

MATH 223: Linear Algebra

William Homier¹

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

January 5th, 2026

Abstract

Contents

1	Introduction	1
2	Prerequisite knowledge	1
2.1	Notation	1
2.1.1	Sets	1
2.1.2	Symbols	1
2.2	Polar Coordinates	1
2.3	Complex Algebra	2
2.3.1	Complex Numbers	2
2.3.2	Complex Operations	2
2.3.3	Complex Conjugate	3
2.3.4	Geometric Interpretation of Complex Numbers	3
2.3.5	Modulus	3
2.3.6	Polar Form of Complex Numbers	4
2.3.7	Roots in \mathbb{C}	4
2.4	Basic Algebraic structures	4
2.4.1	Sets with Multiplication	4
2.4.2	Invertibility	5
2.4.3	Ring	5
2.4.4	Field	6
3	Vector Spaces	6
3.1	Cartesian vector spaces	6
3.2	Vectors	6
3.2.1	Vector operations	6
3.2.2	Span	6
3.2.3	Standard Basis	9
3.3	Abstract Vector Spaces	9
3.3.1	Coordinate Spaces	10
3.3.2	Polynomial Spaces	10
3.3.3	Matrix Spaces	11
3.3.4	Function Spaces	11
3.4	Subspaces	12
3.4.1	Membership in a span	12
3.4.2	Operations on subspaces	13
3.5	Direct sums	14
3.5.1	Direct sums in function spaces	14
4	Basis and Dimension	15
4.1	Finite Dimensional Spaces	15
4.2	Linear Independence	16
4.3	Basis	18
4.3.1	Size of spanning and independent sets	19
4.3.2	Characterizations of a basis	19

4.3.3	Finding a Basis	20
4.3.4	Direct Sums and Unique Decomposition	20
5	Linear Transformation	23
6	Appendix	24
6.1	Proof: Standard Basis is a Basis	24
6.2	Vector Space Axioms	25
7	Solutions	25
8	Useful Links	28

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	$\mathbb{Q} = \frac{a}{b} \mid \forall a, b \in \mathbb{Z} \text{ and } b \neq 0$
\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	$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R} \text{ and } i \subseteq \sqrt{-1}\}$.

We have the following relationships between sets:

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

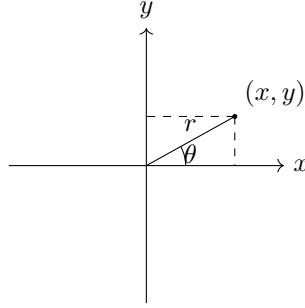
2.1.2 Symbols

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 Polar Coordinates

Definition 1 (Polar coordinates). *Instead of describing a point by (x, y) , we may describe it using polar coordinates (r, θ) , where r 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:



2.3 Complex Algebra

2.3.1 Complex Numbers

Definition 2 (Complex Number). A complex number is of the form: $z = x + iy$ where $x, y \in \mathbb{R}$ and i is the imaginary unit $i = \sqrt{-1}$.

Theorem 1 (Fundamental Theorem of Algebra). The FTA states that any non-constant, single-variable polynomial¹ with complex coefficients has at least one root in \mathbb{C} .

Remark 1. If we have a polynomial f of degree n , then it has n roots, where each root can have a multiplicity².

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.

We can factorize a polynomial in the form of $f = a_n x^n + \dots + a_1 x + a_0$ into a linear factor: $f = a(x - z_1)(x - z_2)\dots(x - z_n)$ where z_i are the roots of f in \mathbb{C} . Therefore, the FTA implies that f has a root $f(z) = a(z - z) = 0$.

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

Multiplying by a complex number z corresponds geometrically to

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

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

²The multiplicity of a root represents how many times the root occurs in the polynomial.

January 09,
2026.

2.3.3 Complex Conjugate

Definition 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:

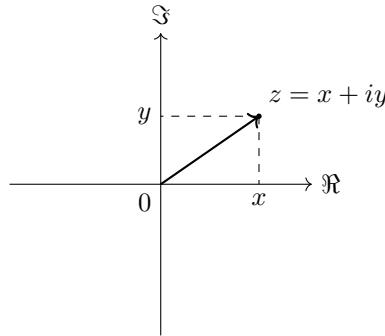
- $\bar{\bar{z}} = z$
- $\overline{z + z'} = \bar{z} + \bar{z'}$
- $\overline{z \cdot z'} = \bar{z} \cdot \bar{z'}$

2.3.4 Geometric Interpretation of Complex Numbers

Definition 4 (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:

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



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.

2.3.5 Modulus

Definition 5 (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) . Recall r in polar coordinates, which is the same as $|z|$.

2.3.6 Polar Form of Complex Numbers

Definition 6 (Euler's formula).

