MATHEMATICAL FORMULAS AND PROPERTIES

Trigonometric formulas

\[
\begin{align*}
\sin^2 A + \cos^2 A &= 1; \quad \tan x &= \frac{\sin x}{\cos x}; \quad \cot x &= \frac{\cos x}{\sin x} = \frac{1}{\tan x} \\
\cos^2 x &= \frac{1}{1 + \tan^2 x}; \quad \sin^2 x &= \frac{1}{1 + \cot^2 x} = \frac{\tan^2 x}{1 + \tan^2 x}
\end{align*}
\]

\[
\sin (A \pm B) = \sin A \cos B \pm \cos A \sin B
\]
\[
\cos (A \pm B) = \cos A \cos B \mp \sin A \sin B
\]
\[
\tan (A \pm B) = \frac{\tan A \pm \tan B}{1 \mp \tan A \tan B}, \quad \cot (A \pm B) = \frac{\cot A \cot B \mp 1}{\cot B \pm \cot A}
\]

\[
\begin{align*}
\sin 2A &= 2 \sin A \cos A \\
\cos 2A &= \cos^2 A - \sin^2 A = 2 \cos^2 A - 1 = 1 - 2 \sin^2 A \\
\tan 2A &= \frac{2 \tan A}{1 - \tan^2 A}, \quad \cot 2A = \frac{\cot^2 A - 1}{2 \cot A}
\end{align*}
\]

\[
\begin{align*}
\sin A + \sin B &= 2 \sin \frac{A + B}{2} \cos \frac{A - B}{2} \\
\sin A - \sin B &= 2 \sin \frac{A - B}{2} \cos \frac{A + B}{2} \\
\cos A + \cos B &= 2 \cos \frac{A + B}{2} \cos \frac{A - B}{2} \\
\cos A - \cos B &= 2 \sin \frac{A + B}{2} \sin \frac{B - A}{2}
\end{align*}
\]

\[
\begin{align*}
\sin A \sin B &= \frac{1}{2} [\cos (A - B) - \cos (A + B)] \\
\cos A \cos B &= \frac{1}{2} [\cos (A + B) + \cos (A - B)] \\
\sin A \cos B &= \frac{1}{2} [\sin (A + B) + \sin (A - B)]
\end{align*}
\]

\[
\begin{align*}
\sin (-A) &= -\sin A, \quad \cos (-A) = \cos A \\
\tan (-A) &= -\tan A, \quad \cot (-A) = -\cot A \\
\sin \left(\frac{\pi}{2} \pm A\right) &= \cos A, \quad \cos \left(\frac{\pi}{2} \pm A\right) = \mp \sin A \\
\sin (\pi \pm A) &= \mp \sin A, \quad \cos (\pi \pm A) = -\cos A
\end{align*}
\]
Basic trigonometric equations

\[
\begin{align*}
\sin x &= \sin \alpha \quad \Rightarrow \quad \begin{cases} 
x = \alpha + 2k\pi \\
x = (2k+1)\pi - \alpha 
\end{cases} \quad (k = 0, \pm 1, \pm 2, \cdots) \\
\cos x &= \cos \alpha \quad \Rightarrow \quad \begin{cases} 
x = \alpha + 2k\pi \\
x = 2k\pi - \alpha 
\end{cases} \quad (k = 0, \pm 1, \pm 2, \cdots) \\
\tan x &= \tan \alpha \quad \Rightarrow \quad x = \alpha + k\pi \quad (k = 0, \pm 1, \pm 2, \cdots) \\
\cot x &= \cot \alpha \quad \Rightarrow \quad x = \alpha + k\pi \quad (k = 0, \pm 1, \pm 2, \cdots) \\
\sin x &= -\sin \alpha \quad \Rightarrow \quad \begin{cases} 
x = 2k\pi - \alpha \\
x = \alpha + (2k+1)\pi 
\end{cases} \quad (k = 0, \pm 1, \pm 2, \cdots) \\
\cos x &= -\cos \alpha \quad \Rightarrow \quad \begin{cases} 
x = (2k+1)\pi - \alpha \\
x = \alpha + (2k+1)\pi 
\end{cases} \quad (k = 0, \pm 1, \pm 2, \cdots)
\end{align*}
\]

Hyperbolic functions

\[
\begin{align*}
\cosh x &= \frac{e^x + e^{-x}}{2} ; \quad \sinh x = \frac{e^x - e^{-x}}{2} ; \quad \tanh x = \frac{\sinh x}{\cosh x} = \frac{e^x - e^{-x}}{e^x + e^{-x}} = \frac{1}{\coth x} \\
\cosh^2 x - \sinh^2 x &= 1 \\
cosh(-x) &= \cosh x , \quad \sinh(-x) = -\sinh x
\end{align*}
\]
Power formulas

\[(a \pm b)^2 = a^2 \pm 2ab + b^2\]

\[(a \pm b)^3 = a^3 \pm 3a^2b + 3ab^2 \pm b^3\]

\[a^2 - b^2 = (a + b)(a - b)\]

\[a^3 \pm b^3 = (a \pm b)(a^2 \mp ab + b^2)\]

\[(a + b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2!}a^{n-2}b^2 + \frac{n(n-1)(n-2)}{3!}a^{n-3}b^3 + \cdots + b^n \quad (n = 1, 2, 3, \ldots)\]

Quadratic equation: \(ax^2 + bx + c = 0\)

Call \(D = b^2 - 4ac\) \quad (discriminant)

Roots: \(x = \frac{-b \pm \sqrt{D}}{2a}\)

Roots are real and distinct if \(D > 0\); real and equal if \(D = 0\); complex conjugate if \(D < 0\).

Geometric formulas

\(A = \) area or surface area ; \(V = \) volume ; \(P = \) perimeter

Parallelogram of base \(b\) and altitude \(h\) : \(A = bh\)

Triangle of base \(b\) and altitude \(h\) : \(A = \frac{1}{2}bh\)

Trapezoid of altitude \(h\) and parallel sides \(a\) and \(b\) : \(A = \frac{1}{2}(a+b)h\)

Circle of radius \(r\) : \(P = 2\pi r\) , \(A = \pi r^2\)

Ellipse of semi-major axis \(a\) and semi-minor axis \(b\) : \(A = \pi ab\)

Parallelepiped of base area \(A\) and height \(h\) : \(V = Ah\)

Cylindroid of base area \(A\) and height \(h\) : \(V = Ah\)

Sphere of radius \(r\) : \(A = 4\pi r^2\) , \(V = \frac{4}{3}\pi r^3\)

Circular cone of radius \(r\) and height \(h\) : \(V = \frac{1}{3}\pi r^2h\)
Properties of inequalities

\[ a < b \text{ and } b < c \Rightarrow a < c \]

\[ a \geq b \text{ and } b \geq a \Rightarrow a = b \]

\[ a < b \Rightarrow -a > -b \]

\[ 0 < a < b \Rightarrow \frac{1}{a} > \frac{1}{b} \]

\[ a < b \text{ and } c \leq d \Rightarrow a + c < b + d \]

\[ 0 < a < b \text{ and } 0 < c \leq d \Rightarrow a c < b d \]

\[ 0 < a < 1 \Rightarrow a > a^2 > a^3 > \cdots, \quad a^n < 1, \quad \sqrt[n]{a} < 1 \]

\[ a > 1 \Rightarrow a < a^2 < a^3 < \cdots, \quad a^n > 1, \quad \sqrt[n]{a} > 1 \]

\[ 0 < a < b \Rightarrow a^n < b^n, \quad \sqrt[n]{a} < \sqrt[n]{b} \]

