Basic Objects

Sets

A set is a collection of objects, such that any object \( x \) is either in the set (written \( x \in S \)) or not in the set (written \( x \notin S \)), but not both: \( S \) is a set \( \iff \forall x, \ x \in S \text{ xor } x \notin S \).

- One way of expressing a set is to explicitly list its elements—e.g., “the set \{ a, b, c \}”, or “the set \( A = \{ 1, 2, 3, \ldots \} \)”.
- More complicated sets are often expressed implicitly using the notation \( \{ x : P(x) \} \), e.g.:

\[
\text{“the set } \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x, y \in \mathbb{R} \text{ and } x = 2y \right\} \text{”}.
\]

- The left side indicates what the elements of the set look like, and the right side indicates the credentials required for inclusion into the set; in practical terms, \( \{ a \in \{ x : P(x) \} \} \text{ means “} a = x, \text{ where } P(x) \text{ is true”} \).

- for example, \( \vec{v} \in \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x, y \in \mathbb{R} \text{ and } x = 2y \right\} \iff \vec{v} = \begin{bmatrix} x \\ y \end{bmatrix} , \text{ where } x, y \in \mathbb{R} \text{ and } x = 2y \).

- Some common sets and the symbols used to represent them:
  - The set of integers: \( \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \)
  - The set of rationals: \( \mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\} \)
  - The set \( \mathbb{R} \) of real numbers
  - The set of complex numbers: \( \mathbb{C} = \{ a + bi : a, b \in \mathbb{R} \} \) (where \( i^2 = -1 \))

Linear algebra basics

- A field is a set \( F \) equipped with binary operations of addition (+) and multiplication (\( \cdot \)) satisfying axioms guaranteeing that arithmetic (+, −, ·, ÷) in \( F \) acts as usual.
  - Within the context of linear algebra, we refer to the elements of our field as scalars.
  - Some commonly-used fields are \( \mathbb{R}, \mathbb{C}, \) and \( \mathbb{Q} \); others include \( \mathbb{Z}_p \) and more exotic fields.

- Given a field \( F \) of scalars, a vector space over \( F \) is a collection \( V \) of objects, referred to as vectors, equipped with:
  - a binary operation of vector addition (giving the sum \( \vec{v} + \vec{w} \) for \( \vec{v}, \vec{w} \in V \)), and
  - an operation of scalar multiplication (giving the product \( \alpha \vec{v} \) for \( \alpha \in F \) and \( \vec{v} \in V \)), satisfying axioms guaranteeing that linear combinations can be formed and behave as usual.

- Some common types of vector spaces are:
  - \( F^n \), the space of column vectors of size \( n \) over \( F \)—e.g., \( \mathbb{R}^3, \mathbb{C}^2, \) etc.
  - \( F[x] \), the space of polynomials in \( x \) over \( F \)—e.g., \( \mathbb{R}[x], \mathbb{C}[z], \) etc.
  - \( C(\mathbb{R}) \) or \( C(I) \), the spaces of continuous functions on \( \mathbb{R} \) (or an interval \( I \), respectively).
  - The space of geometric vectors of some dimension, over \( \mathbb{R} \)—objects with magnitude and direction

- The fundamental operation in a vector space is the linear combination \( \alpha_1 \vec{v}_1 + \alpha_2 \vec{v}_2 + \cdots + \alpha_n \vec{v}_n \), where \( \alpha_1, \alpha_2, \ldots, \alpha_n \in F \) and \( \vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n \in V \).
  - This is computed by first performing the scalar multiplications, then adding the resulting vectors.
  - The operation of linear combination subsumes the operations of addition and scalar multiplication; conversely, each linear combination can be broken down into sums of scalar multiples.
  - The linear combination consisting of “no vectors” results in the zero vector, \( \vec{0} \in V \).

- A subspace \( W \) of a vector space \( V \) is a subset of \( W \subset V \) that is a vector space in its own right—i.e., such that every linear combination of vectors in \( W \) results in a vector in \( W \). [This property is called closure under linear combination.]

