MATH 223: Linear Algebra

William Homier[1]

[1] *McGill University Physics, 3600 Rue University, Montréal, QC H3A 2T8, Canada*

January 5th, 2026

Abstract

Contents

1 Introduction

2 Prerequisite knowledge

2.1 Notation

2.1.1 Sets

Sets are a grouping of objects.

Set	Meaning	Examples
$\mathbb{N}$	The set of natural numbers	(0, 1, 2, 3, ...)
$\mathbb{Z}$	The set of integers	(..., -3, -2, -1, 0, 1, 2, 3, ...)
$\mathbb{Q}$	The set of rational numbers	$\mathbb{Q} = \frac{a}{b} \mid \forall a, b \in \mathbb{Z} \, and \, b \neq 0$
$\mathbb{R}$	The set of all rational and all irrational numbers	$(..., -1, 0, \frac{1}{4}, 1, 1000, ...)$
$\mathbb{C}$	The set of all complex numbers	$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R} \, and \, i \subseteq \sqrt{-1}\}.$

We have the following relationships between sets:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

2.1.2 Symbols

Symbol	Meaning
$\subseteq$	is a subset of or equal to
$\subset$	is a strict subset of
$\in$	is an element of
$\forall$	for all
$\exists$	there exists
$\emptyset$	empty set
$\Rightarrow$	implies
$\Leftrightarrow$	if and only if

2.2 Complex Algebra

2.2.1 Complex Numbers

A complex number is of the form: $z = x + iy$ where $x, y \in \mathbb{R}$ and i is the imaginary unit such that $i^2 + 1 = 0$.

Definition 1 (Powers of i).

k	0	1	2	3	4	5
i^k	1	i	-1	-i	1	i

Theorem 1 (Fundamental Theorem of Algebra). *Any complex polynomial[1] f (except constant functions) has a root in $\mathbb{C}$.*

---

[1]Polynomial is a function such as: $f = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ where $a_i \in \mathbb{R}$ or $\mathbb{C}$ and $n \in \mathbb{N}$.

Remark 1. *If we have a polynomial f of degree n, then it has n roots, where each root can have a multiplicity[2].*

Example. *If we have a polynomial $(x-1)^2$, it has a degree of 2 but only one root, which is 1, with a multiplicity of 2. This means that the root 1 appears twice in the polynomial.*

We can factorize a polynomial in the form of $f = a_n x^n + ... + a_1 x + a_0$ into a linear factor: $f = a(x - z_1)(x - z_2)...(x - z_n)$ where z_i are the roots of f in $\mathbb{C}$.

Using the FTA for a function such as $f = a_n x^n + ... + a_1 x + a_0$, we can say that the FTA implies that f has a root $f(z) = 0$, because $f(z) = a(z - z) = 0$.

2.2.2 Complex Operations

We can define operations on complex numbers as follows:

- Addition: $z + z' = (x + x') + i(y + y')$, where $x, x', y, y' \in \mathbb{R}$.

- Multiplication: $zz' = (x + iy)(x' + iy') = (xx' - yy') + i(xy' + yx')$.

- Inverse: $\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{x - iy}{x^2 + y^2} = \frac{x}{x^2 + y^2} + i\frac{-y}{x^2 + y^2}$

From the definition of inverse, we can see that for any complex number z, its inverse $\frac{1}{z}$ is also a complex number. For example, take $z = 1 + i$, where $x = y = 1$, from the definition of inverse, we can conclude that:

$$\frac{1}{1 + i} \in \mathbb{C}$$

Multiplying by a complex number z corresponds geometrically to

$$\begin{cases} \text{a rotation by some angle } \theta, \\ \text{a rescaling by the factor } |z|. \end{cases}$$

2.2.3 Complex Conjugate

A complex conjugate is a way to "flip" the imaginary part of a complex number. For example, if we have a complex number $z = x + iy$, then the complex conjugate of z is $\bar{z} = x - iy$. Some basic properties of complex conjugates are:

- $\overline{\bar{z}} = z$

- $\overline{z + z'} = \bar{z} + \bar{z'}$

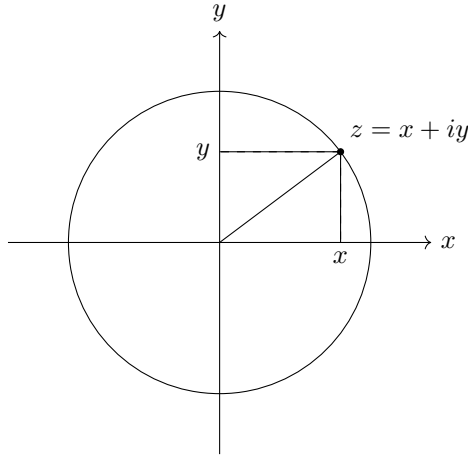- $\overline{z \cdot z'} = \bar{z} \cdot \bar{z'}$

2.2.4 Geometric and Polar Form of Complex Numbers

1. Geometric Interpretation

Definition 2 (Geometric interpretation). *Every complex number $z = x + iy$ can be identified with a point (x, y) in the plane, called the complex plane.*

We define the complex plane as:

$$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}.$$

2. Modulus and Unit Circle

Definition 3 (Modulus). *The modulus of a complex number z is defined by*

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

Geometrically, $|z|$ is the distance from the origin to the point (x, y).