Properties of proportions

Assume that \( \frac{\alpha}{\beta} = \frac{\gamma}{\delta} = \kappa \). Then,

\[ \alpha \delta = \beta \gamma \quad , \quad \frac{\alpha \pm \gamma}{\beta \pm \delta} = \kappa \]

\[ \frac{\alpha \pm \beta}{\beta} = \frac{\gamma \pm \delta}{\delta} \quad , \quad \frac{\alpha}{\beta \pm \alpha} = \frac{\gamma}{\delta \pm \gamma} \]
Properties of absolute values of real numbers

\[ |a| = a, \quad \text{if} \quad a \geq 0 \]
\[ = -a, \quad \text{if} \quad a < 0 \]

\[ |a| \geq 0 \]

\[ |-a| = |a| \]

\[ |a|^2 = a^2 \]

\[ \sqrt{a^2} = |a| \]

\[ |x| \leq \varepsilon \iff -\varepsilon \leq x \leq \varepsilon \quad (\varepsilon > 0) \]

\[ |x| \geq a > 0 \iff x \geq a \quad \text{or} \quad x \leq -a \]

\[ |a - b| \leq |a| + |b| \]

\[ |a - b| = |a| \cdot |b| \]

\[ |a^k| = |a|^k \quad (k \in \mathbb{Z}) \]

\[ \left| \frac{a}{b} \right| = \frac{|a|}{|b|} \quad (b \neq 0) \]
Properties of powers and logarithms

\[ x^0 = 1 \quad (x \neq 0) \]

\[ x^\alpha x^\beta = x^{\alpha + \beta} \]

\[ \frac{x^\alpha}{x^\beta} = x^{\alpha - \beta} \]

\[ \frac{1}{x^\alpha} = x^{-\alpha} \]

\[ (x^\alpha)^\beta = x^{\alpha \beta} \]

\[ (xy)^\alpha = x^\alpha y^\alpha \quad ; \quad \left( \frac{x}{y} \right)^\alpha = \frac{x^\alpha}{y^\alpha} \]

\[ \ln 1 = 0 \]

\[ \ln \left( e^\alpha \right) = \alpha \quad (\alpha \in \mathbb{R}) \quad , \quad e^{\ln \alpha} = \alpha \quad (\alpha \in \mathbb{R}^+) \]

\[ \ln (\alpha \beta) = \ln \alpha + \ln \beta \]

\[ \ln \left( \frac{\alpha}{\beta} \right) = \ln \alpha - \ln \beta = -\ln \left( \frac{\beta}{\alpha} \right) \]

\[ \ln \left( \frac{1}{\alpha} \right) = -\ln \alpha \]

\[ \ln (\alpha^k) = k \ln \alpha \quad (k \in \mathbb{R}) \]
Derivatives and integrals of elementary functions

\[(c)' = 0 \quad (c = \text{const.}) \quad (\sin x)' = \cos x \quad (\arcsin x)' = \frac{1}{\sqrt{1-x^2}}\]
\[(x^\alpha)' = \alpha x^{\alpha-1} \quad (\alpha \in \mathbb{R}) \quad (\cos x)' = -\sin x \quad (\arccos x)' = -\frac{1}{\sqrt{1-x^2}}\]
\[(e^x)' = e^x \quad (\tan x)' = \frac{1}{\cos^2 x} \quad (\arctan x)' = \frac{1}{1+x^2}\]
\[(\ln x)' = \frac{1}{x} \quad (x > 0) \quad (\cot x)' = -\frac{1}{\sin^2 x} \quad (\arc cot x)' = -\frac{1}{1+x^2}\]
\[(\sinh x)' = \cosh x \quad (\cosh x)' = \sinh x\]

\[
\int dx = x + C ; \quad \int x^\alpha \, dx = \frac{x^{\alpha+1}}{\alpha + 1} + C \quad (\alpha \neq -1)
\]
\[
\int \frac{dx}{x} = \ln |x| + C
\]
\[
\int e^x \, dx = e^x + C
\]
\[
\int \cos x \, dx = \sin x + C ; \quad \int \sin x \, dx = -\cos x + C
\]
\[
\int \frac{dx}{\cos^2 x} = \tan x + C ; \quad \int \frac{dx}{\sin^2 x} = -\cot x + C
\]
\[
\int \frac{dx}{\sqrt{1-x^2}} = \arcsin x + C
\]
\[
\int \frac{dx}{1+x^2} = \arctan x + C
\]
\[
\int \frac{dx}{x^2-1} = \frac{1}{2} \ln \left|\frac{x-1}{x+1}\right| + C
\]
\[
\int \frac{dx}{\sqrt{x^2 \pm 1}} = \ln \left(x + \sqrt{x^2 \pm 1}\right) + C
\]
COMPLEX NUMBERS

Consider the equation \( x^2 + 1 = 0 \). This has no solution for real \( x \). For this reason we extend the set of numbers beyond the real numbers by defining the \textit{imaginary unit number} \( i \) by

\[
i^2 = -1 \quad \text{or, symbolically,} \quad i = \sqrt{-1}.
\]

Then, the solution of the above-given equation is \( x = \pm i \).

Given the \textit{real} numbers \( x \) and \( y \), we define the \textit{complex number}

\[
z = x + iy.
\]

This is often represented as an ordered pair

\[
z = x + iy \equiv (x, y).
\]

The number \( x = \text{Re} \ z \) is the \textit{real part} of \( z \) while \( y = \text{Im} \ z \) is the \textit{imaginary part} of \( z \). In particular, the value \( z = 0 \) corresponds to \( x = 0 \) and \( y = 0 \). In general, if \( y = 0 \), then \( z \) is a \textit{real number}.

Given a complex number \( z = x + iy \), the number

\[
\overline{z} = x - iy
\]

is called the \textit{complex conjugate} of \( z \) (the symbol \( z^* \) is also used for the complex conjugate). Furthermore, the \textit{real} quantity

\[
|z| = (x^2 + y^2)^{1/2}
\]

is called the \textit{modulus} (or absolute value) of \( z \). We notice that

\[
|z| = |\overline{z}|
\]

\textit{Example:} If \( z = 3 + 2i \), then \( \overline{z} = 3 - 2i \) and \( |z| = |\overline{z}| = \sqrt{13} \).

\textit{Exercise:} Show that, if \( z = \overline{z} \), then \( z \) is \textit{real}, and conversely.

