

Real Numbers

• The least upper bound

- Let B be any subset of \mathbf{R} . B is bounded above if there is a $k \in \mathbf{R}$ such that $x \leq k$ for all $x \in B$.
- A real number, $k \in \mathbf{R}$ is a unique least upper bound of B , i.e. $k = \text{LUB}(B)$, if
 - (1) k is an upper bound of B .
 - (2) For every $y < k$, y is not an upper bound of B .
- LUB axiom says that every nonempty subset of \mathbf{R} that is bounded above has a least upper bound.
- $\text{LUB}(B)$ may or may not belong to B . (Ex; $B = \{y : y = -1/x, x \in \mathbf{R}^+\}$)
- Note that $A \subset B \Rightarrow \text{LUB}(A) \leq \text{LUB}(B)$.

• The greatest lower bound

- Let B be any subset of \mathbf{R} . If B is bounded below, the greatest lower bound, $\text{GLB}(B)$ is similarly defined.

• Supremum and infimum

- For any subset B of \mathbf{R} , the supremum is defined as

$$\sup B := \begin{cases} \text{LUB}(B), & B \neq \emptyset \text{ and bounded above} \\ +\infty, & B \neq \emptyset \text{ and not bounded above.} \\ -\infty, & B = \emptyset \end{cases}$$

- For any subset C of \mathbf{R} , the infimum is defined as

$$\inf C := \begin{cases} \text{GLB}(C), & C \neq \emptyset \text{ and bounded below} \\ -\infty, & C \neq \emptyset \text{ and not bounded below.} \\ +\infty, & C = \emptyset \end{cases}$$

• Bolzano-Weierstrass theorem

- If x_n is a bounded sequence of real numbers, i.e. $-\infty < a \leq x_n \leq b < +\infty$, then there is a converging subsequence, x_{n_k} whose limit lies in $[a, b]$.

Vector Space

• Field

- A field is a set F on which two operations of addition and multiplication are defined with the **usual** properties.
- An ordered field is a field F with a relation $<$.
- Example: rational numbers, real numbers, complex numbers

• Vector space and subspace

- A nonempty set V is a vector space over a field F if the following properties hold:

There is an operation called vector addition, $+$ such that

- (1) Closure: $\forall \mathbf{u}, \mathbf{v} \in V, \mathbf{u} + \mathbf{v} \in V$
- (2) Commutative law: $\forall \mathbf{u}, \mathbf{v} \in V, \mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$
- (3) Associative law: $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V, (\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$
- (4) Additive identity: $\exists \mathbf{0} \in V \ni \forall \mathbf{u} \in V, \mathbf{u} + \mathbf{0} = \mathbf{u}$
- (5) Additive inverse: $\forall \mathbf{u} \in V, \exists (-\mathbf{u}) \ni \mathbf{u} + (-\mathbf{u}) = \mathbf{0}$ and $(-\mathbf{u})$ is unique.

There is an operation called scalar multiplication such that

- (1) Closure: $\forall a \in F$ and $\forall \mathbf{u} \in V, a\mathbf{u} \in V$
- (2) Associative law: $\forall a, b \in F$ and $\forall \mathbf{u} \in V, a(b\mathbf{u}) = (ab)\mathbf{u}$
- (3) First distributive law: $\forall a \in F$ and $\forall \mathbf{u}, \mathbf{v} \in V, a(\mathbf{u} + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$
- (4) Second distributive law: $\forall a, b \in F$ and $\forall \mathbf{u} \in V, (a+b)\mathbf{u} = a\mathbf{u} + b\mathbf{u}$
- (5) Multiplicative identity of F : $\forall \mathbf{u} \in V, 1\mathbf{u} = \mathbf{u}$.

- A subset W of a vector space V over F is a subspace of V iff $\forall a \in F$ and $\forall \mathbf{u}, \mathbf{v} \in W, a\mathbf{u} + \mathbf{v} \in W$. W itself is a vector space.

