Associative Law

$\vec{u} + \vec{v} + \vec{w} = \vec{u} + (\vec{v} + \vec{w})$

Commutative Law

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

Identity element of addition

$\vec{0} \in \vec{V}$ such that $\vec{0} + \vec{u} = \vec{u}$

Inverse element of addition

$\exists - \vec{u}$ such that $\vec{u} + (-\vec{u}) = \vec{0}$

Identity element of scalar multiplication

$\exists \mathit{1} \in \mathbb{F}$ such that $\mathit{1}\vec{u} = \vec{u}$

Distributivity of scale multiplication with respect to vector addition

$\alpha(\vec{u} + \vec{v}) = \alpha\vec{u} + \alpha\vec{v}$

Distributivity of scale multiplication with respect to field addition

$(\alpha + \beta)\vec{u} = \alpha\vec{u} + \beta\vec{u}$

Definition 2. *Linear Transformation is a function $T : \mathbb{R}^n \to \mathbb{R}^m$ is called linear transformation, if it satisfies following properties*

$$T(\vec{u}+\vec{v}) = T(\vec{u}) + T(\vec{v}) \quad \forall\, \vec{u}\,, \vec{v} \in \mathbb{R}^n$$
$$T(\lambda\vec{u}) = \lambda T(\vec{u}) \qquad \textit{where } \lambda \in \mathbb{R}$$

Definition 3. *Linear Operator: Given $\mathcal{L} : E \to F$, $\mathcal{L}$ is linear operator and E, F are vector spaces over the field $\mathcal{K}$, $\mathcal{L}$ satifys following properties*

$$\mathcal{L}[f(x) + g(x)] = \mathcal{L}[f(x)] + \mathcal{L}[g(x)]$$
$$\mathcal{L}[af(x)] = a\mathcal{L}[f(x)] \quad \textit{where } a \in \mathcal{K}$$
$$\mathcal{L}_1\mathcal{L}_2[f(x)] = \mathcal{L}_2\mathcal{L}_1[f(x)]$$

Proof of Sine Law

Let the diameter of circle is $AC = 1$

$$\Rightarrow \quad \frac{AB}{\cos\beta} = 1 \quad \frac{AD}{\cos\alpha} = 1 \quad \frac{BC}{\sin\beta} = 1 \quad \frac{DC}{\sin\alpha} = 1 \quad \frac{BD}{\sin(\alpha+\beta)} = 1$$

$$\Rightarrow AB = \cos\beta \quad AD = \cos\alpha \quad BC = \sin\beta \quad DC = \sin\alpha \quad BD = \sin(\alpha+\beta)$$

From Ptolemy theorem

$$AC \times BD = BC \times AD + AB \times DC$$

Since $AC = 1$

$$\Rightarrow \quad BD = BC \times AD + AB \times DC$$

$$\Rightarrow \quad \sin(\alpha+\beta) = \sin\beta\cos\alpha + \cos\beta\sin\alpha$$

Definition of Affine Space

An affine space is a set of points that admits free transitive action of a vector space $\vec{V}$ That is, there is a map $X \times \vec{V} \to X : (x, \vec{v}) \mapsto x + \vec{v}$, called translation by a vector $\vec{v}$, such that
1. Addition of vectors corresponds to composition of translation, i.e., for all $x \in X$ and $\vec{u}, \vec{v} \in \vec{V}, (x+\vec{u})+\vec{v} = x + (\vec{u} + \vec{v})$
2. The zero vector $\vec{0}$ acts as the identity vector, i.e., for all $x \in X, x + \vec{0} = x$
3. The action is transitive, i.e., for all $x, y \in X,$ exists $\vec{v} \in \vec{V}$ such that $y = x + \vec{v}$
4. The dimension of X is the dimension of vector space translations, $\vec{V}$

Or There is unique map
$X \times X \to \vec{V} : (x, y) \mapsto y - x$ such that $y = x + (y - x)$ for all $x, y \in X$ It furthermore satifies
1. For all $x, y, z \in X$, z - x = (z - y) + (y - x)
2. For all $x, y, \in X$ and $\vec{u}, \vec{v} \in \vec{V}$, $(y + \vec{v}) - (x + \vec{u}) = (y - x) + (\vec{v} - \vec{u})$
3. For all $x \in X, x - x = \vec{0}$
4. For all $x, y \in X, y - x = -(x - y)$

Affine Space from linear system equation
Consider an $(m \times n)$ linear sytem equations

$$\sum_{k=1}^{n} a_{ik}x_k = c_i, (1 \leq i \leq m) \qquad (1)$$

where $d = n - rank(M), c_i \neq \vec{0} \in \mathbb{R}^m$
When the system has at least one solution x_p then the full set of solution is a d-dimension affine space $A \subset \mathbb{R}^n$
Since $x_p \in A,$ we can declare point x_p as origin of A and then introduct A coordinates as follows:homogenous system

$$\sum_{k=1}^{n} a_{ik}x_k = \vec{0}(1 \leq i \leq m)$$

$\Rightarrow dim(Ker(M)) = d$ (Rank Theorem)
(1) has d-linear independent solution $\vec{b_j} \in \mathbb{R}^n \qquad (1 \leq j \leq d)$
Affine Space A can be written as

$$A = \left\{ x_p + \sum_{j=1}^{d} \alpha_j \vec{b_j} \quad | \quad \alpha_j \in \mathbb{R} \qquad (1 \leq j \leq d) \right\}$$

