Chapter 2

Finite-Dimensional Vector Spaces

2.1 Vectors and Linear Transformations

2.1.1 Vector Spaces

- A **vector space** consists of a set $E$, whose elements are called **vectors**, and a field $\mathbb{F}$ (such as $\mathbb{R}$ or $\mathbb{C}$), whose elements are called **scalars**. There are two operations on a vector space:

  1. **Vector addition**, $+: E \times E \to E$, that assigns to two vectors $u, v \in E$ another vector $u + v$, and
  2. **Multiplication by scalars**, $\cdot: \mathbb{R} \times E \to E$, that assigns to a vector $v \in E$ and a scalar $a \in \mathbb{R}$ a new vector $av \in E$.

The vector addition is an **associative commutative** operation with an **additive identity**. It satisfies the following conditions:

1. $u + v = v + u, \quad \forall u, v, \in E$
2. $(u + v) + w = u + (v + w), \quad \forall u, v, w \in E$
3. There is a vector $0 \in E$, called the **zero vector**, such that for any $v \in E$ there holds $v + 0 = v$.
4. For any vector $v \in E$, there is a vector $(-v) \in E$, called the **opposite** of $v$, such that $v + (-v) = 0$.

The multiplication by scalars satisfies the following conditions:
1. \( a(bv) = (ab)v, \quad \forall v \in E, \forall a, b \mathbb{R}, \)

2. \( (a + b)v = av + bv, \quad \forall v \in E, \forall a, b \mathbb{R}, \)

3. \( a(u + v) = au + av, \quad \forall u, v \in E, \forall a \mathbb{R}, \)

4. \( 1v = v \quad \forall v \in E. \)

- The zero vector is unique.
- For any \( u, v \in E \) there is a unique vector denoted by \( w = v - u \), called the difference of \( v \) and \( u \), such that \( u + w = v \).
- For any \( v \in E, \)
  \[ 0v = 0, \quad \text{and} \quad (-1)v = -v. \]
- Let \( E \) be a real vector space and \( \mathcal{A} = \{e_1, \ldots, e_k\} \) be a finite collection of vectors from \( E \). A **linear combination** of these vectors is a vector
  \[ a_1e_1 + \cdots + a_ke_k, \]
  where \( \{a_1, \ldots, a_n\} \) are scalars.
- A finite collection of vectors \( \mathcal{A} = \{e_1, \ldots, e_k\} \) is **linearly independent** if
  \[ a_1e_1 + \cdots + a_ke_k = 0 \]
  implies \( a_1 = \cdots = a_k = 0 \).
- A collection \( \mathcal{A} \) of vectors is **linearly dependent** if it is not linearly independent.
- Two non-zero vectors \( u \) and \( v \) which are linearly dependent are also called **parallel**, denoted by \( u \| v \).
- A collection \( \mathcal{A} \) of vectors is linearly independent if no vector of \( \mathcal{A} \) is a linear combination of a finite number of vectors from \( \mathcal{A} \).
- Let \( \mathcal{A} \) be a subset of a vector space \( E \). The **span** of \( \mathcal{A} \), denoted by \( \text{span} \mathcal{A} \), is the subset of \( E \) consisting of all finite linear combinations of vectors from \( \mathcal{A} \), i.e.
  \[ \text{span} \mathcal{A} = \{v \in E \mid v = a_1e_1 + \cdots + a_ke_k , \quad e_i \in \mathcal{A}, \quad a_i \in \mathbb{R} \}. \]

We say that the subset \( \text{span} \mathcal{A} \) is spanned by \( \mathcal{A} \).
• **Theorem 2.1.1** The span of any subset of a vector space is a vector space.

• A **vector subspace** of a vector space \( E \) is a subset \( S \subseteq E \) of \( E \) which is itself a vector space.

• **Theorem 2.1.2** A subset \( S \) of \( E \) is a vector subspace of \( E \) if and only if \( \text{span} \; S = S \).

• Span of \( \mathcal{A} \) is the smallest subspace of \( E \) containing \( \mathcal{A} \).