\textit{Exercise:} Show that, if \( z = x + iy \), then

\[
\text{Re} \ z = x = \frac{z + \overline{z}}{2}, \quad \text{Im} \ z = y = \frac{z - \overline{z}}{2i}.
\]
Consider the complex numbers \( z_1 = x_1 + i y_1 \), \( z_2 = x_2 + i y_2 \). As we can show, their sum and their difference are given by

\[
\begin{align*}
\text{z}_1 + \text{z}_2 &= (x_1 + x_2) + i (y_1 + y_2), \\
\text{z}_1 - \text{z}_2 &= (x_1 - x_2) + i (y_1 - y_2).
\end{align*}
\]

**Exercise:** Show that, if \( \text{z}_1 = \text{z}_2 \), then \( x_1 = x_2 \) and \( y_1 = y_2 \).

Taking into account that \( i^2 = -1 \), we find the product of \( \text{z}_1 \) and \( \text{z}_2 \) to be

\[
\text{z}_1 \text{z}_2 = (x_1 x_2 - y_1 y_2) + i (x_1 y_2 + x_2 y_1).
\]

In particular, for \( \text{z}_1 = z = x + i y \) and \( \text{z}_2 = \bar{z} = x - i y \), we have:

\[
\text{z}\bar{z} = x^2 + y^2 = |\text{z}|^2.
\]

To evaluate the ratio \( \text{z}_1 / \text{z}_2 \) (\( \text{z}_2 \neq 0 \)) we apply the following trick:

\[
\frac{\text{z}_1}{\text{z}_2} = \frac{\text{z}_1 \bar{z}_2}{|\text{z}_2|^2} = \frac{(x_1 + i y_1)(x_2 - i y_2)}{x_2^2 + y_2^2} = \frac{x_1 x_2 + y_1 y_2}{x_2^2 + y_2^2} + i \frac{x_2 y_1 - x_1 y_2}{x_2^2 + y_2^2}.
\]

In particular, for \( z = x + iy \),

\[
\frac{1}{z} = \frac{\bar{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2} = \frac{x}{x^2 + y^2} - i \frac{y}{x^2 + y^2}.
\]

**Properties:**

\[
\overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2, \quad \overline{z_1 - z_2} = \overline{z}_1 - \overline{z}_2
\]

\[
\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2, \quad \frac{\overline{z}_1}{\overline{z}_2} = \frac{z_1}{z_2}
\]

\[
|\overline{z}| = |z|, \quad z \overline{z} = |z|^2, \quad |z_1 z_2| = |z_1| |z_2|
\]

\[
|z^n| = |z|^n, \quad \frac{|z_1|}{|z_2|} = \frac{z_1}{z_2}
\]

**Exercise:** Given the complex numbers \( z_1 = 3 - 2i \) and \( z_2 = -2 + i \), evaluate the quantities \( |z_1 \pm z_2|, \overline{z}_1 z_2 \) and \( \frac{z_1}{z_2} \).
**Polar form of a complex number**

![Diagram of a complex number in polar form]

A complex number \( z = x + iy \) corresponds to a point of the \( x\)-\( y \) plane. It may also be represented by a vector joining the origin \( O \) of the axes of the complex plane with this point. The quantities \( x \) and \( y \) are the Cartesian coordinates of the point, or, the orthogonal components of the corresponding vector. We observe that

\[
x = r \cos \theta , \quad y = r \sin \theta
\]

where

\[
r = |z| = (x^2 + y^2)^{1/2} \quad \text{and} \quad \tan \theta = \frac{y}{x}.
\]

Thus, we can write

\[
z = x + iy = r (\cos \theta + i \sin \theta)
\]

The above expression represents the **polar form** of \( z \). Note that

\[
\overline{z} = r (\cos \theta - i \sin \theta).
\]

Let \( z_1 = r_1 (\cos \theta_1 + i \sin \theta_1) \) and \( z_2 = r_2 (\cos \theta_2 + i \sin \theta_2) \) be two complex numbers. As can be shown,

\[
z_1 z_2 = r_1 r_2 [\cos (\theta_1 + \theta_2) + i \sin (\theta_1 + \theta_2)] ,
\]

\[
\frac{z_1}{z_2} = \frac{r_1}{r_2} [\cos (\theta_1 - \theta_2) + i \sin (\theta_1 - \theta_2)] .
\]

In particular, the inverse of a complex number \( z = r (\cos \theta + i \sin \theta) \) is written

\[
z^{-1} = \frac{1}{z} = \frac{1}{r} (\cos \theta - i \sin \theta) = \frac{1}{r} [\cos(-\theta) + i \sin(-\theta)] .
\]

**Exercise:** By using polar forms, show analytically that \( zz^{-1} = 1 \).
Exponential form of a complex number

We introduce the notation

\[ e^{i\theta} = \cos \theta + i \sin \theta \]

(this notation is not arbitrary but has a deeper meaning that reveals itself within the context of the theory of analytic functions). Note that

\[ e^{-i\theta} = e^{i(-\theta)} = \cos (-\theta) + i \sin (-\theta) = \cos \theta - i \sin \theta . \]

Also,

\[ |e^{i\theta}| = |e^{-i\theta}| = \cos^2 \theta + \sin^2 \theta = 1. \]

**Exercise:** Show that

\[ e^{-i\theta} = 1/e^{i\theta} = \bar{e^{i\theta}}. \]

Also show that

\[ \cos \theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \quad \sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i} . \]

The complex number \( z = r (\cos \theta + i \sin \theta) \), where \( r = |z| \), may now be expressed as follows:

\[ z = re^{i\theta} \]

It can be shown that

\[ z^{-1} = \frac{1}{z} = \frac{1}{r} e^{-i\theta} = \frac{1}{r} e^{i(-\theta)}, \quad \overline{z} = r e^{-i\theta} \]

\[ z_1 z_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}, \quad \frac{z_1}{z_2} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)} \]

where \( z_1 = \eta_1 e^{i\theta_1}, \ z_2 = \eta_2 e^{i\theta_2} \).

**Example:** The complex number \( z = \sqrt{2} - i\sqrt{2} \), with \( |z| = r = 2 \), is written

\[ z = 2 \left( \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \right) = 2 \left[ \cos \left( \frac{-\pi}{4} \right) + i \sin \left( \frac{-\pi}{4} \right) \right] = 2e^{i(-\pi/4)} = 2e^{-i\pi/4}. \]
**Powers and roots of complex numbers**

Let $z = r \cos \theta + i \sin \theta = re^{i\theta}$ be a complex number, where $r = |z|$. It can be proven that

$$z^n = r^n e^{in\theta} = r^n \cos n\theta + i \sin n\theta \quad (n = 0, \pm 1, \pm 2, \cdots).$$

In particular, for $z = \cos \theta + i \sin \theta = e^{i\theta}$ (r=1) we find the de Moivre formula

$$(\cos \theta + i \sin \theta)^n = (\cos n\theta + i \sin n\theta).$$

Note also that, for $z \neq 0$, we have that $z^0 = 1$ and $z^{-n} = 1/z^n$.

