Honors Linear Algebra

MATH0540

Professor Melody Chan

Brown University

Edited by

Richard Tang

Contents

Chapter 1

Set Theory

Sets serve as a fundamental construct in higher-level mathematics. We start with a brief introduction to set theory.

§1.1 Sets

Definition 1.1.1: Sets

A **set** is a collection of elements.

1. $x \in X$ means x is an element of X.
2. $x \notin$ means x is not an element of X.
3. $X \subset Y$ means X is a subset of Y (i.e. $\forall x \in X, x \in Y$.)
4. $X = Y \iff X \subset Y \wedge Y \subset X$.
5. $A \cap B := \{x \mid x \in A \wedge x \in B\}$ means set intersection.
6. $A \cup B := \{x \mid x \in A \vee x \in B\}$ means set union.
7. $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$ means set difference.

Example 1. *Let*

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}.$$

denote the set of integers, and let

$$\mathbb{Z}^+ = \{0, 1, \dots\}.$$

denote the set of positive integers.

§1.1.1 Set Builder notation

Sets may be defined formally with set-builder notation:

$$X = \{\ \mathit{expression} \mid \mathit{rule}\}.$$

Example 2. *1. Let E represent the set of all even numbers. This set is expressed*

$$E = \{n \in \mathbb{Q} \mid \exists k \in \mathbb{Z} \ s.t.\ n = 2k\}.$$

2. *Let A represent the set of real numbers whose squares are rational numbers:*

$$A = \{a \in \mathbb{R} \mid a^2 \in \mathbb{Q}\}.$$

§1.1.2 Cartesian Products

Definition 1.1.2: Ordered Tuples

An **ordered pair** is defined (x, y). An **n-ordered tuple** is an ordered list of n items

$$(x_1, \ldots, x_n).$$

Definition 1.1.3: Cartesian Products

Let A, B be sets. The **cartesian product** $A \times B$ is defined

$$A \times B := \{(a, b) \mid a \in A, b \in B\}.$$

Similarly, define the n-fold cartesian product

$$A^n := A \times A \times \cdots \times A.$$

Example 3. $\mathbb{R}^2$ *and* $\mathbb{R}^3$ *are examples of commonly known Cartesian products, which represent the 2D- and 3D-plane respectively.*

Example 4. R^n *is a first example of a* ***vector space.*** *Let* $n \in \mathbb{Z}^+ \cup \{0\}$*:*

1. *(Addition in R^n) We define an* ***addition operation*** *on $\mathbb{R}^n$ by adding coordinate-wise*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

2. *(Scaling) Given $(x_1, \ldots, x_n) \in \mathbb{R}^n, \lambda \in \mathbb{R}$, we define*

$$\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n).$$

Remark 1. $\mathbb{R}_0 = \{0\}$.

§1.1.3 Functions

Let A, B be sets. Informally, a function $f : A \to B$ deterministically returns an element $b \in B$ for each $a \in A$. We write $f(a) = b$.

Example 5. *The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ maps $\mathbb{R}$ to the subset*

$$S \subset \mathbb{R} = \{(x, x^2) \mid x \in \mathbb{R}\}.$$

Definition 1.1.4: Functions

Let A, B be sets. A function $f : A \to B$ is a subset $G_f \subset A \times B$ such that $\forall a \in A, !\exists b \in B$ s.t. $(a, b) \in G_f$. We write $f(a) = b$ when $(a, b) \in G_f$.

Definition 1.1.5: Codomain

Given a function $f : A \to B$, A is the **domain** of f, and B is the **codomain** or **target** of f. Let the **range** of f be defined as

$$\{b \in B \mid f(a) = b, a \in A\}.$$

The range is the subset of B.

Definition 1.1.6: Bijectivity

Let $f : A \to B$ be a function.

1. f is **injective**, or an **injection**, if $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$ implies $a_1 = a_2$.
2. f is **surjective**, or a **surjection**, if $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$. Equivalently, the range is the whole codomain.
3. f is **bijective**, or a **bijection**, if it is both injective and surjective. Equivalently, $\forall b \in B$, there is a unique $a \in A$ such that $f(a) = b$.

§1.2 Fields

Roughly speaking, a **field** is a set, together with operations addition and multiplication. Vector spaces may be defined *over* fields.

Definition 1.2.1: Fields

A **field** is a set $\mathbb{F}$ containing elements named 0 and 1, together with binary operations $+$ and $\cdot$ satisfying:

- **commutativity**: $a + b = b + a, a \cdot b = b \cdot a \ \forall a, b \in \mathbb{F}$.
- **associativity**: $a + (b + c) = (a + b) + c \ \forall a, b, c \in \mathbb{F}$.
- **identities**: $0 + a = a, 1 \cdot a = a \ \forall a \in \mathbb{F}$.

- **additive inverse**: $\forall a \in \mathbb{F}, \exists b \in \mathbb{F}$ s.t. $a + b = 0$.
- **multiplicative inverse**: $\forall a \in \mathbb{F} \setminus \{0\}, \exists c \in \mathbb{F}$ s.t. $ac = 1$.
- **distributivity**: $a \cdot (b + c) = a \cdot b + a \cdot c \ \forall a, b, c \in \mathbb{F}$.

Example 6. $\mathbb{R}^+ \setminus \{0\}$ *is* ***not*** *a field under* $+, \cdot$.

Example 7. *(Finite Fields) Let* p *prime (e.g.* $p = 5$*). Define the field*

$$\mathbb{F}_p = \{0, \dots, p-1\},$$

with binary operations $+_p, \cdot_p$ *given by addition and multiplication modulo* p.