The α_j can be served as coordinates in A, so that A looks as it were a d-dimension coordiate space.
But note that addition(+) in the space refers to the chosen point $x_p,$ and not to the origin of the base vector space

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$

Theorem 1
The image of transformation is spanned by the image of the any basis of its domain. For $T:\vec{V}\to\vec{W},$ if $\beta=\{\vec{b_1},\vec{b_2},...,\vec{b_n}\}$ is a basis of $\vec{V},$ then $T(\beta)=\{T(\vec{b_1}),T(\vec{b_2}),...,T(\vec{b_n})\}$ spans the image of T

Proof
For all $\vec{v}\in\vec{V},\vec{v}=\alpha_1\vec{b_1}+\alpha_2\vec{b_2}+...+\alpha_n\vec{b_n}$
$\Rightarrow T(\vec{v})=T(\alpha_1\vec{b_1}+\alpha_2\vec{b_2}+...+\alpha_n\vec{b_n})$
$\Rightarrow T(\vec{v})=\alpha_1T(\vec{b_1})+\alpha_2T(\vec{b_2})+...+\alpha_nT(\vec{b_n})$
$\Rightarrow\{T(\vec{b_1}),T(\vec{b_2}),...,T(\vec{b_n})\}$ spans the image of T

Rank Theorem
If the domain is finite dimension, then the dimension of domain is the sum of rank and nullity of the transformation
Let $T:\vec{V}\to\vec{W}$ be a linear transformation ,let n be the dimension of $\vec{V}$,
let k be nullity of T and let k be the rank of T
Show $n=k+r$

Let $\beta=\{\vec{b_1},\vec{b_2},...,\vec{b_k}\}$ be the basis of kernal of $T,$ the basis can be extended to $\gamma=\{\vec{b_1},\vec{b_2},...,\vec{b_k},\vec{b_{k+1}},...,\vec{b_n}\}$
let $\vec{v}\in\vec{V}\Rightarrow\vec{v}=\alpha_1\vec{b_1}+\alpha_2+\vec{b_2}+,...,+\alpha_k\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n}$
Let $T(\vec{v})=T(\alpha_1\vec{b_1}+\alpha_2+\vec{b_2}+,...,+\alpha_k\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n})=\vec{0}$
$\Rightarrow\vec{v}=\alpha_1\vec{b_1}+\alpha_2+\vec{b_2}+,...,+\alpha_k\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n}\in\ker(T)\qquad(1)$
$\because\vec{v}=\sigma_1\vec{b_1}+\sigma_2+\vec{b_2}+,...,+\sigma_k\vec{b_k}\in\ker(T)\qquad(2)$
$(1)-(2)\Rightarrow\vec{0}=(\alpha_1-\sigma_1)\vec{b_1}+(\alpha_2-\sigma_2)\vec{b_2}+,...,+(\alpha_k-\sigma_k)\vec{b_k}+\alpha_{k+1}\vec{b}_{k+1}+,...,+\alpha_n\vec{b_n}$
$\because\vec{b}_1,\vec{b}_2,...,\vec{b}_k,\vec{b}_{k+1},\vec{b}_{k+2},...,\vec{b_n}$ are linearly independent
$\therefore\alpha_{k+1},\alpha_{k+2},...,\alpha_n$ are all zero $\qquad(3)$
$T(\vec{v})=T(\alpha_1\vec{b_1})+T(\alpha_2\vec{b_2})+,...,+T(\alpha_k\vec{b_k})+T(\alpha_{k+1}\vec{b}_{k+1})+,...,+T(\alpha_n\vec{b_n})=\vec{0}$
$T(\vec{v})=\alpha_1T(\vec{b_1})+\alpha_2T(\vec{b_2})+,...,+\alpha_kT(\vec{b_k})+\alpha_{k+1}T(\vec{b}_{k+1})+,...,+\alpha_nT(\vec{b_n})=\vec{0}$
$\because\beta=\{\vec{b_1},\vec{b_2},...,\vec{b_k}\}$ is the basis of kernal of T
$\therefore T(\vec{b_1})=\vec{0},...,T(\vec{b_k})=\vec{0}$
$\therefore T(\vec{v})=\alpha_{k+1}T(\vec{b}_{k+1})+,...,+\alpha_nT(\vec{b_n})=\vec{0}\qquad(4)$
(3) and (4) $\Rightarrow\{T(\vec{b}_{k+1}),T(\vec{b_{k+2}}),...,T(\vec{b_n})\}$ are linearly independent
$\Rightarrow\dim(\vec{V})=$ nullity(T) + rank(T) or
$\Rightarrow\dim(\vec{V})=\dim(\ker(T))+\dim(\text{img(T)})$
$\Rightarrow n=k+r\quad\square$