Given a complex number $z = r \cos \theta + i \sin \theta$, where $r = |z|$, an $n$th root of $z$ is any complex number $c$ satisfying the equation $c^n = z$. We write $c = \sqrt[n]{z}$. An $n$th root of a complex number admits $n$ different values given by the formula

$$c_k = \sqrt[n]{r} \left( \cos \frac{\theta + 2k\pi}{n} + i \sin \frac{\theta + 2k\pi}{n} \right), \quad k = 0, 1, 2, \cdots, (n-1).$$

**Example:** Let $z = 1$. We seek the 4th roots of unity, i.e., the complex numbers $c$ satisfying the equation $c^4 = 1$. We write

$$z = 1 \left( \cos 0 + i \sin 0 \right) \quad \text{(that is, } r = 1, \ \theta = 0).$$

Then,

$$c_k = \cos \frac{2k\pi}{4} + i \sin \frac{2k\pi}{4} = \cos \frac{k\pi}{2} + i \sin \frac{k\pi}{2}, \quad k = 0, 1, 2, 3.$$ 

We find:

$$c_0 = 1, \quad c_1 = i, \quad c_2 = -1, \quad c_3 = -i.$$ 

**Example:** Let $z = i$. We seek the square roots of $i$, that is, the complex numbers $c$ satisfying the equation $c^2 = i$. We have:

$$z = 1 \left[ \cos \left( \frac{\pi}{2} \right) + i \sin \left( \frac{\pi}{2} \right) \right] \quad \text{(that is, } r = 1, \ \theta = \pi/2);$$

$$c_k = \cos \left( \frac{\pi}{2} + 2k\pi \right) + i \sin \left( \frac{\pi}{2} + 2k\pi \right), \quad k = 0, 1;$$

$$c_0 = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} = \frac{\sqrt{2}}{2} \left( 1 + i \right),$$

$$c_1 = \cos \frac{5\pi}{4} + i \sin \frac{5\pi}{4} = -\frac{\sqrt{2}}{2} \left( 1 + i \right).$$
ALGEBRA: SOME BASIC CONCEPTS

Sets

Subset: \[ X \subseteq Y \iff (x \in X \Rightarrow x \in Y) ; \]
\[ X = Y \iff X \subseteq Y \text{ and } Y \subseteq X \]

Proper subset: \[ X \subset Y \iff X \subseteq Y \text{ and } X \neq Y \]

Union of sets: \[ X \cup Y = \{ x / x \in X \text{ or } x \in Y \} \]

Intersection of sets: \[ X \cap Y = \{ x / x \in X \text{ and } x \in Y \} \]

Disjoint sets: \[ X \cap Y = \emptyset \]

Difference of sets: \[ X - Y = \{ x / x \in X \text{ and } x \notin Y \} \]

Complement of a subset: \[ X \supset Y \text{ ; } X \setminus Y = X - Y \]

Cartesian product: \[ X \times Y = \{(x, y) / x \in X \text{ and } y \in Y \} \]

Mapping: \[ f : X \rightarrow Y \text{ ; } (x \in X) \rightarrow y = f(x) \in Y \]

Domain/range of \( f \): \[ D(f) = X, \quad R(f) = f(X) = \{ f(x) / x \in X \} \subseteq Y ; \]
\( f \) is defined in \( X \) and has values in \( Y \);
y = f(x) is the image of \( x \) under \( f \)

Composite mapping: \[ f : X \rightarrow Y, \quad g : Y \rightarrow Z ; \]
\[ f \circ g : X \rightarrow Z \text{ ; } (x \in X) \rightarrow g(f(x)) \in Z \]

Injective (1-1) mapping: \[ f(x_1) = f(x_2) \iff x_1 = x_2 \text{ , or } \]
x_1 \neq x_2 \iff f(x_1) \neq f(x_2)

Surjective (onto) mapping: \( f(X) = Y \)

Bijective mapping: \( f \) is both injective and surjective \( \Rightarrow \) invertible

Identity mapping: \[ f_{id} : X \rightarrow X; \quad f_{id}(x) = x, \quad \forall x \in X \]

Internal operation on \( X \): \[ X \times X \rightarrow X \text{ ; } [(x, y) \in X \times X] \rightarrow z \in X \]

External operation on \( X \): \[ A \times X \rightarrow X \text{ ; } [(a, x) \in A \times X] \rightarrow y = a \cdot x \in X \]
Groups

A group is a set $G$, together with an internal operation $G \times G \to G$; $(x, y) \mapsto z = x \cdot y$, such that:

1. The operation is associative: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\exists e \in G$ (identity): $x \cdot e = e \cdot x = x$, $\forall x \in G$
3. $\forall x \in G$, $\exists x^{-1} \in G$ (inverse): $x^{-1} \cdot x = x \cdot x^{-1} = e$

A group $G$ is abelian or commutative if $x \cdot y = y \cdot x$, $\forall x, y \in G$.

A subset $S \subseteq G$ is a subgroup of $G$ if $S$ is itself a group (clearly, then, $S$ contains the identity $e$ of $G$, as well as the inverse of every element of $S$).

Vector space over $R$

Let $V = \{x, y, z, \ldots \}$, and let $a, b, c, \ldots \in R$. Consider an internal operation $+$ and an external operation $\cdot$ on $V$:

$+$ : $V \times V \to V$; $x + y = z$
$\cdot$ : $R \times V \to V$; $a \cdot x = y$

Then, $V$ is a vector space over $R$ iff

1. $V$ is a commutative group with respect to $+$. The identity element is denoted $0$, while the inverse of $x$ is denoted $-x$.
2. The operation $\cdot$ satisfies the following:
   
   $a \cdot (b \cdot x) = (a b) \cdot x$
   
   $a \cdot (x + y) = a \cdot x + a \cdot y$
   
   $1 \cdot x = x$, $0 \cdot x = 0$

A set $\{x_1, x_2, \ldots, x_k\}$ of elements of $V$ is linearly independent iff the equation\(^1\)

\[c_1 x_1 + c_2 x_2 + \ldots + c_k x_k = 0\]

can only be satisfied for $c_1 = c_2 = \ldots = c_k = 0$; otherwise, the set is linearly dependent. The dimension $\dim V$ of $V$ is the largest number of vectors in $V$ that constitute a linearly independent set. If $\dim V = n$, then any system $\{e_1, e_2, \ldots, e_n\}$ of $n$ linearly independent elements is a basis for $V$, and any $x \in V$ can be uniquely expressed as $x = c_1 e_1 + c_2 e_2 + \ldots + c_n e_n$.

A subset $S \subseteq V$ is a subspace of $V$ if $S$ is itself a vector space under the operations $(+)$ and $(\cdot)$. In particular, the sum $x + y$ of any two elements of $S$, as well as the scalar multiple $ax$ and the inverse $-x$ of any element $x$ of $S$, must belong to $S$. Clearly, this set must contain the identity $0$ of $V$. If $S$ is a subspace of $V$, then $\dim S \leq \dim V$. In particular, $S$ coincides with $V$ iff $\dim S = \dim V$.

\(^1\) The symbol $(\cdot)$ will often be omitted in the sequel.
Functionals

A functional \( \omega \) on a vector space \( V \) is a mapping \( \omega: V \to \mathbb{R} \); \( (x \in V) \to t = \omega(x) \in \mathbb{R} \).