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

Definition 7 (Polar and exponential form). If $z = x + iy$ with $r = \sqrt{x^2 + y^2}$, then

$$x = r \cos \theta, \quad y = r \sin \theta,$$

so

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

Definition 8 (Multiplication in polar form).

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

Example.

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

2.3.7 Roots in \mathbb{C}

Definition 9 (n^{th} roots in \mathbb{C}). For any complex number z , an n^{th} 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

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

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

Definition 10 (Roots of unity). The n^{th} 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

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

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

2.4 Basic Algebraic structures

2.4.1 Sets with Multiplication

Definition 11 (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. 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: $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

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.

2.4.2 Invertibility

Definition 12 (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 matrix³ $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \dots & 0 \\ 0 & 0 & 1 \end{bmatrix}$. 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 unique⁴.

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

Example. Let $M = \mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$ 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 (2.3.2), 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.

2.4.3 Ring

Definition 13 (Ring). 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 commutative⁵ and associative⁶.
2. You can multiply any two elements and stay in R . Multiplication is associative, and there is a 1.
3. Multiplication distributes over addition:

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

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

³An 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.

⁴Unique means there is exactly one such element.

⁵Property which focuses on changing order of addition, i.e $a + b = b + a$.

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

January 09,
2026.

2.4.4 Field

Definition 14 (Field). *A field is a ring in which every nonzero element has a multiplicative inverse.*

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

3 Vector Spaces

3.1 Cartesian vector spaces

Definition 15 (\mathbb{R}^n). *Let $n \in \mathbb{N}$. The Cartesian product of n copies of \mathbb{R} is called \mathbb{R}^n .*

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

3.2 Vectors

3.2.1 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 16 (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 $\lambda_1, \dots, \lambda_n \in \mathbb{R}$.*

3.2.2 Span

January 12,
2026.

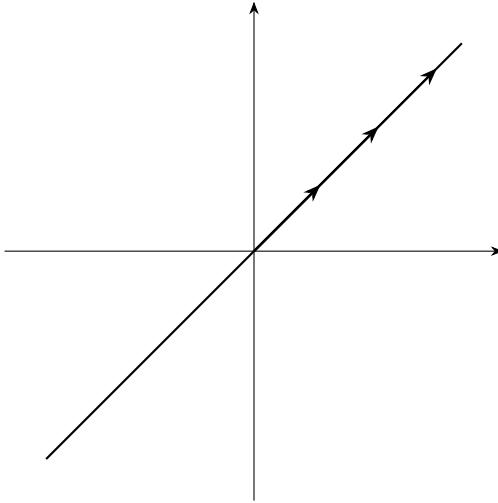
Definition 17 (Span). *Let $A \subset \mathbb{R}^n$. The span of A , denoted $\text{span}(A)$, is the set of all linear combinations of elements of A . In particular, if $A = \{v_1, \dots, v_n\}$, then*

$$\text{span}(v_1, \dots, v_n) = \{\lambda_1 v_1 + \dots + \lambda_n v_n : \lambda_i \in \mathbb{R}\}.$$

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.

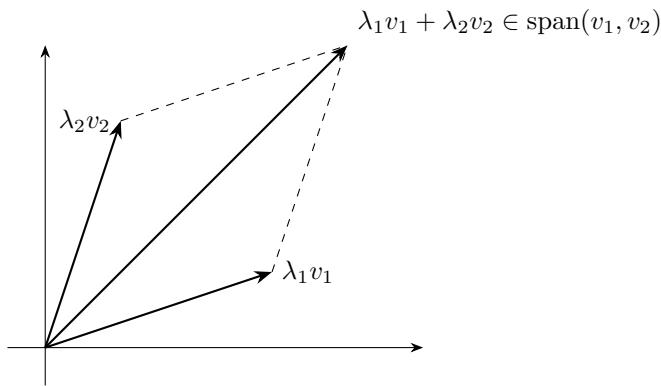
Remark 3. If $A = \{v\} \subset \mathbb{R}^2$ with $v \neq 0$, then $\text{span}(v)$ is a line through the origin.

Example. Let $A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Then $\text{span}(A) = \left\{ t \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mid t \in \mathbb{R} \right\}$, which is a line in \mathbb{R}^2 .

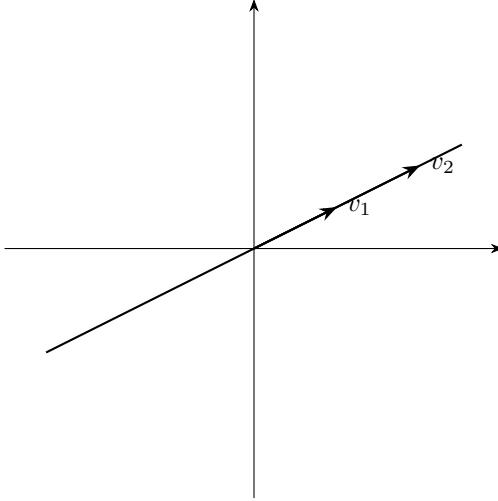


Problem 4 (Span). Let $v_1 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$. Find $\text{span}(v_1, v_2)$.