• A collection \( \mathcal{B} \) of vectors of a vector space \( E \) is a **basis** of \( E \) if \( \mathcal{B} \) is linearly independent and \( \text{span} \; \mathcal{B} = E \).

• A vector space \( E \) is **finite-dimensional** if it has a finite basis.

• **Theorem 2.1.3** If the vector space \( E \) is finite-dimensional, then the number of vectors in any basis is the same.

• The **dimension** of a finite-dimensional real vector space \( E \), denoted by \( \dim E \), is the number of vectors in a basis.

• **Theorem 2.1.4** If \( \{e_1, \ldots, e_n\} \) is a basis in \( E \), then for every vector \( v \in E \) there is a unique set of real numbers \((v^i) = (v^1, \ldots, v^n)\) such that

\[
  v = \sum_{i=1}^{n} v^i e_i = v^1 e_1 + \cdots + v^n e_n.
\]

• The real numbers \( v^i, i = 1, \ldots, n \), are called the **components of the vector** \( v \) **with respect to the basis** \( \{e_i\} \).

• It is customary to denote the components of vectors by **superscripts**, which should not be confused with powers of real numbers

\[
  v^2 \neq (v)^2 = vv, \quad \ldots, \quad v^n \neq (v)^n.
\]

**Examples of Vector Subspaces**

• **Zero subspace** \( \{0\} \).

• **Line** with a tangent vector \( u \):

\[
  S_1 = \text{span} \{u\} = \{v \in E \mid v = tu, \; t \in \mathbb{R}\}.
\]
• **Plane** spanned by two nonparallel vectors \( \mathbf{u}_1 \) and \( \mathbf{u}_2 \)

\[
S_2 = \text{span} \{ \mathbf{u}_1, \mathbf{u}_2 \} = \{ \mathbf{v} \in E \mid \mathbf{v} = t \mathbf{u}_1 + s \mathbf{u}_2, \ t, s \in \mathbb{R} \}.
\]

• More generally, a **\( k \)-plane** spanned by a linearly independent collection of \( k \) vectors \( \{ \mathbf{u}_1, \ldots, \mathbf{u}_k \} \)

\[
S_k = \text{span} \{ \mathbf{u}_1, \ldots, \mathbf{u}_k \} = \{ \mathbf{v} \in E \mid \mathbf{v} = t_1 \mathbf{u}_1 + \cdots + t_k \mathbf{u}_k, \ t_1, \ldots, t_k \in \mathbb{R} \}.
\]

• An \((n - 1)\)-plane in an \( n \)-dimensional vector space is called a **hyperplane**.

• **Examples of vector spaces:** \( P[t], P_n[t], M_{m \times n}, C^k([a, b]), C^\infty([a, b]) \)

### 2.1.2 Inner Product and Norm

• A complex vector space \( E \) is called an **inner product space** if there is a function \( (\cdot, \cdot) : E \times E \to \mathbb{R} \), called the **inner product**, that assigns to every two vectors \( \mathbf{u}, \mathbf{v} \) a complex number \( (\mathbf{u}, \mathbf{v}) \) and satisfies the conditions:

\[
\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in E, \ \forall a \in \mathbb{C}:
\]

1. \( (\mathbf{v}, \mathbf{v}) \geq 0 \)
2. \( (\mathbf{v}, \mathbf{v}) = 0 \) if and only if \( \mathbf{v} = 0 \)
3. \( (\mathbf{u}, \mathbf{v}) = (\mathbf{v}, \mathbf{u}) \)
4. \( (\mathbf{u} + \mathbf{v}, \mathbf{w}) = (\mathbf{u}, \mathbf{w}) + (\mathbf{v}, \mathbf{w}) \)
5. \( (a \mathbf{u}, \mathbf{v}) = a(\mathbf{u}, \mathbf{v}) \)

A finite-dimensional real inner product space is called a **Euclidean space**.

• **Examples:** On \( C([a, b]) \)

\[
(f, g) = \int_a^b \tilde{f}(t)g(t)w(t)dt
\]

where \( w \) is a positive continuous real-valued function called the **weight function**.

