Honors in Linear and Abstract Algebra I

Lecture Notes for
MATH 2131

Department of Mathematics
Hong Kong University of Science and Technology

January 2, 2026

Copyright Notice

Contents

Preface

This book is written by a student in the course MATH 2131 — Honors in Linear and Abstract Algebra I at The Hong Kong University of Science and Technology (HKUST) taught by Professor MENG Guowu during the Fall Semester of the Academic Year 2025–2026.

This book is designed to provide an abstract perspective on linear algebra. The book aims to give rigorous proofs of fundamental theorems in linear algebra while emphasizing the underlying structures and concepts. The book covers topics such as vector spaces, linear transformations, eigenvalues and eigenvectors, inner product spaces and more.

The target audience of this book includes undergraduate students studying linear algebra in a rigorous manner, as well as anyone interested in deepening their understanding of linear algebra from an abstract viewpoint. A solid foundation in basic linear algebra and mathematical proof techniques is recommended for readers.

CHAPTER 1

Linear Spaces

1.1. Introduction

Linear algebra originally arose from the study of systems of linear equations. Over time, it has evolved into a fundamental area of mathematics with applications in various fields such as physics, computer science, and economics. In this chapter, we will explore the concept of linear spaces, also known as vector spaces, which provide a framework for understanding linear combinations, subspaces, and linear transformations.

1.2. Operations and Structures

Before delving into linear spaces, it is essential to understand the basic operations and structures that underpin them.

1.2.1. Operations on Sets. There are several types of operations that can be performed on set S, including:

Definition 1.1 — Unary Operation.
A *unary operation* on a set S is a map

$$\begin{aligned} f : S &\to S \\ a &\mapsto f(a) \end{aligned}$$

Example 1.1. Common examples of unary operations include:

- Logical negation operation $\neg$ on the set $\{\text{True}, \text{False}\}$;
- Numeric negation operation $-$ on the set of real numbers $\mathbb{R}$;
- Complex conjugation operation $\overline{z}$ on the set of complex numbers $\mathbb{C}$.

Definition 1.2 — Binary Operation.
A *binary operation* on a set S is a map

$$\begin{aligned} \cdot : S \times S &\to S \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

Example 1.2. A common example of a binary operation is the addition operation $+$ on the set of natural numbers $\mathbb{N}$ which assigns to each pair of natural numbers (a, b) their sum $a + b$.

1.2.2. Properties of Binary Operations. There are several properties that binary operations may satisfy:

Definition 1.3 — Associative.
A binary operation $\cdot$ on a set S is *associative* if for all $a, b, c \in S$, we have
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Example 1.3. The addition operation $+$ on the set of natural numbers $\mathbb{N}$ is associative since for all $a, b, c \in \mathbb{N}$, we have
$$(a + b) + c = a + (b + c)$$

Definition 1.4 — Unital.
A binary operation $\cdot$ on a set S is *unital* if there exists an element $e \in S$ such that for all $a \in S$, we have
$$e \cdot a = a = a \cdot e$$

Example 1.4. The multiplication operation $\cdot$ on the set of natural numbers $\mathbb{N}$ is unital with the identity element 1 since for all $a \in \mathbb{N}$, we have
$$1 \cdot a = a = a \cdot 1$$

Remark. Such an element e must be unique if it exists and is called the two-sided *identity element* of the operation. To see why, suppose there are two identity elements e and e'. Then we have
$$e = e \cdot e' = e'$$
Note that one-sided identity elements (left or right) may not be unique.

Definition 1.5 — Invertible.
A binary operation $\cdot$ on a set S with identity element e is *invertible* if for each $a \in S$, there exists an element $b \in S$ such that
$$a \cdot b = e = b \cdot a$$

Remark. Note that invertibility requires the existence of an identity element.