Span is a generalization of lines in \mathbb{R}^2 . For example, let v_1 and v_2 be two linearly independent vectors in \mathbb{R}^2 . Any vector in $\text{span}(v_1, v_2)$ has the form $\lambda_1 v_1 + \lambda_2 v_2$. Geometrically, this can be illustrated as the sum of two scaled vectors.



Furthermore, if v_1, v_2 are linearly dependent such that $v_1 = \lambda v_2$, where $\lambda \in \mathbb{R}$ and $\lambda \neq 0$, then $\text{span}(v_1, v_2)$ is a line in \mathbb{R}^2 and $\text{span}(v_1) = \text{span}(v_2)$. Geometrically, this is a straight line through the origin in the direction of v_1 (and v_2).



1. Span in \mathbb{C}^n

Definition 18 (Span in \mathbb{C}^n). *The span over \mathbb{C} of vectors $v_1, \dots, v_n \in \mathbb{C}^n$ is*

$$\text{span}_{\mathbb{C}}(v_1, \dots, v_n) = \{\lambda_1 v_1 + \dots + \lambda_n v_n : \lambda_i \in \mathbb{C}\}.$$

Thus, $\text{span}_{\mathbb{C}}(v_1, \dots, v_n)$ consists of all vectors obtained by complex linear combinations of v_1, \dots, v_n .

Example. Let

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ i \end{pmatrix} \in \mathbb{C}^2.$$

Find $\text{span}_{\mathbb{C}}(v_1, v_2)$.

Take $\lambda_1, \lambda_2 \in \mathbb{C}$. Then

$$\lambda_1 v_1 + \lambda_2 v_2 = \lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ i \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ i\lambda_2 \end{pmatrix}.$$

Let $z_1 = \lambda_1$ and $z_2 = i\lambda_2$. Since λ_2 is arbitrary in \mathbb{C} , z_2 can be any complex number. Hence every vector

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{C}^2$$

can be obtained. Therefore, $\text{span}_{\mathbb{C}}(v_1, v_2) = \mathbb{C}^2$.

3.2.3 Standard Basis

Definition 19 (Standard basis of \mathbb{R}^n). *The standard basis of \mathbb{R}^n is the set $\{e_1, \dots, e_n\}$, where*

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

Proposition 1. *Every vector $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ can be written uniquely as $x = x_1 e_1 + \dots + x_n e_n$.*

To verify that the standard basis really is a basis, two conditions must be satisfied: it spans \mathbb{R}^n and is linearly independent. To prove the standard basis is a basis, please refer to the Appendix (6.1).

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 (Real vs complex span of the same vectors). *Let*

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2.$$

Over \mathbb{C} ,

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

Over \mathbb{R} , complex scalars are not allowed, so we need the four real vectors

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

These form a basis, hence

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

Thus the same space has different dimensions depending on the field.

3.3 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 20 (Vector space over a field). *Let k be a field. A vector space over k is a set V with addition and scalar multiplication such that*

$$(i) v_1 + v_2 \in V, \quad (ii) \lambda v \in V, \quad (iii) 0 \in V,$$

and satisfying the usual vector space axioms (see the Appendix (6.2) for the complete list).

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

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

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

3.3.1 Coordinate Spaces

Definition 21 (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 for a coordinate space is

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

3.3.2 Polynomial Spaces

Definition 22 (Polynomial Spaces). A polynomial space of degree at most n over a field k is

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

which forms a vector space over k . The standard basis for a polynomial space of degree n is

$$\{1, x, x^2, \dots, x^n\}.$$

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

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

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

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

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

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

3.3.3 Matrix Spaces

Definition 23 (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 of $M_n(k)$ is $\dim M_n(k) = n^2$.

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

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = 1 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 2 \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + 3 \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + 4 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 1e_{11} + 2e_{12} + 3e_{21} + 4e_{22}.$$

3.3.4 Function Spaces

16 January,
2026

Definition 24 (Function spaces). Let D be a set and k a field. Define

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

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 $D = \{1, \dots, n\}$. 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 $\{\delta_1, \dots, \delta_n\}$ 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 $F(D, k)$.

January 19,
2026

3.4 Subspaces

Definition 25. 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 2 (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 that

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

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 $v_1, \dots, v_n \in V$. Show that

$$\text{span}(v_1, \dots, v_n) = \{\lambda_1 v_1 + \dots + \lambda_n v_n : \lambda_1, \dots, \lambda_n \in K\}$$

is a subspace of V .

