Linear Algebra

Nikola Mazzola

September 3, 2025

Contents

Chapter 0

Prerequisites

0.1 Sets

Lecture 01: Sets

Definition (Set). Collection of objects where objects can be almost anything (number, symbol, set, shape...)

Note. This definition can lead to paradoxes, but its fine. Axiomatic set theories avoid this (e.g., Zermelo-Fraenkel), but usually the subtleties are not necessary.

- A set is described by the objects that **belong** to it (are **in** it)
- Sets are given (usually single, upper-cased, italicized, roman letter) names: A, B, X, P, R, T
- An object in a set is a **member** or **element** of A
- Belonging to (being a member of, being in) a set is denoted by $\in$ (e.g., $2 \in A$)

Definition 0.1.1 (Equal). Two sets, A and B are **equal** (denoted $A = B$) if every member of A is also a member of B and every member of B is also a member of A

> **Note.** There is no order of members in a set (no "first," or "last" member)

0.1.1 Set-builder notation

- To describe a small set, we can list members explicitly with curly braces, separated by commas (e.g., $A = \text{☺}, \text{☹}, \text{🔔}$)
- For larger (possibly infinite) sets we describe members using a predicate
  - A is the set of students in Quiz Bowl club
  - $\mathbb{N}$ is the set of Natural numbers
- The set-builder notation, $\{x : \Phi(x)\}$, is a concise expression of this
  - $A = \{x : x \text{ is a student in Quiz Bowl club}\}$
  - $B = \{x : x^2 = 4\}$
  - $C = \{2k : k \in \mathbb{N}\}$

Definition (Predicate). A logical formula that evaluates to True ($\top$) or False ($\bot$)

Definition (Domain of Discourse). Universe of objects that can potentially be in the set if they satisfy the predicate

Usually implied from the context, but can be explicitly defined:

$$E \in \mathbb{N} : (x\%2) = 0\}$$

where $\mathbb{N}$ is the set of natural numbers (counting numbers):

$$\mathbb{N} = 1, 2, 3, \ldots$$

0.1.2 Logic

Definition (Conditional Operator). Denoted $p \Rightarrow q$ ("if p then q" or "p implies q")

$$(p \Rightarrow q) = \begin{cases} \bot & \text{if } p = \top, q = \bot \\ \top & \text{otherwise} \end{cases}$$

Definition (Conjunction Operator). Denoted $p \wedge q$ ("p and q")

$$(p \wedge q) = \begin{cases} \top & \text{if } p = \top, q = \top \\ \bot & \text{otherwise} \end{cases}$$

Definition (Disjunction Operator). Denoted $p \vee q$ ("p or q")

$$(p \vee q) = \begin{cases} \bot & \text{if } p = \bot, q = \bot \\ \top & \text{otherwise} \end{cases}$$

Definition (Negation Operator). Denoted $\neg p$ ("not p")

$$(\neg p) = \begin{cases} \top & p = \bot \\ \bot & p = \top \end{cases}$$

Definition (Biconditional Operator). Denoted $p \Leftrightarrow q$ ("p if and only if q")

$$(p \Leftrightarrow q) = (p \Rightarrow q) \wedge (q \Rightarrow p)$$

0.1.3 Set Notation and Terminology

Let A, B be sets from the same domain of discourse

Definition 0.1.2 (Subset). A is called a **subset** of B, denoted $A \subseteq B$, if

$$(x \in A) \Rightarrow (x \in B)$$

Note.

$$A \subseteq A$$

Definition 0.1.3 (Intersection). The **intersection** of A and B, denoted $A \cap B$, is the set

$$(A \cap B) = \{x : (x \in A) \wedge (x \in B)\}$$

Definition 0.1.4 (Union). The **union** of A and B, denoted $A \cup B$, is the set

$$(A \cup B) = \{x : (x \in A) \vee (x \in B)\}$$

Notation. The **empty set**, denoted $\emptyset$, contains no members

Note.

$$\emptyset \subseteq A$$

Definition 0.1.5 (Power Set). Let A be a set; the **power set of** A, denoted $P(A)$, is the set of all subsets of A: Aug

$$P(A) = \{S : S \subseteq A\}$$

Example.

$$\begin{aligned} A &= \{\text{☺}, \text{☹}, \text{🔔}\} \\ P(A) &= \{\emptyset, \{\text{☺}\}, \{\text{☹}\}, \{\text{🔔}\}, \{\text{☺}, \text{☹}\}, \{\text{☺}, \text{🔔}\}, \{\text{☹}, \text{🔔}\}, \{\text{☺}, \text{☹}, \text{🔔}\}\} \end{aligned}$$

Definition 0.1.6 (Cartesian Product). Let A, B be sets; the **Cartesian product** of A with B, denoted $A \times B$ is the set of all ordered pairs of items, the first taken from A and the second taken from B

$$A \times B = \{(x, y) : x \in A, y \in B\}$$

Example.

