Costas J. Papachristou

MATHEMATICAL HANDBOOK

2022

MATHEMATICAL FORMULAS AND PROPERTIES

Trigonometric formulas

$$\sin^2 A + \cos^2 A = 1 \quad ; \quad \tan x = \frac{\sin x}{\cos x} \quad ; \quad \cot x = \frac{\cos x}{\sin x} = \frac{1}{\tan x}$$

$$\cos^2 x = \frac{1}{1+\tan^2 x} \quad ; \quad \sin^2 x = \frac{1}{1+\cot^2 x} = \frac{\tan^2 x}{1+\tan^2 x}$$

$$\sin(A \pm B) = \sin A \cos B \pm \cos A \sin B$$

$$\cos(A \pm B) = \cos A \cos B \mp \sin A \sin B$$

$$\tan(A \pm B) = \frac{\tan A \pm \tan B}{1 \mp \tan A \tan B} \quad , \quad \cot(A \pm B) = \frac{\cot A \cot B \mp 1}{\cot B \pm \cot A}$$

$$\sin 2A = 2 \sin A \cos A$$

$$\cos 2A = \cos^2 A - \sin^2 A = 2\cos^2 A - 1 = 1 - 2\sin^2 A$$

$$\tan 2A = \frac{2\tan A}{1-\tan^2 A} \quad , \quad \cot 2A = \frac{\cot^2 A - 1}{2\cot A}$$

$$\sin A + \sin B = 2\sin\frac{A+B}{2}\cos\frac{A-B}{2}$$

$$\sin A - \sin B = 2\sin\frac{A-B}{2}\cos\frac{A+B}{2}$$

$$\cos A + \cos B = 2\cos\frac{A+B}{2}\cos\frac{A-B}{2}$$

$$\cos A - \cos B = 2\sin\frac{A+B}{2}\sin\frac{B-A}{2}$$

$$\sin A \sin B = \frac{1}{2}[\cos(A-B) - \cos(A+B)]$$

$$\cos A \cos B = \frac{1}{2}[\cos(A+B) + \cos(A-B)]$$

$$\sin A \cos B = \frac{1}{2}[\sin(A+B) + \sin(A-B)]$$

$$\sin(-A) = -\sin A \quad , \quad \cos(-A) = \cos A$$

$$\tan(-A) = -\tan A \quad , \quad \cot(-A) = -\cot A$$

$$\sin(\frac{\pi}{2} \pm A) = \cos A \quad , \quad \cos(\frac{\pi}{2} \pm A) = \mp \sin A$$

$$\sin(\pi \pm A) = \mp \sin A \quad , \quad \cos(\pi \pm A) = -\cos A$$

	sin	cos	tan	cot
0	0	1	0	∞
$\pi/6 = 30^{\circ}$	$\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{3}$	$\sqrt{3}$
$\pi/4 = 45^{\circ}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{2}}{2}$	1	1
$\pi/3 = 60^{\circ}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$	$\sqrt{3}$	$\frac{\sqrt{3}}{3}$
$\pi/2 = 90^{\circ}$	1	0	∞	0
$\pi = 180^{\circ}$	0	–1	0	∞

Basic trigonometric equations

$$\sin x = \sin\alpha \;\Rightarrow\; \begin{cases} x=\alpha+2k\pi \\ x=(2k+1)\pi-\alpha \end{cases} \qquad (k = 0, \pm1, \pm2, \cdots)$$

$$\cos x = \cos\alpha \;\Rightarrow\; \begin{cases} x=\alpha+2k\pi \\ x=2k\pi-\alpha \end{cases} \qquad (k = 0, \pm1, \pm2, \cdots)$$

$$\tan x = \tan\alpha \;\Rightarrow\; x = \alpha + k\pi \qquad (k = 0, \pm1, \pm2, \cdots)$$

$$\cot x = \cot\alpha \;\Rightarrow\; x = \alpha + k\pi \qquad (k = 0, \pm1, \pm2, \cdots)$$

$$\sin x = -\sin\alpha \;\Rightarrow\; \begin{cases} x=2k\pi-\alpha \\ x=\alpha+(2k+1)\pi \end{cases} \qquad (k = 0, \pm1, \pm2, \cdots)$$

$$\cos x = -\cos\alpha \;\Rightarrow\; \begin{cases} x=(2k+1)\pi-\alpha \\ x=\alpha+(2k+1)\pi \end{cases} \qquad (k = 0, \pm1, \pm2, \cdots)$$

Hyperbolic functions

$$\cosh x = \frac{e^x + e^{-x}}{2} \quad ; \quad \sinh x = \frac{e^x - e^{-x}}{2} \quad ; \quad \tanh x = \frac{\sinh x}{\cosh x} = \frac{e^x - e^{-x}}{e^x + e^{-x}} = \frac{1}{\coth x}$$

$$\cosh^2 x - \sinh^2 x = 1$$

$$\cosh(-x) = \cosh x \quad , \quad \sinh(-x) = -\sinh x$$

Power formulas

$$(a \pm b)^2 = a^2 \pm 2ab + b^2$$

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

$$a^2 - b^2 = (a+b)(a-b)$$

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

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

Quadratic equation: $ax^2 + bx + c = 0$

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

Roots: $x = \dfrac{-b \pm \sqrt{D}}{2a}$

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 : $A= (1/2)bh$

Trapezoid of altitude h and parallel sides a and b : $A= (1/2)(a+b)h$

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 : $A=4\pi r^2$, $V= (4/3)\pi r^3$