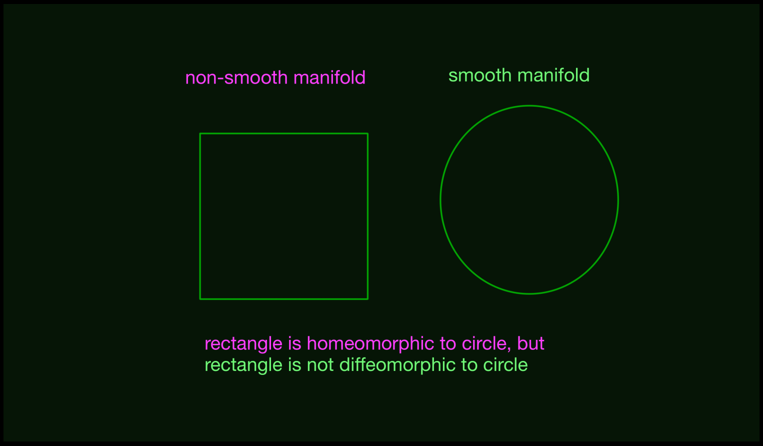
Affine plane
Affine plane is a set, whose elements are called points, and a set of subset, called lines, satifying the following three axioms:
1. Given two distinct points P and Q, there is one and only one containing both P and Q.
2. Given a line l, and a point P not in l, there is one and only one line m which is parallel to l and which passes through P.
3. There exists three non-collinear points.

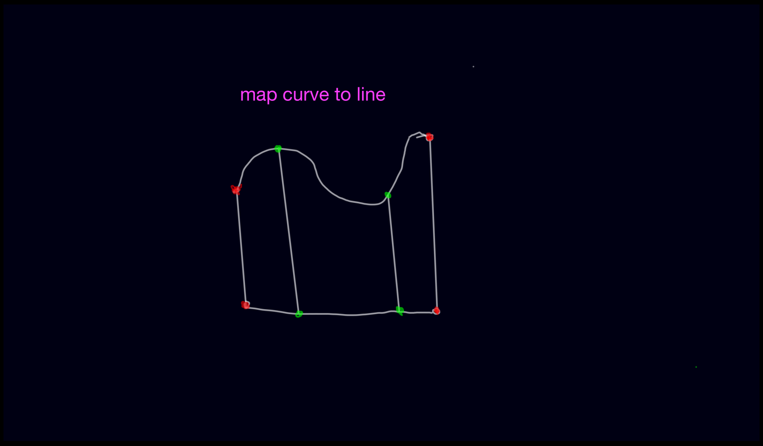
A coordinate system in an affine space $(\mathbf{X},\mathbf{V})$ consists of a point $\mathbf{O}\in\mathbf{X}$ is called origin, and basis $\vec{v_1},...,\vec{v_n}$ for $\vec{V}$ Any point $\mathbf{X}$ can be written as

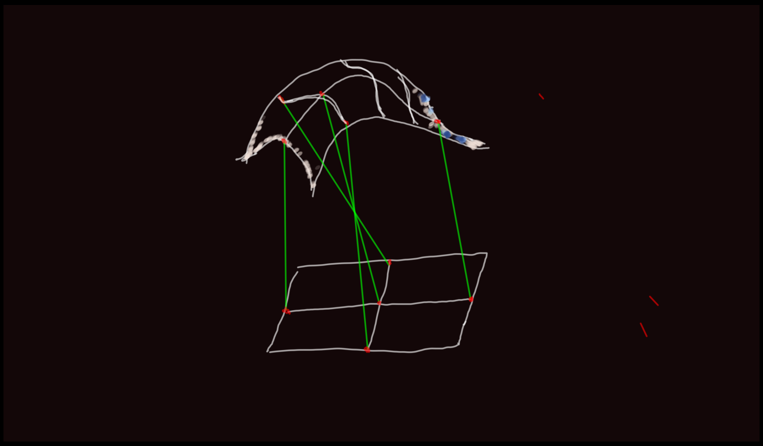
$\mathbf{x}-\mathbf{O}=\mathbf{x}-\mathbf{O}$
$\Rightarrow\mathbf{x}=\mathbf{O}+(\mathbf{x}-\mathbf{O})=\mathbf{O}+\sum_{k=1}^{n}x_k\vec{v_k}$
where the numbers $x_1,...,x_n$ are the coordinates for vector $\mathbf{x}-\mathbf{O}$ with respect to the basis $\vec{v_1},...\vec{v_n}$.
They are now also called the coordinates for $\mathbf{x}$ with respect to the coordinate system $\mathbf{O},\vec{v_1},...,\vec{v_n}$

Projective plane
A projective plane $\mathbb{S}$ is a set, whose elements are called points, and a set of subset, called lines, satifying the following four axioms.
1. Two distinct points meets P, Q of S lie on one and only one line.
2. Any two lines meet in at least one point.
3. There exist three non-colinear points
4. Every line contains at least three points.