• Span, linear independence, and basis

- Let V be a vector space over a field F . Suppose $G \subset V$ and G may not be a subspace and may not be a finite set. The set of all linear combinations of elements of G is denoted by span G , i.e.,

$$\text{span } G := \left\{ \sum_{k=1}^n a_k \mathbf{v}_k : n \text{ is any positive integer, } \forall \mathbf{v}_k \in G, \text{ and } \forall a_k \in F \right\}.$$

Note that

- (1) $G \subset \text{span } G$.
- (2) $\text{span } G$ is a subspace of V .
- (3) If a subspace W contains G , then W contains $\text{span } G$.

- For an arbitrary subset G of V , G is linearly independent if

$$\forall \mathbf{v}_k \in G, \sum_{k=1}^n a_k \mathbf{v}_k = \mathbf{0} \text{ implies } a_1 = a_2 = \dots = a_n = 0.$$

If G is not linearly independent, G is linearly dependent. Note that if $\mathbf{0} \in G$, G is linearly dependent.

- If $\{\mathbf{v}_k\}_{k=1}^n$ are linearly independent, no vector \mathbf{v}_k can be expressed as a linear combination of other vectors in the set.
- Let W be a subspace of V . If there exists a finite subset $G \subset W$, such that $\text{span } G = W$, then W is finite-dimensional. If $\text{span } G = W$ and G is linearly independent, G is a basis for W .
- If $G = \{\mathbf{v}_k\}_{k=1}^n$ is a basis for W , $\mathbf{x} = \sum_{k=1}^n a_k \mathbf{v}_k \forall \mathbf{x} \in W$ and $\{a_k\}_{k=1}^n$ is unique.
- If W is finite-dimensional, then any basis of W contains the same number, n of linearly independent vectors. We say that n is the dimension of W (i.e. $\dim W = n$). If $\dim W = n$ and $\{\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_n\} \subset W$ are linearly independent, then $\text{span } \{\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_n\} = W$.

Mapping

• Function and mapping

- A function is a triple (X, Y, f) , also denoted by $f: X \rightarrow Y$, where X and Y are specified sets of inputs and outputs, respectively.
- f is a rule or mapping that associates to each $x \in X$, a unique element $f(x) \in Y$.
- The set X is the domain of f and the set Y is the co-domain of f .
- The range of f is the set $\{f(x) : x \in X\}$.
- Two functions (X_1, Y_1, f_1) and (X_2, Y_2, f_2) are equal iff $X_1 = X_2, Y_1 = Y_2$, and $f_1(x) = f_2(x) \forall x \in X_1 = X_2$.

• Vector space of mappings

Let V be a vector space over F and U be an arbitrary set.

- $x: U \rightarrow V$ is a mapping if there is a rule that assigns to each $u \in U$, an element $x(u) \in V$.
- We let X be the set of all mappings from U into V . Two mappings, x and y in X are equal iff $x(u) = y(u) \forall u \in U$.
- X is itself a vector space with the following definitions
 - (1) Addition of mappings is defined as $(x + y)(u) := x(u) + y(u) \forall x, y \in X$ and $\forall u \in U$,
 - (2) Additive identity, $z(u) := \mathbf{0} \forall u \in U$,
 - (3) Additive inverse, $(-x)(u) := -x(u) \forall u \in U$,
 - (4) Scalar multiplication, $(ax)(u) := a \cdot x(u) \forall u \in U$ and $a \in F$.

• Linear functional

- Let V be a vector space over F . A mapping $\beta: V \rightarrow F$ is called a linear functional if $\beta(a\mathbf{v}_1 + \mathbf{v}_2) = a\beta(\mathbf{v}_1) + \beta(\mathbf{v}_2), \forall a \in F, \forall \mathbf{v}_1, \mathbf{v}_2 \in V$.
- Given a set of vectors, $\{\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_n\} \subset V$, if there exists a set of linear functionals, $\{\beta_1, \beta_2, \dots, \beta_n\}$ such that $\beta_j(\mathbf{t}_i) = \delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$, then $\{\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_n\}$ is linearly independent.