We can rewrite the definition of the unit circle as follows:

$$S' = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} = \{z \in \mathbb{C} : |z| = 1\},$$

where S' is the unit circle in the complex plane.

3. Polar Coordinates

Definition 4 (Polar coordinates). *Instead of describing a point by (x, y), we may describe it using polar coordinates (r, θ), where $r = |z|$ is the distance to the origin and θ is the angle with the positive x-axis.*

Example. *Consider the point (x, y), where $x = r\cos(\theta)$ and $y = r\sin(\theta)$. We can define (r, θ) as follows:*

---

[2]The multiplicity of a root represents how many times the root occurs in the polynomial.
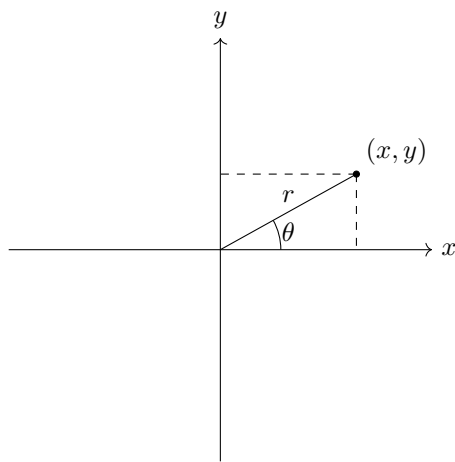
Complex numbers can also be described using polar coordinates.

Definition 5 (Polar and exponential form)**.**

$$z = x + iy = r\cos(\theta) + ir\sin(\theta) = r(\cos(\theta) + i\sin(\theta)) = re^{i\theta}.$$

We can also define multiplication in polar form:

Definition 6 (Multiplication in polar form)**.**

$$z = re^{i\theta}, \quad z' = r'e^{i\theta'}, \quad zz' = rr'e^{i(\theta+\theta')}.$$

Example.

$$(1+i)^{32} = (\sqrt{2}e^{i\pi/4})^{32} = (\sqrt{2})^{32}e^{i8\pi} = 2^{16}(\cos 8\pi + i\sin 8\pi) = 2^{16}.$$

Around the 1740, the mathematician Euler discovered a formula for complex numbers. The formula is known as Euler's formula.

Definition 7 (Euler's formula)**.**

$$e^{i\theta} = \cos(\theta) + i\sin(\theta).$$

This formula is quite useful when dealing with complex numbers, as it allows us to write complex numbers in a more compact form.

4. Roots in $\mathbb{C}$

Definition 8 (n^{th} roots in $\mathbb{C}$)**.** *For any complex number z, an nth root of z is a complex number w such that*

$$w^n = z.$$

Example. *If $z = re^{i\theta}$, then any solution of $w^n = z$ must satisfy*

$$w_k = r^{1/n}e^{i(\theta + 2\pi k)/n}, \quad k = 0, 1, 2, \ldots, n-1,$$

where the nth roots of z are equally spaced on a circle of radius $r^{1/n}$ centered at the origin.

Definition 9 (Roots of unity). *The nth roots of unity are the solutions of a special case where $z = 1$.*

Example. *If $z = 1$, then any solution of $w^n = z$ must satisfy*

$$w_k = e^{i2\pi k/n}, \quad k = 0, 1, 2, \ldots, n-1.$$

Geometrically, they lie on the unit circle and are equally spaced.

3 Basic Algebraic structures

3.1 Sets with Multiplication

Definition 10 (Set with multiplication). *A set M is called a set with multiplication if you can multiply any two elements of M, and the result is still in M. In other words, for any $a, b \in M$, the product ab is also in M.*

Example. *Let $M = \mathbb{R}$. If $a, b \in \mathbb{R}$, then $ab \in \mathbb{R}$. So the real numbers $\mathbb{R}$ form a set with multiplication.*

Example. *An example of a set with multiplication is the set of all 2×2 complex matrices: $M = M_2(\mathbb{C})$. Another example is the nonzero set of all real numbers $\mathbb{R}$ with ordinary multiplication: $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.*

3.2 Invertibility

Definition 11 (Condition for Invertibility). *Let $A \in M$ be an $n \times n$ matrix, and suppose that there exists an $n \times n$ matrix B such that $AB = I_n$ or $BA = I_n$. Where I_n is the $n \times n$ identity matrix[3] $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \ldots & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Then A is invertible, and B is called the inverse of A and is denoted by $B = A^{-1}$.*

Remark 2. *If A is invertible, then A^{-1} exists and is unique[4].*

To determine if an element A in a set with multiplication M is invertible, we can use the following examples:

---

[3]An identity matrix is a square matrix with 1s on its main diagonal and 0s everywhere else. It represents no change in linear transformations, and it's used in finding matrix inverses.

[4]Unique means there is exactly one such element.

Example. *Let $M = \mathbb{Z} = \{... - 2, -1, 0, 1, 2, ...\}$ and $A = 2$. Is A invertible in M?*
Solution: No, because $\frac{1}{2} \notin \mathbb{Z}$.