The functional \( \omega \) is linear if \( \omega(ax+by) = a\omega(x) + b\omega(y) \). The collection of all linear functionals on \( V \) is called the dual space of \( V \), denoted \( V^* \). It is itself a vector space over \( \mathbb{R} \), and \( \dim V^* = \dim V \).

Algebras

A real algebra \( A \) is a vector space over \( \mathbb{R} \) equipped with a binary operation \((\cdot | \cdot): A \times A \to A \); \( (x | y) = z \), such that, for \( a, b \in \mathbb{R} \),

\[
(ax + by | z) = a \cdot (x | z) + b \cdot (y | z)
\]

\[
(x | ay + bz) = a \cdot (x | y) + b \cdot (x | z)
\]

An algebra is commutative if, for any two elements \( x, y \), \( (x | y) = (y | x) \); it is associative if, for any \( x, y, z \), \( (x | (y | z)) = ((x | y) | z) \).

Example: The set \( \Lambda^0(\mathbb{R}^n) \) of all functions on \( \mathbb{R}^n \) is a commutative, associative algebra. The multiplication operation \((\cdot | \cdot) : \Lambda^0(\mathbb{R}^n) \times \Lambda^0(\mathbb{R}^n) \to \Lambda^0(\mathbb{R}^n) \) is defined by

\[
(f | g)(x^1, \ldots, x^n) = f(x^1, \ldots, x^n) g(x^1, \ldots, x^n)
\]

Example: The set of all \( n \times n \) matrices is an associative, non-commutative algebra. The binary operation \((\cdot | \cdot) \) is matrix multiplication.

A subspace \( S \) of \( A \) is a subalgebra of \( A \) if \( S \) is itself an algebra under the same binary operation \((\cdot | \cdot) \). In particular, \( S \) must be closed under this operation; i.e., \( (x | y) \in S \) for any \( x, y \) in \( S \). We write: \( S \subseteq A \).

A subalgebra \( S \subseteq A \) is an ideal of \( A \) iff \( (x | y) \in S \) and \( (y | x) \in S \), for any \( x \in S, y \in A \).

Modules

Note first that \( \mathbb{R} \) is an associative, commutative algebra under the usual operations of addition and multiplication. Thus, a vector space over \( \mathbb{R} \) is a vector space over an associative, commutative algebra. More generally, a module \( M \) over \( A \) is a vector space over an associative but (generally) non-commutative algebra. In particular, the external operation \((\cdot) \) on \( M \) is defined by

\[
\cdot: A \times M \to M ; \quad ax = y \quad (a \in A ; \ x, y \in M)
\]

Example: The collection of all \( n \)-dimensional column matrices, with \( A \) taken to be the algebra of \( n \times n \) matrices, and with matrix multiplication as the external operation.
Vector fields

A vector field $V$ on $\mathbb{R}^n$ is a map from a domain of $\mathbb{R}^n$ into $\mathbb{R}^n$:

$$V : \mathbb{R}^n \supseteq U \to \mathbb{R}^n ; \quad [x = (x^1, \ldots, x^n) \in U \to V(x) = (V^1(x), \ldots, V^n(x)) \in \mathbb{R}^n].$$

The vector $x$ represents a point in $U$, with coordinates $(x^1, \ldots, x^n)$. The functions $V^i(x)$ ($i=1,\ldots,n$) are the components of $V$ in the coordinate system $(x^i)$.

Given two vector fields $U$ and $V$, we can construct a new vector field $W=U+V$ such that $W(x)=U(x)+V(x)$. The components of $W$ are the sums of the respective components of $U$ and $V$.

Given a vector field $V$ and a constant $a \in \mathbb{R}$, we can construct a new vector field $Z=aV$ such that $Z(x)=aV(x)$. The components of $Z$ are scalar multiples (by $a$) of those of $V$.

It follows from the above that the collection of all vector fields on $\mathbb{R}^n$ is a vector space over $\mathbb{R}$.

More generally, given a vector field $V$ and a function $f \in \Lambda^0(\mathbb{R}^n)$, we can construct a new vector field $Z=fV$ such that $Z(x)=f(x)V(x)$. Given that $\Lambda^1(\mathbb{R}^n)$ is an associative algebra, we conclude that the collection of all vector fields on $\mathbb{R}^n$ is a module over $\Lambda^0(\mathbb{R}^n)$ (in this particular case, the algebra $\Lambda^0(\mathbb{R}^n)$ is commutative).

A note on linear independence:

Let $\{V_1, \ldots, V_r\} = \{V_a\}$ be a collection of vector fields on $\mathbb{R}^n$.

(a) The set $\{V_a\}$ is linearly dependent over $\mathbb{R}$ (linearly dependent with constant coefficients) iff there exist real constants $c_1, \ldots, c_r$, not all zero, such that

$$c_1 V_1(x) + \ldots + c_r V_r(x) = 0 , \quad \forall x \in \mathbb{R}^n. $$

If the above relation is satisfied only for $c_1 = \ldots = c_r = 0$, the set $\{V_a\}$ is linearly independent over $\mathbb{R}$.

(b) The set $\{V_a\}$ is linearly dependent over $\Lambda^0(\mathbb{R}^n)$ iff there exist functions $f_1(x)$, ..., $f_r(x)$, not all identically zero over $\mathbb{R}^n$, such that

$$f_1(x) V_1(x) + \ldots + f_r(x) V_r(x) = 0 , \quad \forall x \equiv (x) \in \mathbb{R}^n. $$

If this relation is satisfied only for $f_1(x)=\ldots=f_r(x) \equiv 0$, the set $\{V_a\}$ is linearly independent over $\Lambda^0(\mathbb{R}^n)$.

There can be at most $n$ elements in a linearly independent system over $\Lambda^0(\mathbb{R}^n)$. These elements form a basis $\{e_1, \ldots, e_n\}=\{e_k\}$ for the module of all vector fields on $\mathbb{R}^n$. An element of this module, i.e. an arbitrary vector field $V$, is written as a linear combination of the $\{e_k\}$ with coefficients $V^k \in \Lambda^0(\mathbb{R}^n)$. Thus, at any point $x \equiv (x^i) \in \mathbb{R}^n$, ...
\[ V(x) = V^1(x^k) e_1 + ... + V^n(x^k) e_n \equiv (V^1(x^k), ..., V^n(x^k)) . \]

In particular, in the basis \{\(e_k\)\},

\[ e_1 \equiv (1,0,0,0,0), \quad e_2 \equiv (0,1,0,0,0), \quad \ldots , e_n \equiv (0,0,0,0,1) . \]

**Example:** Let \( n=3 \), i.e., \( \mathbb{R}^n=\mathbb{R}^3 \). Call \{\(e_1, e_2, e_3\)\} \(= \{i, j, k\} \). Let \( V \) be a vector field on \( \mathbb{R}^3 \). Then, at any point \( x \equiv (x, y, z) \in \mathbb{R}^3 \),

\[ V(x) = V_1(x, y, z) i + V_2(x, y, z) j + V_3(x, y, z) k \equiv (V_x, V_y, V_z) . \]

Now, consider the six vector fields

\[ V_1 = i , \quad V_2 = j , \quad V_3 = k , \quad V_4 = y j - y i , \quad V_5 = y k - z j , \quad V_6 = z i - x k . \]