Manifold
An subset $\mathbf{S}$ of $\mathbb{R}^m$ is called a manifold of dimension of d if every point p of $\mathbf{S}$ has a neighbourhood in $\mathbf{S}$ which is **homeomorphic** to an open set of $\mathbf{R}^d$
If we magnify a point on a surface, then the point is like on a flat surface.
Homeomorphic - continuous and invertable function, there is an unique point from line to a curve and from a curve to a point
Diffeomorphic - smooth and **invertable** function. Question
If two **smooth** functions are composed, then the new function is **smooth**.







Homeomorphism
Let S be a subset of $\mathbb{R}^m$ and sp be the subset of $\mathbb{R}^n$. A map $f : \mathbb{R}^m \mapsto \mathbb{R}^n$
is called homeomorphism if f is continuous and bijective and f^{-1} is continuous

It may seem faily obvious that you can not draw an accurate map of a portion of the earth becuse the earth is curved, but the map $\psi : \mathbb{R}^2 \to C$ defined by $\psi(s,t) = (\cos t, \sin t, s)$ preserves lengths of curves, i.e. $L(\psi \circ \gamma) = L(\gamma)$ for any curve $\gamma : [a,b] \to \mathbb{R}^2$. Prove this.

Definition Open and Close Sets
1. $\mathbf{S}$ is said to be open set if every point of $\mathbf{S}$ is an interior of $\mathbf{S}$
2. $\mathbf{S}$ is said to be closed set if $\mathbb{R} \setminus \mathbf{S}$ is open

Proposition
1. $\mathbf{S}$ is open if there exists $\delta > 0$ such that $(s-\delta, s+\delta) \subseteq \mathbf{S}$
2. $\mathbf{S}$ is open if any $s \in \mathbf{S}$ there exists a neighbourhood of s included in $\mathbf{S}$

Terminology
$\mathcal{M}$ Set (ZFC) book
$\mathcal{Q}$ topology =: set of open set
$(\mathcal{M}, \mathcal{Q})$ toplogy space
$\mathcal{U} \in \mathcal{Q} \iff$ all $\mathcal{U} \subseteq \mathcal{M}$ and open set
$\mathcal{M} \setminus \mathcal{A} \iff$ all $\mathcal{A} \subseteq \mathcal{M}$ closed set
open $\not\Longrightarrow$ closed
open $\not\Longleftarrow$ closed

Definition of Inner Product Positivity
$\langle \vec{v}, \vec{v} \rangle \geq 0$
$\langle \vec{v}, \vec{v} \rangle = \vec{0} \iff \vec{v} = \vec{0}$

Bilinearity
$\langle c_1\vec{v_1} + c_2\vec{v_2}, \vec{v_3} \rangle = c_1\langle \vec{v_1}, \vec{v_3} \rangle + c_2\langle \vec{v_2}, \vec{v_3} \rangle$

Conjugate Symmetic
$\langle \vec{v_1}, \vec{v_2} \rangle = \overline{\langle \vec{v_2}, \vec{v_1} \rangle}$
Proof Cauchy-Schwarz Inequality by picture
$|a \cdot b| \leq \|a\|\|b\|$

Calculate the Excel Sheet Row number algorithm Latex Environment has different mode
Math mode
Text mode
Command mode

Elliptic Curve and Group Structure Conic Curve
$$\begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$$
$ax^2 + ey^2 + iz^2 + (b+d)xy + (c+g)xz + (f+h)yz = 0$

$(x, y, z) = (x/z, y/z, 1)(z \neq 0)$

$$\begin{aligned} ax^2 + ey^2 + (b+d)xy + (c+g)x + (f+h)y + i &= 0 \\ ax + by + c &= 0 \end{aligned}$$
sub (1) into (2) $\Rightarrow ax^2 + bx + c = 0$
$\Rightarrow x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

Exponential backoff algorithm

$\frac{1}{N+1} \sum_{i=1}^{N} i$
For example, the expected backoff time for the third collision, one could calculate the maximum backoff time, N
$N = 2^c - 1 (c = 3)$ $N = 7$
Calculate the mean of backoff time for the third collision(c=3)
$\mathbf{E(c)} = \frac{1}{N+1} \sum_{i=0}^{N} i$
$\mathbf{E(c)} = \frac{1}{N+1} \sum_{i=0}^{N} \Rightarrow \frac{1}{N+1} \frac{N(N+1)}{2} = \frac{N}{2}$
$\mathbf{E(3)} = \frac{1}{7+1} \sum_{i=0}^{N} i = \frac{1}{8}(0+1+2+3+4+5+6+7) = \frac{28}{8}$
$\mathbf{E(3)} = 3.5$