• The **Euclidean norm** is a function \( \| \cdot \| : E \to \mathbb{R} \) that assigns to every vector \( \mathbf{v} \in E \) a real number \( \| \mathbf{v} \| \) defined by

\[
\| \mathbf{v} \| = \sqrt{(\mathbf{v}, \mathbf{v})}.
\]
• The norm of a vector is also called the **length**.

• A vector with unit norm is called a **unit vector**.

• The natural **distance function** (a **metric**) is defined by

  \[ d(u, v) = ||u - v|| \]

• **Example.**

• **Theorem 2.1.5** For any \( u, v \in E \) there holds

  \[ ||u + v||^2 = ||u||^2 + 2\text{Re}(u, v) + ||v||^2. \]

• If the norm satisfies the parallelogram law

  \[ ||u + v||^2 + ||u - v||^2 = 2||u||^2 + 2||v||^2 \]

  then the inner product can be defined by

  \[ (u, v) = \frac{1}{4} \left( ||u + v||^2 - ||u - v||^2 - i||u + iv||^2 + i||u - iv||^2 \right) \]

• **Theorem 2.1.6** A normed linear space is an inner product space if and only if the norm satisfies the parallelogram law.

• **Theorem 2.1.7** Every finite-dimensional vector space can be turned into an inner product space.

• **Theorem 2.1.8** Cauchy-Schwarz’s Inequality. **For any** \( u, v \in E \) **there holds**

  \[ |(u, v)| \leq ||u|| \cdot ||v||. \]

  The equality

  \[ |(u, v)| = ||u|| \cdot ||v|| \]

  holds if and only if \( u \) and \( v \) are parallel.

• **Corollary 2.1.1** Triangle Inequality. **For any** \( u, v \in E \) **there holds**

  \[ ||u + v|| \leq ||u|| + ||v||. \]
• In real vector space the **angle between two non-zero vectors** $u$ and $v$ is defined by

$$
\cos \theta = \frac{(u, v)}{||u|| \ ||v||}, \quad 0 \leq \theta \leq \pi.
$$

Then the inner product can be written in the form

$$(u, v) = ||u|| \ ||v|| \cos \theta.
$$

• Two non-zero vectors $u, v \in E$ are **orthogonal**, denoted by $u \perp v$, if

$$(u, v) = 0.
$$

• A basis \{e_1, \ldots, e_n\} is called **orthonormal** if each vector of the basis is a unit vector and any two distinct vectors are orthogonal to each other, that is,

$$(e_i, e_j) = \begin{cases} 
1, & \text{if } i = j \\
0, & \text{if } i \neq j
\end{cases}.
$$

**Theorem 2.1.9** Every Euclidean space has an orthonormal basis.

• Let $S \subset E$ be a nonempty subset of $E$. We say that $x \in E$ is **orthogonal** to $S$, denoted by $x \perp S$, if $x$ is orthogonal to every vector of $S$.

• The set

$$S^\perp = \{x \in E \mid x \perp S\}
$$

of all vectors orthogonal to $S$ is called the **orthogonal complement** of $S$.

**Theorem 2.1.10** The orthogonal complement of any subset of a Euclidean space is a vector subspace.

• Two subsets $A$ and $B$ of $E$ are **orthogonal**, denoted by $A \perp B$, if every vector of $A$ is orthogonal to every vector of $B$.

• Let $S$ be a subspace of $E$ and $S^\perp$ be its orthogonal complement. If every element of $E$ can be uniquely represented as the sum of an element of $S$ and an element of $S^\perp$, then $E$ is the **direct sum** of $S$ and $S^\perp$, which is denoted by

$$E = S \oplus S^\perp.
$$

• The union of a basis of $S$ and a basis of $S^\perp$ gives a basis of $E.$
2.1. VECTORS AND LINEAR TRANSFORMATIONS

2.1.3 Exercises

1. Show that if $\lambda v = 0$, then either $v = 0$ or $\lambda = 0$.

2. Prove that the span of a collection of vectors is a vector subspace.

3. Show that the Euclidean norm has the following properties
   (a) $||v|| \geq 0, \forall v \in E$;
   (b) $||v|| = 0$ if and only if $v = 0$;
   (c) $||\lambda v|| = |\lambda||v||, \forall v \in E, \forall \lambda \in \mathbb{R}$.

