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.

- $\mathbb{N}$ is the set of natural numbers: (0, 1, 2, 3, ...).
- $\mathbb{Z}$ is the set of integers: (..., -3, -2, -1, 0, 1, 2, 3, ...).
- $\mathbb{Q}$ is the set of rational numbers (numbers that can be expressed as a fraction of two integers): $\mathbb{Q} = \frac{a}{b}|a, b \in \mathbb{Z}, b \neq 0$.
- $\mathbb{R}$ = all rational + all irrational numbers.
- $\mathbb{C} = \{x+iy|x, y \in \mathbb{R}\}$, basically: $\mathbb{C}$ = all real ($\mathbb{R}$) + all imaginary numbers (i), where i is defined to be a root of $x^2 + 1$, which is $i \subseteq \sqrt{-1}$.

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

We will be using the following symbols:

- $\subseteq$ means "is a subset of or equal to".
- $\subset$ means "is a subset of" or "is contained in", it could also mean the same thing as $\subseteq$, but not all the time.
- $\forall$ means "for all".
- $\exists$ means "there exists".

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 $i^2 + 1 = 0$.

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:

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

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:

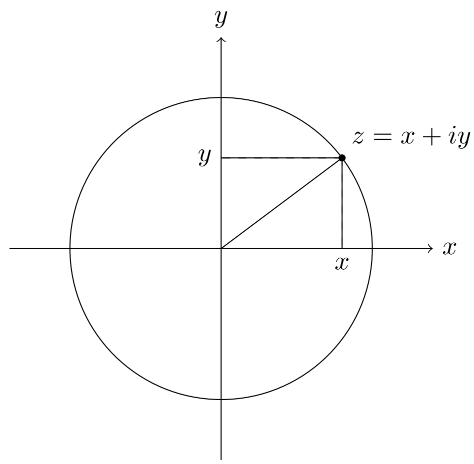
- $\overline{z} = z$
- $\overline{z + z'} = \overline{z} + \overline{z'}$
- $\overline{z \cdot z'} = \overline{z} \cdot \overline{z'}$

January 09, 2026.

2.2.4 Geometric and Polar Form of Complex Numbers

Definition 1 (Geometric interpretation). *Every complex number $z = x + iy$ can be identified with a point (x, y) in the plane, called the* complex plane. *This allows us to study complex numbers using geometry.*

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



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

Definition 2 (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:

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

Thus, S' is the *unit circle* in the complex plane.

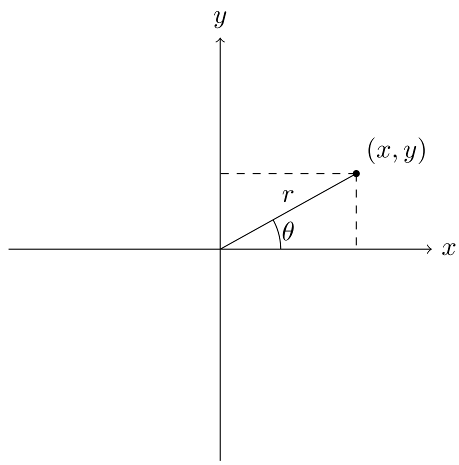
Definition 3 (Powers of i)**.**

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

Definition 4 (Geometric meaning of multiplication)**.** *Multiplying by a complex number z corresponds geometrically to*

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

Definition 5 (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.

$$x = r\cos(\theta), \quad y = r\sin(\theta).$$

Definition 6 (Polar and exponential form)**.**

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

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

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

Definition 8 (Multiplication in polar form)**.**

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

Example.

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

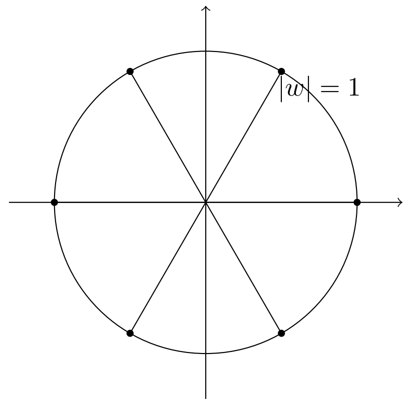
Definition 9 (n^{th} roots)**.** *An n^{th} root of z is a complex number w such that*

$$w^n = z.$$

Definition 10 (Roots of unity)**.** *The n^{th} roots of unity are the solutions of*

$$w^n = 1, \quad w \in \mathbb{C}.$$

Geometrically, they lie on the unit circle $|w| = 1$.



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

3 Basic Algebraic structures

"Let V be a vector space over a field K"

3.1 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] $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & ... & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. *Then A is invertible, and $B = A^{-1}$.*

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 $\frac{1}{2} \in \mathbb{R}$.

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

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

3.2 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 $\mathbb{Z}$.

3.3 Field

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

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

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

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

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.

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

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

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

$$Span\{r\} =$$

line spanned by v

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