Proof. If x is rational and y is irrational, then x + y is irrational
Assume $x + y$ is rational
$\Rightarrow \frac{n}{m} = x + y \quad m, n \in \mathbb{N}$
$\Rightarrow \frac{n}{m} - \frac{n_1}{m_1} = y \quad m_1, n_1 \in \mathbb{N}$
$\Rightarrow \frac{nm_1}{mm_1} - \frac{n_1 m}{mm_1} = y$
$\Rightarrow \frac{nm_1 - n_1 m}{mm_1} = y$
$\Rightarrow$ y is rational
$\Rightarrow$ this contracts y is irrational
$\Rightarrow$ y is irrational

□

Prove Square root of two is irrational $\sqrt{2} \notin \mathbb{Q}$
Assume $\sqrt{2} \in \mathbb{Q}$
let $n = min\{n \in \mathbb{N} \mid n * \sqrt{2} \in \mathbb{N}\}$
$\Rightarrow n * (\sqrt{2} - 1) * \sqrt{2} \in \mathbb{Q}$
$\because \sqrt{2} - 1 < 1$
$\Rightarrow n * (\sqrt{2} - 1) * \sqrt{2} < n * \sqrt{2}$
$\Rightarrow n * (\sqrt{2} - 1) < n$ such as $n * (\sqrt{2} - 1) * \sqrt{2} \in \mathbb{N}$

$\Rightarrow$ This contracts our assumption $\square$

Prove Square root of 2 is irrational [Geometric proof]

Assume $\sqrt{2} \in \mathbb{Q}$

$\Rightarrow \frac{a}{b} = \sqrt{2} \quad a, b \in \mathbb{N}$ and $\gcd(a, b) = 1, a > b$

given a right issoseles triangle

$AB = AC = AE, \quad FE$ tangles to arc at point E

$\Rightarrow AF = EF$

Let $AB = AC = 1$

$\Rightarrow BC = \sqrt{2}$

$\Rightarrow FB = 1 - EB = 1 - (\sqrt{2} - 1) = 2 - \sqrt{2}$

$\because \frac{AC}{CB} = \frac{EB}{FB} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}-1}{2-\sqrt{2}}$

$\therefore \frac{1}{\sqrt{2}} = \frac{1}{\frac{a}{b}} = \frac{\sqrt{2}-1}{2-\sqrt{2}} = \frac{\frac{a}{b}-1}{2-\frac{a}{b}}$

$\therefore \frac{b}{a} = \frac{\frac{a-b}{b}}{\frac{2b-a}{b}} = \frac{a-b}{2b-a}$

$\because \sqrt{2} < \sqrt{4} = 2 \therefore a < 2b$

$\Rightarrow a - b < b$

$\because 2a > 2b$

$\Rightarrow 2b - a < a$

That contracts our assumption $\gcd(a, b) = 1$

$\Rightarrow \frac{a}{b} \notin \mathbb{Q}$

Geometric proof: square root of two is irrational
Given an isosceles right triangle from above and let $\gcd(a,b)=1,$ from Pythagorean theorem
$\Rightarrow a^2=b^2+b^2$
$\Rightarrow \sqrt{2}=\frac{a}{b}$

singular point on affine plane curve
If $p\in(x,y)$ and $\frac{df}{dx},\frac{df}{dy}$ are undefined on $p\in(x,y),$ then $p\in(x,y)$ is singular point

Eisenstein series

$L=[w_1,w_2]\in\mathbb{C}, G(L)=\sum_{w\in L\setminus\{0,0\}}\frac{1}{w^k}$
Let lattices $L=[1,\tau]$ and parametrized by τ in the upper half plane $\mathbb{H}=\{z\in\mathbb{C}:\Im(z)>0\}$
$G(L)=G([1,\tau])=G(\tau)=\sum'_{m,n\in\mathbb{Z}}\frac{1}{(m+n\tau)^k}$

Show $G_k(\tau+1)=G_k(\tau)$

$G_k(\tau+1)=\sum'_{m,n\in\mathbb{Z}}\frac{1}{(m+n(\tau+1))^k}=\sum'_{m,n\in\mathbb{Z}}\frac{1}{(m+n+n\tau)^k}=\sum'_{m',n\in\mathbb{Z}}\frac{1}{(m'+n\tau)^k}$
$\Rightarrow G_k(\tau+1)=G_k(\tau)$

Show $G_k(\tau)=\tau^{-k}G_k(\dfrac{-1}{\tau})$

$\tau^{-k}G_k(\frac{-1}{\tau})=\tau^{-k}\sum'_{(m,n\in\mathbb{Z})}\frac{1}{(m+\frac{n}{\tau})^k}$
$\tau^{-k}\sum'_{m,n\in\mathbb{Z}}\frac{1}{(m+\frac{n}{\tau})^k}=\tau^{-k}\sum'_{m,n\in\mathbb{Z}}\frac{1}{(\frac{m\tau}{\tau}+\frac{n}{\tau})^k}=\sum'_{m,n\in\mathbb{Z}}(\tau^{-k}\tau^{k})(m\tau+n)^{-k})$
$\Rightarrow G_k(\tau)=\tau^{-k}G_k(\frac{-1}{\tau})$