Metric Space

• Metric space

- Let X be a nonempty set and define a mapping $\rho: X \times X \rightarrow [0, \infty)$ with the following properties:

$$(1) \rho(x, y) \geq 0 \text{ and } \rho(x, y) = 0 \text{ iff } x = y$$

$$(2) \rho(x, y) = \rho(y, x)$$

$$(3) \rho(x, z) \leq \rho(x, y) + \rho(y, z).$$

Then, ρ is called a metric. The pair (X, ρ) or X is a metric space.

- We define a ball as $B(x, r) = B_r(x) := \{y \in X : \rho(x, y) < r\}$, for some $x \in X$.

• Convergence

- A sequence $x_n \in X$ converges to $x \in X$ if $\forall \varepsilon > 0, \rho(x_n, x) < \varepsilon$ for all sufficiently large n (i.e., there exists an integer N such that the condition holds for all $n > N$). We denote this as $x_n \rightarrow x$ or $\lim_{n \rightarrow \infty} x_n = x$.

- A sequence $x_n \in X$ converges to $x \in X$ if $x_n \in B(x, \varepsilon), \forall \varepsilon > 0$ for all sufficiently large n .

- A set E in a metric space is closed iff every converging sequence of points in E converges to a point in E .

- (Approximation) If $x \in \bar{E}$, there is a sequence $x_n \in E$ and $x_n \rightarrow x$. In other words, if $x \in \bar{E}$, then there is a point $y \in E$ such that $\rho(x, y) < \varepsilon$ for any $\varepsilon > 0$.

• Subsequence

- Let n_1, n_2, \dots be integers such that $n_k \rightarrow \infty$ as $k \rightarrow \infty$.

- If $x_n \in X$ is a sequence, x_{n_k} is a subsequence of x_n .

• Sequential compactness

- A subset D is sequentially compact if for every sequence $x_n \in D$, there is a converging

subsequence x_{n_k} whose limit lies in D .

- From Bolzano-Weierstrass, $[a, b]$ with $-\infty < a < b < \infty$ is sequentially compact.
- Sequentially compact subset of a metric space must be closed.

• Cauchy sequence

- A sequence x_n in a metric space is Cauchy if $\rho(x_n, x_m) < \varepsilon, \forall \varepsilon > 0$ and for all sufficiently large n and m .
- In a Cauchy sequence, all the points in the tail of the sequence are close together.
- Every converging sequence is Cauchy. The converse is not true.
- A Cauchy sequence is bounded.

• Complete space

- If every Cauchy sequence of a metric space converges to a point in the space, the space is complete.
- If x_n is a Cauchy sequence in a metric space, and if x_{n_k} is a converging subsequence of x_n , then x_n converges to the same limit as x_{n_k} .
- The real numbers \mathbb{R} with the metric $\rho(x, y) = |x - y|$ is a complete metric space.
- The space \mathbb{R}^d is complete under the usual Euclidian distance, i.e.

$$\rho(\mathbf{x}, \mathbf{y}) = \sqrt{\sum_{i=1}^d |x^{(i)} - y^{(i)}|^2}.$$

- Any closed and bounded subset of \mathbb{R}^d is sequentially compact.
- The spaces of complex numbers \mathbb{C} and \mathbb{C}^d are complete. Any closed and bounded subset of \mathbb{C}^d is sequentially compact.