Circular cone of radius r and height h : $V= (1/3)\pi r^2 h$

Properties of inequalities

$a < b \;\; and \;\; b < c \;\Rightarrow\; a < c$

$a \geq b \;\; and \;\; b \geq a \;\Rightarrow\; a = b$

$a < b \;\Rightarrow\; -a > -b$

$0 < a < b \;\Rightarrow\; \dfrac{1}{a} > \dfrac{1}{b}$

$a < b \;\; and \;\; c \leq d \;\Rightarrow\; a + c < b + d$

$0 < a < b \;\; and \;\; 0 < c \leq d \;\Rightarrow\; a\,c < b\,d$

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

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

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

Properties of proportions

Assume that $\dfrac{\alpha}{\beta} = \dfrac{\gamma}{\delta} = \kappa$. Then,

$\alpha\delta = \beta\gamma$, $\qquad \dfrac{\alpha \pm \gamma}{\beta \pm \delta} = \kappa$

$\dfrac{\alpha \pm \beta}{\beta} = \dfrac{\gamma \pm \delta}{\delta}$, $\qquad \dfrac{\alpha}{\beta \pm \alpha} = \dfrac{\gamma}{\delta \pm \gamma}$

Properties of absolute values of real numbers

$$|a| = a, \quad if \quad a \geq 0$$
$$\quad = -a, \quad if \quad a < 0$$

$$|a| \geq 0$$

$$|-a| = |a|$$

$$|a|^2 = a^2$$

$$\sqrt{a^2} = |a|$$

$$|x| \leq \varepsilon \quad \Leftrightarrow \quad -\varepsilon \leq x \leq \varepsilon \quad (\varepsilon > 0)$$

$$|x| \geq a > 0 \quad \Leftrightarrow \quad x \geq a \quad or \quad x \leq -a$$

$$\big||a| - |b|\big| \leq |a \pm b| \leq |a| + |b|$$

$$|a \cdot b| = |a||b|$$

$$|a^k| = |a|^k \quad (k \in Z)$$

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|} \quad (b \neq 0)$$

Properties of powers and logarithms

$$x^0 = 1 \qquad (x \neq 0)$$

$$x^\alpha x^\beta = x^{\alpha+\beta}$$

$$\frac{x^\alpha}{x^\beta} = x^{\alpha-\beta}$$

$$\frac{1}{x^\alpha} = x^{-\alpha}$$

$$\left(x^\alpha\right)^\beta = x^{\alpha\beta}$$

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

$$\ln 1 = 0$$

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

$$\ln(\alpha\beta) = \ln\alpha + \ln\beta$$

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

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

$$\ln\left(\alpha^k\right) = k\ln\alpha \quad (k \in \mathbb{R})$$

Derivatives and integrals of elementary functions

$(c)' = 0 \quad (c = const.)$ $\qquad (\sin x)' = \cos x$ $\qquad (\arcsin x)' = \dfrac{1}{\sqrt{1-x^2}}$

$(x^{\alpha})' = \alpha x^{\alpha-1} \quad (\alpha \in R)$ $\qquad (\cos x)' = -\sin x$ $\qquad (\arccos x)' = -\dfrac{1}{\sqrt{1-x^2}}$

$(e^x)' = e^x$ $\qquad (\tan x)' = \dfrac{1}{\cos^2 x}$ $\qquad (\arctan x)' = \dfrac{1}{1+x^2}$

$(\ln x)' = \dfrac{1}{x} \quad (x > 0)$ $\qquad (\cot x)' = -\dfrac{1}{\sin^2 x}$ $\qquad (\operatorname{arc}\cot x)' = -\dfrac{1}{1+x^2}$

$(\sinh x)' = \cosh x$ $\qquad (\cosh x)' = \sinh x$

$$\int dx = x + C \quad ; \qquad \int x^a dx = \frac{x^{a+1}}{a+1} + C \qquad (a \neq -1)$$

$$\int \frac{dx}{x} = \ln|x| + C$$

$$\int e^x dx = e^x + C$$

$$\int \cos x\, dx = \sin x + C \quad ; \qquad \int \sin x\, dx = -\cos x + C$$

$$\int \frac{dx}{\cos^2 x} = \tan x + C \quad ; \qquad \int \frac{dx}{\sin^2 x} = -\cot x + C$$

$$\int \frac{dx}{\sqrt{1-x^2}} = \arcsin x + C$$

$$\int \frac{dx}{1+x^2} = \arctan x + C$$

$$\int \frac{dx}{x^2-1} = \frac{1}{2}\ln\left|\frac{x-1}{x+1}\right| + C$$

$$\int \frac{dx}{\sqrt{x^2 \pm 1}} = \ln\left(x + \sqrt{x^2 \pm 1}\right) + C$$

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 *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 *real* numbers x and y, we define the *complex number*

$$z=x+iy\ .$$

This is often represented as an ordered pair

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

The number $x=\mathrm{Re}\,z$ is the *real part* of z while $y=\mathrm{Im}\,z$ is the *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 *real* number.

Given a complex number $z=x+iy$, the number

$$\bar{z}=x-iy$$

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

$$|z|=(x^2+y^2)^{1/2}$$

is called the *modulus* (or absolute value) of z. We notice that

$$|z|=|\bar{z}|\ .$$

Example: If $z=3+2i$, then $\bar{z}=3-2i$ and $|z|=|\bar{z}|=\sqrt{13}$.

Exercise: Show that, if $z=\bar{z}$, then z is *real*, and conversely.