Show $G_k(\tau)=0$ if $k=(2j+1)\quad j\in\mathbb{Z}$

For each $\omega=(m+n\tau)\in L,$ there exists $-\omega=-(m+n\tau)\in L$
$\because \omega^{-(2J+1)}+(-1)^{-(2J+1)}\omega^{-(2j+1)}=0$
$\therefore \sum'_{m,n\in\mathbb{Z}}(m+n\tau)^{-k}=0\quad$ for all $k\in(2j+1)$

Theorem 1. *Show for any lattices L, the sum $\sum'_{\omega\in L}\frac{1}{\omega^k}$ converges absoluately for all $k>2$*

$$\text{Show } \frac{1}{(1-x)^2} = \sum_{n=0}^{\infty}(n+1)x^n \quad |x| < 1$$

Proof: For all $|x| < 1,$ power series expansion

$$(\frac{1}{1-x}) = (\sum_{n=0}^{\infty} x^n)$$

Differentiate both sides

$$\begin{aligned}
(\frac{1}{1-x})' &= (\sum_{n=0}^{\infty} x^n)' \\
(\frac{1}{1-x})' &= (1-x)^{-2} \\
\sum_{n=1}^{\infty} nx^{n-1} &= \sum_{i=0}^{\infty}(i+1)x^i \quad (n-1=i) \\
\frac{1}{(1-x)^2} &= \sum_{n=0}^{\infty}(n+1)x^n \quad \text{sub } (i=n)
\end{aligned} \tag{1}$$

Weierstrass function $\wp$-function of lattice L is defined by

$\wp(z) = \wp(z;L) = \frac{1}{z^2} + \sum'_{w\in L}\left[\frac{1}{(z-\omega)^2} + \frac{1}{\omega^2}\right]$

Holomorphic

A function $f(z)$ defined on some open neibourhood of a point $z_0 \in \mathbb{C}$ is said to be holomorphic at z_0 if the complex derivative

$$f'(z_0) = \lim_{h\to 0}\frac{f(z_0+h) - f(z_0)}{h}$$

exists. We said f is holomorphic on an open set Ω if it is holomorphic at every $z_0 \in \Omega$ and we said f is holomorphic in a closed set $\mathbf{C}$ if it is holomorphic on some open set Ω containing $\mathbf{C}$. Functions are holomorphic on all of $\mathbb{C}$ are said to be *entire*

$$\text{Show } f(z) = z^2 \text{ is holomorphic}$$

$$f'(z) = \lim_{h\to 0}\frac{(z+h)^2 - z^2}{h}$$

$$f'(z) = \lim_{h\to 0}\frac{z^2 + 2hz + h^2 - z^2}{h}$$

$$f'(z) = \lim_{h\to 0}\frac{2hz + h^2}{h}$$

$$f'(z) = \lim_{h\to 0} 2z + h$$

$$f'(z) = 2z$$

Differential
A function $f(x)$ is differential on $x_0 \in \mathbb{R}$ if

$$f'(x_0) = \lim_{h \to 0} \frac{f(x_0 + h) - f(x_0)}{h}$$

exists

$$\text{Show } f(x) = x^2 \text{ is differentiable for all } x \in \mathbb{R}$$

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

$$f'(x) = \lim_{h \to 0} \frac{x^2 + h^2 + 2xh - x^2}{h}$$

$$f'(x) = \lim_{h \to 0} \frac{h^2 + 2xh}{h}$$

$$f'(x) = \lim_{h \to 0} h + 2x$$

$$f'(x) = 2x \quad \text{for all } x \in \mathbb{R}$$

Elliptic Curve

$$S(n) = \sum_{k=1}^{n} k^2$$

$$S(n) = \frac{(2n+1)(n+1)n}{2 \times 3}$$

Let $y^2 = S(n)$ and $x = n$

$$y^2 = \frac{1}{6}x(x+1)(2x+1)$$

$(x, y) = (0, 0), (-1, 0), (-\frac{1}{2}, 0)$ are on the curve

Proof. How to derive $y^2 = x'^3 + Ax' + B$ from $y^2 = x^3 + bx^2 + cx + d$
We use following trick similar to **Completing the square** in quadratic polynomial