$$\begin{aligned} A &= \{\text{☺}, \text{☹}, \text{🔔}\}, B = \{\text{⬡}, \text{𝅗𝅥}\} \\ A \times B &= \{(\text{☺}, \text{⬡}), (\text{☺}, \text{𝅗𝅥}), (\text{☹}, \text{⬡}), (\text{☹}, \text{𝅗𝅥}), (\text{🔔}, \text{⬡}), (\text{🔔}, \text{𝅗𝅥})\} \end{aligned}$$

Note. We denote an ordered pair with parenthesis, not curly braces

- (x, y) is not the same as x, y because order maters
- $x, y = y, x$ but $(x, y) \neq (y, x)$

0.2 Proofs

Lecture 02: Proofs Aug

Definition (Deductive Reasoning). The process of making deductive arguments

Definition (Deductive Argument). Process of making a logical inference

Definition (Inference). Claim that a certain predicate, called the **conclusion**, follows from one or more predicates, called the **premises**.

Predicate B **follows from** A if it is impossible simultaneously for A to be True and B to be False

An inference is **valid** if the conclusion follows from the premises

A deductive argument is **sound** if the inference is valid and its premises are True

Definition (Universal Quantification Symbol ($\forall$)). Denotes that a proposition is True for all members

Example.

$$\forall x \in \mathbb{N} : x^2 \geq x$$

Read: "**for all** (every, any, each) x in $\mathbb{N}$ the predicate $(x^2 \geq x)$ evaluates to True"

Definition (Existential Quantification Symbol($\exists$)). Denotes that a proposition is True for at least one member

Example.

$$\exists x \in \mathbb{N} : x^2 < x$$

Read: "**there exists** an x in $\mathbb{N}$ such that the predicate $x^2 < x$ evaluates to true"

Note. This is an example of a False proposition

0.2.3 Contraposition

Definition (Contraposition). Let p, q be predicates and consider the conditional statement

$$p \Rightarrow q$$

The **contrapositive** form of the statement is

$$\neg q \Rightarrow \neg p$$

A conditional statement and its contrapositive form are **equivalent**

$$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$$

When judging truthfulness of a statement, it sometimes helps to consider its contrapositive

Also existing, but not as common are:

- The **inverse**: $\neg p \Rightarrow \neg q$
- The **converse**: $q \Rightarrow p$
- The **complement**: $\neg(p \Rightarrow q)$

0.2.4 Proofs

Definition (Mathematical Proof). A deductive argument about something related to math. Uses spken/written language, or even sketches/diagrams.

Usually rigorous (spells out assumptions and deductive steps as is convenient) but informal (some natural language with occasionally ambiguous symbols/rules) deductive reasoning

Proposition 0.2.1. Let $n, m \in \mathbb{N}$ and suppose n, m are even; then $(n+m)$ is even

Proof.

- Since n is even $\exists k \in \mathbb{N}$ such that $n = 2k$
- Since m is even $\exists q \in \mathbb{N}$ such that $n = 2q$
- Then $(n+m) = (2k+2q) = 2(k+q)$
- Therefore, $(n+m)$ is even

Note. We used a method called **direct proof**

■

0.2.5 Mathematical Induction

Definition (Mathematical Induction). If asked to prove that a certain proposition, $P(n)$ is true for any $n \in \mathbb{N}$, we will accept as proof the following inference, if sound:

$$\begin{matrix} P(1) = \mathrm{T} \\ \left(P(k) \overset{2}{=} \mathrm{T}\right) \Rightarrow (P(k+1) = \mathrm{T}) \end{matrix} \overset{3}{\Rightarrow} P(n) = \mathrm{T}, \forall n \in \mathbb{N} \qquad (1)$$

Where (1) is called the **base case**; (2) is called the **induction hypothesis**; (3) is the **induction step**

A variant called **complete** (or strong/generalized) induction uses a stronger hypothesis in the induction step:

$$(P(j), \forall j \leq k) \Rightarrow P(k+1)$$

Proposition 0.2.2. For any $n \in \mathbb{N}$

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Proof. By induction

- Base case: for $n = 1, \frac{n(n+1)}{2} = 1$
- Induction step: suppose, for some $k \in \mathbb{N}$, $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$, then

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{(k+1)(k+2)}{2} \end{aligned}$$

■

Proposition 0.2.3. Let $n \in \mathbb{N}$, if n^2 is even then n is even

Proof. By Contraposition
Suppose n were not even, then

- n is odd, therefore
- $\exists k \in \mathbb{N}$ such that $n = 2k - 1$, and therefore
- $n^2 = n \cdot n = (2k-1)(2k-1) = 4k^2 - 4k + 1 = 4(k^2 - k) + 1$
- Let $p = 4(k^2 - k)$, then
- $p \div 2 = 2(k^2 - k)$, therefore
- p is even, therefore
- $n^2 = p + 1$ is odd
- Since n^2 is not odd, n cannot be not even