4. **Parallelogram Law.** Show that for any $u, v \in E$

   $$||u + v||^2 + ||u - v||^2 = 2(||u||^2 + ||v||^2)$$

5. Show that any orthogonal system in $E$ is linearly independent.

6. **Gram-Schmidt orthonormalization process.** Let $G = \{u_1, \cdots, u_k\}$ be a linearly independent collection of vectors. Let $O = \{v_1, \cdots, v_k\}$ be a new collection of vectors defined recursively by

   $$v_1 = u_1,$$

   $$v_j = u_j - \sum_{i=1}^{j-1} \frac{v_i(u_i, u_j)}{||v_i||^2}, \quad 2 \leq j \leq k,$$

   and the collection $B = \{e_1, \ldots, v_k\}$ be defined by

   $$e_i = \frac{v_i}{||v_i||}.$$

   Show that: a) $O$ is an orthogonal system and b) $B$ is an orthonormal system.

7. **Pythagorean Theorem.** Show that if $u \perp v$, then

   $$||u + v||^2 = ||u||^2 + ||v||^2.$$

8. Let $B = \{e_1, \cdots, e_n\}$ be an orthonormal basis in $E$. Show that for any vector $v \in E$

   $$v = \sum_{i=1}^{n} e_i(e_i, v)$$

   and

   $$||v||^2 = \sum_{i=1}^{n} (e_i, v)^2.$$
9. Prove that the orthogonal complement of a subset $S$ of $E$ is a vector subspace of $E$.

10. Let $S$ be a subspace in $E$. Prove that

a) $E^\perp = \{0\}$, 
b) $\{0\}^\perp = E$, 
c) $(S^\perp)^\perp = S$.

11. Show that the intersection of orthogonal subsets of a Euclidean space is either empty or consists of only the zero vector. That is, for two subsets $A$ and $B$, if $A \perp B$, then $A \cap B = \{0\}$ or $\emptyset$.

2.1.4 Linear Transformations.

- A **linear transformation** from a vector space $V$ to a vector space $W$ is a map

  $$ T : V \rightarrow W $$

  satisfying the condition:

  $$ T(\alpha u + \beta v) = \alpha Tu + \beta T v $$

  for any $u, v \in V$ and $\alpha, \beta \in \mathbb{C}$.

- Zero transformation maps all vectors to the zero vector.

- The linear transformation is called an **endomorphism** (or a linear **operator**) if $V = W$.

- The linear transformation is called a **linear functional** if $W = \mathbb{C}$.

- A linear transformation is uniquely determined by its action on a basis.

- The set of linear transformations from $V$ to $W$ is a vector space denoted by $L(V, W)$.

- The set of endomorphisms (operators) on $V$ is denoted by $\text{End}(V)$ or $L(V)$.

- The set of linear functionals on $V$ is called the **dual space** and is denoted by $V^*$.

- **Example.**

  - The **kernel (null space)** (denoted by $\text{Ker} T$) of a linear transformation $T : V \rightarrow W$ is the set of vectors in $V$ that are mapped to zero.
• **Theorem 2.1.11** *The kernel of a linear transformation is a vector space.*

- The dimension of a finite-dimensional kernel is called the **nullity** of the linear transformation.

\[ \text{null } T = \dim \text{Ker } T \]

• **Theorem 2.1.12** *The range of a linear transformation is a vector space.*

- The dimension of a finite-dimensional range is called the **rank** of the linear transformation.

\[ \text{rank } T = \dim \text{Im } T \]

• **Theorem 2.1.13** *Dimension Theorem.* Let \( T : V \rightarrow W \) be a linear transformation between finite-dimensional vector spaces. Then

\[ \dim \text{Ker } T + \dim \text{Im } T = \dim V. \]

• **Theorem 2.1.14** *A linear transformation is injective if and only if its kernel is zero.*

• An endomorphism of a finite-dimensional space is bijective if it is either injective or surjective.