$$
\begin{aligned}
(x+\frac{b}{3})^3 &= x^3 + 3x^2\frac{b}{3} + 3x(\frac{b}{3})^2 + (\frac{b}{3})^3 \\
(x+\frac{b}{3})^3 &= x^3 + bx^2 + 3x(\frac{b}{3})^2 + (\frac{b}{3})^3 \\
(x+\frac{b}{3})^3 - [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] &= x^3 + bx^2 + [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] - [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] \\
(x+\frac{b}{3})^3 &= x^3 + 3x^2\frac{b}{3} + 3x(\frac{b}{3})^2 + (\frac{b}{3})^3 \\
(x+\frac{b}{3})^3 &= x^3 + bx^2 + 3x(\frac{b}{3})^2 + (\frac{b}{3})^3 \\
(x+\frac{b}{3})^3 - [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] &= x^3 + bx^2 + [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] - [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] \\
(x+\frac{b}{3})^3 - [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] + cx + d &= x^3 + bx^2 + [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] - [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] + cx + d \\
(x+\frac{b}{3})^3 - 3x(\frac{b}{3})^2 - (\frac{b}{3})^3 + cx + d &= x^3 + bx^2 + [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] - [3x(\frac{b}{3})^2 + (\frac{b}{3})^3] + cx + d \qquad (2) \\
(x+\frac{b}{3})^3 - [3(\frac{b}{3})^2 - c]x - (\frac{b}{3})^3 + d &= x^3 + bx^2 + cx + d \\
\text{Let } x + \frac{b}{3} = x' &\text{ or } x = x' - \frac{b}{3} \\
x'^3 - [3(\frac{b}{3})^2 - c](x' - \frac{b}{3}) + d - (\frac{b}{3})^3 &= x^3 + bx^2 + cx + d \\
x'^3 - [3(\frac{b}{3})^2 - c]x' + [3(\frac{b}{3})^2 - c]\frac{b}{3} + d &= x^3 + bx^2 + cx + d \\
x'^3 - [3(\frac{b}{3})^2 - c]x' + 3(\frac{b}{3})^3 - \frac{b}{3}c + d &= x^3 + bx^2 + cx + d \\
x'^3 + [c - 3(\frac{b}{3})^2]x' + 3(\frac{b}{3})^3 - \frac{b}{3}c + d &= x^3 + bx^2 + cx + d \\
\therefore A = [c - 3(\frac{b}{3})^2] \quad B &= 3(\frac{b}{3})^3 - \frac{b}{3}c + d
\end{aligned}
$$

□

Definition of topology

Let $\mathcal{M}$ be a set. A topology $\mathcal{Q}$ is a subset $\mathcal{Q} \subseteq \mathcal{P}(\mathcal{M})$
Satisfy
1.$\varnothing \subseteq \mathcal{Q}, \mathcal{M} \subseteq \mathcal{Q}$
2.$\mathcal{U} \subseteq \mathcal{Q}, \mathcal{V} \subseteq \mathcal{Q} \implies \mathcal{U} \cap \mathcal{V} \in \mathcal{Q}$
3.$\mathcal{U} \in \mathcal{Q} \implies \bigcup_{\alpha \in \mathcal{A}} \mathcal{U}_\alpha \in \mathcal{Q}$

Note 1. *In topology, two topology space is equivalent if one topologic space can be deformed to other topologic space continuously. Intuitively speaking, these topologic spaces are seen being made out of ideal rubber which can be deformed somehow. However, such a continuous deformation is constrained by the fact that the dimension is unchanged.*

Topological Space

a topological space is pair (X, τ) where X is a set and τ is subset of X satifying certain axioms. τ is called topology
1. $\emptyset$ and space X are both in τ
2. the union of any collection of set in τ is contained in τ
3. the intersection of any finitly many sets in τ is contained in τ

Binomial Identity

$$\binom{n}{k} = \binom{n}{k-1} + \binom{n-1}{k-1}$$

$$\binom{n}{0} = 1 \text{ with } 1 \leq k \leq n$$

$$\text{LHS} \quad \binom{n}{k} = \frac{P(n,k)}{k!} = \frac{\frac{n!}{(n-k)!}}{k!} = \frac{n!}{(n-k)!k!}$$

$$\text{RHS} \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{P(n-1,k)}{k!} + \frac{P(n-1,k-1)}{(k-1)!}$$

$$\text{RHS} \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{\frac{(n-1)!}{(n-1-k)!}}{k!} + \frac{(n-1)!}{[(n-1)-(k-1))]!(k-1)!}$$

$$\text{RHS} \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{(n-k-1)!k!} + \frac{(n-1)!}{(n-k)!(k-1)!}$$

$$\text{RHS} \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-k)(n-1)!}{(n-k)(n-k-1)!k!} + \frac{k(n-1)!}{k(n-k)!(k-1)!}$$

$$\text{RHS} \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-k)(n-1)!}{(n-k)!k!} + \frac{k(n-1)!}{(n-k)!k!}$$

$$\text{RHS} \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!(n-k+k)}{(n-k)!k!}$$

$$\text{RHS} \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n!}{(n-k)!k!} \quad \square$$

$$\binom{n+1}{k} = \binom{n}{k-1}\binom{n-1}{k-1}$$

/Users/cat/myfile/bitbucke

Computer Graphic Matrix

Identity

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

Scalar

$$\begin{bmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{bmatrix}$$

Translation

$$\begin{bmatrix} 1 & 0 & 0 & x \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & z \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Computer Graphic Matrix