• Continuity

- Let (X, ρ) and (Y, m) be metric spaces. Let $f: X \rightarrow Y$ be a function.
- (Continuity of a point) A function f is continuous at a point \mathbf{x}_0 if
 - $\forall \varepsilon > 0, \exists \delta = \delta(\mathbf{x}_0, \varepsilon) \ni \forall \mathbf{x} \in X, \rho(\mathbf{x}, \mathbf{x}_0) < \delta \Leftrightarrow m(f(\mathbf{x}), f(\mathbf{x}_0)) < \varepsilon$, or
 - $\forall \varepsilon > 0, \exists \delta = \delta(\mathbf{x}_0, \varepsilon) \ni \forall \mathbf{x} \in X, \mathbf{x} \in B_\rho(\mathbf{x}_0, \delta) \Leftrightarrow f(\mathbf{x}) \in B_m(f(\mathbf{x}_0), \varepsilon)$.
- (Continuity on a set) A function f is continuous on a subset $D \subset X$ if f is continuous at

each point $\mathbf{x}_0 \in D$.

- A function f is continuous at a point $\mathbf{x}_0 \Leftrightarrow$ for every sequence $\mathbf{x}_n \rightarrow \mathbf{x}_0, f(\mathbf{x}_n) \rightarrow f(\mathbf{x}_0)$.

In other words, f is *convergence preserving* iff f is continuous.

- (Uniform continuity) A function f is *uniformly continuous on a subset* $D \subset X$ if

$$\forall \varepsilon > 0, \exists \delta = \delta(\varepsilon) > 0 \ni \forall \mathbf{x}, \mathbf{x}_0 \in D, \rho(\mathbf{x}, \mathbf{x}_0) < \delta \Leftrightarrow m(f(\mathbf{x}), f(\mathbf{x}_0)) < \varepsilon.$$

Topology

Let X be a metric space with a metric ρ .

• Ball

- A ball is defined as $B(x, r) = B_r(x) := \{y \in X : \rho(x, y) < r\}, x \in X$.

• Open set

- A set $U \subset X$ is open if $\forall x \in U, \exists \varepsilon > 0$ with $B(x, \varepsilon) \subset U$.

- A set $U \subset X$ is not open if $\forall \varepsilon > 0, \exists x \in U$ with $B(x, \varepsilon) \not\subset U$.

- The whole space X and \emptyset are both open.

- The set $B(x, r)$ is open, i.e. it is an open ball.

• Closed set

- A set $F \subset X$ is closed if its complement $F^c := \{x \in X : x \notin F\}$ is open.

- X, \emptyset , and $B(x, r)^c = \{y \in X : \rho(x, y) \geq r\}$ are all closed sets.

- Every (possibly infinite) union of open sets is an open set.

- Every intersection of finite number of open sets is an open set.

• Topological space

- Let X be a nonempty set and \mathfrak{T} be a collection of subsets of X . \mathfrak{T} is called a topology for X if

(1) $\emptyset \in \mathfrak{T}$ and $X \in \mathfrak{T}$

(2) If $U_\alpha \in \mathfrak{T}$, then $\cup_\alpha U_\alpha \in \mathfrak{T}$

(3) If $U_1 \in \mathfrak{T}$ and $U_2 \in \mathfrak{T}$, then $U_1 \cap U_2 \in \mathfrak{T}$.

- The pair (X, \mathfrak{T}) or X is called a topological space.

- The elements of \mathfrak{T} are open sets.

- A set F is closed if $F^c \in \mathfrak{T}$.

• Properties of topological space

- A set U is open \Leftrightarrow for every $x \in U$, there is an open set containing x , say O_x , with $O_x \subset U$.

- The closure of a set E is $\bar{E} := \bigcap_{\substack{C: E \subset C \text{ and} \\ C \text{ is closed}}} C$ and $E \subset \bar{E}$. \bar{E} is the smallest closed set containing E .
- A set E is closed $\Leftrightarrow E = \bar{E}$.
- A point x is an accumulation point (or cluster point or limit point) of a set E if for every open set containing x , say O_x , there is a point $y \neq x$ with $y \in O_x \cap E$. We let E' denote the set of accumulation points of E . The point x may or may not be in E .
- E is closed $\Leftrightarrow E' \subset E$.
- $\bar{E} = E \cup E'$
- The boundary of E is ∂E and $\partial E := \bar{E} \cap \overline{E^c}$.
- The interior of E is E^o and $E^o := (\overline{E^c})^c$. E^o is an open set with $E^o \subset E$ and $\bar{E} \setminus E^o = \bar{E} \cap \overline{E^c} = \partial E$.

