Fons

Ryan Joo Rui An

The mathematician does not study mathematics because it is useful; he studies it because he delights in it and he delights in it because it is beautiful.

— Henri Poincaré (1854–1912)
French mathematician and theoretical physicist

This is (still!) an incomplete draft. Please send corrections and comments to `ryanjooruian18@gmail.com`, or pull-request at `https://github.com/Ryanjoo18/fons`.

Last updated August 20, 2024.

Preface

Fons, derived from the Latin word for source or fountain, introduces the core concepts of university-level mathematics. Just as a fountain provides a continuous wellspring of water, *Fons* aims to be a continuous source of knowledge for you.

At this moment of writing, I am a high school student working on my A Level studies in Singapore. I have about 11 years of participating in mathematics competitions, including three years of experience in mental arithmetic and the rest few years in mathematics olympiad.

This book mainly serves as my notes when studying mathematics at the university level. Feel free to refer to it too.

Ryan Joo Rui An
August 20, 2024
Singapore, SG

Introduction

The book is divided into the following sections:

1. **preliminary topics** such as basic logic and set theory,
2. **abstract algebra** which follows [DF04],
3. **linear algebra** which follows [Axl15],
4. **real analysis** which follows [Rud53; Apo57], and
5. **complex analysis** which follows [Ahl79],
6. **topology** which follows [Mun18],
7. **calculus** which follows [Spi08; Ste08].

The chapters in this book are structured as follows:

- A **theoretical portion**, which starts off with a couple of definitions coupled with examples, followed by theorems and propositions built upon the definitions.
- A series of **exercises**.
- Full **solutions** to the exercises.

The reader is not assumed to have any mathematical prerequisites, although some experience with proofs may be helpful.

Problem Solving

In [Pól45], George Pólya outlined the following problem solving cycle:

1. **Understand the problem**

   Ask yourself the following questions:

   - Do you understand all the words used in stating the problem?
   - Is it possible to satisfy the condition? Is the condition sufficient to determine the unknown? Or is it insufficient? Or redundant? Or contradictory?
   - What are you asked to find or show? Can you restate the problem in your own words?
   - Draw a figure. Introduce suitable notation.
   - Is there enough information to enable you to find a solution?

2. **Devise a plan**

   A partial list of heuristics – good rules of thumb to solve problems – is included:

- Guess and check
- Look for a pattern
- Make an orderly list
- Draw a picture
- Eliminate possibilities
- Solve a simpler problem
- Use symmetry
- Use a model
- Consider special cases
- Work backwards
- Use direct reasoning
- Use a formula
- Solve an equation
- Be ingenious

3. **Execute the plan**

   This step is usually easier than devising the plan. In general, all you need is care and patience, given that you have the necessary skills. Persist with the plan that you have chosen. If it continues not to work discard it and choose another. Don't be misled, this is how mathematics is done, even by professionals.

   - Carrying out your plan of the solution, check each step. Can you see clearly that the step is correct? Can you prove that it is correct?

4. **Check and expand**

   Pólya mentions that much can be gained by taking the time to reflect and look back at what you have done, what worked, and what didn't. Doing this will enable you to predict what strategy to use to solve future problems.

   Look back reviewing and checking your results. Ask yourself the following questions:

   - Can you check the result? Can you check the argument?
   - Can you derive the solution differently? Can you see it at a glance?
   - Can you use the result, or the method, for some other problem?

Building on Pólya's problem solving strategy, Schoenfeld [Sch92] came up with the following framework for problem solving, consisting of four components:

1. **Cognitive resources**: the body of facts and procedures at one's disposal.

2. **Heuristics**: 'rules of thumb' for making progress in difficult situations.

3. **Control**: having to do with the efficiency with which individuals utilise the knowledge at their disposal. Sometimes, this is referred to as metacognition, which can be roughly translated as 'thinking about one's own thinking'.