Example. *Let $M = \mathbb{R}$ and $A = 2$, is A invertible in M?*
Solution: Yes, because $\frac{1}{2} \in \mathbb{R}$.

Example. *Is $1 + i$ invertible in $\mathbb{C}$?*
Solution: Yes, using our previous definition of inverse (2.2.2), we get that

$$\frac{1}{1+i} = \frac{1-i}{2} \in \mathbb{C}.$$

Problem 1 (Invertibility). *Show that if an inverse of A in $\mathbb{M}$ exists, then it is unique.*

Problem 2 (Invertibility 2). *Let K be a field. Prove that this matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ $\in M_2(K)$ is not invertible.*

3.3 Ring

Definition 12. *A **ring** is a set R where you can **add** and **multiply** elements, and the following are true:*

1. *You can add any two elements and stay in R. There is a zero, every element has a negative, and addition is commutative and associative.*

2. *You can multiply any two elements and stay in R. Multiplication is associative, and there is a 1.*

3. *Multiplication distributes over addition:*

$$a(b + c) = ab + ac \quad and \quad (a + b)c = ac + bc.$$

The main example of a ring is the set of integers $\mathbb{Z}$.

3.4 Field

Definition 13. *A field is a set of numbers which can be added, subtracted, multiplied, and divided (except for division by zero) in a way that satisfies certain rules. These rules are:*

1. *You can add any two elements and stay in the field. There is a zero, every element has a negative, and addition is commutative[5] and associative[6].*

---

[5]Property which focuses on changing order of addition, i.e $a + b = b + a$.
[6]Property which focuses on changing grouping of addition, i.e $a + (b + c) = (a + b) + c$.

2. *You can multiply any two elements and stay in the field. Multiplication is associative, and there is a 1[7].*

3. *Multiplication distributes over addition:*

$$a(b + c) = ab + ac \quad and \quad (a + b)c = ac + bc.$$

Examples of fields include the set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$.

Problem 3 (Field)**.** *Construct a field with 2 elements.*

4   Vector Spaces

4.1   Cartesian vector spaces

Definition 14 (R^n)**.** *Let $n \in \mathbb{N}$. The Cartesian product of n copies of $\mathbb{R}$ is called $\mathbb{R}^n$.*

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} : x_1, \dots, x_n \in \mathbb{R} \right\}$$

4.2   Vectors

4.2.1   Vector operations

Vector operations are defined as follows:

Addition:
$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}.$$

Scalar multiplication:
$$\lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix},$$

where $\lambda \in \mathbb{R}$.

Definition 15 (Linear combination)**.** *A linear combination of vectors $v_1, \dots, v_n$ is a vector v of the form $v = \lambda_1 v_1 + \dots + \lambda_n v_n$, where $\lambda_1, \dots, \lambda_n \in \mathbb{R}$.*

---

[7]Like literally the number 1.

Example. *A linear combination could look like this:*

$$\xi((v_1 + 2v_2) + v_3) + v_4,$$

where $\xi \in \mathbb{R}$.

4.2.2 Span

Definition 16 (Span)**.** *Let $A \subset \mathbb{R}^n$. The span of A, denoted $\mathrm{Span}(A)$, is the set of all linear combinations of elements of A. In particular, if $A = \{v_1, \ldots, v_n\}$, then*

$$\mathrm{Span}(v_1, \ldots, v_n) = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : \lambda_i \in \mathbb{R}\}.$$

When working in $\mathbb{R}^n$, the span describes all points you can reach by scaling and adding the given vectors. Depending on the vectors, the span can be a line (if the vectors are dependent), a plane, or a higher-dimensional subspace. The following examples show what spans look like in $\mathbb{R}^2$.

Remark 3. *If $A = \{v\}$ contains one nonzero vector, then $\mathrm{Span}(v)$ is a line through the origin.*

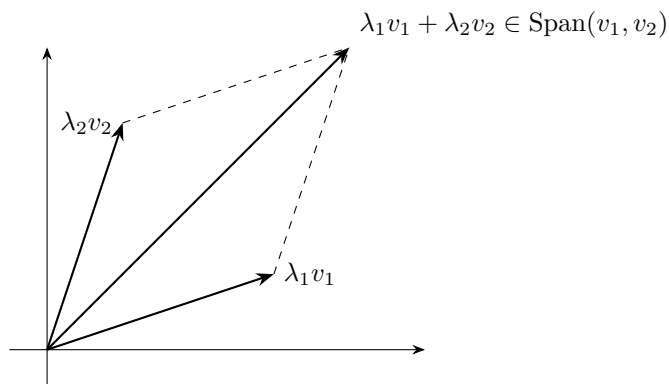**Example.** *Let $A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Then*

$$\mathrm{Span}(A) = \left\{ t \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mid t \in \mathbb{R} \right\},$$

which is a line in $\mathbb{R}^2$.
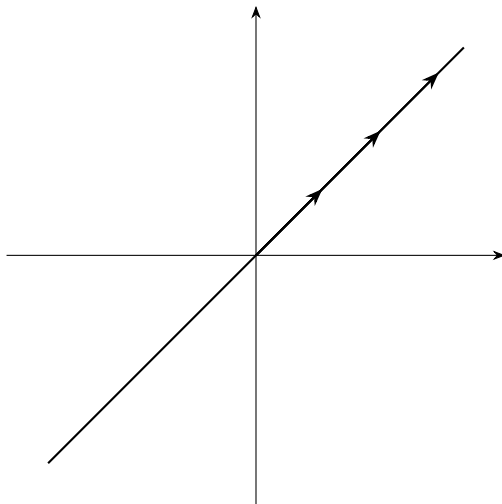
Problem 4 (Span)**.** *Let $v_1 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$. Find $\mathrm{Span}(v_1, v_2)$.*