Normed Vector Space

Let F denote \mathbb{R} or \mathbb{C} and V be a vector space over F .

• Norm

- $\|\bullet\|$ is a norm if

$$(1) \quad 0 \leq \|\mathbf{v}\| < \infty, \forall \mathbf{v} \in V \quad \text{and} \quad \|\mathbf{v}\| = 0 \quad \text{iff} \quad \mathbf{v} = \mathbf{0},$$

$$(2) \quad \|a\mathbf{v}\| = |a| \|\mathbf{v}\|, \forall \mathbf{v} \in V, \forall a \in F, \text{ and}$$

$$(3) \quad \|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|, \forall \mathbf{v}, \mathbf{w} \in V \quad (\text{triangular inequality}).$$

- Every normed vector space is a metric space with $\rho(\mathbf{v}, \mathbf{w}) = \|\mathbf{v} - \mathbf{w}\|$.

- A sequence \mathbf{v}_n converges to \mathbf{v} (i.e., $\mathbf{v}_n \rightarrow \mathbf{v}$) iff $\|\mathbf{v}_n - \mathbf{v}\| \rightarrow 0$.

$$- \quad \left| \|\mathbf{v}\| - \|\mathbf{w}\| \right| \leq \|\mathbf{v} - \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|.$$

• Banach space

- A complete normed vector space is called Banach space.

• Examples of norm

- The p -norm on $V = \mathbb{R}^n$ or \mathbb{C}^n . Let $\mathbf{v} = (v_1, v_2, \dots, v_n)$, then

$$\|\mathbf{v}\|_p := \begin{cases} \left(\sum_{k=1}^n |v_k|^p \right)^{1/p}, & 1 \leq p < \infty \\ \max_{1 \leq k \leq n} |v_k|, & p = \infty \end{cases}.$$

- When $p = 2$, we call it Euclidean norm.

- The uniform norm. Let U be any set and let $F = \mathbb{R}$ or \mathbb{C} . Let X denote the vector space of mappings from U into F . Let X_b denote the set of bounded mappings, i.e.

$$X_b := \left\{ x \in X : \sup_{u \in U} |x(u)| < \infty \right\}. \text{ Note that if } U \text{ is a finite set, then } X = X_b. \text{ The uniform}$$

norm of $x \in X_b$ is $\|x\| := \sup_{u \in U} |x(u)|$. X_b with the uniform norm is a Banach space.

• The ℓ^p spaces

- Let $U = \{1, 2, 3, \dots\}$. For $k \in U$, we write x_k instead of $x(k)$. Then, X denotes the set

of all real- or complex-valued sequences. For $1 \leq p < \infty$, let

$$\ell^p := \left\{ x \in X : \sum_{k=1}^{\infty} |x_k|^p < \infty \right\},$$

and set

$$\ell^\infty := \left\{ x \in X : \sup_k |x_k| < \infty \right\}.$$

- ℓ^p spaces is equipped with the corresponding p -norm.

• Projections

- Let V be a normed vector space and G be a subset of V . If there exists a vector $\hat{\mathbf{v}} \in G$

such that $\|\mathbf{v} - \hat{\mathbf{v}}\| \leq \|\mathbf{v} - \mathbf{w}\|, \forall \mathbf{w} \in G, \mathbf{v} \in V$, then $\hat{\mathbf{v}}$ is a projection of \mathbf{v} onto G .

- A projection may not exist (for example, if G is open) and may not be unique (for example, if G is not convex).

- Projections exist when G is a closed ball in an arbitrary, possibly infinite-dimensional, normed vector space.

• Finite-dimensional subspaces

- Let W be a finite-dimensional normed vector space or a finite-dimensional subspace of a normed vector space. W may be a subspace of a larger infinite-dimensional space V .