   (a) These are questions to ask oneself to monitor one's thinking.
   - What (exactly) am I doing? [Describe it precisely.] Be clear what I am doing NOW. Why am I doing it? [Tell how it fits into the solution.]
   - Be clear what I am doing in the context of the BIG picture – the solution. Be clear what I am going to do NEXT.

   (b) Stop and reassess your options when you
   - cannot answer the questions satisfactorily [probably you are on the wrong track]; OR
   - are stuck in what you are doing [the track may not be right or it is right but it is at that moment too difficult for you].

   (c) Decide if you want to
   - carry on with the plan,
   - abandon the plan, OR
   - put on hold and try another plan.

4. **Belief system**: one's perspectives regarding the nature of a discipline and how one goes about working on it.

Study Skills

The Faculty of Mathematics of the University of Cambridge has produced a leaflet called "Study Skills in Mathematics". The Faculty also has guidance notes intended to help students prepare for exams.

Similarly, the Mathematical Institute of the University of Oxford has a study guide and thoughts on preparing for exams.

Contents

Part I

Preliminaries

1 Mathematical Reasoning and Logic

§1.1 Logical statements and notation

It is useful to be familiar with the following terminology.

- A *definition* is a precise and unambiguous description of the meaning of a mathematical term. It characterises the meaning of a word by giving all the properties and only those properties that must be true.
- A *theorem* is a true mathematical statement that can be proven mathematically. In a mathematical paper, the term theorem is often reserved for the most important results.
- A *lemma* is a minor result whose sole purpose is to help in proving a theorem. It is a stepping stone on the path to proving a theorem. Very occasionally lemmas can take on a life of their own.
- A *corollary* is a result in which the (usually short) proof relies heavily on a given theorem.
- A *proposition* is a proven and often interesting result, but generally less important than a theorem.
- A *conjecture* is a statement that is unproved, but is believed to be true.
- An *axiom* is a statement that is assumed to be true without proof. These are the basic building blocks from which all theorems are proven.
- An *identity* is a mathematical expression giving the equality of two (often variable) quantities.
- A *paradox* is a statement that can be shown, using a given set of axioms and definitions, to be both true and false. Paradoxes are often used to show the inconsistencies in a flawed theory.

A *proof* is a sequence of true statements, without logical gaps, that is a logical argument establishing some conclusion.

A *proposition* is a sentence which has exactly one truth value, i.e. it is either true or false, but not both and not neither. A proposition is denoted by uppercase letters such as P and Q. If the proposition P depends on a variable x, it is sometimes helpful to denote it by $P(x)$.

We can so some algebra on propositions, which include

(i) *equivalence*, denoted by $P \iff Q$, which means P and Q are logically equivalent statements;

(ii) *conjunction*, denoted by $P \wedge Q$, which means "P and Q";

(iii) *disjunction*, denoted by $P \vee Q$, which means "P or Q";

(iv) *negation*, denoted by $\neg P$, which means "not P".

Here are some useful properties when handling logical statements. You can easily prove all of them using truth tables.

Proposition 1.1 (Double negation law)**.**

$$P \iff \neg(\neg P)$$

Proposition 1.2 (Commutative property)**.**

$$P \wedge Q \iff Q \wedge P, \quad P \vee Q \iff Q \vee P$$

Proposition 1.3 (Associative property for conjunction)**.**

$$(P \wedge Q) \wedge R \iff P \wedge (Q \wedge R)$$

Proposition 1.4 (Associative property for disjunction)**.**

$$(P \vee Q) \vee R \iff P \vee (Q \vee R)$$

Proposition 1.5 (Distributive property for conjunction across disjunction)**.**

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge Q)$$

Proposition 1.6 (Distributive property for disjunction across conjunction)**.**

$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$$

Proposition 1.7 (De Morgan's laws)**.**

$$\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$$

$$\neg(P \wedge Q) \iff (\neg P \vee \neg Q)$$

Exercise 1

Assume that x is a fixed real number. What is the negation of the statement $1 < x < 2$?