• Two vector spaces are **isomorphic** if they can be related by a bijective linear transformation (which is called an **isomorphism**).

• An isomorphism is called an **automorphism** if \( V = W \).

• The set of all automorphisms of \( V \) is denoted by \( \text{Aut}(V) \) or \( GL(V) \).

• A linear surjection is an isomorphism if and only if its nullity is zero.

• **Theorem 2.1.15** *An isomorphism maps linearly independent sets onto linearly independent sets.*

• **Theorem 2.1.16** *Two finite-dimensional vector spaces are isomorphic if and only if they have the same dimension.*

• All \( n \)-dimensional complex vector spaces are isomorphic to \( \mathbb{C}^n \).

• All \( n \)-dimensional real vector spaces are isomorphic to \( \mathbb{R}^n \).
• The **dual basis** $f_i$ in the dual space $V^*$ is defined by
  \[ f_i(e_j) = \delta_{ij}, \]
  where $e_j$ is the basis in $V$.

• **Theorem 2.1.17** *The dual space $V^*$ is isomorphic to $V$.*

• The **dual** (or the **pullback**) of a linear transformation $T : V \rightarrow W$ is the linear transformation $T^* : W^* \rightarrow V^*$ defined for any $g \in W^*$ by
  \[ (T^*g)\nu = g(T\nu), \quad \nu \in V. \]

• Graph.

• If $T$ is surjective then $T^*$ is injective.

• If $T$ is injective then $T^*$ is surjective.

• If $T$ is an isomorphism then $T^*$ is an isomorphism.

### 2.1.5 Algebras

• An **algebra** $A$ is a vector space together with a binary operation called multiplication satisfying the conditions:
  \[ u(\alpha v + \beta w) = \alpha uv + \beta uw \]
  \[ (\alpha v + \beta w)u = \alpha vu + \beta wu \]
  for any $u, v, w, \alpha, \beta \in \mathbb{C}$.

• **Examples.** Matrices, functions, operators.

• The dimension of the algebra is the dimension of the vector space.

• The algebra is **associative** if
  \[ u(vw) = (uv)w \]
  and **commutative** if
  \[ uv = vu \]
• An **algebra with identity** is an algebra with an identity element $1$ satisfying
\[ u1 = 1u = u \]
for any $u \in A$.

• An element $v$ is a **left inverse** of $u$ if
\[ vu = 1 \]
and the **right inverse** if
\[ uv = 1. \]

• **Example.** Lie algebras.

• An operator $D : A \to A$ on an algebra $A$ is called a **derivation** if it satisfies
\[ D(uv) = (Du)v + uDv \]

• **Example.** Let $A = \text{Mat}(n)$ be the algebra of square matrices of dimension $n$ with the binary operation being the commutator of matrices.

• It is easy to show that for any matrices $A, B, C$ the following identity (**Jacobi identity**) holds
\[ [A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0 \]

• Let $C$ be a fixed matrix. We define an operator $\text{Ad}_C$ on the algebra by
\[ \text{Ad}_C B = [C, B] \]
Then this operator is a derivation since for any matrices $A, B$
\[ \text{Ad}_C [A, B] = [\text{Ad}_C A, B] + [A, \text{Ad}_C B] \]

• A linear transformation $T : A \to B$ from an algebra $A$ to an algebra $B$ is called an **algebra homomorphism** if
\[ T(uv) = T(u)T(v) \]
for any $u, v \in A$. 
• An algebra homomorphism is called an **algebra isomorphism** if it is bijective.

