

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	Complex Algebra	1
2.2.1	Complex Numbers	1
2.2.2	Complex Operations	2
2.2.3	Complex Conjugate	2
2.2.4	Geometric and Polar Form of Complex Numbers	2
3	Basic Algebraic structures	5
3.1	Sets with Multiplication	5
3.2	Invertibility	6
3.3	Ring	6
3.4	Field	6
4	Vector Spaces	7
4.1	Cartesian vector spaces	7
4.2	Vectors	7
4.2.1	Vector operations	7
4.2.2	Span	8
5	Appendix	12
6	Solutions	12
7	Useful Links	13

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	$(0, 1, 2, 3, \dots)$
\mathbb{Z}	The set of integers	$(\dots, -3, -2, -1, 0, 1, 2, 3, \dots)$
\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	$(\dots, -1, 0, \frac{1}{4}, 1, 1000, \dots)$
\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 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). $\frac{k}{i^k} \mid \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & i & -1 & -i & 1 & i \end{array}$

Theorem 1 (Fundamental Theorem of Algebra). *Any polynomial¹ f (except constant functions) has a root in \mathbb{C} .*

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 $n \in \mathbb{N}$.

Remark 1. If we have a polynomial f of degree n , then it has n roots, where each root can have a multiplicity². For 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 $f = a_n x^n + \dots + a_1 x + a_0$ 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} .

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

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:

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

2.2.4 Geometric and Polar Form of Complex Numbers

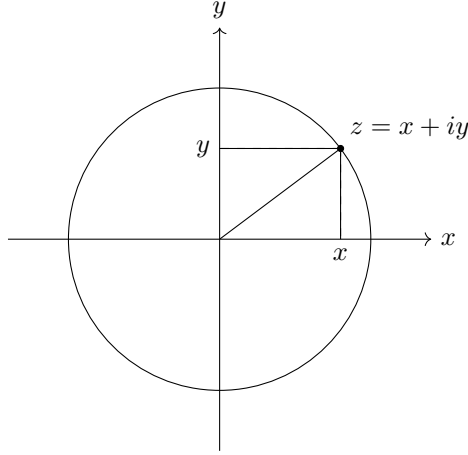
1. Geometric Interpretation

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

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:

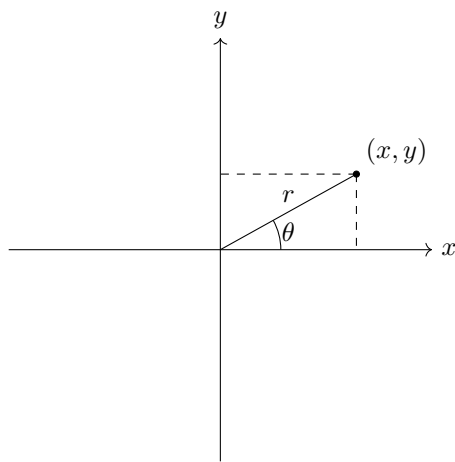
$$S' = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} = \{z \in \mathbb{C} : |z| = 1\},$$

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:*



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

Definition 8 (n^{th} roots). *An n^{th} root of z is a complex number w such that*

$$w^n = z.$$

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

$$w^n = re^{i\theta}.$$

Writing $w = \rho e^{i\varphi}$, we obtain

$$\rho^n = r, \quad n\varphi = \theta + 2\pi k, \quad k \in \mathbb{Z}.$$

Hence, all n^{th} roots of z are

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

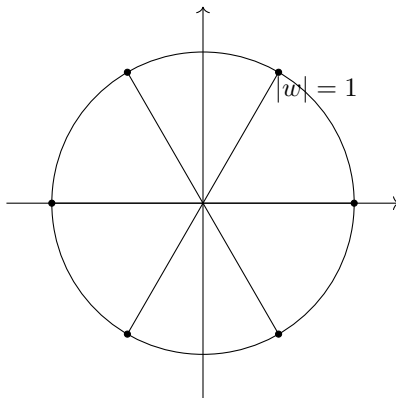
Definition 9 (Roots of unity). *The n^{th} roots of unity are the solutions of*

$$w^n = (e^{i2\pi/n})^n = e^{i2\pi} = 1, \quad w \in \mathbb{C}.$$

Since $1 = e^{i2\pi k}$, they are given by

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

Geometrically, the n^{th} roots of unity 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 with multiplication is a set M where you can multiply any two elements of M , and the result is still an element of M . Formally, this means there is a rule \cdot that takes any pair (a, a) from M and produces an element ab that is also in M :*

$$\cdot : M \times M \rightarrow M$$

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 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 (2.2.2), we get that

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

3.3 Ring

Definition 12. A ring is a set R with the following properties:

1. R is an abelian group under addition.
2. R is a monoid under multiplication.
3. The distribution law holds: $a(b + c) = ab + ac$ for all $a, b, c \in R$.