Example 1.5. The addition operation $+$ on the set of integers $\mathbb{Z}$ is invertible since for each integer $a \in \mathbb{Z}$, there exists an integer $-a \in \mathbb{Z}$ such that
$$a + (-a) = 0 = (-a) + a$$

Remark. Such an element b must be unique if it exists and is called the two-sided *inverse* of the element a, denoted by a^{-1}. To see why, suppose there are two inverses b and b'. Then we have
$$b = e \cdot b = (a \cdot b') \cdot b = a \cdot (b' \cdot b) = a \cdot e = b'$$
Note that one-sided inverses (left or right) may not be unique.

Definition 1.6 — Commutative.

A binary operation $+$ on a set S is *commutative* if for all $a, b \in S$, we have

$$a + b = b + a$$

Example 1.6. The addition operation $+$ on the set of natural numbers $\mathbb{N}$ is commutative since for all $a, b \in \mathbb{N}$, we have

$$a + b = b + a$$

Definition 1.7 — Distributive.

A binary operation $\cdot$ on a set S is *distributive* over another binary operation $+$ on S if for all $a, b, c \in S$, we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

and

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

The professor prefers to use the term "harmonic" instead of "distributive". Note that it is important to specify the order of the operations when discussing distributivity, as the two operations may not be commutative with each other.

Example 1.7. The multiplication operation $\cdot$ on the set of integers $\mathbb{Z}$ is distributive over the addition operation $+$ since for all $a, b, c \in \mathbb{Z}$, we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

and

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

1.2.3. Algebraic Structures. Most objects in mathematics can be described with the following template.

A _____ *is a set with a* _____ *structure on it.*

Some common algebraic structures include:

Definition 1.8 — Monoidic Structure.

A *monoidic structure* on a set M is a binary operation $\cdot$ that is associative and unital. The pair $(M, \cdot)$ is called a *monoid*.

Definition 1.9 — Groupic Structure.

A *groupic structure* on a set G is a binary operation $\cdot$ that is associative, unital, and invertible. The pair $(G, \cdot)$ is called a *group*.

Example 1.8. The pair $(\mathbb{R} \setminus \{0\}, \times)$, where $\times$ is the multiplication operation on real numbers, forms a group since multiplication is associative, unital (with identity element 1), and invertible (with inverse element $a^{-1} = \frac{1}{a}$ for each $a \in \mathbb{R} \setminus \{0\}$). Note that $(\mathbb{R}, \times)$ is not a group since 0 does not have an inverse.

Definition 1.10 — Abelian Structure.
An *abelian structure* on a monoid or group $(A, +)$ is a binary operation $+$ that is also commutative. The pair $(A, +)$ is called an *abelian monoid* or *abelian group* respectively.

Example 1.9. The pair $(\mathbb{Z}, +)$, where $+$ is the addition operation on integers, forms an abelian group since addition is associative, unital (with identity element 0), invertible (with inverse element $-a$ for each $a \in \mathbb{Z}$), and commutative.

Definition 1.11 — Ringic Structure.
A *ringic structure* on a set R is two binary operations $+$ and $\cdot$ such that

- $(R, +)$ is an abelian group;
- $(R, \cdot)$ is a monoid; and
- the operation $\cdot$ is distributive over the operation $+$.

The triple $(R, +, \cdot)$ is called a *ring*.

Remark. In this book, we will only consider unital rings and refer to them simply as "rings".

Definition 1.12 — Commutative Ring.
A *commutative ring* is a ring $(R, +, \cdot)$ where the operation $\cdot$ is also commutative.

Definition 1.13 — Field.
A *field* is a commutative ring $(F, +, \cdot)$ where the operation $\cdot$ is also invertible on $F \setminus \{0\}$.

Example 1.10. The triples $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$, where $+$ is the addition operation and $\times$ is the multiplication operation on rational numbers, real numbers, and complex numbers respectively, all form fields.

Example 1.11 — Finite Field. The set $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ with XOR as addition and AND as multiplication forms a field. More generally, for any prime number p, the set $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ with addition and multiplication defined modulo p forms a field.

1.3. Homomorphisms

In mathematics, a *homomorphism* is a structure-preserving map between two algebraic structures of the same type.

Definition 1.14 — Monoid Homomorphism.