January 21,
2026

3.4.1 Membership in a span

Problem 9 (Span membership). Let

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

Decide whether $v \in \text{span}(v_1, v_2, v_3)$.

Problem 10 (Span membership 2). Let

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

Decide whether $f \in \text{span}(f_1, f_2, f_3)$.

3.4.2 Operations on subspaces

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

Definition 26 (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 $\{0\}$.

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

Definition 27 (Sum of subspaces).

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

Proposition 3. 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

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

□

Proposition 4.

$$U + V = \text{span}(U \cup V).$$

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

Proof that $U + V = \text{span}(U \cup V)$. (\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 $w \in \text{span}(U \cup V)$.

(\supseteq) Let $w \in \text{span}(U \cup V)$. 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 $w \in U + V$. □

3.5 Direct sums

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

Definition 28 (Direct sum). *We say that U and V are in direct sum if*

$$U \cap V = \{0\}.$$

In this case, their sum

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

is denoted by $U \oplus V$. We write

$$W = U \oplus V$$

if and only if

$$\begin{cases} W = U + V, \\ U \cap V = \{0\}. \end{cases}$$

Remark 6. *To prove $W = U \oplus V$, one must show:*

- Every $w \in W$ can be written as $w = u + v$ with $u \in U, v \in V$.
- If $w \in U$ and $w \in V$, then $w = 0$.

Analogy with sets

Sets	Vector spaces
$A \cap B$	$U \cap V$
$A \cup B$	$U + V$
$A \sqcup B, A \cap B = \emptyset$	$U \oplus V, U \cap V = \{0\}$

Example. Let

$$D = \{1, 2, 3, 4, 5\}, \quad A = \{1, 2, 3\}, \quad B = \{4, 5\}.$$

Then

$$D = A \sqcup B.$$

3.5.1 Direct sums in function spaces

Let D be a set and $A \subseteq D$. Consider the function space $F(D, \mathbb{R})$.

Definition 29. Define

$$U = \{f \in F(D, \mathbb{R}) : f(x) = 0 \text{ for all } x \notin A\}.$$

Then U is a subspace of $F(D, \mathbb{R})$, and U can be identified with $F(A, \mathbb{R})$.

Remark 7. Every function in U is completely determined by its values on A and vanishes outside A .

4 Basis and Dimension

4.1 Finite Dimensional Spaces

Let V be a vector space over a field k . Then there are two possibilities:

- The zero vector space: $V = \{0\}$
- The non-zero vector space: $V \neq \{0\}$

In the second case, there exists a non-zero vector $v_1 \in V$ such that $v_1 \neq 0$. Then $\text{span}(v_1)$ is a subspace of V , and there are two possibilities:

- $V = \text{span}(v_1)$, i.e., v_1 is a generator of V .
- $V \neq \text{span}(v_1)$, i.e., there exists a $v_2 \in V$ such that $v_2 \notin \text{span}(v_1)$.

In the second case, $\text{span}(v_1, v_2) \subseteq V$. This process can be repeated to obtain a sequence of vectors v_1, v_2, \dots, v_n such that $\text{span}(v_1, \dots, v_n) \subseteq V$. The maximum number of linearly independent vectors in V is called the dimension of V , denoted by $\dim V$.

2 cases (2d space plane):

- $v = v_2 = \text{span}(v_1, v_2)$
- $v \neq v_2 \quad \exists v_3 \notin v_2$, where $v_3 = \text{span}(v_1, v_2, v_3) \subseteq v$

2 cases (3d space):

- $v_3 = v$
- $v_3 \neq v \quad \exists v_4 \dots$

Definition 30. V is finite dimensional if it can be spanned by finitely many vectors.

$$\exists v_1, \dots, v_n : V = \text{span}(v_1, \dots, v_n).$$

$\dim V$ = smallest n such that $V = \text{span}(v_1, \dots, v_n)$.

$\dim_k V$ = min n such that $V = \text{span}_k(v_1, \dots, v_n)$.

Example. $(\mathbb{C}^n, n = 1) \quad \mathbb{C} = \text{span}_{\mathbb{R}}(1, i) = 2$

$$x \cdot 1 + y \cdot i$$

$M_n(\mathbb{C})$

$$A = \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1} & z_{n2} & \cdots & z_{nn} \end{pmatrix} = \begin{pmatrix} x_{11} + y_{11}i & x_{12} + y_{12}i & \cdots & x_{1n} + y_{1n}i \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} + y_{n1}i & x_{n2} + y_{n2}i & \cdots & x_{nn} + y_{nn}i \end{pmatrix}$$

First matrix is of $\dim_{\mathbb{C}} M_n(\mathbb{C}) = n^2$, and the second matrix is of $\dim_{\mathbb{R}} M_n(\mathbb{C}) = 2n^2$.