■

Proposition 0.2.4. $\sqrt{2}$ is irrational

Proof. By contradiction
Suppose $\sqrt{2}$ is rational, then

- $\exists p, q \in \mathbb{N}$ such that $\sqrt{2} = \frac{p}{q}$ and p and q have no common factors,

■

0.2.6 Things that often need proving

- Existence: $\exists x$ such that $P(x)$ Proof by construction describes who the required x is, and verifies $P(x) = \top$ (Don't need to actually find the thing)
- Uniqueness: $(P(x) \wedge P(y)) \Rightarrow (x = y)$ Name two things with the property and show they must be equal

0.2.7 Proof of Equivalence

To prove $P \Leftrightarrow Q$, prove both $P \Rightarrow Q$ and $Q \Rightarrow P$ Related: show two sets A, B are equal by showing $A \subseteq B$ and $B \subseteq A$ To prove the following are equivalent (TFAE) you could prove a circular chain of implications

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (C \Rightarrow D) \wedge (D \Rightarrow A)$$

0.3 Operations

Lecture 03: Operations

Aug

0.3.1 Function

Definition 0.3.1 (Function). A function comprises three objects:

- A set, called the **domain**
- Another set, called the **range**
- A mapping of each member of the domain to a single member of the range, called its **image**

Notation. Often we use lower-case Latin letters to name functions.

The notation $f : D \to R$ reads "f is a function from the domain set D into the range set R".

The image of $x \in D$ is denoted $f(x)$ (read "f of x").

Definition 0.3.2 (Image of a Set). Let $f : D \to R$ be a function and let $U \subseteq D$.

The set of images of members of U is called the **image of** U, and denoted $f(U)$:

$$f(U) = \{f(x) : x \in U\}$$

The set of images of all members of the domain, $f(D)$, is called the **image of the function**.

Example. Let $D = \{-2, 2, 3, 5, 7\}$ and let $h : D \to \mathbb{N}$ be the mapping

$$h(-2) = 4, \quad h(2) = 4, \quad h(3) = 9, \quad h(5) = 25, \quad h(7) = 49$$

The domain and range are given explicitly. The image is evident from the mapping; the image of h is the set

$$S = \{4, 9, 25, 49\}$$

With D and S as above, let $f : D \to S$ be the mapping

$$f(-2) = 4, \quad f(2) = 4, \quad f(3) = 9, \quad f(5) = 25, \quad f(7) = 49$$

Strictly speaking, $f : D \to S$ and $h : D \to \mathbb{N}$ are different functions (they have different ranges). This distinction is not that important.

0.3.2 Ways to Describe a Function

There are many different ways to describe a function:

- **A table:**

Domain	-2	2	3	5	7
Image	4	4	9	25	49

- **A formula:** $f(x) = x^2$
- **A set of ordered pairs:** $f = \{(-2, 4), (2, 4), (3, 9), (5, 25), (7, 49)\}$
- **A set of ordered pairs in set builder notation:**

$$f = \{(x, y) : x \in \{-2, 2, 3, 5, 7\}, y = x^2\}$$

Note. Not every set of ordered pairs describes a valid function. For example:

$$\{(2, 2), (2, 3), (3, 1)\}$$

is not a function because the element 2 in the domain maps to two different values.

0.3.3 Bijection

Definition 0.3.3 (Injective, Surjective, Bijective). Let $f : D \to R$ be a function.

(i) f is called **injective** (or **one-to-one**) if distinct members of D are mapped to distinct members of R:

$$\forall x, x' \in D, \quad x \neq x' \Rightarrow f(x) \neq f(x')$$

(ii) f is called **surjective** (or **onto**) if every element of R is the image of some element of D:

$$\forall y \in R, \quad \exists x \in D : y = f(x)$$

(iii) f is called **bijective** if it is both injective and surjective (one-to-one and onto).

Note. Students are sometimes confused about the surjective part because, in calculus, it is customary to let the range of a function be implicitly defined as equal to its image, making every function surjective.

0.3.4 Binary Operations

Remember the four basic arithmetic operations? What they have in common is that they each take two numbers as input and produce one number as output.

Definition 0.3.4 (Binary Operation). Let A be a set. A **binary operation** on A is a function whose domain is the Cartesian Product $A \times A$.

Notation. An operation is often denoted with a symbol, like $\star$, instead of a letter, and the image of a pair from the domain is denoted with the operator between the pair items:

$$x \star y \quad \text{instead of} \quad f(x, y)$$

Example. Some examples of binary operations $\star$ on $\mathbb{N}$ are:

- $a \star b := a + b + 8$
- $a \star b := \max(a, b)$
- $a \star b :=$ the digit in the ones place of $a + b^2$

0.3.5 Range of Operations and Closure

The sum and product of any two natural numbers is a natural number:

$$\forall a, b \in \mathbb{N}, \quad a + b \in \mathbb{N}$$
$$\forall a, b \in \mathbb{N}, \quad ab \in \mathbb{N}$$

This is not true for subtraction and division:

$$\exists a, b \in \mathbb{N} : a - b \notin \mathbb{N}$$
$$\exists a, b \in \mathbb{N} : a/b \notin \mathbb{N}$$

This convenient property of addition and multiplication is called **closure**.

