MATH 223: Linear Algebra

William Homier[1]

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

January 5^{th}, 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 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]*. 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 $f = a_n x^n + ... + a_1 x + a_0$ 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 $f(z) = 0$.

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

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 $\overline{z} = x - iy$. Some basic properties of complex conjugates are:

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

2.2.4 Geometric and Polar Form of Complex Numbers

January 09, 2026.

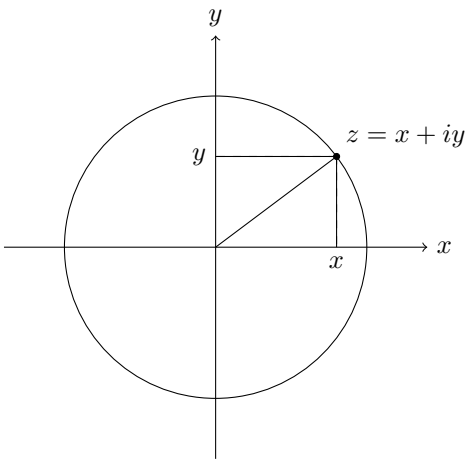
1. Geometric Interpretation

[2]The 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*

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

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

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

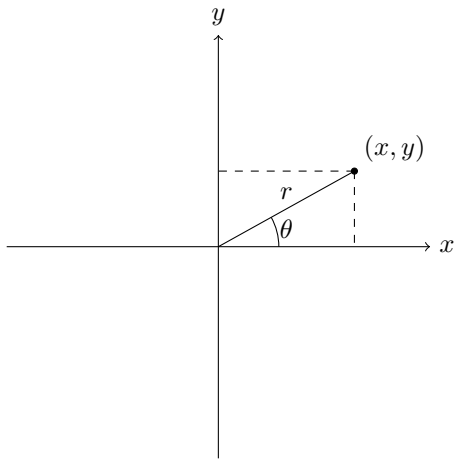
$$S' = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\} = \{z \in \mathbb{C} : |z| = 1\},$$

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

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

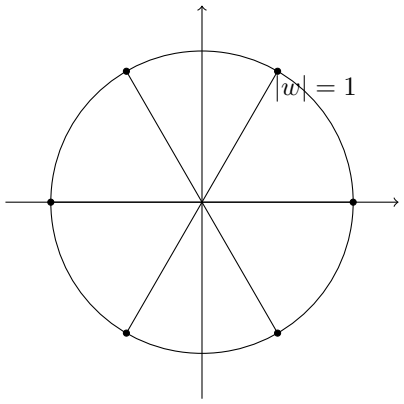
Definition 9 (Roots of unity)**.** *The n^{th} roots of unity are the solutions of*

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

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

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

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 equipped with a binary operation*

$$\cdot : M \times M \to M$$

that assigns to every pair (a, b) an element $ab \in M$.

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 matrix*[3] $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \dots & 0 \\ 0 & 0 & 1 \end{bmatrix}$*. 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 unique*[4]*.*

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

Example. *Let $M = \mathbb{Z} = \{... - 2, -1, 0, 1, 2, ...\}$ 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

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

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.*

[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.

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 multiplication[5]. 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

January 09, 2026.

4.1 Cartesian space

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

You can add two vectors:

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

Scalar multiplication:

$$\lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}$$

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

A linear combination is a vector v of the form $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$.

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

Set A inside $\mathbb{R}^2$ $Span(A)$ = all linear combinations of elements in A.

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{R}^2$$

$$A = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right.$$

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

Draw a graph with one long diagonal line in the +x, +y and three arrows on the same line showing the vector grows.

$$Span\{r\} =$$

January 12, 2026.

line spanned by v.

$\mathbb{R}^n$ and $\mathbb{C}^n$. $v_1, \ldots, v_n \in \mathbb{R}^n$. Linear combination: $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$, where lambda is a scalar and v is a vector. example: $\lambda_1 v_1 + \lambda_2 v_2 = 2\begin{pmatrix}1\\3\end{pmatrix} + 4\begin{pmatrix}2\\5\end{pmatrix}$

Span:

$$Span(v_1, \ldots, v_n) = \{\lambda_2 v1 + \ldots + \lambda_n v_n : \lambda_i \in \mathbb{R}\}$$

example:

$$span\begin{pmatrix}1\\1\end{pmatrix}$$

draw a graf with a linear function with $span\begin{pmatrix}1\\1\end{pmatrix}$ in $\mathbb{R}^2$

Draw a graph with 2 linear functions one v1 and the other v2 and a point lambda1v1 on line v1, draw a line parallel to v2 from this point, and lamda2v2 on line v2, draw a line parallel to v1 from this point, and both new lines should intersect at lambda1v1 +lambda2v2, and v3 in span(v1,v2).

draw a graph with one linear function which is v1 and v2 together but v2 has the arrow at a later distance than v1 on the linear function and this graph says span(v1,v2) = span(v1) = span(v2).

now in $\mathbb{C}$: $v_1, \ldots, v_n \in \mathbb{C}^n$. Linear combination: $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$, where lambda is a scalar and v is a vector and $\lambda_i \in \mathbb{C}$. example: $\lambda_1 v_1 + \lambda_2 v_2 = 2\begin{pmatrix}1\\3\end{pmatrix} + 4\begin{pmatrix}2\\5\end{pmatrix}$

Span:

$$Span_{\mathbb{C}}(v_1, \ldots, v_n) = \{\lambda_2 v1 + \ldots + \lambda_n v_n : \lambda_i \in \mathbb{C}\}$$

example:

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

So:

$$\mathbb{R}^n = \{\begin{pmatrix}x_1\\\ldots\\x_n\end{pmatrix} : x_i \in \mathbb{R}\} \qquad \mathbb{C}^n = \{\begin{pmatrix}x_1\\\ldots\\x_n\end{pmatrix} : x_i \in \mathbb{C}\}$$

Standard basis:

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

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

Basis -¿ (span + LI)

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

$$Let \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} x_2 \\ \vdots \\ x_n \end{pmatrix} + \ldots + \begin{pmatrix} 0 \\ \vdots \\ x_n \end{pmatrix} = x_1e_1 + x_2e_2 + \ldots + x_ne_n : Linearcombination$$

Example:

$$\mathbb{C}^2 = span_{\mathbb{C}}(e_1, e_2) = \{z_1e_1 + z_2e_2 : z_1, z_2 \in \mathbb{C}\}$$

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

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

$$= x_1e_1 + x_2e_2 + y_1(ie_1) + y_2(ie_2)$$

$$= span_{\mathbb{R}}(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} i \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ i \end{pmatrix})$$

Draw a graph in $\mathbb{C}$ where there is an arrow on the x-axis named 1 and one on the y-axis named i.

$$\mathbb{C} = span_{\mathbb{C}}(1) = \{\lambda : \lambda \in \mathbb{C}\}$$

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

Abstract vector space: V = a set vector space = addition $(v_1 + v_2)$, scalar multiplication (λv 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

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

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

.

4 rules for addition:

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

There exists a zero $0(originofV) \in V[0 + v = v]$ $-v$ 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

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

is a vector space over K Remark:

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

Draw graph with unit vectors e_1 on x and e_2 on y.

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

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