Example ($\dim V = \infty$).

$$P_\infty$$

$$v_1 = 1 \quad v_2 = x \quad v_3 = x^2$$

$\text{span}(v_1) = \text{constant polynomials}$

$$V_1 = \text{span}(v_1, v_2) = P_1$$

$$v_{n+1} = x^n \notin P_{n-1}$$

4.2 Linear Independence

Definition 31. v_1, \dots, v_n are linearly independent if $\lambda_1 v_1 + \dots + \lambda_n v_n = 0 \implies \lambda_1 = \dots = \lambda_n = 0$.

Example.

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Prove LI. Assume $xe_1 + ye_2 = 0$. Prove $x = y = 0$.

$$xe_1 + ye_2 = x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} = 0 \implies x = y = 0.$$

Proposition 5. The "standard basis" are both spanning and LI. (e_1, \dots, e_n) of k^n $(1, x, \dots, x^n)$ of P_n (e_{11}, \dots, e_{nn}) of $M_n(k)$ $(\delta_1, \dots, \delta_n)$ of $F(D)$, where $D = \{1, \dots, n\}$

Definition 32. basis = set(v_1, \dots, v_n) both span and LI.

$$\dim(\mathbb{V}) = \#\text{basis}$$

Problem 11. Prove $\dim P_\infty = \infty$. Assume $\dim P_\infty < \infty$. Proof by contradiction. $\exists f_1, \dots, f_n$ polynomials $P_\infty = \text{span}(f_1, \dots, f_n)$. Let $d = \max \text{ degree of } f_k$.

$$x^{d+1} \notin \text{span}(f_1, \dots, f_n)$$

$$\text{degree} \leq d.$$

January 28,
2026

Problem 12.

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 4 \\ 9 \\ 5 \end{pmatrix}.$$

Are these vectors linearly independent? Are there $x, y, z \in \mathbb{R}$ such that

$$xv_1 + yv_2 + zv_3 = 0?$$

Solution 1. x, y, z not all zero.

$$x \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix} + z \begin{pmatrix} 4 \\ 9 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{cases} x + 3y + 4z = 0 \\ 1 + 3y + 9z = 0 \\ 0 + 2y + 5z = 0 \end{cases}$$

Find a non-trivial solution. $x = 3, y = 5, z = -2$. Not LI: $3v_1 + 5v_2 - 2v_3 = 0$.

Definition 33 (Linear Dependence). *Linearly dependent (LD) just means not LI.*

Proposition 6. v_1, \dots, v_n are linearly dependent if and only if one vector is in the span of the other vectors.

Example.

$$3v_1 + 5v_2 - 2v_3 = 0$$

As we can see, v_1 is in the span of v_2 and v_3 .

$$v_1 = \frac{1}{3}(-5v_2 + 2v_3)$$

Remark 8. If one vector $v_1 = 0$ then the family is LD.

Proof. Proof of \rightarrow : Assumption $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$. Not all λ_i are zero, at least one is nonzero, say $\lambda_k \neq 0$. The goal is to write v_k in the span of the other vectors.

$$v_k = \frac{-1}{\lambda_k} \sum_{i \neq k} \lambda_i v_i.$$

$$v_k \in \text{span}(v_1, \dots, v_k, \dots, v_n).$$

Converse: Assume one vector, say v_k is in the span of the other vectors.

$$v_k \in \text{span}(v_1, \dots, v_k, \dots, v_n).$$

There exists coefficients $\lambda_1, \dots, \lambda_n$ such that

$$v_k = \lambda_1 v_1 + \dots + \lambda_{k-1} v_{k-1} + \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n.$$

LD: non trivial dependency between the v_i 's. \square

Example.

$$V = \mathbb{R}^3$$

$$v_1 = \begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} b_1 \\ b_2 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}.$$

LI:

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}.$$

LD:

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix}.$$

Assume $xv_1 + yv_2 + zv_3 = 0$.

$$x \begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix} + y \begin{pmatrix} b_1 \\ b_2 \\ 0 \end{pmatrix} + z \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}.$$

$$\begin{cases} a_1x + b_1y + c_1z = 0 \\ b_2y + c_2z = 0 \\ c_3z = 0 \end{cases}$$

If $a_1 = 0$. $v_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. Answer: LD. Can assume $a_1 \neq 0$. If $b_2 = 0$.

$$v_1 = \begin{pmatrix} a_1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} b_1 \\ 0 \\ 0 \end{pmatrix}. \text{ Answer: LD.}$$

4.3 Basis

January 30,
2026

Definition 34 (Basis). A list (v_1, \dots, v_n) in a vector space V is a **basis** if

1. it spans V , and
2. it is linearly independent.