A *monoid homomorphism* is a set map $\phi : M_1 \to M_2$ between two monoids $(M_1, \cdot)$ and $(M_2, \odot)$ which respects the monoidic structure, i.e., for all $a, b \in M_1$, we have

- $\phi(a \cdot b) = \phi(a) * \phi(b)$;
- $\phi(e_1) = e_2$, where e_1 and e_2 are the identity elements of M_1 and M_2 respectively.

Definition 1.15 — Group Homomorphism.

A *group homomorphism* is a set map $\phi : G_1 \to G_2$ between two groups $(G_1, \cdot)$ and $(G_2, \odot)$ which respects the groupic structure, i.e., for all $a, b \in G_1$, we have

- $\phi(a \cdot b) = \phi(a) * \phi(b)$;
- $\phi(e_1) = e_2$, where e_1 and e_2 are the identity elements of G_1 and G_2 respectively;
- $\phi(a^{-1}) = (\phi(a))^{-1}$.

Proposition 1.1. The second and third properties in the definition of group homomorphism are consequences of the first property.

Proof. Let $\phi : G_1 \to G_2$ be a group homomorphism satisfying the first property. For any $a \in G_1$, we have

$$\phi(a) = \phi(a \cdot e_1) = \phi(a) * \phi(e_1).$$

So $\phi(e_1)$ is the identity element of G_2, i.e., $\phi(e_1) = e_2$. Similarly, we have

$$e_2 = \phi(e_1) = \phi(a \cdot a^{-1}) = \phi(a) * \phi(a^{-1}).$$

Thus, $\phi(a^{-1})$ is the inverse of $\phi(a)$, i.e., $\phi(a^{-1}) = (\phi(a))^{-1}$. □

For monoid homomorphisms, the second property cannot be derived from the first property. Consider the identity element e_1 in M_1. If we apply the first property, we get $\phi(e_1 \cdot e_1) = \phi(e_1) * \phi(e_1)$. This simplifies to $\phi(e_1) = \phi(e_1) * \phi(e_1)$, which does not necessarily imply that $\phi(e_1)$ is the identity element in M_2, i.e., $\phi(e_1) \neq e_2$. Therefore, the second property must be explicitly stated for monoid homomorphisms.

However in the case of group homomorphisms, the existence of inverses ensures that there is only one element that can be idempotent under the group operation, which is the identity element. Thus, for group homomorphisms, the second property can be derived from the first property.

Definition 1.16 — Ring Homomorphism.

A *ring homomorphism* is a set map $\phi : R_1 \to R_2$ between two rings $(R_1, +, \cdot)$ and $(R_2, \oplus, \odot)$ which respects the ringic structure, i.e., for all $a, b \in R_1$, we have

- $\phi(a + b) = \phi(a) \oplus \phi(b)$;
- $\phi(a \cdot b) = \phi(a) \odot \phi(b)$;
- $\phi(\mathrm{id}_{R_1}) = \mathrm{id}_{R_2}$, where id_{R_1} and id_{R_2} are the multiplicative identity elements of R_1 and R_2 respectively.

Remark. Originally, there are 6 properties in the definition of ring homomorphism, including the preservation of additive identity, additive inverses and commutative property. However, it can be shown that these properties are consequences of the first property. Also, we do not include the trivial ring homomorphism, as it does not preserve the multiplicative identity.

On top of homomorphisms, we have the following special types of maps, which are important for future discussions.

Definition 1.17 — Isomorphism.
An *isomorphism* is a homomorphism $\phi : A \to B$ between two algebraic structures of the same type that has an inverse map $\phi^{-1} : B \to A$ which is also a homomorphism.

Definition 1.18 — Endomorphism.
An *endomorphism* is a homomorphism $\phi : A \to A$ from an algebraic structure to itself.

Definition 1.19 — Automorphism.
An *automorphism* is an isomorphism $\phi : A \to A$ from an algebraic structure to itself.

Several maps can form a set as below.

Definition 1.20 — Homomorphism Set.
Given two algebraic structures A and B of the same type, the *homomorphism set* from A to B, denoted by $\mathrm{Hom}(A, B)$, is the set of all homomorphisms from A to B.