Exercise: Show that, if $z=x+iy$, then

$$\mathrm{Re}\,z=x=\frac{z+\bar{z}}{2}\ , \quad \mathrm{Im}\,z=y=\frac{z-\bar{z}}{2i}\ .$$

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

$$z_1 + z_2 = (x_1 + x_2) + i\,(y_1 + y_2)\ ,$$

$$z_1 - z_2 = (x_1 - x_2) + i\,(y_1 - y_2)\ .$$

Exercise: Show that, if $z_1 = z_2$, then $x_1 = x_2$ and $y_1 = y_2$.

Taking into account that $i^2 = -1$, we find the product of z_1 and z_2 to be

$$z_1 z_2 = (x_1 x_2 - y_1 y_2) + i\,(x_1 y_2 + x_2 y_1)\ .$$

In particular, for $z_1 = z = x + i\,y$ and $z_2 = \bar{z} = x - i\,y$, we have:

$$z\bar{z} = x^2 + y^2 = |\,z\,|^2\ .$$

To evaluate the ratio z_1 / z_2 $(z_2 \neq 0)$ we apply the following trick:

$$\frac{z_1}{z_2} = \frac{z_1\bar{z}_2}{z_2\bar{z}_2} = \frac{z_1\bar{z}_2}{|\,z_2\,|^2} = \frac{(x_1 + i\,y_1)(x_2 - i\,y_2)}{x_2{}^2 + y_2{}^2} = \frac{x_1 x_2 + y_1 y_2}{x_2{}^2 + y_2{}^2} + i\ \frac{x_2 y_1 - x_1 y_2}{x_2{}^2 + y_2{}^2}\ .$$

In particular, for $z = x + i\,y$,

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|\,z\,|^2} = \frac{x - i\,y}{x^2 + y^2} = \frac{x}{x^2 + y^2} - i\ \frac{y}{x^2 + y^2}\ .$$

Properties:

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2\ , \qquad \overline{z_1 - z_2} = \bar{z}_1 - \bar{z}_2$$

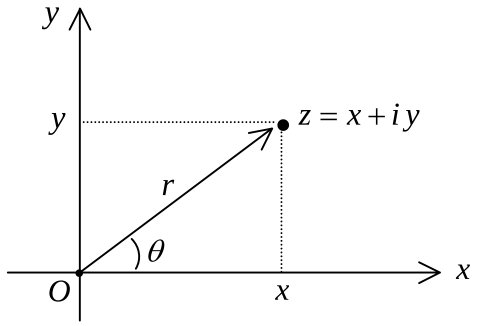
$$\overline{z_1 z_2} = \bar{z}_1\,\bar{z}_2\ , \qquad \overline{\left(\frac{z_1}{z_2}\right)} = \frac{\bar{z}_1}{\bar{z}_2}$$

$$|\,\bar{z}\,| = |\,z\,|\ , \qquad z\bar{z} = |\,z\,|^2\ , \qquad |\,z_1 z_2\,| = |\,z_1\,|\,|z_2\,|$$

$$|\,z^n\,| = |\,z\,|^n\ , \qquad \left|\frac{z_1}{z_2}\right| = \frac{|\,z_1\,|}{|\,z_2\,|}$$

Exercise: Given the complex numbers $z_1 = 3 - 2\,i$ and $z_2 = -2 + i$, evaluate the quantities $|\,z_1 \pm z_2\,|$, $\bar{z}_1 z_2$ and $\overline{z_1 / z_2}$.

Polar form of a complex number



A complex number $z = x + i\,y \equiv (x, y)$ 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

$$\boxed{z = x + i\,y = r\,(\cos\theta + i\sin\theta)}$$

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

$$\bar{z} = r\,(\cos\theta - i\sin\theta)\,.$$

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 $z\,z^{-1} = 1$.

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

$$e^{-i\theta} = 1/e^{i\theta} = \overline{e^{i\theta}} .$$

Also show that

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

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

$$\boxed{z = r\,e^{i\theta}}$$

It can be shown that

$$z^{-1} = \frac{1}{z} = \frac{1}{r}\,e^{-i\theta} = \frac{1}{r}\,e^{i(-\theta)} , \qquad \bar{z} = r\,e^{-i\theta}$$

$$z_1 z_2 = r_1 r_2\, e^{i(\theta_1+\theta_2)} , \qquad \frac{z_1}{z_2} = \frac{r_1}{r_2}\, e^{i(\theta_1-\theta_2)}$$

where $z_1 = r_1 e^{i\theta_1}$, $z_2 = r_2 e^{i\theta_2}$.

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

$$z = 2\left(\frac{\sqrt{2}}{2} - i\,\frac{\sqrt{2}}{2}\right) = 2\left[\cos\left(-\frac{\pi}{4}\right) + i\sin\left(-\frac{\pi}{4}\right)\right] = 2\,e^{i(-\pi/4)} = 2\,e^{-i\pi/4} .$$

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

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

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 *nth root of* z is any complex number c satisfying the equation $c^n = z$. We write $c = \sqrt[n]{z}$. An nth 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

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

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:

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

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

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

$$c_1 = \cos(5\pi/4) + i\sin(5\pi/4) = -\frac{\sqrt{2}}{2}(1 + i) \ .$$

ALGEBRA: SOME BASIC CONCEPTS

Sets

Subset:	$X \subseteq Y \Leftrightarrow (x \in X \Rightarrow x \in Y)$; $X = Y \Leftrightarrow X \subseteq Y$ *and* $Y \subseteq X$
Proper subset:	$X \subset Y \Leftrightarrow X \subseteq Y$ *and* $X \neq Y$
Union of sets:	$X \cup Y = \{ x \,/\, x \in X$ *or* $x \in Y \}$
Intersection of sets:	$X \cap Y = \{ x \,/\, x \in X$ *and* $x \in Y \}$
Disjoint sets:	$X \cap Y = \varnothing$
Difference of sets:	$X - Y = \{ x \,/\, x \in X$ *and* $x \notin Y \}$
Complement of a subset:	$X \supset Y$; $X \setminus Y = X - Y$
Cartesian product:	$X \times Y = \{(x, y) \,/\, x \in X$ *and* $y \in Y \}$
Mapping:	$f : X \to Y$; $(x \in X) \to y = f(x) \in Y$
Domain / range of f *:*	$D(f) = X$, $R(f) = f(X) = \{ f(x) \,/\, x \in X \} \subseteq Y$; f is *defined* in X and *has values* in Y ; $y = f(x)$ is the *image* of x under f
Composite mapping:	$f : X \to Y$, $g : Y \to Z$; $f \circ g : X \to Z$; $(x \in X) \to g(f(x)) \in Z$
Injective (1-1) mapping:	$f(x_1) = f(x_2) \Leftrightarrow x_1 = x_2$, *or* $x_1 \neq x_2 \Leftrightarrow f(x_1) \neq f(x_2)$
Surjective (onto) mapping:	$f(X) = Y$
Bijective mapping:	f *is both injective and surjective* $\Rightarrow$ *invertible*
Identity mapping:	$f_{id} : X \to X$; $f_{id}(x) = x$, $\forall x \in X$
Internal operation on X:	$X \times X \to X$; $[(x, y) \in X \times X] \to z \in X$
External operation on X:	$A \times X \to X$; $[(a, x) \in A \times X] \to y = a \cdot x \in X$

Groups

A *group* is a set G, together with an internal operation $G \times G \to G$; $(x, y) \to z = x \cdot y$, 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 $V = \{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, ...\}$, and let $a, b, c, ... \in R$. Consider an internal operation + and an external operation $\cdot$ on V :

$$+ :\ V \times V \to V \ ; \quad \boldsymbol{x} + \boldsymbol{y} = \boldsymbol{z}$$
$$\cdot :\ R \times V \to V \ ; \quad a \cdot \boldsymbol{x} = \boldsymbol{y}$$

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

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

A set $\{\boldsymbol{x}_1 , \boldsymbol{x}_2 , ... , \boldsymbol{x}_k\}$ of elements of V is *linearly independent* iff the equation[1]

$$c_1 \boldsymbol{x}_1 + c_2 \boldsymbol{x}_2 + ... + c_k \boldsymbol{x}_k = 0$$

can only be satisfied for $c_1 = c_2 = ... = c_k = 0$; 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 $\{\boldsymbol{e}_1 , \boldsymbol{e}_2 , ... , \boldsymbol{e}_n\}$ of n linearly independent elements is a *basis* for V, and any $\boldsymbol{x} \in V$ can be uniquely expressed as $\boldsymbol{x} = c_1 \boldsymbol{e}_1 + c_2 \boldsymbol{e}_2 + ... + c_n \boldsymbol{e}_n$.

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 $\boldsymbol{x} + \boldsymbol{y}$ of any two elements of S, as well as the scalar multiple $a\boldsymbol{x}$ and the inverse $-\boldsymbol{x}$ of any element $\boldsymbol{x}$ of S, must belong to S. Clearly, this set must contain the identity $\mathbf{0}$ of V. If S is a subspace of V, then $\dim S \le \dim V$. 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* $\boldsymbol{\omega}$ on a vector space V is a mapping $\boldsymbol{\omega}: V \to R$; $(\boldsymbol{x}\in V) \to t = \boldsymbol{\omega}(\boldsymbol{x})\in R$. The functional $\boldsymbol{\omega}$ is *linear* if $\boldsymbol{\omega}(a\cdot\boldsymbol{x}+b\cdot\boldsymbol{y})=a\cdot\boldsymbol{\omega}(\boldsymbol{x})+b\cdot\boldsymbol{\omega}(\boldsymbol{y})$. The collection of all linear functionals on V is called the *dual space* of V, denoted V^*. It is itself a vector space over R, and $\dim V^* = \dim V$.

Algebras

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

$$(a\cdot\boldsymbol{x} + b\cdot\boldsymbol{y}\,|\,\boldsymbol{z}) = a\cdot(\boldsymbol{x}\,|\,\boldsymbol{z}) + b\cdot(\boldsymbol{y}\,|\,\boldsymbol{z})$$
$$(\boldsymbol{x}\,|\,a\cdot\boldsymbol{y} + b\cdot\boldsymbol{z}) = a\cdot(\boldsymbol{x}\,|\,\boldsymbol{y}) + b\cdot(\boldsymbol{x}\,|\,\boldsymbol{z})$$

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

Example: The set $\Lambda^0(R^n)$ of all functions on R^n is a commutative, associative algebra. The multiplication operation $(\cdot\,|\,\cdot) : \Lambda^0(R^n)\times \Lambda^0(R^n)\to \Lambda^0(R^n)$ 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., $(\boldsymbol{x}\,|\,\boldsymbol{y})\in S$ for any $\boldsymbol{x}, \boldsymbol{y}$ in S. We write: $S\subset A$.

A subalgebra $S\subset A$ is an *ideal* of A iff $(\boldsymbol{x}\,|\,\boldsymbol{y})\in S$ and $(\boldsymbol{y}\,|\,\boldsymbol{x})\in S$, for any $\boldsymbol{x}\in S$, $\boldsymbol{y}\in A$.