Example (Standard basis of \mathbb{R}^3).

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

These vectors form a basis of \mathbb{R}^3 .

Proof. Let $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$. Then

$$v = xe_1 + ye_2 + ze_3$$

so the set spans \mathbb{R}^3 . If

$$xe_1 + ye_2 + ze_3 = 0 \implies x = y = z = 0,$$

hence the vectors are linearly independent. \square

Proposition 7 (Common standard bases). • $\mathbb{R}^n: (e_1, \dots, e_n)$

- $M_n(k): e_{ij}$
- $P_n(k): (1, x, \dots, x^n)$
- $F(D)$ for finite D : $\{\delta_x, x \in D\}$

4.3.1 Size of spanning and independent sets

For $(v_1, \dots, v_n) \in \mathbb{R}^3$:

- If $n < 3$ then the vectors cannot span \mathbb{R}^3 .
- If $n > 3$ then the vectors cannot be linearly independent.

Lemma 2. *If u_1, \dots, u_n span V and v_1, \dots, v_m are linearly independent in V , then*

$$n \geq m.$$

We can conclude, that a spanning set \geq LI set.

4.3.2 Characterizations of a basis

Theorem 3 (Equivalent Conditions). *Let (v_1, \dots, v_n) be vectors in V . The following are equivalent:*

1. Basis: (v_1, \dots, v_n) is a basis.
2. Minimal span: It spans V and n is minimal among spanning sets.
3. Maximal LI: It is linearly independent and n is maximal among independent sets.
4. Coordinates: Every $v \in V$ has a unique representation.

$$v = x_1 v_1 + \dots + x_n v_n.$$

The vector

$$[v]_e = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

is called the coordinate vector of v .

Corollary 3.1. *Any two bases of V have the same number of vectors. This number is the dimension of V .*

Proof. Let (e_1, \dots, e_n) and (f_1, \dots, f_m) be bases. Since one spans and the other is linearly independent, the lemma gives $n \geq m$ and $m \geq n$, hence $n = m$. \square

4.3.3 Finding a Basis

Let $(v_1, \dots, v_n) \in k^m$ and set $U = \text{span}(v_1, \dots, v_n)$.

1. Put the vectors as rows of a matrix A .
2. Row reduce A to echelon form B .
3. The nonzero rows of B form a basis of U .

1. Proving a set of vectors is a Basis Let V be finite dimensional.

Method 1 (dimension test).

$$(v_1, \dots, v_n) \text{ is a basis} \iff \dim(\text{span}(v_1, \dots, v_n)) = n.$$

Compute the dimension using row reduction.

Method 2 (basis criterion when $\dim V = n$).

Proposition 8. Let $\dim V = n$ and $v_1, \dots, v_n \in V$. The following are equivalent:

1. (v_1, \dots, v_n) is a basis,
2. (v_1, \dots, v_n) spans V ,
3. (v_1, \dots, v_n) is linearly independent.

Idea. A spanning set of $n = \dim V$ vectors is minimal, hence linearly independent. An independent set of n vectors is maximal, hence spans. \square

2. Transfer (exchange) principle If

$$u_1, \dots, u_n \text{ span } V \quad \text{and} \quad v_1, \dots, v_n \text{ are linearly independent,}$$

then both lists are bases of V .

Example. In P_n ,

$$(1, x, \dots, x^n) \text{ spans,} \quad ((x - a)^0, \dots, (x - a)^n) \text{ is LI,}$$

February 4,
2026
so both are bases.

4.3.4 Direct Sums and Unique Decomposition

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

Definition 35 (Direct Sum). *The sum of subspaces is*

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

We say the sum is *direct*, written $U \oplus V$, if

$$U \cap V = \{0\}.$$

Proposition 9. *The following are equivalent:*

1. $U \oplus V$ (i.e. $U \cap V = \{0\}$),
2. every $w \in U + V$ can be written uniquely as $w = u + v$ with $u \in U$, $v \in V$.

Proof. (\Rightarrow) Suppose $w = u_1 + v_1 = u_2 + v_2$. Then

$$u_1 - u_2 = v_2 - v_1 \in U \cap V = \{0\},$$

so $u_1 = u_2$ and $v_1 = v_2$.

(\Leftarrow) If decomposition is unique and $w \in U \cap V$, then

$$0 = 0 + 0 = w + (-w),$$

so uniqueness forces $w = 0$. \square

Coordinates relative to a basis If (e_1, \dots, e_n) is a basis of V , every $v \in V$ can be written uniquely as

$$v = \lambda_1 e_1 + \dots + \lambda_n e_n.$$

The vector

$$[v]_e = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

is called the coordinate vector of v .