Clearly, the \{\(V_1, V_2, V_3\)\} are linearly independent over \( \Lambda^0(\mathbb{R}^3) \), since they constitute the basis \( \{i, j, k\} \). On the other hand, the \( V_4, V_5, V_6 \) are separately linearly dependent on the \{\(V_1, V_2, V_3\)\} over \( \Lambda^0(\mathbb{R}^3) \). Moreover, the set \{\(V_4, V_5, V_6\)\} is also linearly dependent over \( \Lambda^2(\mathbb{R}^3) \), since \( z V_4 + x V_5 + y V_6 = 0 \). Thus, the set \{\(V_1, \ldots, V_6\)\} is linearly dependent over \( \Lambda^1(\mathbb{R}^3) \). On the other hand, the system \{\(V_1, \ldots, V_6\)\} is linearly independent over \( \mathbb{R} \), since the equation \( c_1 V_1 + \ldots + c_6 V_6 = 0 \), with \( c_1 , \ldots , c_6 \in \mathbb{R} \) (constant coefficients), can only be satisfied for \( c_1 = \ldots = c_6 = 0 \). In general,

*there is an infinite number of linearly independent vector fields on \( \mathbb{R}^n \) over \( \mathbb{R} \), but only \( n \) linearly independent fields over \( \Lambda^0(\mathbb{R}^n) \).*

**Derivation on an algebra**

Let \( L \) be an operation on an algebra \( A \) (an operator on \( A \)):

\[ L : A \rightarrow A ; \quad (x \in A) \rightarrow y = Lx \in A . \]

\( L \) is a derivation on \( A \) iff, \( \forall x, y \in A \) and \( a, b \in \mathbb{R} \),

\[ L(ax+by) = aL(x) + bL(y) \quad \text{(linearity)} \]

\[ L(x \mid y) = (Lx \mid y) + (x \mid Ly) \quad \text{(Leibniz rule)} \]

**Example:** Let \( A=\Lambda^0(\mathbb{R}^n)=\{ f(x^1, \ldots, x^n) \} \), and let \( L \) be the linear operator

\[ L = \phi^1(x^k) \partial / \partial x^1 + \ldots + \phi^n(x^k) \partial / \partial x^n \equiv \phi^i(x^k) \partial / \partial x^i , \]

where the \( \phi^i(x^k) \) are given functions. As can be shown,

\[ L \left[ f(x^k) g(x^k) \right] = [L f(x^k)] g(x^k) + f(x^k) L g(x^k) . \]

Hence, \( L \) is a derivation on \( \Lambda^0(\mathbb{R}^n) \).
Lie algebra

An algebra \( \mathcal{L} \) over \( R \) is a (real) Lie algebra with binary operation \( [\cdot, \cdot]: \mathcal{L} \times \mathcal{L} \to \mathcal{L} \) (Lie bracket) iff this operation satisfies the properties:

\[
[ax + by, z] = a[x, z] + b[y, z] \\
[x, y] = -[y, x] \quad (\text{antisymmetry}) \\
[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0 \quad (\text{Jacobi identity})
\]

(where \( x, y, z \in \mathcal{L} \) and \( a, b \in R \)). Note that, by the antisymmetry of the Lie bracket, the first and third properties are written, alternatively,

\[
[ax + by + bz] = a[x, y] + b[x, z], \\
[[x, y], z] + [[y, z], x] + [[z, x], y] = 0.
\]

A Lie algebra is a non-associative algebra, since, as follows by the above properties,

\[
[x, [y, z]] \neq [[x, y], z].
\]

Example: The algebra of \( n \times n \) matrices, with \( [A, B] = AB - BA \) (commutator).

Example: The algebra of all vectors in \( \mathbb{R}^3 \), with \( [a, b] = a \times b \) (vector product).

Lie algebra of derivations

Consider the algebra \( A = \Lambda^0(\mathbb{R}^n) = \{ f(x^1, \ldots, x^n) \} \). Consider also the set \( D(A) \) of linear operators on \( A \), of the form

\[
L = \varphi^i(x^i) \frac{\partial}{\partial x^i} \quad (\text{sum on } i = 1, 2, \ldots, n).
\]

These first-order differential operators are derivations on \( A \) (the Leibniz rule is satisfied). Now, given two such operators \( L_1, L_2 \), we construct the linear operator (Lie bracket of \( L_1 \) and \( L_2 \)), as follows:

\[
[L_1, L_2] = L_1 L_2 - L_2 L_1; \\
[L_1, L_2] f(x^k) = L_1(L_2 f(x^k)) - L_2(L_1 f(x^k)) .
\]

It can be shown that \( [L_1, L_2] \) is a first-order differential operator (a derivation), hence is a member of \( D(A) \). (This is not the case with second-order operators like \( L_1 L_2 \)!) Moreover, the Lie bracket of operators satisfies all the properties of the Lie bracket of a general Lie algebra (such as antisymmetry and Jacobi identity). It follows that

the set \( D(A) \) of derivations on \( \Lambda^0(\mathbb{R}^n) \) is a Lie algebra, with binary operation defined as the Lie bracket of operators.
**Direct sum of subspaces**

Let $V$ be a vector space over a field $K$ (where $K$ may be $R$ or $C$), of dimension $\dim V=n$. Let $S_1$, $S_2$ be disjoint (i.e., $S_1 \cap S_2 = \{0\}$) subspaces of $V$. We say that $V$ is the direct sum of $S_1$ and $S_2$ if each vector of $V$ can be uniquely represented as the sum of a vector of $S_1$ and a vector of $S_2$. We write: $V = S_1 \oplus S_2$. In terms of dimensions, $\dim V = \dim S_1 + \dim S_2$. We similarly define the vector sum of three subspaces of $V$, each of which is disjoint from the direct sum of the other two (i.e., $S_1 \cap (S_2 \oplus S_3) = \{0\}$, etc.).

**Homomorphism of vector spaces**

Let $V$, $W$ be vector spaces over a field $K$. A mapping $\Phi: V \rightarrow W$ is said to be a linear mapping or homomorphism if it preserves linear operations, i.e.,

$$\Phi(x+y) = \Phi(x) + \Phi(y), \quad \Phi(kx) = k \Phi(x), \quad \forall \, x, y \in V \text{ and } k \in K.$$

A homomorphism which is also bijective (1-1) is called an isomorphism.

The set of vectors $x \in V$ mapping under $\Phi$ into the zero of $W$ is called the kernel of the homomorphism $\Phi$:

$$\text{Ker } \Phi = \{ x \in V : \Phi(x) = 0 \}.$$

Note that $\Phi(0)=0$, for any homomorphism (clearly, the two zeros refer to different vector spaces). Thus, in general, $0 \in \text{Ker } \Phi$.

If $\text{Ker } \Phi = \{0\}$, then the homomorphism $\Phi$ is also an isomorphism of $V$ onto a subspace of $W$. If, moreover, $\dim V = \dim W$, then the map $\Phi: V \rightarrow W$ is itself an isomorphism. In this case, $\text{Im } \Phi = W$, where, in general, $\text{Im } \Phi$ (image of the homomorphism) is the collection of images of all vectors of $V$ under the map $\Phi$.