Definition 1.21 — Endomorphism Ring.
Given an abelian group $(G, +)$, the *endomorphism ring* of G, denoted by $\mathrm{End}(G)$, is the set of all endomorphisms from G to itself, equipped with the pointwise addition and composition of functions as the two binary operations. The two operations are defined as follows:

$$\begin{aligned} +&: \mathrm{End}\, G \times \mathrm{End}\, G \to \mathrm{End}\, G \\ &\qquad (\phi, \psi) \mapsto (\phi + \psi) : G \to G, \quad (\phi + \psi)(a) = \phi(a) + \psi(a) \\ \circ&: \mathrm{End}\, G \times \mathrm{End}\, G \to \mathrm{End}\, G \\ &\qquad (\phi, \psi) \mapsto (\phi \circ \psi) : G \to G, \quad (\phi \circ \psi)(a) = \phi(\psi(a)) \end{aligned}$$

The identity element for the addition operation is the zero map $0 : G \to G$ defined by $0(a) = 0_G$ for all $a \in G$, where 0_G is the identity element of the group $(G, +)$. The identity element for the composition operation is the identity map $\mathrm{id}_G : G \to G$ defined by $\mathrm{id}_G(a) = a$ for all $a \in G$.

Remark. Endomorphisms in $\mathrm{End}(G)$ are group homomorphisms since $(G, +)$ is an abelian group. So $\mathrm{End}(G) = \mathrm{Hom}(G, G)$.

1.4. Linear Spaces

A linear space, or vector space, is a set with a linear structure defined over a field. We then need to define what a linear structure is.

Definition 1.22 — Linear Structure.

A *linear structure* on a set V over a field F is a pair of binary operations $(+,\cdot)$ where $(V,+)$ is an abelian group with a ring action $\cdot$ of F on $(V,+)$. A ring action of F on $(V,+)$ is equivalent to a ring homomorphism

$$\begin{aligned} \cdot : F &\to \mathrm{End}(V) \\ \alpha &\mapsto \alpha\cdot : V \to V, \quad (\alpha\cdot)(v) = \alpha \cdot v \end{aligned}$$

Remark. The actual definition of a ring action of F over $(V,+)$ is a map

$$\begin{aligned} \cdot : F \times V &\to V \\ (\alpha, v) &\mapsto \alpha \cdot v \end{aligned}$$

such that it satisfies the following four properties for all $\alpha, \beta \in F$ and $u, v \in V$:

- Distributivity over vector addition: $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$;
- Distributivity over field addition: $(\alpha+\beta)\cdot v = \alpha \cdot v + \beta \cdot v$;
- Compatibility of scalar multiplication: $(\alpha\beta)\cdot v = \alpha \cdot (\beta \cdot v)$;
- Identity element of scalar multiplication: $1_F \cdot v = v$, where 1_F is the multiplicative identity element of the field F.

In usual textbooks, there are 8 axioms in the definition of linear structure. For all $\alpha, \beta \in F$ and $u, v \in V$:

1. Addition is associative: $(u+v)+w = u+(v+w)$;
2. Addition is unital: there exists an element $0_V \in V$ such that $0_V + v = v = v + 0_V$;
3. Addition is invertible: for each $v \in V$, there exists an element $-v \in V$ such that $v + (-v) = 0_V = (-v) + v$;
4. Addition is commutative: $u + v = v + u$;
5. Distributivity over vector addition: $\alpha \cdot (u+v) = \alpha \cdot u + \alpha \cdot v$;
6. Distributivity over field addition: $(\alpha+\beta)\cdot v = \alpha \cdot v + \beta \cdot v$;
7. Compatibility of scalar multiplication: $(\alpha\beta)\cdot v = \alpha \cdot (\beta \cdot v)$;
8. Identity element of scalar multiplication: $1_F \cdot v = v$, where 1_F is the multiplicative identity element of the field F.