Span is a generalization of lines in $\mathbb{R}^2$. For example, let $v_1 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$ and $v_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$. Any vector in $\mathrm{Span}(v_1, v_2)$ has the form $\lambda_1 v_1 + \lambda_2 v_2$. Geometrically, this can be illustrated as the sum of two scaled vectors.
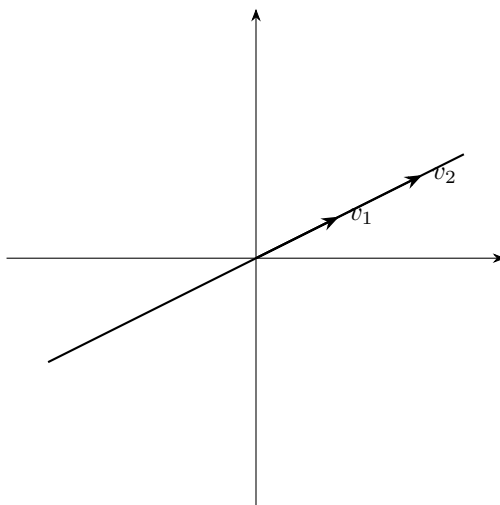
$$\lambda_1 v_1 + \lambda_2 v_2 \in \mathrm{Span}(v_1, v_2)$$

Furthermore, if v_1, v_2 are linearly dependent, then $\mathrm{Span}(v_1, v_2)$ is a line in $\mathbb{R}^2$. For example, let $v_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$ and $v_2 = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$. Then $v_2 = 2v_1$, so $\mathrm{Span}(v_1) = \mathrm{Span}(v_2)$. Geometrically, this is a straight line through the origin in the direction of v_1 (and v_2). Let

$$v_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 4 \\ 2 \end{pmatrix}.$$

Then $v_2 = 2v_1$, so

$$\mathrm{Span}(v_1) = \mathrm{Span}(v_2).$$

Span in $\mathbb{C}^n$ The definition of span is the same in complex vector spaces, except the scalars are complex numbers.

Definition 17. *The span over $\mathbb{C}$ of vectors $v_1, \ldots, v_n \in \mathbb{C}^n$ is*

$$\mathrm{Span}_{\mathbb{C}}(v_1, \ldots, v_n) = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : \lambda_i \in \mathbb{C}\}.$$

Thus, $\mathrm{Span}_{\mathbb{C}}(v_1, \ldots, v_n)$ consists of all vectors obtained by complex linear combinations of $v_1, \ldots, v_n$.

4.2.3 Standard Basis

Definition 18 (Standard basis of $\mathbb{R}^n$). *The standard basis of $\mathbb{R}^n$ is the set $\{e_1, \ldots, e_n\}$, where*

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \; \ldots, \; e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Every vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ can be written uniquely as

$$x = x_1 e_1 + \cdots + x_n e_n.$$

We now verify that the standard basis really is a basis, by checking that it spans $\mathbb{R}^n$ and is linearly independent.

Claim 1. The vectors $e_1, \ldots, e_n$ span $\mathbb{R}^n$.

Proof. We show that any vector in $\mathbb{R}^n$ can be written as a linear combination of $e_1, \ldots, e_n$:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_n \end{pmatrix} = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n.$$

$\square$

Claim 2. The vectors $e_1, \ldots, e_n$ are linearly independent.

Proof. Suppose

$$\lambda_1 e_1 + \cdots + \lambda_n e_n = 0.$$

10

Then

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

so $\lambda_1 = \cdots = \lambda_n = 0$. Therefore $e_1, \ldots, e_n$ are linearly independent. $\square$

The standard basis also helps clarify the difference between real and complex vector spaces. In particular, the same vectors can generate very different spans depending on whether the scalars are real or complex.