Then,

(1) W is complete, i.e., W is a Banach space.

(2) Every closed and bounded subset G of W is (sequentially) compact.

• Projections onto closed finite-dimensional subsets

- If G is a nonempty closed and bounded subset of a finite-dimensional subspace W of a larger normed vector space V , then the projection of every $\mathbf{v} \in V$ onto G always exists.

- If W is a finite-dimensional subspace of a larger normed vector space V , then the projection of any $\mathbf{v} \in V$ onto W always exists.

Inner Product Spaces

Let F denote \mathbb{R} or \mathbb{C} and V be a vector space over F . For $a \in \mathbb{C}$, \bar{a} denotes the complex conjugate of a .

• Inner product space (pre-Hilbert space)

- $\langle \cdot, \cdot \rangle$ is an *inner product* on V if the following properties hold:

$$(1) \quad 0 \leq \langle \mathbf{v}, \mathbf{v} \rangle < \infty, \forall \mathbf{v} \in V \quad \text{and} \quad \langle \mathbf{v}, \mathbf{v} \rangle = 0 \text{ iff } \mathbf{v} = \mathbf{0},$$

$$(2) \quad \langle \mathbf{v}, \mathbf{w} \rangle = \overline{\langle \mathbf{w}, \mathbf{v} \rangle}, \forall \mathbf{v}, \mathbf{w} \in V$$

$$(3) \quad \langle a\mathbf{u} + b\mathbf{v}, \mathbf{w} \rangle = a\langle \mathbf{u}, \mathbf{w} \rangle + b\langle \mathbf{v}, \mathbf{w} \rangle, \forall a, b \in F, \forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in V.$$

- $\langle \mathbf{v}, \mathbf{w} \rangle$ is in general complex number but $\langle \mathbf{v}, \mathbf{v} \rangle$ is always real.

$$- \langle \mathbf{w}, a\mathbf{u} + b\mathbf{v} \rangle = \bar{a}\langle \mathbf{w}, \mathbf{u} \rangle + \bar{b}\langle \mathbf{w}, \mathbf{v} \rangle$$

- $\langle \mathbf{v}, \mathbf{0} \rangle = 0$. If $\langle \mathbf{v}, \mathbf{w} \rangle = 0, \forall \mathbf{w} \in V$, then $\mathbf{v} = \mathbf{0}$.

• Hilbert space

- A complete inner product space is *Hilbert space*.

• Norm on an inner product space

- Given any inner product, $\|\mathbf{v}\| := \langle \mathbf{v}, \mathbf{v} \rangle^{1/2}$ defines a norm on V .

• Parallelogram equality

$$- \|\mathbf{u} + \mathbf{v}\|^2 + \|\mathbf{u} - \mathbf{v}\|^2 = 2(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2)$$

• Cauchy-Schwarz inequality

$$- |\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\| \|\mathbf{v}\|$$

- If $\mathbf{v} \neq \mathbf{0}$, then equality holds iff $\mathbf{u} = a\mathbf{v}$ for some $a \in F$.

- Angle between \mathbf{u} and \mathbf{v} , $\theta = \angle(\mathbf{u}, \mathbf{v}) = \cos^{-1} \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\| \|\mathbf{v}\|}$ and $\langle \mathbf{u}, \mathbf{v} \rangle = \|\mathbf{u}\| \|\mathbf{v}\| \cos \theta$

(a) $\theta = 0 \Rightarrow \mathbf{u}$ and \mathbf{v} are aligned $\Rightarrow \langle \mathbf{u}, \mathbf{v} \rangle = \|\mathbf{u}\| \|\mathbf{v}\|$, $\mathbf{v} = \alpha \mathbf{u}$ for some $\alpha \geq 0$

(b) $\theta = \pi \Rightarrow \mathbf{u}$ and \mathbf{v} are opposed $\Rightarrow \langle \mathbf{u}, \mathbf{v} \rangle = -\|\mathbf{u}\| \|\mathbf{v}\|$, $\mathbf{v} = \alpha \mathbf{u}$ for some $\alpha < 0$