The first four axioms ensure that $(V,+)$ is an abelian group. The fifth axiom describes the distributivity inside $\mathrm{End}(V)$, while the last three axioms corresponds to the properties of ring homomorphism from F to $\mathrm{End}(V)$. Thus, the 8 axioms can be reduced to the 2 conditions in the definition of linear structure.

Example 1.12. The field F itself can be considered as a linear space over F with the usual addition and multiplication operations. Here, the set V is F, the addition operation $+$ is the field addition, and the scalar multiplication $\cdot$ is the field multiplication.

Example 1.13. The set of all F-valued functions defined on a non-empty set X, i.e., $\{f : X \to F\}$, denoted by $\mathrm{Map}(X, F)$, forms a linear space over F with the following operations:

$$\begin{aligned} + : \mathrm{Map}(X,F) \times \mathrm{Map}(X,F) &\to \mathrm{Map}(X,F) \\ (f,g) &\mapsto (f+g) : X \to F, \quad (f+g)(x) = f(x) + g(x) \\ \cdot : F \times \mathrm{Map}(X,F) &\to \mathrm{Map}(X,F) \\ (\alpha, f) &\mapsto (\alpha \cdot f) : X \to F, \quad (\alpha \cdot f)(x) = \alpha \cdot f(x) \end{aligned}$$

Remark. In fact, as long as the codomain is a linear space, the set of all functions from a non-empty set to that codomain forms a linear space with pointwise addition and scalar multiplication.

Example 1.14. The set of all finitely supported F-valued functions defined on a non-empty set X, i.e., $\{f : X \to F \mid f(x) \neq 0_F \text{ for only finitely many } x \in X\}$, denoted by $\mathrm{Map}_{\mathrm{fin}}(X, F)$, forms a linear space over F with the same operations as in the previous example.

Example 1.15. The formal power series ring $F[[x]]$ over a field F forms a linear space over F with the usual addition and multiplication operations on formal power series. Formal means that we treat the elements as symbols without considering their convergence.

Example 1.16. The polynomial ring $F[x]$ over a field F forms a linear space over F with the usual addition and multiplication operations on polynomials.

Example 1.17. The set of all *column vectors* with n entries from F, denoted by F^n, forms a linear space over F with the operations defined entrywisely.

$$\begin{aligned} + : F^n \times F^n &\to F^n \\ (\vec{u}, \vec{v}) &\mapsto \vec{u} + \vec{v} \\ \left(\begin{bmatrix} u^1 \\ \vdots \\ u^n \end{bmatrix}, \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \right) &\mapsto \begin{bmatrix} u^1 + v^1 \\ \vdots \\ u^n + v^n \end{bmatrix} \end{aligned} \qquad \begin{aligned} \cdot : F \times F^n &\to F^n \\ (\alpha, \vec{v}) &\mapsto \alpha \cdot \vec{v} \\ \left(\alpha, \begin{bmatrix} v^1 \\ \vdots \\ v^n \end{bmatrix} \right) &\mapsto \begin{bmatrix} \alpha \cdot v^1 \\ \vdots \\ \alpha \cdot v^n \end{bmatrix} \end{aligned}$$

Remark. Here, we use superscripts to denote the entries of a column matrix due to the elements in vectors are *contravariant*. That is, when we change the basis, the coordinates of the vectors change in the opposite way compared to the basis transformation. This is in contrast to *covariant* elements, such as the entries of row matrices (or covectors), which change in the same way as the basis transformation. We will discuss covariance and contravariance in Chapter 4.

Example 1.18. The set of all *matrices* with m rows and n columns from F, denoted by $\mathrm{Mat}_{m\times n}(F)$, forms a linear space over F with the operations defined entrywisely.

1.5. Linear Subspaces, Linear Combinations and Linear Span

Definition 1.23 — Linear Subspace.
A *linear subspace* of a linear space $(V, +, \cdot)$ over F is a non-empty subset $W \subseteq V$ with the operations $+$ and $\cdot$ inherited from V such that $(W, +, \cdot)$ is also a linear space over F.