Example (Standard basis and real vs complex span). *Consider the standard basis $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ in $\mathbb{C}^2$.*

- *Over $\mathbb{C}$, any vector in $\mathbb{C}^2$ can be written as*

$$z_1 e_1 + z_2 e_2, \quad z_1, z_2 \in \mathbb{C}.$$

  So the complex span is

$$\mathrm{Span}_{\mathbb{C}}(e_1, e_2) = \mathbb{C}^2, \quad \dim_{\mathbb{C}} \mathbb{C}^2 = 2.$$

- *Each complex scalar can be written as $z_k = x_k + iy_k$, $x_k, y_k \in \mathbb{R}$. Then*

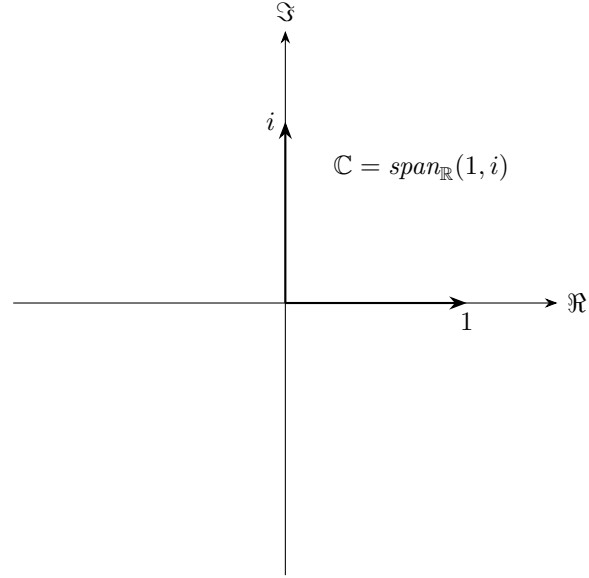$$z_1 e_1 + z_2 e_2 = x_1 e_1 + y_1(ie_1) + x_2 e_2 + y_2(ie_2),$$

  showing that every complex linear combination is also a real linear combination of the four vectors

$$e_1, e_2, ie_1, ie_2.$$

  Hence, as a real vector space, $\mathbb{C}^2$ has dimension 4:

$$\dim_{\mathbb{R}} \mathbb{C}^2 = 4.$$

$$\Im$$

$$i$$

$$\mathbb{C} = span_{\mathbb{R}}(1, i)$$

$$1 \qquad \Re$$

4.3 Abstract Vector Spaces

An abstract vector space generalizes the idea of vectors in $\mathbb{R}^n$. It is a set equipped with two operations (vector addition and scalar multiplication) that satisfy certain rules (axioms).

Definition 19 (Vector space over a field)**.** *Let k be a field. A **vector space over** k is a set V together with two operations:*

$$v_1 + v_2 \in V, \quad \forall v_1, v_2 \in V, \qquad \lambda v \in V, \quad \forall v \in V, \ \lambda \in k,$$

satisfying the following axioms:

1. *Commutativity of addition: $v_1 + v_2 = v_2 + v_1$*

2. *Associativity of addition: $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$*

3. *Existence of additive identity: $\exists 0 \in V$ such that $v + 0 = v$*

4. *Existence of additive inverses: $\forall v \in V, \exists -v \in V$ with $v + (-v) = 0$*

5. *Compatibility of scalar multiplication with field multiplication: $\lambda(\mu v) = (\lambda\mu)v$*

6. *Identity element of scalar multiplication: $1v = v$*

7. *Distributivity of scalar multiplication over vector addition: $\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$*

8. *Distributivity of scalar multiplication over field addition: $(\lambda + \mu)v = \lambda v + \mu v$*

12

Example (Cartesian vector space). *Let K be a field. Then*

$$K^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in K \right\}$$

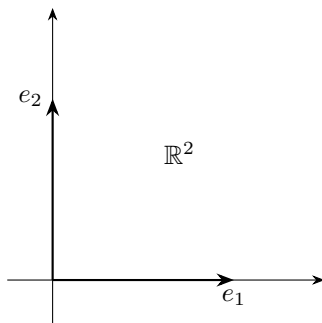*is a vector space over K. Its standard basis is*

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

and $\dim K^n = n$.

Remark 4 (Span over integers is not a vector space).

$$\mathrm{Span}_{\mathbb{Z}}(e_1, e_2) = \{\lambda_1 e_1 + \lambda_2 e_2 : \lambda_i \in \mathbb{Z}\}$$

is an additive subgroup but not a vector space over $\mathbb{R}$, because $\mathbb{Z}$ is not a field.

4.3.1 Coordinate Spaces

Definition 20 (Coordinate Spaces). *A coordinate space of dimension n over a field k $(k = \mathbb{R}$ or $k = \mathbb{C})$ is defined as*

$$k^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in k \right\}.$$

The standard basis is

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

13

4.3.2 Polynomial Spaces

Definition 21 (Polynomial Spaces). *A polynomial space of degree at most n over a field k is*

$$P_n(k) = \{a_n x^n + \cdots + a_1 x + a_0 : a_i \in k\},$$

which forms a vector space over k.