Modules

Note first that R is an associative, commutative algebra under the usual operations of addition and multiplication. Thus, a vector space over 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

$$\cdot : A \times M \to M ; \quad a\cdot\boldsymbol{x} = \boldsymbol{y} \quad (a\in A ;\ \boldsymbol{x}, \boldsymbol{y} \in M) .$$

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* $\boldsymbol{V}$ on R^n is a map from a domain of R^n into R^n :

$$\boldsymbol{V} : R^n \supseteq U \to R^n \;;\quad [\boldsymbol{x} \equiv (x^1,..., x^n) \in U\,] \to \boldsymbol{V}(\boldsymbol{x}) \equiv (V^1(x^k),...,V^n(x^k)) \in R^n \;.$$

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

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

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

It follows from the above that *the collection of all vector fields on R^n is a vector space over R* .

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

A note on linear independence:

Let $\{\boldsymbol{V}_1, ... ,\boldsymbol{V}_r\} \equiv \{\boldsymbol{V}_a\}$ be a collection of vector fields on R^n.

(a) The set $\{\boldsymbol{V}_a\}$ is *linearly dependent over R* (linearly dependent with constant coefficients) iff there exist real constants $c_1,...,c_r$, *not all zero*, such that

$$c_1\boldsymbol{V}_1(\boldsymbol{x}) + \dots + c_r\boldsymbol{V}_r(\boldsymbol{x}) = 0 \;,\quad \forall \boldsymbol{x} \in R^n \;.$$

If the above relation is satisfied only for $c_1 = \dots = c_r = 0$, the set $\{\boldsymbol{V}_a\}$ is *linearly independent over R*.

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

$$f_1(x^k)\, \boldsymbol{V}_1(\boldsymbol{x}) + \dots + f_r(x^k)\, \boldsymbol{V}_r(\boldsymbol{x}) = 0 \;,\quad \forall \boldsymbol{x} \equiv (x^k) \in R^n \;.$$

If this relation is satisfied only for $f_1(x^k)=\dots= f_r(x^k) \equiv 0$, the set $\{\boldsymbol{V}_a\}$ is *linearly independent over* $\Lambda^0(R^n)$.

There can be at most n elements in a linearly independent system over $\Lambda^0(R^n)$. These elements form a *basis* $\{\boldsymbol{e}_1, ..., \boldsymbol{e}_n\} \equiv \{\boldsymbol{e}_k\}$ for the module of all vector fields on R^n. An element of this module, i.e. an arbitrary vector field $\boldsymbol{V}$, is written as a linear combination of the $\{\boldsymbol{e}_k\}$ with coefficients $V^k \in \Lambda^0(R^n)$. Thus, at any point $\boldsymbol{x} \equiv (x^k) \in R^n$,

$$\boldsymbol{V}(\boldsymbol{x}) = V^1(x^k)\,\boldsymbol{e}_1 + ...+ V^n(x^k)\,\boldsymbol{e}_n \equiv (V^1(x^k), ... ,V^n(x^k)) \,.$$

In particular, in the basis $\{\boldsymbol{e}_k\}$,

$$\boldsymbol{e}_1 \equiv (1,0,0,...,0), \quad \boldsymbol{e}_2 \equiv (0,1,0,...,0), \quad \dots \quad , \boldsymbol{e}_n \equiv (0,0,...,0,1) \,.$$

Example: Let $n=3$, i.e., $R^n=R^3$. Call $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3\} \equiv \{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$. Let $\boldsymbol{V}$ be a vector field on R^3. Then, at any point $\boldsymbol{x} \equiv (x, y, z)\in R^3$,

$$\boldsymbol{V}(\boldsymbol{x}) = V_x\,(x, y, z)\,\boldsymbol{i} + V_y\,(x, y, z)\,\boldsymbol{j} + V_z\,(x, y, z)\,\boldsymbol{k} \equiv (V_x\,, V_y\,, V_z\,) \,.$$

Now, consider the six vector fields

$$\boldsymbol{V}_1 = \boldsymbol{i}\,,\ \boldsymbol{V}_2 = \boldsymbol{j}\,,\ \boldsymbol{V}_3 = \boldsymbol{k}\,,\ \boldsymbol{V}_4 = x\,\boldsymbol{j} - y\,\boldsymbol{i}\,,\ \boldsymbol{V}_5 = y\,\boldsymbol{k} - z\,\boldsymbol{j}\,,\ \boldsymbol{V}_6 = z\,\boldsymbol{i} - x\,\boldsymbol{k}\,.$$

Clearly, the $\{\boldsymbol{V}_1, \boldsymbol{V}_2, \boldsymbol{V}_3\}$ are linearly independent over $\Lambda^0(R^3)$, since they constitute the basis $\{\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$. On the other hand, the $\boldsymbol{V}_4, \boldsymbol{V}_5, \boldsymbol{V}_6$ are separately linearly dependent on the $\{\boldsymbol{V}_1, \boldsymbol{V}_2, \boldsymbol{V}_3\}$ over $\Lambda^0(R^3)$. Moreover, the set $\{\boldsymbol{V}_4, \boldsymbol{V}_5, \boldsymbol{V}_6\}$ is also linearly dependent over $\Lambda^0(R^3)$, since $z\boldsymbol{V}_4 + x\boldsymbol{V}_5 + y\boldsymbol{V}_6 = 0$. Thus, the set $\{\boldsymbol{V}_1, \dots, \boldsymbol{V}_6\}$ is *linearly dependent over* $\Lambda^0(R^3)$. On the other hand, the system $\{\boldsymbol{V}_1, \dots, \boldsymbol{V}_6\}$ is *linearly independent over R*, since the equation $c_1\boldsymbol{V}_1 + \dots + c_6\boldsymbol{V}_6 = 0$, with $c_1 ,...,c_6\in R$ (constant coefficients), can only be satisfied for $c_1 = ...= c_6 = 0$. In general,