Proposition 1.2. W is a linear subspace of V if and only if W is non-empty and closed under the operations $+$ and $\cdot$, i.e., for all $u, v \in W$ and $\alpha \in F$, we have

- $u + v \in W$;
- $\alpha \cdot v \in W$.

Proof. If W is a linear subspace of V, then by definition V is non-empty, as it contains the zero vector. Also, since $(W, +, \cdot)$ is a linear space, it must be closed under the operations $+$ and $\cdot$. If W is non-empty and closed under the operations $+$ and $\cdot$, then we can easily verify that $(W, +, \cdot)$ satisfies all the axioms of a linear space over F. It is left as an exercise to the reader to check the axioms. □

We can actually combine two propoties into one by considering linear combinations.

Definition 1.24 — Linear Combination.
A *linear combination* of vectors $v_1, v_2, \ldots, v_n$ in a linear space V over F is any vector of the form

$$\alpha^1 v_1 + \alpha^2 v_2 + \cdots + \alpha^n v_n,$$

where $\alpha^1, \alpha^2, \ldots, \alpha^n$ are scalars in F.

To use linear combinations showing the condition for linear subspaces, we can consider the following example. We normally use $n = 2$ to proof the condition, and the general case can be proved by induction.

Proposition 1.3. The intersection of any collection of linear subspaces of a linear space V over F is also a linear subspace of V.

Proof. Let $\{W_i\}_{i \in I}$ be a collection of linear subspaces of V, where I is an index set. Define

$$W = \bigcap_{i \in I} W_i.$$

Then we have to show that W is a linear subspace of V. For any $i \in I$, we have $0_V \in W_i$ since W_i is a linear space. Thus, $0_V \in W$, so W is non-empty. Then, for any $u, v \in W$ and $\alpha, \beta \in F$, we have $u, v \in W_i$ for all $i \in I$. Since each W_i is a linear space, we have $\alpha u + \beta v \in W_i$ for all $i \in I$. Thus, $\alpha u + \beta v \in W$. Therefore, W is closed under the operations $+$ and $\cdot$. By the previous proposition, W is a linear subspace of V. □

Then it is natural to ask: the union of any collection of linear subspaces of a linear space V over F is also a linear subspace of V? The answer is no in general. However, if we perform "completion", or technically taking the *linear span*, we can obtain a linear subspace.

Definition 1.25 — Linear Span.

The *linear span* of a subset S of a linear space V over F, denoted by $\operatorname{Span}_F S$ or simply $\operatorname{Span} S$, $\overline{S}$ or $\langle S \rangle$, is the completion of S inside V under linear combinations, which is

$$\operatorname{Span} S = \left\{ \sum_{i=1}^{|S|} \alpha^i s_i \;\middle|\; \alpha^i \in F, s_i \in S \right\}$$

where $|S|$ is the cardinality of the set S (if S is infinite, we only consider finite linear combinations). Equivalently, the linear span of S is the smallest linear subspace of V that contains S. It can be written as

$$\operatorname{Span} S = \bigcap_{i \in I} W_i \subseteq V,$$

where $\{W_i\}_{i \in I}$ is the collection of all linear subspaces of W that contain S.

Definition 1.26 — Linear Spanning Set.

A subset S of a linear space V over F is a *linear spanning set*, or *linear generating set*, of V if its linear span is equal to V, i.e., $\operatorname{Span} S = V$.

For simplicity, we may omit the word "linear" when there is no ambiguity.

Example 1.19. Consider the linear space F^3 with vectors $\vec{e}_1$, $\vec{e}_2$, and $\vec{e}_3$. The set $S = \{\vec{e}_1, \vec{e}_2, \vec{e}_1 + \vec{e}_2\}$ is not a spanning set of F^3 since $\operatorname{Span} S$ is the same as $\operatorname{Span}\{\vec{e}_1, \vec{e}_2\}$. However, the set $T = \{\vec{e}_1, \vec{e}_1 + \vec{e}_2, \vec{e}_1 + \vec{e}_2, \vec{e}_3\}$ is a spanning set of F^3 since $\operatorname{Span} T = F^3$.