Example (Polynomial Spaces). *Some examples of polynomials in these spaces are*

$$1 + x^2 \in P_2(\mathbb{R}), \qquad 1 + ix^3 \in P_3(\mathbb{C}).$$

The subscript n indicates that $\deg(f) \leq n$. All polynomials can be collected in

$$P_\infty = \{a_n x^n + \cdots + a_1 x + a_0 : a_i \in k, \ n \geq 0\},$$

which is an infinite-dimensional vector space over k. We have the natural inclusions

$$P_0 \subseteq P_1 \subseteq P_2 \subseteq \cdots \subseteq P_\infty.$$

A standard basis for $P_n(k)$ is

$$\{1, x, x^2, \ldots, x^n\},$$

and every $f \in P_n(k)$ can be written uniquely as

$$f = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_n x^n, \quad \lambda_i \in k.$$

4.3.3 Matrix Spaces

Definition 22 (Matrix Spaces). *The set of all $n \times n$ matrices over a field k is*

$$M_n(k) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} : a_{ij} \in k \right\},$$

which forms a vector space over k. A standard basis for $M_n(k)$ is the set of matrices $\{e_{ij} : 1 \leq i, j \leq n\}$, where e_{ij} has a 1 in the (i,j)-th entry and 0 elsewhere. The dimension is

$$\dim M_n(k) = n^2.$$

Example (Matrix Spaces). *For $M_2(\mathbb{R})$,*

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 1e_{11} + 2e_{12} + 3e_{21} + 4e_{22}.$$

4.3.4 Function Spaces

Definition 23 (Function spaces)**.** *Let D be a set and k a field. Define*

$$F(D, k) = \{f : D \to k\}.$$

With pointwise operations

$$(f + g)(x) = f(x) + g(x), \quad (\lambda f)(x) = \lambda f(x),$$

$F(D, k)$ is a vector space over k.

1. Finite case: standard basis Assume $D = \{1, \ldots, n\}$. For each $i \in D$, define the Kronecker delta function

$$\delta_i(j) = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Then $\{\delta_1, \ldots, \delta_n\}$ is a basis of $F(D, k)$. Moreover, every $f \in F(D, k)$ can be written uniquely as

$$f = \sum_{i=1}^{n} f(i)\, \delta_i.$$

Indeed, evaluating at j gives

$$\sum_{i=1}^{n} f(i)\delta_i(j) = f(j),$$

so the functions span, and linear independence is immediate.

2. Infinite case If D is infinite, $F(D, k)$ has no finite basis. The family $\{\delta_x : x \in D\}$ is linearly independent but does not span $F(D, k)$.

4.4 Subspaces

Definition 24. *A subspace is a subset of a larger vector space that is itself a vector space, meaning it contains the zero vector and is closed under vector addition and scalar multiplication. Subspaces are essential because they allow focus on smaller, self-contained structures where standard linear algebra operations (like finding spans, bases, and transformations) still hold, with examples including lines through the origin in $\mathbb{R}^2$, the null space of a matrix, or the entire space itself.*

Proposition 1 (Subspace criterion)**.** *Let V be a vector space over a field k and let $U \subseteq V$. Then U is a vector subspace of V if and only if:*

1. *$0 \in U$,*

2. *$u, v \in U \Rightarrow u + v \in U$,*

3. $u \in U$, $\lambda \in k \Rightarrow \lambda u \in U$.

Problem 5 (Subspace criterion). *Let $A \in M_n(K)$ be a fixed matrix. Prove thet*

$$U = \{x \in K^n : Ax = \vec{0}\}$$

is a subspace, null space or kernel.

Problem 6 (Subspace criterion 2). *Let $A \in M_n(K)$. Show that*

$$U = \{Ax : x \in K^n\}$$

is a subspace of K^n. The set U is called the image (or range) of A.

Problem 7 (Subspace criterion 3). *Let $V = K$, viewed as a vector space over K. Show that the only subspaces of V are $\{0\}$ and V itself.*

Problem 8 (Subspace criterion 4). *Let V be a vector space over K and let $v_1, \ldots, v_n \in V$. Show that*

$$\mathrm{Span}(v_1, \ldots, v_n) = \{\lambda_1 v_1 + \cdots + \lambda_n v_n : \lambda_1, \ldots, \lambda_n \in K\}$$

is a subspace of V.

4.4.1 Membership in a span

Problem 9 (Span membership). *Let*

$$v = \begin{pmatrix} 3 \\ 5 \\ -5 \end{pmatrix}, \quad v_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \ v_2 = \begin{pmatrix} 2 \\ 5 \\ 4 \end{pmatrix}, \ v_3 = \begin{pmatrix} 1 \\ 3 \\ 6 \end{pmatrix}.$$

Decide whether $v \in \mathrm{Span}(v_1, v_2, v_3)$.

Problem 10 (Span membership 2). *Let*

$$f = 3x^2 + 5x - 5, \quad f_1 = x^2 + 2x + 1, \ f_2 = 2x^2 + 5x + 4, \ f_3 = x^2 + 3x + 6.$$

Decide whether $f \in \mathrm{Span}(f_1, f_2, f_3)$.

4.4.2 Operations on subspaces

Let W be a vector space and $U, V \subseteq W$ subspaces.

Definition 25 (Intersection).

$$U \cap V = \{w \in W : w \in U \text{ and } w \in V\}.$$

The intersection of subspaces is a subspace. In particular, the smallest possible intersection is $\{0\}$.