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

Derivation on an algebra

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

$$L : A\to A \,; \quad (\boldsymbol{x}\in A) \to \boldsymbol{y} = L\,\boldsymbol{x} \in A \,.$$

L is a *derivation* on A iff, $\forall \boldsymbol{x}, \boldsymbol{y} \in A$ and $a, b \in R$,

$$L\,(a\boldsymbol{x}+b\boldsymbol{y}) = aL(\boldsymbol{x}) + bL(\boldsymbol{y}) \qquad (\textit{linearity})$$
$$L\,(\boldsymbol{x}\,|\,\boldsymbol{y}) = (L\,\boldsymbol{x}\,|\,\boldsymbol{y}) + (\boldsymbol{x}\,|\,L\,\boldsymbol{y}) \qquad (\textit{Leibniz rule})$$

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

$$L = \varphi^1(x^k)\,\partial/\partial x^1 + \dots + \varphi^n(x^k)\,\partial/\partial x^n \equiv \varphi^i(x^k)\,\partial/\partial x^i \,,$$

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

$$L\,[\,f\,(x^k)\,g(x^k)] = [L\,f\,(x^k)]\,g(x^k) + f\,(x^k)\,L\,g(x^k) \,.$$

Hence, L is a derivation on $\Lambda^0(R^n)$.

Lie algebra

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

$$[a\boldsymbol{x}+b\boldsymbol{y}\,,\boldsymbol{z}] = a\,[\boldsymbol{x}\,,\boldsymbol{z}] + b\,[\boldsymbol{y}\,,\boldsymbol{z}]$$
$$[\boldsymbol{x}\,,\boldsymbol{y}] = -[\boldsymbol{y}\,,\boldsymbol{x}] \qquad \text{(\textit{antisymmetry})}$$
$$[\boldsymbol{x}\,,[\boldsymbol{y}\,,\boldsymbol{z}]] + [\boldsymbol{y}\,,[\boldsymbol{z}\,,\boldsymbol{x}]] + [\boldsymbol{z}\,,[\boldsymbol{x}\,,\boldsymbol{y}]] = 0 \qquad \text{(\textit{Jacobi identity})}$$

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

$$[\boldsymbol{x}\,,a\boldsymbol{y}+b\boldsymbol{z}] = a\,[\boldsymbol{x}\,,\boldsymbol{y}] + b\,[\boldsymbol{x}\,,\boldsymbol{z}]\,,$$
$$[[\boldsymbol{x}\,,\boldsymbol{y}]\,,\boldsymbol{z}] + [[\boldsymbol{y}\,,\boldsymbol{z}]\,,\boldsymbol{x}] + [[\boldsymbol{z}\,,\boldsymbol{x}]\,,\boldsymbol{y}] = 0\,.$$

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

$$[\boldsymbol{x}\,,[\boldsymbol{y}\,,\boldsymbol{z}]] \neq [[\boldsymbol{x}\,,\boldsymbol{y}]\,,\boldsymbol{z}]\,.$$

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

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

Lie algebra of derivations

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

$$L = \varphi^i(x^k)\,\partial/\partial x^i \qquad \text{(sum on } i = 1, 2, \ldots, n)\,.$$

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:

$$[L_1\,,L_2] = L_1L_2 - L_2L_1\;;$$
$$[L_1\,,L_2]\,f(x^k) = L_1(L_2\,f(x^k)) - L_2(L_1\,f(x^k))\,.$$

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_1L_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 $\Lambda^0(R^n)$ 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., $S_1 \cap S_2 =\{\mathbf{0}\}$) 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., $S_1 \cap (S_2\oplus S_3)=\{\mathbf{0}\}$, etc.).

Homomorphism of vector spaces

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

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

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

The set of vectors $\boldsymbol{x}\in V$ mapping under Φ into the zero of W is called the *kernel* of the homomorphism Φ:

$$\mathrm{Ker}\,\Phi = \{\ \boldsymbol{x}\in V : \Phi(\boldsymbol{x}) = \mathbf{0}\} .$$

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

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

The algebra of linear operators

Let V be a vector space over a field K. A *linear operator* $\boldsymbol{A}$ on V is a homomorphism $\boldsymbol{A} : V\to V$. Thus,

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

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

$$(\boldsymbol{A}+\boldsymbol{B})\,\boldsymbol{x} = \boldsymbol{A}\,\boldsymbol{x} + \boldsymbol{B}\,\boldsymbol{x} \ , \quad (k\boldsymbol{A})\,\boldsymbol{x} = k\,(\boldsymbol{A}\,\boldsymbol{x}) \ .$$

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

Since $\boldsymbol{A}$ and $\boldsymbol{B}$ are mappings, their composition may be defined. This is regarded as their *product* $\boldsymbol{AB}$:

$$(\boldsymbol{AB})\,\boldsymbol{x} \equiv \boldsymbol{A}(\boldsymbol{Bx}) \ , \quad \forall \boldsymbol{x} \in V.$$

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

$$(\boldsymbol{AB})\boldsymbol{C} = \boldsymbol{A}\,(\boldsymbol{BC}) \equiv \boldsymbol{ABC} \ , \quad \boldsymbol{A}\,(\boldsymbol{B}+\boldsymbol{C}) = \boldsymbol{AB}+\boldsymbol{AC} \ .$$

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

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

An operator $\boldsymbol{A}$ 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* $\boldsymbol{A}^{-1}$ exists such that $\boldsymbol{AA}^{-1}= \boldsymbol{A}^{-1}\boldsymbol{A}=\boldsymbol{E}$. Practically this means that, if $\boldsymbol{A}$ maps $\boldsymbol{x} \in V$ onto $\boldsymbol{y} \in V$, then $\boldsymbol{A}^{-1}$ maps $\boldsymbol{y}$ back onto $\boldsymbol{x}$. For an invertible operator $\boldsymbol{A}$, $\mathrm{Ker}\,\boldsymbol{A}=\{\boldsymbol{0}\}$ and $\mathrm{Im}\,\boldsymbol{A}=V$.