Example. In \mathbb{R}^3 with the standard basis,

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow [v]_e = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

February 6,
2026

example:

$$v = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, f_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, f_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

$$[v]_f = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

LL example: Find coordinate of $v = \begin{pmatrix} 5 \\ 3 \\ 4 \end{pmatrix}$ in basis $f = (f_1, f_2, f_3)$, with $f_1 =$

$$\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, f_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, f_3 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

$$\begin{pmatrix} 5 \\ 3 \\ 4 \end{pmatrix} = x \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + z \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

Find x, y, z .

$$[v]_f = \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} \in \mathbb{R}^3.$$

Example: $D = \{0, 1, 2, 3, 4\}$, $V = F(D)$, $g(x) = x^2$, $g \in V$, find coordinate of y in standard basis $\delta = (\delta_0, \delta_1, \delta_2, \delta_3, \delta_4)$. $\dim V = 5$. $[g]_\delta = \begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_4 \end{pmatrix}$, where $g = \lambda_0\delta_0 + \lambda_1\delta_1 + \lambda_2\delta_2 + \lambda_3\delta_3 + \lambda_4\delta_4$.

No Basis theorem: Basis extraction theorem: v_1, \dots, v_n spans V can extract a basis $\{e_1, \dots, e_n\}$ from $\{v_1, \dots, v_n\}$. Example: $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, v_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ spans \mathbb{R}^3 . Proof: Let $\{e_1, \dots, e_m\} \subseteq \{v_1, \dots, v_n\}$ be a subset which is spanning with m minimal. Claim: e_1, \dots, e_m is a basis. Proof by contradiction: Assumption: (e_1, \dots, e_n) not LI: Proposition: one vector is in the span of the other ($\lambda_1 e_1 + \dots + \lambda_n e_n = 0$). $e_k \in \text{span}(e_1, e_2, \dots, e_k, \dots, e_n)$.

February 2, 2026

V vector space (finite dimensional) v_1, \dots, v_n LI set. Can extend v_1, \dots, v_n to a basis of V . Proof: $\text{span}(v_1, \dots, v_n) = U \subseteq V$. Step 1: Case 1: If $U = V \rightarrow$ basis (LI + span) Case 2: $U \neq V \implies \exists v_{n+1} \in V \setminus U$ Claim: (v_1, \dots, v_{n+1}) LI V minus U .

$$U_{n+1} = \text{span}(v_1, \dots, v_{n+1})$$

Step 2: Case 1: $U_{n+1} = V \implies (v_1, \dots, v_{n+1})$ is a basis. Case 2: $U_{n+1} \neq V \implies$ a m add v_{m+2}

Step 3: ... This stops at v_n for some $n \geq m$, $n = \dim V \implies n$ LI vectors in V .

Coronary: $U \subseteq V$, $\dim U \leq \dim V$ or $U \not\subseteq V$ and $\dim U < \dim V$.⁷ If for $U \subseteq V$, $U = V \iff \dim U = \dim V$.

Coronary: $U \subseteq V$. U admits a supplement, meaning there exists a subspace $U' \subseteq V$ such that $V = U \oplus U'$. $\dim V = \dim U + \dim U'$.

Basis concatenation: Theorem: Suppose $U \oplus U'$ are in direct sum in V . (e_1, \dots, e_n) basis of U . (f_1, \dots, f_m) basis of U' . $\implies (e_1, \dots, e_n, f_1, \dots, f_m)$ is a basis of $U \oplus U'$, which means $\dim U \oplus U' = m + n = \dim U + \dim U'$. Theorem: $U, U' \subset V$, $\dim U + U' = \dim U + \dim U' - \dim(U \cap U')$.

proof of: Suppose $U \oplus U'$ are in direct sum in V Assume: $\begin{cases} e_1, \dots, e_n \text{ basis of } U \\ f_1, \dots, f_m \text{ basis of } U' \end{cases}$

Prove $(e_1, \dots, e_n, f_1, \dots, f_m)$ is a basis LI: $a_1e_1 + \dots + a_ne_n + b_1f_1 + \dots + b_mf_m = 0$
 $w = a_1e_1 + \dots + a_ne_n = -b_1f_1 - \dots - b_mf_m$. $w \in U$, $w \in U' \implies w \neq 0 \implies a_1e_1 + \dots + a_ne_n = 0 \implies a_i = 0$. $\implies b_1f_1 + \dots + b_mf_m = 0 \implies b_i = 0$.

February 11, 2026

⁷ $\not\subseteq$ means it is a subset but not equal to.