More informally, a ring is a set with two operations (addition and multiplication) that satisfy certain properties.

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

3.4 Field

Definition 13. A field is a commutative ring in which every element is invertible.

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.

The main example of a field is the real numbers \mathbb{R} or the complex numbers \mathbb{C} . Mathematically, $K = \mathbb{R}$ or \mathbb{C} , where K is the field.

In the following explanation, we will denote M to be a set with multiplication⁵. 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: $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Problem 1. *Construct a field with 2 elements.*

Problem 2. *Show that if an inverse of A in \mathbb{M} exists, then it is unique.*

Problem 3. *Let K be a field. Prove that this matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(K)$ is not invertible.*

4 Vector Spaces

4.1 Cartesian vector spaces

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

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

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

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

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

January 12,
2026.

4.2.2 Span

Definition 16 (Span). *Let $A \subset \mathbb{R}^2$. The span of A , denoted $\text{Span}(A)$, is the set of all linear combinations of elements of A .*

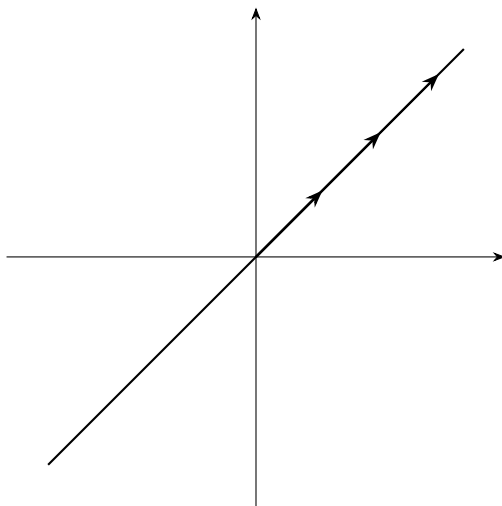
Span in \mathbb{R}^n

Remark 3. *If $A = \{v\}$ contains one nonzero vector, 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 .



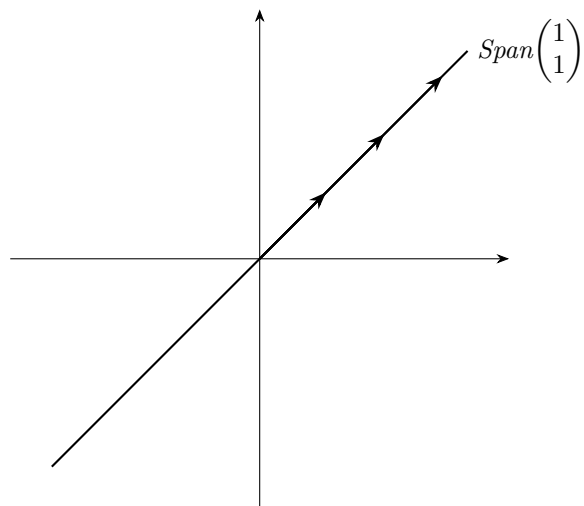
Example. *The span of n vectors v_1, \dots, v_n is the set of all linear combinations of v_1, \dots, v_n . Then any vector in $\text{Span}(v_1, \dots, v_n)$ has the form*

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

Example. *Let $v_1 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$. Then $\text{Span}(v_1, v_2) = \{\lambda_1 v_1 + \lambda_2 v_2 : \lambda_1, \lambda_2 \in \mathbb{R}\}$*

Example. *Let $A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Then $\text{Span}(A) = \{\lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix} : \lambda \in \mathbb{R}\}$*

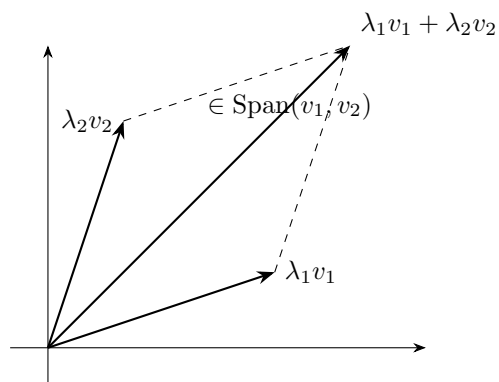
⁵A set of objects where you can multiply any two of them.



Example. Let

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

Any vector in $\text{Span}(v_1, v_2)$ has the form $\lambda_1 v_1 + \lambda_2 v_2$. Geometrically, this is illustrated below.