Definition 0.3.5 (Closure). A set A is said to be **closed with respect to an operation** $\star$ if

$$\forall a, b \in A, \quad (a \star b) \in A$$

Example.

- The set $\mathbb{N}$ is closed with respect to addition and with respect to multiplication
- The set $\mathbb{N}$ is not closed with respect to subtraction
- The set $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is closed with respect to subtraction

Definition 0.3.6 (Associative Operation). An operation $\star$ on a set A is called **associative** if, $\forall a, b, c \in A$:

$$(a \star b) \star c = a \star (b \star c)$$

Example.

- Addition and multiplication are associative operations on $\mathbb{Z}$
- Subtraction is not associative on $\mathbb{Z}$

Note. If $\star$ is an associative operation on A, it is customary to neglect parentheses:

$$(a \star b) \star c = a \star (b \star c) = a \star b \star c$$

It is implied in the definition of associativity that the set A is closed with respect to $\star$.

Problem (CFU). If $\star$ is associative on A, is it true that $\forall a, b, c, d \in A$:

$$(a \star b) \star (c \star d) = a \star (b \star c) \star d$$

Bonus CFU: can you prove your answer?
Answer. Yes.

$$(a \star b) \star (c \star d) = ((a \star b) \star c) \star d = (a \star (b \star c)) \star d = a \star (b \star c) \star d$$

⊛

Theorem 0.3.1 (Generalized Associativity). Let $\star$ be an associative operation on a set F. Then, for any $a_1, a_2, \ldots, a_n \in F$, every possible parenthesis ordering of

$$a_1 \star a_2 \star a_3 \star \cdots \star a_{n-1} \star a_n$$

is equivalent to the left-associated ordering:

$$(\cdots((a_1 \star a_2) \star a_3) \star \cdots \star a_n)$$

Proof. By generalized (strong) induction.

Base case: For $n = 1$ or $n = 2$ there is nothing to prove, and for $n = 3$, there are two possible orderings, and regular associativity guarantees that $(a_1 \star a_2) \star a_3$ is equal to the left-associated ordering $((a_1 \star a_2) \star a_3)$.

Inductive step: For $n > 3$, we suppose that every parenthesis ordering of an expression with fewer than n operands is equivalent to the left-associated ordering, and proceed to consider the expression with n operands:

$$E = a_1 \star a_2 \star \cdots \star a_n$$

Any ordering of parentheses ends with a final step:

$$E = L \star R$$

where L is some parenthesis ordering of $a_1 \star \cdots \star a_q$ and R is some parenthesis ordering of $a_{q+1} \star \cdots \star a_n$, and $q < n$.

By the induction hypothesis, both L and R are equal to their respective left-associated orderings:

$$L = (\cdots((a_1 \star a_2) \star \cdots) \star a_q)$$
$$R = (\cdots((a_{q+1} \star a_{q+2}) \star \cdots) \star a_n)$$

If $q = n - 1$, so that $R = a_n$, then $E = L \star R$ is already left-associated. Otherwise, write

$$R = M \star a_n = (\cdots((a_{q+1} \star a_{q+2}) \star \cdots) \star a_{n-1}) \star a_n$$

and

$$E = L \star (M \star a_n) = (L \star M) \star a_n$$

by regular associativity. By the induction hypothesis, since $L \star M$ includes $n-1$ operands, it is equivalent to the left-associated ordering of $a_1 \star \cdots \star a_{n-1}$, making $E = (L \star M) \star a_n$ the left-associated ordering of the original expression. ∎

0.3.7 Neutrality

Definition 0.3.7 (Neutral Element). Let $\star$ be an operation on the set A. An element $e \in A$ is called **neutral with respect to** $\star$ if

$$\forall a \in A, \quad a \star e = e \star a = a$$

Theorem 0.3.2 (Uniqueness of the Neutral). Let $\star$ be an operation on a set A. There is at most one element in A that is neutral with respect to $\star$.

Proof. Suppose $p, q \in A$ are both neutral with respect to $\star$. In that case:

- $p \star q = q$, because p is neutral
- $p \star q = p$, because q is neutral
- Therefore, $p = q$

∎

Note. Since a neutral element in A is unique, if it exists, we can call it **the** neutral.

Problem (Exercise). Let $\star$ denote the operation on $\mathbb{N}$ defined by $a \star b := a^b$.

(i) Is there, in $\mathbb{N}$, a neutral with respect to $\star$?

(ii) Can you prove your answer?