Remark. If you have learnt linear algebra before, consider the matrix whose columns are the vectors in a spanning set, then the matrix must have full row rank.

Example 1.20. Consider the subset $S = \{1, x, x^2, \cdots\} \subset F[[x]]$. The linear span of S is the polynomial ring $F[x]$, i.e., $\operatorname{Span} S = F[x]$. The reason is that any polynomial can be expressed as a finite linear combination of the elements in S, while any formal power series that is not a polynomial cannot be expressed as such.

Definition 1.27 — Minimal Spanning Set.

A minimal spanning set of a linear space V over F is a spanning set S of V such that for any proper subset $S' \subset S$, we have $\operatorname{Span} S' \subset \operatorname{Span} S = V$.

Remark. An ordered minimal spanning set is called a *basis*.

1.6. Linear Independence

Definition 1.28 — Linear Independence.
The non-trivial subspaces $W_1, W_2, \ldots, W_n$ of a linear space V over F are *linearly independent* if there is one and only one way to express the zero vector 0_V as a linear combination of vectors from these subspaces, i.e., if

$$w_1 + w_2 + \cdots + w_n = 0_V,$$

where $w_i \in W_i$ for each $i = 1, 2, \ldots, n$, then we must have $w_1 = w_2 = \cdots = w_n = 0_V$.

We also have a slightly weaker version of linear independence for future discussions.

Definition 1.29 — Weak Linear Independence.
The subspaces $W_1, W_2, \ldots, W_n$ of a linear space V over F are *weakly linearly independent* if the only way to express the zero vector 0_V as a linear combination of vectors from these subspaces is the trivial way, i.e., if

$$w_1 + w_2 + \cdots + w_n = 0_V,$$

where $w_i \in W_i$ for each $i = 1, 2, \ldots, n$, then we must have $w_1 = w_2 = \cdots = w_n = 0_V$.

Remark. Weak linear independence allows subspaces to be trivial, i.e., equal to $\{0_V\}$.

Definition 1.30 — Linearly Independent Set.
A subset S of a linear space V over F is linearly independent if and only if there is only one way to express the zero vector 0_V as a linear combination of vectors from S, i.e., if

$$\alpha^1 s_1 + \alpha^2 s_2 + \cdots + \alpha^n s_n = 0_V,$$

where $s_i \in S$ and $\alpha^i \in F$ for each $i = 1, 2, \ldots, n$, then we must have $\alpha^1 = \alpha^2 = \cdots = \alpha^n = 0_F$.

Remark. Equivalently, a subset S of a linear space V over F is linearly independent if no elements in S can be expressed as a linear combination of other elements in S.

Also, similar to minimal spanning sets, we have the following definition.

Definition 1.31 — Maximal Linearly Independent Set.
A maximal linearly independent set of a linear space V over F is a linearly independent set S of V such that for any proper superset $S' \supset S$, we have S' is not linearly independent.

Remark. A minimal spanning set and a maximal linearly independent set describe the same concept. We will use minimal spanning sets in this book.

CHAPTER 2

Linear Maps and Matrices

Linear maps are fundamental objects in linear algebra. In this chapter, we will explore their definitions and properties.

2.1. Linear Maps and Linear Combinations

Definition 2.1 — Linear Map.

A *linear map*, or *linear transformation*, between two linear spaces V and W over the same field F is a set map $T : V \to W$ that respects the linear structure; that is, for all $u, v \in V$ and all scalars $\alpha \in F$, the following properties hold:

- $T(u+v) = T(u) + T(v)$;
- $T(\alpha \cdot u) = \alpha \cdot T(u)$.

Remark. Originally, linear maps required 8 properties to be satisfied. However, it can be shown easily that these two properties imply the rest.

For simplicity, we often write Tu instead of $T(u)$ for the image of a vector u under the linear map T.

The set of all linear maps from V to W is denoted by $\mathrm{Hom}_F(V, W)$ or simply $\mathrm{Hom}(V, W)$ when the field is clear from context. Some author use $\mathcal{L}(V, W)$ instead.