16

Remark 5. *In general, the union $U \cup V$ is not a subspace unless $U \subseteq V$ or $V \subseteq U$.*

Definition 26 (Sum of subspaces).

$$U + V = \{u + v : u \in U, v \in V\}.$$

Proposition 2. *If U and V are subspaces of W, then $U + V$ is a subspace of W.*

Proof that $U + V$ is a subspace. We apply the subspace criterion. (0) Since $0 \in U$ and $0 \in V$, we have $0 = 0 + 0 \in U + V$. (1) Let $w_1, w_2 \in U + V$. Then

$$w_1 = u_1 + v_1, \quad w_2 = u_2 + v_2$$

with $u_1, u_2 \in U$ and $v_1, v_2 \in V$. Hence

$$w_1 + w_2 = (u_1 + u_2) + (v_1 + v_2) \in U + V.$$

(2) Let $w \in U + V$ and $\lambda \in K$. Then $w = u + v$ and

$$\lambda w = \lambda u + \lambda v \in U + V.$$

$\square$

Proposition 3.
$$U + V = \operatorname{Span}(U \cup V).$$

Equivalently, $U + V$ is the smallest subspace of W containing both U and V.

. ($\subseteq$) Let $w \in U + V$. Then $w = u + v$ with $u \in U$, $v \in V$. Since $u, v \in U \cup V$, we have $w \in \operatorname{Span}(U \cup V)$.
 ($\supseteq$) Let $w \in \operatorname{Span}(U \cup V)$. Then

$$w = a_1 u_1 + \cdots + a_n u_n + b_1 v_1 + \cdots + b_m v_m$$

with $u_i \in U$, $v_j \in V$. Grouping terms,

$$w = (a_1 u_1 + \cdots + a_n u_n) + (b_1 v_1 + \cdots + b_m v_m),$$

so $w \in U + V$.

$\square$

January 23, 2026

4.5 Direct sums

U, V subspaces in W (ambiant space).

Definition 27. *U and V are in direct sum if $U \cap V = \{0\}$. Its a sum where the intersection is zero. Sum:*

$$U + V = \{u + v : u \in U, v \in V\}$$

Now if $U \cap V = \{0\}$ we write $U \oplus V$, and $U, V \subseteq W$. Sol: $W = U \oplus V$ means
$$\begin{cases} W = U + V \\ U \cap V = \{0\} \end{cases} \quad \text{To prove } W = U \oplus V,$$

17

- $W = U + V$, $\subseteq$ *Let* $w \in W$. *Prove: there exist* $u \in U$, $v \in V$ *such that* $w = u + v$.

- $U \cap V = \{0\}$. $\supseteq$ *automatic. Pick* $w \in \{0\}$. *Prove* $w \in U \cap V$. *By assumption* $w = 0$. *Prove* $w \in U$ *and* $w \in V$ *hold by definition of subspace. Only need to show* $U \cap V \subseteq \{0\}$. *Let* $w \in U$ *and* $w \in V$. *Prove* $w = 0$.

Sets	Vector Spaces
intersection $A \cap B$	intersection $U \cap V$
union $A \cup B$	union $U + V$
Disjoint union $A \sqcup B$ and $A \cap B = \emptyset$	Direct sum $U \cap V = \{0\}$

Example.

$$D = \{1, 2, 3, 4, 5\}$$

$$A = \{1, 2, 3\}, B = \{4, 5, 6\}$$

Then

$$D = A \sqcup B$$

$\rightarrow$ function spaces $F(d) =$ functions on D.

$$f \in F(D)$$

Example of a function: $f(1) = 2, f(2) = \sqrt{2}, f(3) = \pi$... View $F(A)$ as a subspace of $F(D)$. Claim: $F(A)$ can be "identified" with a subspace U of $F(D)$.

$$U = \{f : D \to \mathbb{R} : f(x) = 0, x \notin A\}$$

5   Appendix

6   Solutions

Solution 1 (Invertibility). *Suppose B and B' are both inverses of A. Then*

$$B = BI = B(AB') = (BA)B' = IB' = B'.$$

Therefore, $B = B'$, so the inverse is unique.

Solution 2 (Invertibility 2). *We can answer this problem with proof by contradiction. Let's suppose this matrix is invertible. By definition there exists* $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *such that* $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. *We can rewrite this equation into:* $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}^{-1}$. *The inverse of our matrix can be rewritten as* $\frac{1}{0*0-1*0} \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}$[8]. *But this is undefined since division by 0 is undefined. Therefore, our initial assumption that the matrix is invertible is false, and thus the matrix is not invertible.*

---

[8]Recall that an inverse of a 2×2 matrix is equal to its determinant multiplied with its conjugate

Solution 3 (Field). *A field with 2 elements can be constructed as follows: Let $F = \{0, 1\}$ be a set with two elements. We define addition and multiplication operations on F as follows:*

- $0 + 0 = 0$

- $0 + 1 = 1$

- $1 + 0 = 1$

- $1 + 1 = 0$

- $0 \times 0 = 0$

- $0 \times 1 = 0$

- $1 \times 0 = 0$

- $1 \times 1 = 1$

Solution 4 (Span).

$$\text{Span}(v_1, v_2) = \{xv_1 + yv_2 : x, y \in \mathbb{R}\} = \left\{ \begin{pmatrix} 3x + y \\ x + 3y \end{pmatrix} : x, y \in \mathbb{R} \right\}.$$

Solution 5 (Subspace Criterion). *Let $A \in M_n(K)$ be fixed and define*

$$U = \{x \in K^n : Ax = \vec{0}\}.$$

We verify the subspace criterion.
   (0) Non-empty: Since $A0 = 0$, we have $0 \in U$.
   (1) Closed under addition: Let $x, y \in U$. Then $Ax = 0$ and $Ay = 0$. Hence

$$A(x + y) = Ax + Ay = 0 + 0 = 0,$$

so $x + y \in U$.
   (2) Closed under scalar multiplication: Let $x \in U$ and $\lambda \in K$. Then

$$A(\lambda x) = \lambda Ax = \lambda 0 = 0,$$

so $\lambda x \in U$.
   Therefore, by the subspace criterion, U is a subspace of K^n. It is called the null space (kernel) of A.