Answer. (i) No

(ii) Yes:

- If $a^x = a, \forall a \in \mathbb{N}$, then in particular $2^x = 2$ and therefore $x = 1$
- So, the only candidate for being a neutral with respect to $\star$ is 1
- However, if 1 is neutral with respect to $\star$, then $1^a = a, \forall a \in \mathbb{N}$, and in particular $1^2 = 2$
- Which it is not
- So there is no neutral element

⊛

0.3.8 Invertible Elements

Definition 0.3.8 (Invertible Element). Let $\star$ be an operation on A and let $e \in A$ be the neutral with respect to $\star$. An element $a \in A$ is called **invertible** if there exists an element $b \in A$ such that

$$a \star b = e$$
$$b \star a = e$$

If such an element b exists, it is called **an inverse of** a.

Example.

- Every element of $\mathbb{Z}$ is invertible with respect to addition
- In $\mathbb{N}$, 1 is the only invertible element with respect to multiplication
- In $\mathbb{Z}$, 1 and -1 are the only invertible elements with respect to multiplication

Chapter 1

Fields

1.1 Definition

Lecture 04: Definition

1.1.1 Algebra

Algebra is the study of equations and calculations. Calculations are done by carrying out operations on objects of an **algebraic structure**.

Definition (Algebraic Structure). A set of objects with operations defined on it.

1.1.2 Numbers as Models

Numbers are an algebraic structure constructed to model certain types of physical objects and their interactions:

- Objects such as apples and skittles
- Interactions such as trading skittles for apples

Interactions in the natural world have certain characteristics, discovered by observation. Operations on numbers have properties matching those observations.

1.1.3 The Natural Numbers Model

The natural numbers $\mathbb{N}$ consist of:

- A set $\mathbb{N}$ of objects, called numbers
- An algorithm assigning each number a unique name
- An algorithm for deciding which number is "next"
- A binary operation called addition, denoted by $+$
- An algorithm for finding $a+b$ for any $a, b \in \mathbb{N}$

These algorithms are constructed to have properties modeled after observed characteristics of combining physical objects.

1.1.4 The Integer Numbers Model

Additional observations reveal interactions not adequately modeled by $\mathbb{N}$. The integers $\mathbb{Z}$ extend $\mathbb{N}$ by:

- Adding a new number, called zero and denoted 0
- Matching each number $a \in \mathbb{N}$ with a new number $-a$
- Extending the addition algorithm for these new numbers

1.1.5 Abstraction and Generalization

Exploration in mathematics proceeds by abstraction and generalization:

1. Start with a familiar mathematical model whose properties are understood
2. Investigate a hypothetical, abstract structure defined by those properties
3. Any claim proven about the abstract structure is true for any concrete model satisfying the same axioms

1.1.6 Groups

Definition 1.1.1 (Group). A group is a set G equipped with an operation $\star$ that satisfies:

(i) $\forall a, b \in G,\ a \star b \in G$ (closure)

(ii) $\forall a, b, c \in G,\ (a \star b) \star c = a \star (b \star c)$ (associativity)

(iii) $\exists e \in G$ such that $\forall a \in G,\ a \star e = e \star a = a$ (neutral element)

(iv) $\forall a \in G,\ \exists b \in G$ such that $a \star b = b \star a = e$ (invertibility)

Definition 1.1.2 (Commutative Group). A commutative group is a group that also satisfies $\forall a, b \in G,\ a \star b = b \star a$.

Example.

- $(\mathbb{Z}, +)$ is a group
- $(\mathbb{Z}, \cdot)$ is not a group (fails invertibility)
- Hours on a clock with "passage of time" operation forms a group

Groups are important because many different things can be modeled as groups, but they don't capture everything we need for linear algebra.

1.1.7 The Rational Numbers Model

Additional observations lead to the need for division. The rational numbers are:

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

We can represent rational numbers as ordered pairs (a, b) where:

- Equality: $(a, b) = (c, d) \Leftrightarrow ad = bc$
- Addition: $(a, b) + (c, d) = (ad + bc, bd)$
- Multiplication: $(a, b) \cdot (c, d) = (ac, bd)$

1.1.8 Properties of $\mathbb{Q}$

From the definition of operations on $\mathbb{Q}$:

(i) $\mathbb{Q}$ is closed with respect to both addition and multiplication

(ii) Both operations are associative

(iii) Both operations are commutative

(iv) $(0, 1) \in \mathbb{Q}$ is neutral with respect to addition, $(1, 1) \in \mathbb{Q}$ is neutral with respect to multiplication

(v) Multiplication is distributive over addition: $a(b + c) = ab + ac$

(vi) Every $q \in \mathbb{Q}$ is invertible with respect to addition; every $q \neq (0, 1)$ is invertible with respect to multiplication

1.1.9 Fields

Definition 1.1.3 (Field). A field is a set F equipped with two binary operations, called addition and multiplication and denoted $+$ and $\cdot$ respectively, that satisfy:

(i) $\forall a, b \in F$: $a + b \in F$ and $a \cdot b \in F$ (closure)

(ii) $\forall a, b, c \in F$: $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativity) Aug