Solution. The negation of $1 < x < 2$ is "it is not the case that $1 < x < 2$". However this is not useful.

Note that $1 < x < 2$ means $1 < x$ and $x < 2$. Let $P : 1 < x$ and $Q : x < 2$. Then the statement $1 < x < 2$ is $P \wedge Q$.

By De Morgan's Laws, we have $\neg(P \wedge Q) \iff \neg P \vee \neg Q$.

The *Trichotomy Axiom of real numbers* states that given fixed real numbers a and b, exactly one of the statements $a < b, a = b, b < a$ is true. Hence $\neg P \iff \neg(1 < x) \iff (x \leq 1)$ and $\neg Q \iff \neg(x < 2) \iff (x \geq 2)$.

Thus

$$\neg(1 < x < 2) \iff \neg(P \wedge Q) \iff \neg P \vee \neg Q \iff (1 \geq x) \vee (x \geq 2).$$

Therefore the negation of $1 < x < 2$ is logically iffalent to the statement $x \leq 1$ or $x \geq 2$. □

Exercise 2

Assume that n is a fixed positive integer. Find a useful denial of the statement

$$n = 2 \text{ or } n \text{ is odd.}$$

Solution. Using De Morgan's Laws,

$$\begin{aligned} \neg[(n = 2) \vee (n \text{ is odd})] &\iff \neg(n = 2) \wedge \neg(n \text{ is odd}) \\ &\iff (n \neq 2) \wedge (n \text{ is even}) \end{aligned}$$

where we are using the fact that every integer is either even or odd, but not both.

Thus a useful denial of the given statement is: n is an even integer other than 2. □

§1.1.1 If, only if

Implication is denoted by $P \implies Q$, which means "P implies Q", i.e. if P holds then Q also holds. It is equivalent to saying "If P then Q". The only case when $P \implies Q$ is false is when the hypothesis P is true and the conclusion Q is false.

$P \implies Q$ is known as a *conditional statement*. P is known as the *hypothesis*, Q is known as the *conclusion*.

Statements of this form are probably the most common, although they may sometimes appear quite differently. The following all mean the same thing:

(i) if P then Q;

(ii) P implies Q;

(iii) P only if Q;

(iv) P is a sufficient condition for Q;

(v) Q is a necessary condition for P.

The *converse* of $P \implies Q$ is given by $Q \implies P$; both are not logically equivalent.

The *inverse* of $P \implies Q$ is given by $\neg P \implies \neg Q$, i.e. the hypothesis and conclusion of the statement are both negated.

The *contrapositive* of $P \implies Q$ is given by $\neg Q \implies \neg P$; both are logically equivalent.

How to prove: To prove $P \implies Q$, start by assuming that P holds and try to deduce through some logical steps that Q holds too. Alternatively, start by assuming that Q does not hold and show that P does not hold (that is, we prove the contrapositive).

§1.1.2 If and only if, iff

Bidirectional implication is denoted by $P \iff Q$, which means both $P \implies Q$ and $Q \implies P$. We can read this as "P if and only if Q". The letters "iff" are also commonly used to stand for "if and only if".

$P \iff Q$ is true exactly when P and Q have the same truth value.

$P \iff Q$ is known as a *biconditional statement*.

These statements are usually best thought of separately as 'if' and 'only if' statements.

How to prove: To prove $P \iff Q$, prove the statement in both directions, i.e. prove both $P \implies Q$ and $Q \implies P$. Remember to make very clear, both to yourself and in your written proof, which direction you are doing.

§1.1.3 Quantifiers

The *universal quantifier* is denoted by $\forall$, which means "for all" or "for every". An universal statement has the form $\forall x \in X, P(x)$.

The *existential quantifier* is denoted by $\exists$, which means "there exists". An existential statement has the form $\exists x \in X, P(x)$, where X is known as the *domain*.