Solution 6 (Subspace Criterion 2). *We verify the subspace criterion.*
   (0) Non-empty: Since $A0 = 0$, we have $0 \in U$.
   (1) Closed under addition: Let $y_1, y_2 \in U$. Then there exist $x_1, x_2 \in K^n$ such that

$$y_1 = Ax_1, \quad y_2 = Ax_2.$$

Hence,

$$y_1 + y_2 = Ax_1 + Ax_2 = A(x_1 + x_2) \in U.$$

(2) Closed under scalar multiplication: Let $y \in U$ and $\lambda \in K$. Then $y = Ax$ for some $x \in K^n$, and

$$\lambda y = \lambda Ax = A(\lambda x) \in U.$$

Therefore, by the subspace criterion, U is a subspace of K^n. It is called the image of A.

Solution 7 (Subspace Criterion 3). *Let $U \subseteq K$ be a subspace. We show that either $U = \{0\}$ or $U = K$. If $U = \{0\}$, we are done. Otherwise, $U \neq \{0\}$. Then there exists $v \in U$ with $v \neq 0$. We prove that $U = K$. Let $x \in K$ be arbitrary. Since $v \neq 0$, there exists $\lambda \in K$ such that*

$$x = \lambda v.$$

Because U is closed under scalar multiplication, $\lambda v \in U$, hence $x \in U$. Therefore every $x \in K$ belongs to U, so $U = K$. Conclusion: the only subspaces of K are $\{0\}$ and K.

Solution 8 (Subspace Criterion 4). *We verify the subspace criterion. (0) Non-empty: Taking $\lambda_1 = \cdots = \lambda_n = 0$ gives*

$$0 = 0v_1 + \cdots + 0v_n \in \mathrm{Span}(v_1, \ldots, v_n).$$

(1) Closed under addition: Let $u, v \in \mathrm{Span}(v_1, \ldots, v_n)$. Then there exist scalars $a_1, \ldots, a_n, b_1, \ldots, b_n \in K$ such that

$$u = a_1 v_1 + \cdots + a_n v_n, \quad v = b_1 v_1 + \cdots + b_n v_n.$$

Hence,

$$u + v = (a_1 + b_1)v_1 + \cdots + (a_n + b_n)v_n \in \mathrm{Span}(v_1, \ldots, v_n).$$

(2) Closed under scalar multiplication: Let $u \in \mathrm{Span}(v_1, \ldots, v_n)$ and $\lambda \in K$. Then

$$u = a_1 v_1 + \cdots + a_n v_n$$

for some scalars a_i, and

$$\lambda u = (\lambda a_1)v_1 + \cdots + (\lambda a_n)v_n \in \mathrm{Span}(v_1, \ldots, v_n).$$

Therefore, $\mathrm{Span}(v_1, \ldots, v_n)$ is a subspace of V.

Solution 9 (Span Membership). *We look for scalars $x, y, z \in \mathbb{R}$ such that*

$$xv_1 + yv_2 + zv_3 = v.$$

That is,

$$x \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} + y \begin{pmatrix} 2 \\ 5 \\ 4 \end{pmatrix} + z \begin{pmatrix} 1 \\ 3 \\ 6 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \\ -5 \end{pmatrix}.$$

This gives the system

$$\begin{cases} x + 2y + z = 3, \\ 2x + 5y + 3z = 5, \\ x + 4y + 6z = -5. \end{cases}$$

Solving, we obtain

$$x = 3, \quad y = 1, \quad z = -2.$$

Therefore,

$$v = 3v_1 + v_2 - 2v_3,$$

so $v \in \mathrm{Span}(v_1, v_2, v_3).$

Solution 10 (Span Membership 2). *We seek scalars* $x, y, z \in \mathbb{R}$ *such that*

$$f = x f_1 + y f_2 + z f_3.$$

Comparing coefficients,

$$x(x^2 + 2x + 1) + y(2x^2 + 5x + 4) + z(x^2 + 3x + 6) = 3x^2 + 5x - 5,$$

which gives

$$\begin{cases} x + 2y + z = 3, \\ 2x + 5y + 3z = 5, \\ x + 4y + 6z = -5. \end{cases}$$

Solving,

$$x = 3, \quad y = 1, \quad z = -2.$$

Hence,

$$f = 3f_1 + f_2 - 2f_3,$$

and therefore $f \in \mathrm{Span}(f_1, f_2, f_3).$

7　Useful Links