(iii) $\forall a, b \in F$: $a + b = b + a$ and $a \cdot b = b \cdot a$ (commutativity)

(iv) $\forall a, b, c \in F$: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ (distributivity)

(v) $\exists \tilde{0} \in F$ and $\exists \tilde{1} \in F$ such that $\forall a \in F$: $a + \tilde{0} = a$ and $a \cdot \tilde{1} = a$ (neutral elements)

(vi) $\forall a \in F$, $\exists a' \in F$ such that $a + a' = \tilde{0}$ (additive inverses)

(vii) $\forall a \neq \tilde{0} \in F$, $\exists a' \in F$ such that $a \cdot a' = \tilde{1}$ (multiplicative inverses)

(viii) $\tilde{0} \neq \tilde{1}$ (distinct neutral elements)

Note. The two operations are not completely symmetric

- Multiplication distributes over addition, but not vice versa
- The additive neutral is not required to have a multiplicative inverse

1.1.10 Notation and Terminology

- Elements of a field are called **scalars**
- We drop the tildes and refer to $\tilde{0}$ and $\tilde{1}$ as "zero" and "one"
- Multiplication precedes addition in order of operations
- We often omit the multiplication symbol: $ab + ac$ instead of $a \cdot b + a \cdot c$

1.1.11 Uniqueness of Inverses

Proposition 1.1.1 (Uniqueness of Additive Inverse). Let F be a field and $a \in F$. There exists a unique $a' \in F$ such that $a + a' = 0$.

Proof. Let $a \in F$ and suppose $a', a'' \in F$ such that

$$a' + a = a + a' = 0$$
$$a'' + a = a + a'' = 0$$

Then:

$$a' = a' + 0 = a' + (a + a'') = (a' + a) + a'' = 0 + a'' = a''$$

■

Proposition 1.1.2 (Uniqueness of Multiplicative Inverse). Let F be a field and $a \neq 0 \in F$. There exists a unique $a' \in F$ such that $a \cdot a' = 1$.

Proof. Let $a \in F$ and suppose $a', a'' \in F$ such that

$$a' \cdot a = a \cdot a' = 1$$
$$a'' \cdot a = a \cdot a'' = 1$$

Then:

$$a' = a' \cdot 1 = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = 1 \cdot a'' = a''$$

■

1.1.12 Inverse Notation and Operations

Since inverses are unique:

- The additive inverse of a is denoted $(-a)$
- The multiplicative inverse of a is denoted a^{-1}
- Subtraction: $a - b := a + (-b)$
- Division: when $b \neq 0$, $a/b := a \cdot b^{-1}$

1.2 Consequences

Lecture 05: Consequences

1.2.1 Properties of Zero Aug

Proposition 1.2.1 (Zero Property). Let F be a field. Then $\forall a \in F$, $a \cdot 0 = 0$.

Proof. Let $a \in F$. Then:

$$\begin{aligned} a \cdot \tilde{0} &= a \cdot \tilde{0} + \tilde{0} \\ &= a \cdot \tilde{0} + (a \cdot \tilde{0} + (-(a \cdot \tilde{0}))) = (a \cdot \tilde{0} + a \cdot \tilde{0}) + (-(a \cdot \tilde{0})) \\ &= a \cdot (\tilde{0} + \tilde{0}) + (-(a \cdot \tilde{0})) = a \cdot \tilde{0} + (-(a \cdot \tilde{0})) = \tilde{0} \end{aligned}$$

■

Proposition 1.2.2 (Zero Product Property). Let F be a field. Then $\forall a, b \in F$:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ or } b = 0$$

Proof. Either $a = 0$ or $a \neq 0$.

If $a = 0$, then the conclusion is satisfied.

If $a \neq 0$, then by field axiom (vii), $\exists a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Therefore:

$$b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = 0 \cdot a^{-1} = 0$$

∎

Proposition 1.2.3 (Zero Non-Invertible). Let F be a field. Then $0 \in F$ is not invertible with respect to multiplication.

Proof. Suppose, for contradiction, that $\exists a \in F$ such that $a \cdot 0 = 1$.

Then by Proposition 1.2.1, $1 = a \cdot 0 = 0$.

But by field axiom (viii), $0 \neq 1$, which is a contradiction. ∎

1.2.2 Modular Arithmetic

The integers modulo m is the set $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ with addition and multiplication defined by taking remainders after division by m.

Example. $\mathbb{Z}_2 = \{0, 1\}$ with operation tables:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

This is a field.

Example. $\mathbb{Z}_3 = \{0, 1, 2\}$ with operation tables:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

This is a field.

Example. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is not a field because $2 \cdot 2 = 0$ but $2 \neq 0$, violating the zero product property.