These are versions of De Morgan's laws for quantifiers:

$$\neg\forall x \in X, P(x) \iff \exists x \in X, \neg P(x)$$
$$\neg\exists x \in X, P(x) \iff \forall x \in X, \neg P(x)$$

Exercise 3

Find a useful denial of the statement

$$\text{for all real numbers } x,\ \text{if } x > 2,\ \text{then } x^2 > 4$$

Solution. In logical notation, this statement is $(\forall x \in \mathbf{R})[x > 2 \implies x^2 > 4]$.

$$\begin{aligned}\neg\{(\forall x \in \mathbf{R})[x > 2 \implies x^2 > 4]\} &\iff (\exists x \in \mathbf{R})\neg[x > 2 \implies x^2 > 4]\\ &\iff (\exists x \in \mathbf{R})\neg[(x \leq 2) \vee (x^2 > 4)]\\ &\iff (\exists x \in \mathbf{R})[(x > 2) \wedge (x^2 \leq 4)]\end{aligned}$$

Therefore a useful denial of the statement is:

there exists a real number x such that $x > 2$ and $x^2 \leq 4$.

□

Exercise 4

Negate surjectivity.

Solution. If $f : X \to Y$ is not surjective, then it means that there exists $y \in Y$ not in the image of X, i.e. for all x in X we have $f(x) \neq y$.

$$\begin{aligned}\neg\forall y \in Y, \exists x \in X, f(x) = y &\iff \exists y \in Y, \neg(\exists x \in X, f(x) = y)\\ &\iff \exists y \in Y, \forall x \in X, \neg(f(x) = y)\\ &\iff \exists y \in Y, \forall x \in X, f(x) \neq y\end{aligned}$$

□

How to prove: To prove a statement of the form $\forall x \in X$ s.t. $P(x)$', start the proof with 'Let $x \in X$.' or 'Suppose $x \in X$ is given.' to address the quantifier with an arbitrary x; provided no other assumptions about x are made during the course of proving $P(x)$, this will prove the statement for all $x \in X$.

How to prove: To prove a statement of the form $\exists x \in X$ s.t. $P(x)$, there is not such a clear steer about how to continue: you may need to show the existence of an x with the right properties; you may need to demonstrate logically that such an x must exist because of some earlier assumption, or it may be that you can show constructively how to find one; or you may be able to prove by contradiction, supposing that there is no such x and consequently arriving at some inconsistency.

Remark. Read from left to right, and as new elements or statements are introduced they are allowed to depend on previously introduced elements but cannot depend on things that are yet to be mentioned.

Remark. To avoid confusion, it is a good idea to keep to the convention that the quantifiers come first, before any statement to which they relate.

§1.2 Proofs

A *direct proof* of $P \implies Q$ is a series of valid arguments that start with the hypothesis P and end with the conclusion Q. It may be that we can start from P and work directly to Q, or it may be that we make use of P along the way.

A *proof by contrapositive* of $P \implies Q$ is to prove instead $\neg Q \implies \neg P$.

A *disproof by counterexample* is to providing a counterexample in order to refute or disprove a conjecture. The counterexample must make the hypothesis a true statement, and the conclusion a false statement. In seeking counterexamples, it is a good idea to keep the cases you consider simple, rather than searching randomly. It is often helpful to consider "extreme" cases; for example, something is zero, a set is empty, or a function is constant.

A *proof by cases* is to first dividing the situation into cases which exhaust all the possibilities, and then show that the statement follows in all cases.

A *proof by contradiction* of P involves first supposing P is false, i.e. $\neg P$; to prove $P \implies Q$ by contradiction, suppose that Q is false, i.e. $P \wedge \neg Q$. Then show through some logical reasoning that this leads to a contradiction or inconsistency. We may arrive at something that contradicts the hypothesis P, or something that contradicts the initial supposition that Q is not true, or we may arrive at something that we know to be universally false.