The two properties in the definition can be combined into one property which is called *preserving linear combinations*.

From Example 1.13, we know that $\mathrm{Map}(V, W)$ forms a linear space over F with pointwise addition and scalar multiplication. Then $\mathrm{Hom}(V, W)$ is a subset of $\mathrm{Map}(V, W)$. It turns out that $\mathrm{Hom}(V, W)$ is actually a linear subspace of $\mathrm{Map}(V, W)$, or in other words, linear maps also form a linear space with the same operations. We will introduce linear subspace in Chapter 3.

Proposition 2.1. The set $\mathrm{Hom}(V, W)$ of all linear maps from V to W forms a linear space over F with pointwise addition and scalar multiplication.

Proof. We need to show that $\mathrm{Hom}(V,W)$ is closed under pointwise addition and scalar multiplication.
Let T_1 and T_2 be two linear maps from V to W. For all $u,v \in V$ and all $\alpha,\beta \in F$, we have

$$\begin{aligned}(T_1+T_2)(\alpha\cdot u+\beta\cdot v) &= T_1(\alpha\cdot u+\beta\cdot v)+T_2(\alpha\cdot u+\beta\cdot v)\\ &= \alpha\cdot T_1u+\beta\cdot T_1v+\alpha\cdot T_2u+\beta\cdot T_2v\\ &= \alpha\cdot(T_1u+T_2u)+\beta\cdot(T_1v+T_2v)\\ &= \alpha\cdot(T_1+T_2)(u)+\beta\cdot(T_1+T_2)(v),\end{aligned}$$

□

2.2. Matrices

Matrices provide a convenient way to represent linear maps between finite-dimensional linear spaces. Let A be an $m\times n$ matrix with entries from F. Then the map

$$\begin{aligned}F^n &\to F^m\\ \vec{x} &\mapsto A\vec{x}\end{aligned}$$

is a linear map over F.

Proposition 2.2. Every linear map $T : F^n \to F^m$ can be represented as multiplication by a unique $m\times n$ matrix A over F. The matrix A is called the *standard matrix*, or the *matrix representation*, of the linear map T. There is an isomorphism between two linear spaces $\mathrm{Hom}(F^n,F^m)$ and $\mathrm{Mat}_{m\times n}(F)$. Then we have

– The standard matrix of the linear map T is given by

$$A=\begin{bmatrix} | & | & & | \\ T\vec{e}_1 & T\vec{e}_2 & \cdots & T\vec{e}_n \\ | & | & & | \end{bmatrix},$$

where $\vec{e}_i$ is the column vector with 1 in the i-th entry and 0 elsewhere.

– For any matrix A in $\mathrm{Mat}_{m\times n}(F)$, the corresponding linear map $T_A : F^n \to F^m$ is given by

$$T_A\vec{x}=A\vec{x},\quad \text{for all } \vec{x}\in F^n.$$

Proof. Let $T : F^n \to F^m$ be a linear map. Define the matrix A as above. For any vector $\vec{x}\in F^n$, we can express $\vec{x}$ as a linear combination of $\vec{e}_1,\vec{e}_2,\dots,\vec{e}_n$:

$$\vec{x}=x^1\vec{e}_1+x^2\vec{e}_2+\cdots+x^n\vec{e}_n.$$

Then, using the linearity of T, we have

$$\begin{aligned}T\vec{x} &= T(x^1\vec{e}_1+x^2\vec{e}_2+\cdots+x^n\vec{e}_n)\\ &= x^1T\vec{e}_1+x^2T\vec{e}_2+\cdots+x^nT\vec{e}_n\\ &= A\vec{x}.\end{aligned}$$

This shows that $T\vec{x}$ can be computed as the matrix-vector product $A\vec{x}$. Conversely, given a matrix A in $\mathrm{Mat}_{m\times n}(F)$, we can define a linear map $T_A : F^n \to F^m$ by $T_A\vec{x}=A\vec{x}$. The linearity of T_A follows from the properties of matrix multiplication. □