Note. These facts are important in applications but not central to linear algebra

- When m is prime, $\mathbb{Z}_m$ is a field
- When m is not prime, $\mathbb{Z}_m$ is not a field (by the zero product property) (doesn't mean no field with m members isn't possible)

1.2.3 Operations Involving Inverses

Proposition 1.2.4 (Inverse Properties). Let F be a field and let $a, b \in F$. Then:

(i) $-0 = 0$

(ii) $1^{-1} = 1$

(iii) $-(-a) = a$

(iv) $(a^{-1})^{-1} = a$ (when $a \neq 0$)

(v) $(-1) \cdot a = -a$

(vi) $(-a) \cdot b = -(a \cdot b)$

(vii) $(-a) \cdot b = a \cdot (-b)$

(viii) $(-a) \cdot (-b) = a \cdot b$

Proof.

(i) Since $0 + 0 = 0$, we have $-0 = 0$ by uniqueness of additive inverses.

(ii) Since $1 \cdot 1 = 1$, we have $1^{-1} = 1$ by uniqueness of multiplicative inverses.

(iii) Since $(-a) + a = 0$, we have $-(-a) = a$ by uniqueness of additive inverses.

(iv) Since $a^{-1} \cdot a = 1$, we have $(a^{-1})^{-1} = a$ by uniqueness of multiplicative inverses.

(v) $a + ((-1) \cdot a) = 1 \cdot a + ((-1) \cdot a) = (1 + (-1)) \cdot a = 0 \cdot a = 0$

(vi) $(-a) \cdot b = ((-1) \cdot a) \cdot b = (-1) \cdot (a \cdot b) = -(a \cdot b)$

(vii) $(-a) \cdot b = ((-1) \cdot a) \cdot b = (-1) \cdot (a \cdot b) = a \cdot ((-1) \cdot b) = a \cdot (-b)$

(viii) $(-a) \cdot (-b) = ((-1) \cdot a) \cdot ((-1) \cdot b) = (-1) \cdot (-1) \cdot a \cdot b$

Since $(-1) \cdot (-1) = (-1)^{-1} \cdot (-1) = 1$, we get: $(-a) \cdot (-b) = 1 \cdot a \cdot b = a \cdot b$

∎

1.3 Numbers

Lecture 06: Numbers

1.3.1 Essential vs Nonessential Properties

Note. The essential properties of natural numbers relate to counting and ordering. Other properties (like primality) are nonessential but useful for examples.

Example. The set $\{0, 1, 2, \ldots, p-1\}$ with addition and multiplication modulo p is a field if and only if p is prime.

1.3.2 Number System Extensions

Definition (Integers). Starting with $\mathbb{N}$ and adding zero and additive inverses:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-x : x \in \mathbb{N}\}$$

Definition (Rationals). Taking ordered pairs of integers:

$$\mathbb{Q} = \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$$

Note. Algorithms for addition, multiplication, and ordering extend from $\mathbb{N}$ to $\mathbb{Z}$ to $\mathbb{Q}$. The rigorous justification is handled in real analysis.

1.3.3 Irrational Numbers

The Pythagorean theorem reveals distances that cannot be expressed as ratios of integers.

Example (Pythagoras of Samos). Two unit-length sticks at right angles create a distance $\sqrt{2}$ between their free ends. No ratio of integers accurately describes this distance

Note. The existence of irrational numbers has been known since antiquity. Their rigorous construction (e.g., Dedekind cuts) is handled in real analysis.

1.3.4 Real Numbers

Definition (Real Numbers). We accept $\mathbb{R}$ as the union of rational and irrational numbers, using geometric intuition of "length" and the number line.

1.3.5 Complex Numbers

Definition 1.3.1 (Complex Numbers). We denote by $\mathbb{C}$ the set of ordered pairs of real numbers:

$$\mathbb{C} = \{(x, y) : x, y \in \mathbb{R}\}$$

with operations:

Equality: $(x, y) = (x', y') \Leftrightarrow x = x' \wedge y = y'$

Addition: $(x, y) + (x', y') = (x + x', y + y')$

Multiplication: $(x, y)(x', y') = (xx' - yy', xy' + x'y)$

Proposition 1.3.1 (Complex Field). The set $\mathbb{C}$ with addition and multiplication as defined is a field.

Proof. We verify each field axiom:

(i) **Closure:** Since $\mathbb{R}$ is closed under addition and multiplication, both $(x + x', y + y')$ and $(xx' - yy', xy' + x'y)$ belong to $\mathbb{C}$.