Matrix representation of a linear operator

Let $\boldsymbol{A}$ be a linear operator on V. Let $\{\boldsymbol{e}_i\}$ ($i=1,\dots,n$) be a basis of V. Let

$$\boldsymbol{A}\,\boldsymbol{e}_k = \boldsymbol{e}_i\,A_{i\,k} \qquad \text{(sum on } i\text{)}$$

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 $A=[A_{i\,k}]$ is called the *matrix of the operator* $\boldsymbol{A}$ *in the basis* $\{\boldsymbol{e}_i\}$.

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

$$y_i = A_{i\,k}\,x_k \qquad \text{(sun on } k\text{)} .$$

In matrix form,

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

Next, let $\boldsymbol{A}$, $\boldsymbol{B}$ be linear operators on V. Define their product $\boldsymbol{C}=\boldsymbol{AB}$ by

$$\boldsymbol{C}\,\boldsymbol{x} = (\boldsymbol{AB})\,\boldsymbol{x} \equiv \boldsymbol{A}\,(\boldsymbol{Bx}) \ , \quad \boldsymbol{x} \in V \ .$$

Then, for any basis $\{\boldsymbol{e}_i\}$, $\boldsymbol{C}\,\boldsymbol{e}_k = \boldsymbol{A}\,(\boldsymbol{B}\,\boldsymbol{e}_k\,) = \boldsymbol{e}_i\,A_{i\,j}\,B_{j\,k} \equiv \boldsymbol{e}_i\,C_{i\,k} \quad \Rightarrow$

$$C_{ik} = A_{ij} B_{jk}$$

or, in matrix form,

$$C = AB\ .$$

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* $T = [T_{ik}]$:

$$\boldsymbol{e}_k{}' = \boldsymbol{e}_i\, T_{ik}\ \ .$$

The inverse transformation is

$$\boldsymbol{e}_k = \boldsymbol{e}_i{}'\, (T^{-1})_{ik}\ \ .$$

Under this basis change, the matrix A of an operator $\boldsymbol{A}$ transforms as

$$A' = T^{-1} A\, T \quad (\textit{similarity transformation})\ .$$

Under basis transformations, *the trace and the determinant of A remain unchanged*:

$$trA' = trA \ \ , \qquad detA' = detA\ \ .$$

An operator $\boldsymbol{A}$ 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 $\boldsymbol{A}^{-1} \in Op(V)$ such that $\boldsymbol{A}\,\boldsymbol{A}^{-1} = \boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{E}$. Since an invertible operator represents a bijective mapping (i.e., both 1-1 and onto), it follows that $\mathrm{Ker}\boldsymbol{A} = \{\boldsymbol{0}\}$ and $\mathrm{Im}\boldsymbol{A} = V$. If $\boldsymbol{A}$ is invertible (nonsingular), then, for any basis $\{\boldsymbol{e}_i\}$ ($i = 1,..., n$) of V, the vectors $\{\boldsymbol{A}\boldsymbol{e}_i\}$ 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 $\boldsymbol{A}$ be a linear operator on V. The subspace S of V is said to be *invariant under* $\boldsymbol{A}$ if, for every vector $\boldsymbol{x}$ of S, the vector $\boldsymbol{A}\boldsymbol{x}$ again belongs to S. Symbolically, $\boldsymbol{A}S \subseteq S$.

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

$$\boldsymbol{A}\,\boldsymbol{x} = \lambda\,\boldsymbol{x}\ \ .$$

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

It can be shown that *the eigenvalues of* $\boldsymbol{A}$ *are basis-independent quantities*. Indeed, let $A=[A_{ik}]$ be the $(n\times n)$ matrix representation of $\boldsymbol{A}$ in some basis $\{\boldsymbol{e}_i\}$ of V, and let $\boldsymbol{x}=x_i\boldsymbol{e}_i$ be an eigenvector belonging to λ. We denote by $X=[x_i]$ the column vector representing $\boldsymbol{x}$ in that basis. The eigenvalue equation for $\boldsymbol{A}$ 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 λ_i $(i=1,...,n)$ (not necessarily all different from each-other) of $\boldsymbol{A}$. Since the determinant of the matrix representation of an operator [in particular, of the operator $(\boldsymbol{A}-\lambda\boldsymbol{E})$ for any given λ] is a basis-independent quantity, it follows that, if the above equation is satisfied for a certain λ in a certain basis (where $\boldsymbol{A}$ is represented by the matrix A), it will also be satisfied *for the same* λ in any other basis (where $\boldsymbol{A}$ 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 $\{\boldsymbol{x}_i\}$ of $\boldsymbol{A}$, belonging to the corresponding eigenvalues λ_i , we can use these vectors to define a basis for V. In this basis, the matrix representation of $\boldsymbol{A}$ has a particularly simple *diagonal* form:

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

Using this expression, and the fact that the quantities trA, $detA$ and λ_i are invariant under basis transformations, we conclude that, in *any* basis of V,

$$trA = \lambda_1 + \lambda_2 +\ldots+ \lambda_n \ , \qquad detA = \lambda_1\, \lambda_2 \ldots \lambda_n \ .$$

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

An operator $\boldsymbol{A}$ is called *nilpotent* if $\boldsymbol{A}^m=\boldsymbol{0}$ 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 $\boldsymbol{A}$ is called *idempotent* (or *projection operator*) if $\boldsymbol{A}^2=\boldsymbol{A}$. It follows that $\boldsymbol{A}^m=\boldsymbol{A}$, for any natural number m. *The eigenvalues of an idempotent operator can take the values 0 or 1.*

BASIC MATRIX PROPERTIES

$(A+B)^T = A^T + B^T$; $(AB)^T = B^T A^T$

$(A+B)^\dagger = A^\dagger + B^\dagger$; $(AB)^\dagger = B^\dagger A^\dagger$ where $M^\dagger \equiv (M^T)^* = (M^*)^T$

$(kA)^T = kA^T$; $(kA)^\dagger = k^* A^\dagger$ $(k \in C)$

$(AB)^{-1} = B^{-1} A^{-1}$; $(A^T)^{-1} = (A^{-1})^T$; $(A^\dagger)^{-1} = (A^{-1})^\dagger$

$[A,B]^T = [B^T, A^T]$; $[A,B]^\dagger = [B^\dagger, A^\dagger]$

$$A^{-1} = \frac{1}{\det A}\, adjA \quad (\det A \neq 0)$$

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

$tr(\kappa A + \lambda B) = \kappa\, trA + \lambda\, trB$

$trA^T = trA$; $trA^\dagger = (trA)^*$

$tr(AB) = tr(BA)$, $tr(ABC) = tr(BCA) = tr(CAB)$, *etc.*

$tr[A,B] = 0$

$\det A^T = \det A$; $\det A^\dagger = (\det A)^*$

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

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

$\det(cA) = c^n \det A \quad \left(c \in C,\ A \in gl(n,C)\right)$

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

$[A,B] = -[B,A] \equiv AB - BA$

$[A,\ B+C] = [A,B] + [A,C]$; $[A+B,\ C] = [A,C] + [B,C]$

$[A,BC] = [A,B]C + B[A,C]$; $[AB,C] = A[B,C] + [A,C]B$

$[A,\ [B,C]] + [B,\ [C,A]] + [C,\ [A,B]] = 0$

$[[A,B],\ C] + [[B,C],\ A] + [[C,A],\ B] = 0$

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

$$\left(\frac{dA}{dt}\right)_{ij} = \frac{d}{dt}\, a_{ij}(t) \ .$$

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

$$\left(\int A(t)\, dt\right)_{ij} = \int a_{ij}(t)\, dt \ .$$

$$\frac{d}{dt}(A \pm B) = \frac{dA}{dt} \pm \frac{dB}{dt} \;; \quad \frac{d}{dt}(AB) = \frac{dA}{dt}B + A\frac{dB}{dt}$$

$$\frac{d}{dt}[A, B] = \left[\frac{dA}{dt}, B\right] + \left[A, \frac{dB}{dt}\right]$$

$$\frac{d}{dt}(A^{-1}) = -A^{-1}\frac{dA}{dt}A^{-1} \quad \Rightarrow \quad d(A^{-1}) = -A^{-1}(dA)A^{-1}$$

$$tr\left(\frac{dA}{dt}\right) = \frac{d}{dt}(trA)$$

Let $A = A(x, y)$. Call $\partial A/\partial x \equiv \partial_x A \equiv A_x$, etc.:

$$\partial_x(A^{-1}A_y) - \partial_y(A^{-1}A_x) + [A^{-1}A_x\,,\ A^{-1}A_y] = 0$$

$$\partial_x(A_yA^{-1}) - \partial_y(A_xA^{-1}) - [A_xA^{-1}\,,\ A_yA^{-1}] = 0$$

$$A(A^{-1}A_x)_y A^{-1} = (A_yA^{-1})_x \quad \Leftrightarrow \quad A^{-1}(A_yA^{-1})_x A = (A^{-1}A_x)_y$$

$$e^A \equiv \exp A = \sum_{n=0}^{\infty}\frac{A^n}{n!} = 1 + A + \frac{A^2}{2} + \cdots$$

$$B e^A B^{-1} = e^{BAB^{-1}}$$

$$\left(e^A\right)^* = e^{A^*} \;; \quad \left(e^A\right)^T = e^{A^T} \;; \quad \left(e^A\right)^\dagger = e^{A^\dagger} \;; \quad \left(e^A\right)^{-1} = e^{-A}$$

$e^Ae^B = e^Be^A = e^{A+B}$ when $[A, B] = 0$

In general, $e^Ae^B = e^C$ where

$$C = A + B + \frac{1}{2}[A, B] + \frac{1}{12}\left([A, [A, B]] + [B, [B, A]]\right) + \cdots$$

By definition, $\log B = A \Leftrightarrow B = e^A$.

$$\det\left(e^A\right) = e^{trA} \quad \Leftrightarrow \quad \det B = e^{tr\,(\log B)} \quad \Leftrightarrow \quad tr\,(\log B) = \log(\det B)$$

$\det(1 + \delta A) \simeq 1 + tr\,\delta A$, for infinitesimal δA

$$tr\,(A^{-1}A_x) = tr\,(A_xA^{-1}) = tr\,(\log A)_x = [tr\,(\log A)]_x = [\log(\det A)]_x$$