**Example.** The isomorphism of the Lie algebra $so(3)$ and $\mathbb{R}^3$ with the cross product.

Let $X_i, i = 1, 2, 3$ be the antisymmetric matrices defined by

$$(X_i)^j_k = \varepsilon^j_{ik}.$$ 

They form an algebra with respect to the commutator

$$[X_i, X_j] = \varepsilon^{k}_{ijk}X_k.$$ 

We define a map $T : \mathbb{R}^3 \rightarrow so(3)$ as follows. Let $v = v^i e_i$ be a vector in $\mathbb{R}^3$. Then

$$T(v) = v^i X_i.$$ 

let $\mathbb{R}^3$ be equipped with the cross product. Then

$$T(v \times u) = (Tv)(Tu)$$

Thus $T$ is an isomorphism (linear bijective algebra homomorphism).

• Any finite dimensional vector space can be converted into an algebra by defining the multiplication of the basis vectors by

$$e_i e_j = \sum_{k=1}^{n} C_{ij}^k e_k$$

where $C_{ij}^k$ are some scalars called the **structure constants** of the algebra.

**Example.** Lie algebra $su(2)$.

Pauli matrices are defined by

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (2.1)$$

They are Hermitian traceless matrices satisfying

$$\sigma_i \sigma_j = \delta_{ij} I + i \varepsilon_{ijk} \sigma_k. \quad (2.2)$$
They satisfy the following commutation relations

\[ [\sigma_i, \sigma_j] = 2i \epsilon_{ijk} \sigma_k \]  \hspace{1cm} (2.3)

and the anti-commutation relations

\[ \sigma_i \sigma_j + \sigma_j \sigma_i = 2 \delta_{ij} I \]  \hspace{1cm} (2.4)

Therefore, Pauli matrices form a representation of Clifford algebra in 2 dimensions.

The matrices

\[ J_i = -\frac{i}{2} \sigma_i \]  \hspace{1cm} (2.5)

are the generators of the Lie algebra \( su(2) \) with the commutation relations

\[ [J_i, J_j] = \epsilon_{ijk} J_k \]  \hspace{1cm} (2.6)

Algebra homomorphism \( \Lambda : su(2) \rightarrow so(3) \) is defined as follows. Let \( v = v^i J_i \in su(2) \). Then \( \Lambda(v) \) is the matrix defined by

\[ \Lambda(v) = v^i X_i. \]

\textbf{Example. Quaternions.} The algebra of quaternions \( \mathbb{H} \) is defined by (here \( i, j, k = 1, 2, 3 \))

\[ e_0^2 = e_0, \quad e_i^2 = -e_0, \quad e_0 e_i = e_i e_0 = e_i, \]

\[ e_i e_j = \epsilon_{ijk} e_k \quad i \neq j \]

There is an algebra homomorphism \( \rho : \mathbb{H} \rightarrow su(2) \)

\[ \rho(e_0) = I, \quad \rho(e_j) = -i \sigma_j \]

\textbullet{} A subspace of an algebra is called a \textbf{subalgebra} if it is closed under algebra multiplication.

\textbullet{} A subset \( B \) of an algebra \( A \) is called a \textbf{left ideal} if \( AB \subseteq B \), that is, for any \( u \in A \) and any \( v \in B \), \( uv \in B \).

\textbullet{} A subset \( B \) of an algebra \( A \) is called a \textbf{right ideal} if \( BA \subseteq B \), that is, for any \( u \in A \) and any \( v \in B \), \( vu \in B \).
A subset $B$ of an algebra $A$ is called a **two-sided ideal** if it is both left and right ideal, that is, if $ABA \subseteq B$, or for any $u, w \in A$ and any $v \in B$, $uvw \in B$.

- Every ideal is a subalgebra.
- A proper ideal of an algebra with identity cannot contain the identity element.
- A proper left ideal cannot contain an element that has a left inverse.
- If an ideal does not contain any proper subideals then it is the minimal ideal.

**Examples.** Let $x$ be an element of an algebra $A$. Let $Ax$ be the set defined by

$$Ax = \{ux | u \in A\}$$

Then $Ax$ is a left ideal.

- Similarly $xA$ is a right ideal and $AxA$ is a two-sided ideal.