**The algebra of linear operators**

Let $V$ be a vector space over a field $K$. A linear operator $A$ on $V$ is a homomorphism $A : V \rightarrow V$. Thus,

$$A(x+y) = A(x) + A(y), \quad A(kx) = kA(x), \quad \forall \, x, y \in V \text{ and } k \in K.$$

The sum $A + B$ and the scalar multiplication $kA$ ($k \in K$) are linear operators defined by

$$(A + B)x = A x + B x, \quad (kA)x = k(Ax).$$

Under these operations, the set $\text{Opt}(V)$ of all linear operators on $V$ is a vector space. The zero element of that space is a zero operator $0$ such that $0x=0$, $\forall \, x \in V$.  

19
Since \( A \) and \( B \) are mappings, their composition may be defined. This is regarded as their product \( AB \):

\[
(AB)x \equiv A(Bx) \quad \forall x \in V.
\]

Note that \( AB \) is a linear operator on \( V \), hence belongs to \( \text{Op}(V) \). In general, operator products are non-commutative: \( AB \neq BA \). However, they are associative and distributive over addition:

\[
(AB)C = A(BC) \equiv ABC, \quad A(B+C) = AB + AC.
\]

The identity operator \( E \) is the mapping of \( \text{Op}(V) \) which leaves every element of \( V \) fixed: \( E x = x \). Thus, \( AE = EA = A \). Operators of the form \( kE \) \((k \in K)\), called scalar operators, are commutative with all operators. In fact, any operator commutative with every operator of \( \text{Op}(V) \) is a scalar operator.

It follows from the above that the set \( \text{Op}(V) \) of all linear operators on a given vector space \( V \) is an algebra. This algebra is associative but (generally) non-commutative.

An operator \( A \) is said to be invertible if it represents a bijective (1-1) mapping, i.e., if it is an isomorphism of \( V \) onto itself. In this case, an inverse operator \( A^{-1} \) exists such that \( AA^{-1} = A^{-1}A = E \). Practically this means that, if \( A \) maps \( x \in V \) onto \( y \in V \), then \( A^{-1} \) maps \( y \) back onto \( x \). For an invertible operator \( A \), \( \ker A = \{0\} \) and \( \text{im} A = V \).

**Matrix representation of a linear operator**

Let \( A \) be a linear operator on \( V \). Let \( \{e_i\} \) \((i=1,...,n)\) be a basis of \( V \). Let

\[
A e_k = e_i A_{ik} \quad \text{(sum on } i)\]

where the \( A_{ik} \) are real or complex, depending on whether \( V \) is a vector space over \( R \) or \( C \). The \( n \times n \) matrix \( A = [A_{ik}] \) is called the matrix of the operator \( A \) in the basis \( \{e_i\} \).

Now, let \( x = x_i e_i \) (sum on \( i \)) be a vector in \( V \), and let \( y = A x \). If \( y = y_i e_i \), then, by the linearity of \( A \),

\[
y_i = A_{ik} x_k \quad \text{(sum on } k)\.
\]

In matrix form,

\[
[y]_{n \times 1} = [A]_{n \times n} [x]_{n \times 1}.
\]

Next, let \( A, B \) be linear operators on \( V \). Define their product \( C = AB \) by

\[
Cx = (AB)x \equiv A(Bx) \quad x \in V.
\]

Then, for any basis \( \{e_i\} \),

\[
Ce_k = A(Be_k) = e_i A_{ij} B_{jk} = e_i C_{ik} \quad \Rightarrow
\]
\[ C_{ik} = A_{ij} B_{jk} \]

or, in matrix form,

\[ C = A B . \]

That is,

the matrix of the product of two operators is the product of the matrices of these operators, in any basis of \( V \).

Consider now a change of basis defined by the transition matrix \( T = [T_{ik}] \):

\[ e_k' = e_i T_{ik} . \]

The inverse transformation is

\[ e_k = e_i' (T^{-1})_{ik} . \]

Under this basis change, the matrix \( A \) of an operator \( A \) transforms as

\[ A' = T^{-1} A T \quad \text{(similarity transformation)} . \]

Under basis transformations, the trace and the determinant of \( A \) remain unchanged:

\[ tr A' = tr A , \quad det A' = det A . \]

An operator \( A \) is said to be nonsingular (singular) if \( detA \neq 0 \) (\( detA = 0 \)). Note that this is a basis-independent property. Any nonsingular operator is invertible, i.e., there exists an inverse operator \( A^{-1} \in Op(V) \) such that \( A A^{-1} = A^{-1} A = E \). Since an invertible operator represents a bijective mapping (i.e., both 1-1 and onto), it follows that \( \text{Ker} A = \{0\} \) and \( \text{Im} A = V \). If \( A \) is invertible (nonsingular), then, for any basis \( \{e_i\} \) \((i = 1, \ldots, n)\) of \( V \), the vectors \( \{A e_i\} \) are linearly independent and hence also constitute a basis.

**Invariant subspaces and eigenvectors**

Let \( V \) be an \( n \)-dimensional vector space over a field \( K \), and let \( A \) be a linear operator on \( V \). The subspace \( S \) of \( V \) is said to be invariant under \( A \) if, for every vector \( x \) of \( S \), the vector \( A x \) again belongs to \( S \). Symbolically, \( A S \subseteq S \).

A vector \( x \neq 0 \) is said to be an eigenvector of \( A \) if it generates a one-dimensional invariant subspace of \( V \) under \( A \). This means that an element \( \lambda \in K \) exists, such that

\[ A x = \lambda x . \]

The element \( \lambda \) is called an eigenvalue of \( A \), to which eigenvalue the eigenvector \( x \) belongs. Note that, trivially, the null vector \( 0 \) is an eigenvector of \( A \), belonging to any
eigenvalue $\lambda$. The set of all eigenvectors of $A$, belonging to a given $\lambda$, is a subspace of $V$ called the proper subspace belonging to $\lambda$.

It can be shown that the eigenvalues of $A$ are basis-independent quantities. Indeed, let $A=[A_{ik}]$ be the $(n\times n)$ matrix representation of $A$ in some basis $\{e_i\}$ of $V$, and let $x=x_ie_i$ be an eigenvector belonging to $\lambda$. We denote by $X=[x_i]$ the column vector representing $x$ in that basis. The eigenvalue equation for $A$ is written, in matrix form,

$$A_{ik}x_k = \lambda x_i \quad \text{or} \quad A X = \lambda X .$$

This is written

$$(A-\lambda 1_n) X = 0 .$$

This equation constitutes a linear homogeneous system for $X=[x_i]$, which has a nontrivial solution iff

$$\det (A-\lambda 1_n) = 0 .$$

This polynomial equation determines the eigenvalues $\lambda_i \ (i=1,...,n)$ (not necessarily all different from each-other) of $A$. Since the determinant of the matrix representation of an operator [in particular, of the operator $(A-\lambda E)$ for any given $\lambda$] is a basis-independent quantity, it follows that, if the above equation is satisfied for a certain $\lambda$ in a certain basis (where $A$ is represented by the matrix $A$), it will also be satisfied for the same $\lambda$ in any other basis (where $A$ is represented by another matrix, say, $A \,'$). We conclude that the eigenvalues of an operator are a property of the operator itself and do not depend on the choice of basis of $V$.