  - A three-point checklist allows us to check or prove whether a subset \( W \subset V \) is a subspace of \( V \):
    - \( \vec{0} \in W \)
    - \( \forall \alpha \in F \) and \( \vec{w}_1 \in W \), \( \alpha \vec{w}_1 \in W \)
    - \( \forall \vec{w}_1, \vec{w}_2 \in W \), \( \vec{w}_1 + \vec{w}_2 \in W \)

If all three hold, then \( W \) is a subspace of \( V \); if even one fails, then it is not.
Modern mathematics centers on logical statements (which may be either true or false) about mathematical concepts. Rather than judging such “truth” subjectively on the basis of faith or intuition, or relying on non-absolute methods such as experimental testing, in mathematics we demand that a statement be justified by a proof in order to be accepted—once proven, a statement achieves special status in mathematics and is often called a theorem (usually when it’s a final result) or lemma (when it’s a step toward something larger).

Aside: Mathematics is the study of logical relationships between mathematical concepts. Important concepts are given names and formal definitions in order to allow proper study of them, and proofs establish the logical connections between points of interest, providing us pathways of truth through the mathematical landscape. At first, we work with basic definitions and establish short logical pathways; building on this, we then establish theorems that allow us to jump greater logical distances in a single step; in turn, we use these theorems to prove larger theorems that span even greater logical distances, and so on... the result is a logical infrastructure in the mathematical landscape, which represents our understanding of mathematics—including logical reasoning skills, concepts, definitions, theorems, and proofs.

Proof

A proof is a sequence of logical statements, in which each statement is logically justified by some combination of axioms, definitions, established theorems, and the statements preceding it in the proof.

- The steps in a proof must build from start to finish.
- Proofs are not just about a statement being true—they’re about establishing the necessary connections to justify its truth.
  - If each step in a proof is valid, then the entire logical chain of the proof is valid.
  - Any improperly justified step in a proof invalidates the entire proof (even if the statement itself is true)!
- A few tips to keep in mind when writing a proof:
  - Keep close track of what you already know (!) and what you’re trying to show (?).
  - The first step of many proofs is to use definitions of terms to unravel them into the logical expressions that they represent; once this has been done, these logical expressions can be analyzed and combined to construct a proof.
  - Keep an eye out for any known results or theorems that relate to the statement you’re trying to prove—when something is already known about the concepts at play, a theorem can allow you to prove your statement without unraveling definitions—this becomes increasingly important as the concepts being studied increase in complexity.

Proof techniques

Noting how the statement we’d like to prove breaks down into smaller statements tells us a great deal about how to prove it:

- Each possible outermost logical construction leads us to a corresponding direct line of proof:
  - \( \forall x, \ P \): “Let \( x \) be given.” \( \leftarrow \) you must take the \( x \) that’s given to you, not choose one yourself
  - Show that \( P \) is true.
  - \( \exists x \text{ such that } \ P \): [Find an \( x \) that makes \( P \) true] \( \leftarrow \) this is only scratch work, not part of the proof
    - “Let \( x = \ldots \)”
    - Show that \( P \) is true for this \( x \).
  - \( p \Rightarrow q \): “Suppose \( P \)”
    - Show that \( Q \) is true.
  - \( p \Leftrightarrow q \): Show \( [p \Rightarrow q \text{ and } q \Rightarrow p] \) \( \leftarrow \) connect \( P \) to \( Q \) via a chain of \( \Leftrightarrow \)’s.
- A statement can also be proven indirectly by showing that its logical negation is false; the advantage that this sometimes provides is that negation changes the outermost operation of the expression, allowing a different line of attack.
- There are four common means of proving the most common type of mathematical assertion, the implication \( P \Rightarrow q \):
  - Suppose \( P \) and show \( Q \). (directly)
  - Suppose \( \neg Q \) and show \( \neg P \). (by the contrapositive)
  - Show that \( Q \text{ or not } P \) is true. (by definition)
  - Show that \( P \text{ and not } Q \) is false. (by contradiction)