5 Linear Transformation

Today general trans/function/map U, V are sets where U is the domain and V is the codomain. $u \in U$ and $T(u) \in V$. Image of $T = Im(T) = \{T(u) : u \in U\} \subseteq V$. Example: $\sin : \mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto \sin(x)$. $Im(\sin) = (-1, 1)$. $F(D)$ is a vector space with D set, codomain $K = \mathbb{R}$ or \mathbb{C} . Definition: $T : U \rightarrow V$, $u \mapsto T(u)$ is surjective, if $\Im(T) = V$. Definition: $T : U \rightarrow V$, $u \mapsto T(u)$ is injective, if you have u and v where $u \neq v$, but $T(u) = T(v)$. Injective: if $u, v \in U$ satisfy $T(u) = T(v)$, then $u = v$. Example: x^3 is injective. Definition: T is a bijection if it is both injective and surjective. Example: x^3 is bijective whilst x^2 is not. More precisely: $f : \mathbb{R} \rightarrow \mathbb{R}$ $x \mapsto x^2$ is not injective nor surjective. Example: $y : \mathbb{C} \rightarrow \mathbb{C}$ $z \mapsto z^2$ injective? $(-1)^2 = (1)^2$. surjective? $z^2 = w$ where $w \in \mathbb{C}$ is any complex number. Fix w , solve for z , $g(z) = w$. Composition of transformations:

$$\begin{aligned} R &\longrightarrow T \longrightarrow V \longrightarrow S \longrightarrow W \\ u &\longrightarrow T(u) \longrightarrow S(T(u)) \end{aligned}$$

Composition:

$$\begin{aligned} R : U &\longrightarrow W \\ u &\longrightarrow S(T(u)) \\ g : \mathbb{R} &\xrightarrow[A]{x^2} \mathbb{R} \xrightarrow[B]{\sin} \mathbb{R} \\ g &= \sin(x^2) \\ R : U &\xrightarrow{T} V \xrightarrow[S]{} W \\ R(u) &= S(T(u)) \\ R &= S \circ T \end{aligned}$$

(\circ) is called composition. A inverse = a matrix B such that $AB = Id$ and $BA = Id$. Proposition: $T : U \rightarrow V$ is bijective \iff T admits an inverse, $\exists S$ such that $\begin{cases} ST = id \\ TS = id \end{cases}$. Let U be a vector space:

$T : U \longrightarrow U$ Id transformation

$$\begin{aligned} u &\longrightarrow u \\ U &= \mathbb{R}^n \\ T \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} &= \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \end{aligned}$$

Example: $U = \mathbb{R}^n$, $V = \mathbb{R}^n$, $A \in M_n(\mathbb{R})$, $T_A : u \rightarrow v$, $T_A = \text{trans with } A$.

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \rightarrow A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Example:

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$A \begin{pmatrix} x \\ y \end{pmatrix}$$

$$T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} x + 2y \\ 3x + 4y \end{pmatrix}$$

Definition: U, V vector spaces over K . $T : U \rightarrow V$ transformation. Say T is linear if $T(u + v) = T(u) + T(v)$ and $T(\lambda u) = \lambda T(u)$. Proposition: S, T are linear, here $S \circ T$ is linear.

6 Appendix

6.1 Proof: Standard Basis is a Basis

Claim 1. The vectors e_1, \dots, 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, \dots, e_n :

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

□

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

Proof. Suppose

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

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, \dots, e_n are linearly independent. □

6.2 Vector Space 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: $(\lambda + \mu)v = \lambda v + \mu v$

7 Solutions

Solution 2 (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 3 (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.

Solution 4 (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:

- $0 + 0 = 0$
- $0 + 1 = 1$

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

- $1 + 0 = 1$
- $1 + 1 = 0$
- $0 \times 0 = 0$
- $0 \times 1 = 0$
- $1 \times 0 = 0$
- $1 \times 1 = 1$

Solution 5 (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 6 (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 7 (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 8 (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 9 (Subspace Criterion 4). We verify the subspace criterion. (0) Non-empty: Taking $\lambda_1 = \dots = \lambda_n = 0$ gives

$$0 = 0v_1 + \dots + 0v_n \in \text{span}(v_1, \dots, v_n).$$

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

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

Hence,

$$u + v = (a_1 + b_1)v_1 + \dots + (a_n + b_n)v_n \in \text{span}(v_1, \dots, v_n).$$

(2) Closed under scalar multiplication: Let $u \in \text{span}(v_1, \dots, v_n)$ and $\lambda \in K$. Then

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

for some scalars a_i , and

$$\lambda u = (\lambda a_1)v_1 + \dots + (\lambda a_n)v_n \in \text{span}(v_1, \dots, v_n).$$

Therefore, $\text{span}(v_1, \dots, v_n)$ is a subspace of V .

Solution 10 (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 $v \in \text{span}(v_1, v_2, v_3)$.

Solution 11 (Span Membership 2). We seek scalars $x, y, z \in \mathbb{R}$ such that

$$f = xf_1 + yf_2 + zf_3.$$

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 $f \in \text{span}(f_1, f_2, f_3)$.

8 Useful Links