Identity

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

Scalar

$$\begin{bmatrix} x & 0 & 0 \\ 0 & y & 0 \\ 0 & 0 & z \end{bmatrix}$$

Translation

$$\begin{bmatrix} 1 & 0 & 0 & x \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & z \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Rotation

$$\begin{aligned} M_z(\beta) &= \begin{bmatrix} \cos\beta & -\sin\beta & 0 \\ \sin\beta & \cos\beta & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ M_y(\beta) &= \begin{bmatrix} \cos\beta & sin\beta & 0 \\ 0 & 1 & 0 \\ -sin\beta & \cos\beta & 0 \end{bmatrix} \\ M_x(\beta) &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\beta & -\sin\beta \\ 0 & sin\beta & \cos\beta \end{bmatrix} \end{aligned} \tag{3}$$

Find the matrix reflects a point with respect to x-axis

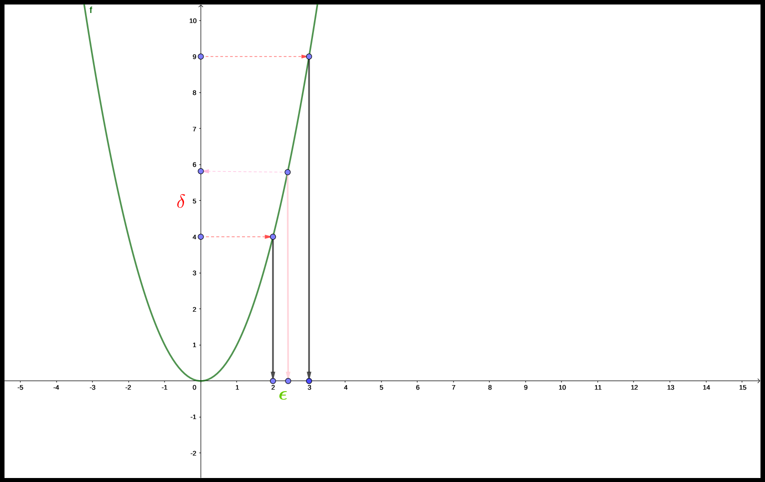
$$A \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Definition 4. *C^0 it means the function continuous*
C^1 it means the function has first order derivative and the function is continuous
C^k it means the function has k derivatives and all the functions are continuous

Definition 5. *Given $f : X \to Y$, if f is continuous on X, and has first order derivative on X, then f is called C^1 mapping*

Definition 6. *Function $f : X \to Y$ is continuous if followings are True*

$$\exists\, \epsilon > 0 \in X \text{ such that } \exists\, \delta > 0 \in Y \text{ and } |\, f(x+\epsilon)\,| < \delta$$



Definition 7. *Let U be open subset of X and $f : U \to V$ be C^1 mapping, where U, V are Eclidean spaces. We say that f is* ***$\mathbf{C^1}$-invertible*** *on U if the image of f is an open set V on Y, and if there is C^1-invertable mapping $g : V \to U$ such that f and g are inverse to each other, i.e.*

$$g(f(x)) = x \text{ and } f(g(y)) = y$$

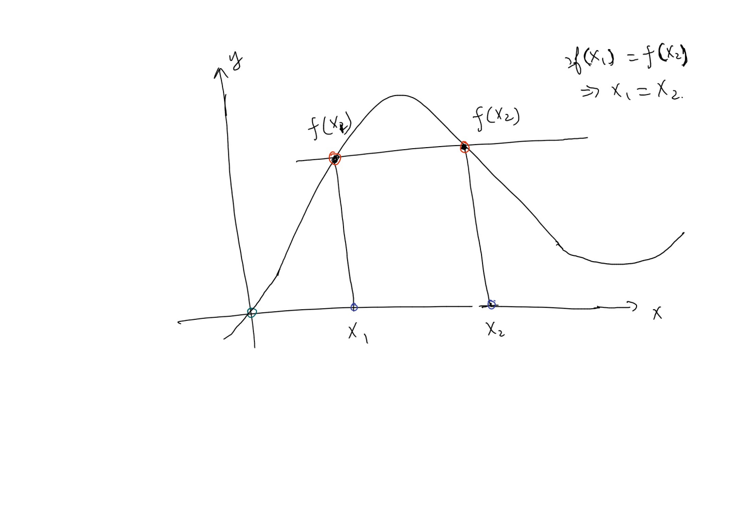
for all $x \in U$, $y \in V$
However, if f is C^1 mapping and has continuous inverse, it is not necessary C^1**-invertible**, e.g.

$$f(x) = x^3$$
$$f^{-1}(x) = x^{\frac{1}{3}}$$

f and f^{-1} are both continuous, but f^{-1} is not differentiable at 0
Intermediate Value Theorem

Theorem 2. *If f is continuous in $[a, b] \in \mathbb{R}$ such that $f(a) < 0$ and $f(b) > 0$, then there exists $c \in [a, b]$ such that $f(c) = 0$*

Definition 8 (Injective function)**.** *A function* $f : X \to Y$*, if* $f(x_1) = f(x_2) \in Y$ *then* $x_1 = x_2 \in X$



Definition 9 (Subjective function)**.** *A function* $f : X \to Y$*,* $\forall y \in Y \quad \exists x \in X$ *such as* $f(x) = y$