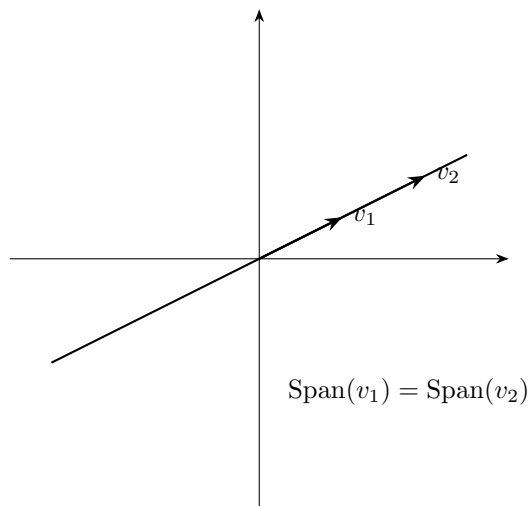


Example. Let

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

Then $v_2 = 2v_1$, so

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



Span in \mathbb{C}^n

Definition 17.

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

Example.

$$\text{span} \begin{pmatrix} 2i \\ 2 \end{pmatrix} + i \begin{pmatrix} 3 \\ 1+i \end{pmatrix} \in \mathbb{C}^2$$

So:

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in \mathbb{R} \right\} \quad \mathbb{C}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in \mathbb{C} \right\}$$

Standard basis:

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

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

Basis -> (span + LI)

Claim: These vectors span \mathbb{R}^n Proof: To show an arbitrary vector in \mathbb{R}^n can be written as a linear combination of e_1, \dots, e_n .

$$\text{Let } \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 e_1 + x_2 e_2 + \dots + x_n e_n : \text{Linear combination}$$

Example:

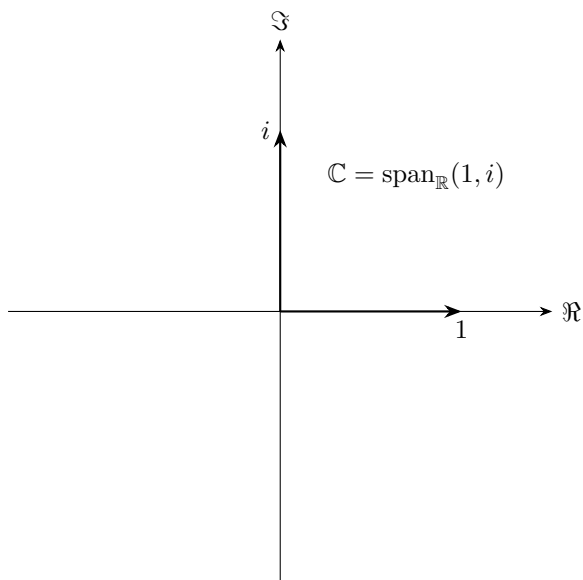
$$\mathbb{C}^2 = \text{span}_{\mathbb{C}}(e_1, e_2) = \{z_1 e_1 + z_2 e_2 : z_1, z_2 \in \mathbb{C}\}$$

where $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and e_1, e_2 are in $\dim_{\mathbb{C}} \mathbb{C}^2 = 2$ and $\dim_{\mathbb{R}} \mathbb{C}^2 = 4$.

$$= \{(x_1 + iy_1)e_1 + (x_2 + iy_2)e_2 : x_1, x_2, y_1, y_2 \in \mathbb{R}\}$$

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

$$= \text{span}_{\mathbb{R}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} i \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ i \end{pmatrix}\right)$$



$$\mathbb{C} = \text{span}_{\mathbb{C}}(1) = \{\lambda : \lambda \in \mathbb{C}\}$$

$$\mathbb{C} = \text{span}_{\mathbb{R}}(1, i) = \{x + iy : x, y \in \mathbb{R}\}$$

Abstract vector space: V = a set vector space = addition $(v_1 + v_2)$, scalar multiplication $(\lambda v$ where λ is a field k) + axioms

Def: Let k be a field. A vector space over k is a set V and two operations

$$\begin{cases} v_1 + v_2 \in V, v_1, v_2 \in V \\ \lambda v \in V, v \in V, \lambda \in k \end{cases} + 8 \text{ axioms.}$$

$$\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$$

4 rules for addition:

$$(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$$

There exists a zero $0(\text{origin of } V) \in V$ $[0 + v = v]$ $-v$ makes sense $u + v = v + u$
 2 rules (axioms) for scaling:

$$1 \cdot v = v$$

$$\lambda_1(\lambda_2 v) = (\lambda_1 \lambda_2) v$$

compatibility: distributivity

$$(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$$

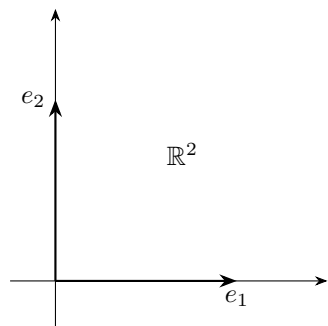
$$\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$$

Example 1: Let K be a Field

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

is a vector space over K Remark:

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



5 Appendix

6 Solutions

Solution 1. 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 2. 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. 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 $\frac{1}{0*0-1*0} \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}$ ⁶. 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.

7 Useful Links

⁶Recall that an inverse of a 2×2 matrix is equal to its determinant multiplied with its conjugate