(c) $\theta = \pm\pi/2 \Rightarrow \mathbf{u}$ and \mathbf{v} are orthogonal $\Rightarrow \langle \mathbf{u}, \mathbf{v} \rangle = 0$, $\mathbf{v} \perp \mathbf{u}$

• Orthogonality

- A collection of vectors G is (mutually) orthogonal if $\langle \mathbf{u}, \mathbf{v} \rangle = 0$, $\forall \mathbf{u}, \mathbf{v} \in G$ with $\mathbf{u} \neq \mathbf{v}$.

- If, in addition, $\|\mathbf{u}\| = 1$, $\forall \mathbf{u} \in G$, then they are orthonormal.

- Orthonormal set of vectors are linearly independent. The converse may not be true.

• Some identities

- (Parallelogram law) In any inner product space, $\|\mathbf{u} + \mathbf{v}\|^2 + \|\mathbf{u} - \mathbf{v}\|^2 = 2(\|\mathbf{u}\|^2 + \|\mathbf{v}\|^2)$.

- (Polarization identity) In a complex inner product space,

$$4\langle \mathbf{u}, \mathbf{v} \rangle = \|\mathbf{u} + \mathbf{v}\|^2 - \|\mathbf{u} - \mathbf{v}\|^2 + j\|\mathbf{u} + j\mathbf{v}\|^2 - j\|\mathbf{u} - j\mathbf{v}\|^2.$$

• The orthogonality principle (OP)

- Let V be an inner product space. Let W be a subspace of V . Fix any $\mathbf{v} \in V$. Then, a vector $\tilde{\mathbf{v}} \in W$ has the property that

$$\|\mathbf{v} - \tilde{\mathbf{v}}\| \leq \|\mathbf{v} - \mathbf{w}\|, \forall \mathbf{w} \in W \quad \text{iff} \quad \langle \mathbf{v} - \tilde{\mathbf{v}}, \mathbf{w} \rangle = 0, \forall \mathbf{w} \in W.$$

Furthermore, there is at most one element $\tilde{\mathbf{v}} \in W$ satisfying the condition.

- If $\tilde{\mathbf{v}} \in W$ exists, it is unique. But it may not exist.

- If $\tilde{\mathbf{v}} \in W$ exists, then $\tilde{\mathbf{v}}$ is the orthogonal projection of \mathbf{v} onto W .

- Note that

$$(1) \quad \|\mathbf{v}\|^2 = \|\mathbf{v} - \tilde{\mathbf{v}}\|^2 + \|\tilde{\mathbf{v}}\|^2$$

$$(2) \quad \|\mathbf{v} - \tilde{\mathbf{v}}\|^2 = \|\mathbf{v}\|^2 - \|\tilde{\mathbf{v}}\|^2$$

$$(3) \quad \|\mathbf{v}\| \geq \|\tilde{\mathbf{v}}\|$$

• Projections onto finite-dimensional spaces

- Let V be an inner product space. Let W be a finite-dimensional subspace of V . Then,

$\exists \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\} \ni \text{span}\{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\} = W$ and OP is as follows.

$$\|\mathbf{v} - \tilde{\mathbf{v}}\| \leq \|\mathbf{v} - \mathbf{w}\|, \forall \mathbf{w} \in W \quad \text{iff} \quad \langle \mathbf{v} - \tilde{\mathbf{v}}, \mathbf{w}_i \rangle = 0, i = 1, 2, \dots, n.$$

- If $\tilde{\mathbf{v}}$ exists, $\tilde{\mathbf{v}} = \sum_{j=1}^n c_j \mathbf{w}_j$ (i.e. $\tilde{\mathbf{v}} \in W$).