If we can find $n$ linearly independent eigenvectors $\{x_i\}$ of $A$, belonging to the corresponding eigenvalues $\lambda_i$, we can use these vectors to define a basis for $V$. In this basis, the matrix representation of $A$ has a particularly simple diagonal form:

$$A = \text{diag} \ (\lambda_1, \ldots, \lambda_n) .$$

Using this expression, and the fact that the quantities $\text{tr}A$, $\det A$ and $\lambda_i$ are invariant under basis transformations, we conclude that, in any basis of $V$,

$$\text{tr}A = \lambda_1 + \lambda_2 + \ldots + \lambda_n , \quad \det A = \lambda_1 \lambda_2 \ldots \lambda_n .$$

We note, in particular, that all eigenvalues of an invertible (nonsingular) operator are nonzero. Indeed, if even one is zero, then $\det A=0$ and $A$ is singular.

An operator $A$ is called nilpotent if $A^m=0$ for some natural number $m>1$. The smallest such value of $m$ is called the degree of nilpotency, and it cannot exceed $n$. All eigenvalues of a nilpotent operator are zero. Thus, such an operator is singular (non-invertible).

An operator $A$ is called idempotent (or projection operator) if $A^2=A$. It follows that $A^n=A$, for any natural number $m$. The eigenvalues of an idempotent operator can take the values 0 or 1.
BASIC MATRIX PROPERTIES

\[(A + B)^T = A^T + B^T \quad \text{and} \quad (AB)^T = B^T A^T\]
\[(A + B)^\dagger = A^\dagger + B^\dagger \quad \text{where} \quad M^\dagger \equiv (M^T)^\ast = (M^\ast)^T\]
\[(kA)^T = kA^T \quad \text{and} \quad (kA)^\dagger = k^\ast A^\dagger \quad (k \in C)\]
\[(AB)^{-1} = B^{-1} A^{-1} \quad \text{and} \quad (A^T)^{-1} = (A^{-1})^T \quad \text{and} \quad (A^\dagger)^{-1} = (A^{-1})^\dagger\]
\[[A, B]^T = [B^T, A^T] \quad \text{and} \quad [A, B]^\dagger = [B^\dagger, A^\dagger]\]

\[A^{-1} = \frac{1}{\det A} \text{adj} A \quad (\det A \neq 0)\]
\[
\begin{bmatrix}
a & b \\
c & d \\
\end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix}
d & -b \\
-c & a \\
\end{bmatrix}
\]

tr(κA + λB) = κtrA + λtrB

trA^T = trA \quad \text{and} \quad trA^\dagger = (trA)^\ast

tr(AB) = tr(BA), \quad tr(ABC) = tr(BCA) = tr(CAB), \quad \text{etc.}

\[tr[A, B] = 0\]

\[\det A^T = \det A \quad \text{and} \quad \det A^\dagger = (\det A)^\ast\]

\[\det(AB) = \det(BA) = \det A \cdot \det B\]

\[\det(A^{-1}) = 1/\det A\]

\[\det(cA) = c^n \det A \quad (c \in C, \ A \in gl(n, C))\]

If any row or column of A is multiplied by c, then so is det A.

\[[A, B] = -[B, A] \equiv AB - BA\]
\[[A, B + C] = [A, B] + [A, C] \quad \text{and} \quad [A + B, C] = [A, C] + [B, C]\]
\[[A, BC] = [A, B][C + B[A, C]] \quad \text{and} \quad [AB, C] = A[B, C] + [A, C]B\]
\[[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0\]
\[[[A, B], C] + [[B, C], A] + [[C, A], B] = 0\]

Let \(A = A(t) = [a_{ij}(t)], \ B = B(t) = [b_{ij}(t)], \) be \((n\times n)\) matrices. The derivative of A (similarly, of B) is the \((n\times n)\) matrix \(dA/dt\), with elements

\[
\left(\frac{dA}{dt}\right)_{ij} = \frac{d}{dt} a_{ij}(t) \quad .
\]

The integral of A (similarly, of B) is the \((n\times n)\) matrix defined by

\[
\left(\int A(t) \, dt\right)_{ij} = \int a_{ij}(t) \, dt \quad .
\]
\[
\frac{d}{dt} (A \pm B) = \frac{dA}{dt} \pm \frac{dB}{dt} ; \quad \frac{d}{dt} (AB) = \frac{dA}{dt} B + A \frac{dB}{dt}
\]
\[
\frac{d}{dt} [A, B] = \left[ \frac{dA}{dt}, B \right] + \left[ A, \frac{dB}{dt} \right]
\]
\[
\frac{d}{dt} (A^{-1}) = -A^{-1} \frac{dA}{dt} A^{-1} \quad \Rightarrow \quad d (A^{-1}) = -A^{-1} (dA) A^{-1}
\]
\[
tr \left( \frac{dA}{dt} \right) = \frac{d}{dt} (trA)
\]

Let \( A = A(x, y) \). Call \( \partial_\alpha / \partial x \equiv \partial_x A \equiv A_x \), etc.:
\[
\partial_x (A^{-1} A_x) - \partial_y (A^{-1} A_y) + [A^{-1} A_x, A^{-1} A_y] = 0
\]
\[
\partial_x (A_x A^{-1}) - \partial_y (A_x A^{-1}) - [A_x A^{-1}, A_y A^{-1}] = 0
\]
\[
A(A^{-1} A_x)_y A^{-1} = (A_y A^{-1})_x \Leftrightarrow A^{-1} (A_y A^{-1})_x A = (A^{-1} A_x)_y
\]

\[
e^A = \exp A = \sum_{n=0}^{\infty} \frac{A^n}{n!} = 1 + A + \frac{A^2}{2} + \cdots
\]
\[
B e^A B^{-1} = e^{BAB^{-1}}
\]
\[
(e^A)^* = e^{A^*} ; \quad (e^A)^T = e^{A^T} ; \quad (e^A)^* = e^{A^*} ; \quad (e^A)^{-1} = e^{-A}
\]
\[
e^A e^B = e^B e^A = e^{A+B} \quad \text{when} \quad [A, B] = 0
\]
In general, \( e^A e^B = e^C \) where
\[
C = A + B + \frac{1}{2} [A, B] + \frac{1}{12} ([A, [A, B]] + [B, [B, A]]) + \cdots
\]

By definition, \( \log B = A \Leftrightarrow B = e^A \).
\[
\det (e^A) = e^{trA} \Leftrightarrow \det B = e^{tr(\log B)} \Leftrightarrow tr (\log B) = \log (\det B)
\]
\[
\det (1 + \delta A) \simeq 1 + tr \delta A , \quad \text{for infinitesimal} \quad \delta A
\]
\[
tr (A^{-1} A_x) = tr (A_x A^{-1}) = tr (\log A)_x = [tr (\log A)]_x = [\log (\det A)]_x
\]