(ii) **Associativity:** For addition:

$$[(x, y) + (x', y')] + (x'', y'') = (x + x', y + y') + (x'', y'')$$
$$= ((x + x') + x'', (y + y') + y'') = (x + (x' + x''), y + (y' + y''))$$
$$= (x, y) + [(x', y') + (x'', y'')]$$

For multiplication:

$$[(x, y)(x', y')](x'', y'') = (xx' - yy', xy' + x'y)(x'', y'')$$
$$= ((xx' - yy')x'' - (xy' + x'y)y'', (xx' - yy')y'' + (xy' + x'y)x'')$$
$$= (x(x'x'' - y'y'') - y(x'y'' + y'x''), x(x'y'' + y'x'') + y(x'x'' - y'y''))$$
$$= (x, y)[(x', y')(x'', y'')]$$

(iii) **Commutativity:** For addition:

$$(x, y) + (x', y') = (x + x', y + y') = (x' + x, y' + y) = (x', y') + (x, y)$$

For multiplication:

$$(x, y)(x', y') = (xx' - yy', xy' + x'y) = (x'x - y'y, x'y + y'x) = (x', y')(x, y)$$

(iv) **Distributivity:**

$$(x, y)[(x', y') + (x'', y'')] = (x, y)(x' + x'', y' + y'')$$
$$= (x(x' + x'') - y(y' + y''), x(y' + y'') + y(x' + x''))$$
$$= (xx' - yy' + xx'' - yy'', xy' + yx' + xy'' + yx'')$$
$$= (x, y)(x', y') + (x, y)(x'', y'')$$

(v) **Neutral elements:** Let $\tilde{0} = (0, 0)$ and $\tilde{1} = (1, 0)$. Then:

$$(x, y) + (0, 0) = (x, y)$$
$$(x, y)(1, 0) = (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y)$$

(vi) **Additive inverses:** Let $-(x, y) = (-x, -y)$. Then:

$$(x, y) + (-x, -y) = (0, 0)$$

(vii) **Multiplicative inverses:** For $(x, y) \neq (0, 0)$, let:

$$(x, y)^{-1} = \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$$

Then $(x, y) \cdot (x, y)^{-1} = (1, 0)$.

(viii) **Distinct neutrals:** Since $0 \neq 1$ in $\mathbb{R}$, we have $(0, 0) \neq (1, 0)$.

∎

Aug

1.3.6 Real Numbers as Complex Subset

The mapping $x \leftrightarrow (x, 0)$ identifies $\mathbb{R}$ with the subset $\{(x, 0) : x \in \mathbb{R}\} \subset \mathbb{C}$.

This preserves operations:

$$x + y \leftrightarrow (x + y, 0) = (x, 0) + (y, 0) \tag{1.1}$$
$$xy \leftrightarrow (xy, 0) = (x, 0)(y, 0) \tag{1.2}$$

1.3.7 The Imaginary Unit

Definition (Imaginary Unit). We define $i = (0, 1)$, which satisfies $i^2 = -1$:

$$i \cdot i = (0, 1)(0, 1) = (0 - 1, 0 + 0) = (-1, 0)$$

Notation. Every complex number can be written uniquely as:

$$(x, y) = (x, 0) + (0, y) = x + yi$$

Definition 1.3.2 (Real and Imaginary Parts). For $z = x + yi \in \mathbb{C}$:

$$\Re(z) = x \quad \text{(real part)} \tag{1.3}$$
$$\Im(z) = y \quad \text{(imaginary part)} \tag{1.4}$$

1.3.8 Geometric Interpretation

Complex numbers correspond to points in the Cartesian plane, with the real part as x-coordinate and imaginary part as y-coordinate.

Polar Form

Definition 1.3.3 (Absolute Value and Argument). For $z = x + yi \in \mathbb{C}$:

$$|z| = \sqrt{x^2 + y^2} \quad \text{(absolute value)} \tag{1.5}$$
$$\arg(z) = \arctan\left(\frac{y}{x}\right) \quad \text{(argument, with correct quadrant)} \tag{1.6}$$

For complex numbers $z = |z|(\cos\theta + i\sin\theta)$ and $z' = |z'|(\cos\theta' + i\sin\theta')$:

$$zz' = |z||z'|[\cos(\theta + \theta') + i\sin(\theta + \theta')]$$

The absolute value of the product equals the product of absolute values, and the argument of the product equals the sum of arguments.

1.3.9 Complex Conjugate

Definition 1.3.4 (Complex Conjugate). For $z = x + yi \in \mathbb{C}$, the complex conjugate is:

$$\overline{z} = x - yi$$

Theorem 1.3.1 (Conjugate Properties). For $z, z_1, z_2 \in \mathbb{C}$:

(i) $\overline{\overline{z}} = z$

(ii) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

(iii) $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$

(iv) $z\overline{z} = |z|^2$

(v) $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$

1.3.10 Division

For $z, z' \in \mathbb{C}$ with $z' \neq 0$:

$$\frac{z}{z'} = \frac{z\overline{z'}}{z'\overline{z'}} = \frac{z\overline{z'}}{|z'|^2} = \frac{xx' + yy'}{x'^2 + y'^2} + i\frac{x'y - y'x}{x'^2 + y'^2}$$

Note. Elementary functions (exponential, trigonometric, logarithmic) extend to $\mathbb{C}$ while preserving many properties. The exponential function leads to what many consider the most beautiful equation in mathematics: Euler's identity, $e^{i\pi} + 1 = 0$, while considering functions brings us to complex analysis.