- Note that

$$(1) \quad \langle \mathbf{v}, \mathbf{w}_i \rangle = \sum_{j=1}^n \langle \mathbf{w}_j, \mathbf{w}_i \rangle c_j, i = 1, 2, \dots, n, \text{ or equivalently}$$

$$(2) \quad \mathbf{A}\mathbf{c} = \mathbf{b} \quad \text{where} \quad A_{ij} := \langle \mathbf{w}_j, \mathbf{w}_i \rangle, \mathbf{b} := [\langle \mathbf{v}, \mathbf{w}_1 \rangle, \dots, \langle \mathbf{v}, \mathbf{w}_n \rangle]^T, \mathbf{c} := [c_1, \dots, c_n]^T.$$

And, \mathbf{A} is nonsingular if $\{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\}$ is linearly independent.

- If $\{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\}$ is orthonormal, then $\mathbf{A} = \mathbf{I}$ and $c_i = \langle \mathbf{v}, \mathbf{w}_i \rangle$, and thus

$$\tilde{\mathbf{v}} = \sum_{j=1}^n \langle \mathbf{v}, \mathbf{w}_j \rangle \mathbf{w}_j \quad \text{and} \quad \|\tilde{\mathbf{v}}\|^2 = \sum_{j=1}^n |\langle \mathbf{v}, \mathbf{w}_j \rangle|^2$$

- Bessel's inequality for an orthonormal basis is $\sum_{j=1}^n |\langle \mathbf{v}, \mathbf{w}_j \rangle|^2 \leq \|\mathbf{v}\|^2 < \infty$.

- Since $\mathbf{v} = \tilde{\mathbf{v}}$ iff $\mathbf{v} \in W$, $\|\mathbf{v}\|^2 = \sum_{j=1}^n |\langle \mathbf{v}, \mathbf{w}_j \rangle|^2, \forall \mathbf{v} \in W$.

• Orthogonal complement

- For any subset W of an inner product space V , we define the orthogonal complement of W as

$$W^\perp := \{\mathbf{v} \in V : \langle \mathbf{w}, \mathbf{v} \rangle = 0, \forall \mathbf{w} \in W\}$$

- W^\perp is a subspace of V .

- W^\perp is a closed set.

- $W \subset (W^\perp)^\perp$. If W is a closed subspace of a Hilbert space, $W = (W^\perp)^\perp$.
- If W is an arbitrary subset of a Hilbert space, $(W^\perp)^\perp = \overline{\text{span } W}$.

- **Convex set**

- Let X be an arbitrary vector space over \mathbb{R} or \mathbb{C} . A subset $C \subset X$ is convex if $\lambda \mathbf{x} + (1-\lambda)\mathbf{y} \in C, \forall \mathbf{x}, \mathbf{y} \in C, \forall \lambda \in [0, 1]$.
- In a normed vector space, open balls are convex.
- A subspace is a convex set.

- **Projection theorem**

- Let C be a closed, convex subset of a Hilbert space X . Then, for every $\mathbf{x} \in X$, there exists the unique $\tilde{\mathbf{x}} \in C$ such that $\|\mathbf{x} - \tilde{\mathbf{x}}\| \leq \|\mathbf{x} - \mathbf{y}\|, \forall \mathbf{y} \in C$.
- If M is a closed subspace of a Hilbert space X , then $\mathbf{x} = \tilde{\mathbf{x}} + (\mathbf{x} - \tilde{\mathbf{x}}), \forall \mathbf{x} \in X$ where $\tilde{\mathbf{x}} \in M$ and $\mathbf{x} - \tilde{\mathbf{x}} \in M^\perp$.

- **Sums and direct sums of subspaces**

- If U and W are two subspaces of a vector space V , their sum is

$$U + W := \{\mathbf{u} + \mathbf{w} : \mathbf{u} \in U \text{ and } \mathbf{w} \in W\}.$$

- If every element in $U + W$ has a unique representation, their sum becomes the direct sum as $U \oplus W$.
- $U + W = U \oplus W$ iff $U \cap W = \{\mathbf{0}\}$.
- If M is a closed subspace of a Hilbert space X , then $X = M \oplus M^\perp$.