Exercise 5 (Irrationality of $\sqrt{2}$)

Prove that $\sqrt{2}$ is irrational.

Proof. We prove by contradiction. Suppose otherwise, that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbf{Z}, b \neq 0$, a, b coprime.

Squaring both sides gives

$$a^2 = 2b^2.$$

Since RHS is even, LHS must also be even. Hence it follows that a is even. Let $a = 2k$ where $k \in \mathbf{Z}$. Substituting $a = 2k$ into the above equation and simplifying it gives us

$$b^2 = 2k^2.$$

This means that b^2 is even, from which follows again that b is even.

This contradicts the assumption that a, b coprime. Hence proven. □

Exercise 6

For any $n \in \mathbf{Z}$, prove that there is no integer $a > 1$ such that $a \mid n$ and $a \mid (n+1)$.

Proof. Suppose otherwise, that there exists an integer n and integer $a > 1$ such that $a \mid n$ and $a \mid (n+1)$.

Then $n = ak$ and $n + 1 = ah$ for some integers k and h.

$$ak + 1 = ah \implies 1 = a(h-k) \implies a \mid 1 \implies a = \pm 1$$

This contradicts $a > 1$.

Hence we conclude that, for any n, there is no integer $a > 1$ such that $a \mid n$ and $a \mid (n+1)$. □

To *prove uniqueness*, we can either assume $\exists x, y \in S$ such that $P(x) \wedge P(y)$ is true and show $x = y$, or argue by assuming that $\exists x, y \in S$ are distinct such that $P(x) \wedge P(y)$, then derive a contradiction. $\exists!$ denotes "there exists a unique". To prove uniqueness and existence, we also need to show that $\exists x \in S$ s.t. $P(x)$ is true.

§1.2.1 Proof of existence

To prove existential statements, we can adopt two approaches:

1. Constructive proof (direct proof):

   To prove statements of the form $\exists x \in X$ s.t. $P(x)$, find or construct *a specific example* for x. To prove statements of the form $\forall y \in Y$, $\exists x \in X$ s.t. $P(x,y)$, construct example for x *in terms of* y (since x is dependent on y).

   In both cases, you have to justify that your example x

   (a) belongs to the domain X, and

   (b) satisfies the condition P.

2. Non-constructive proof (indirect proof):

   Use when specific examples are not easy or not possible to find or construct. Make arguments why such objects have to exist. May need to use proof by contradiction. Use definition, axioms or results that involve existential statements.

Exercise 7

Prove that we can find 100 consecutive positive integers which are all composite numbers.

Proof. We can prove this existential statement via constructive proof.

Our goal is to find integers $n, n+1, n+2, \dots, n+99$, all of which are composite.

Take $n = 101! + 2$. Then n has a factor of 2 and hence is composite. Similarly, $n+k = 101! + (k+2)$ has a factor $k+2$ and hence is composite for $k = 1, 2, \dots, 99$.

Hence the existential statement is proven. □

Exercise 8

Prove that for all rational numbers p and q with $p < q$, there is a rational number x such that $p < x < q$.

Proof. We prove this by construction. Our goal is to find such a rational x *in terms of* p *and* q.

We take the average. Let $x = \frac{p+q}{2}$ which is a rational number.

Since $p < q$,

$$x = \frac{p+q}{2} < \frac{q+q}{2} = q \implies x < q$$

Similarly,

$$x = \frac{p+q}{2} > \frac{p+p}{2} = p \implies p < x$$

Hence we have shown the existence of rational number x such that $p < x < q$.

Remark. For this type of question, there are two parts to prove: firstly, x satisfies the given statement; secondly, x is within the domain (for this question we do not have to prove x is rational since $\mathbf{Q}$ is closed under addition).

□

Exercise 9

Prove that for all rational numbers p and q with $p < q$, there is an irrational number r such that $p < r < q$.

Proof. We prove this by construction. Similarly, our goal is to find an irrational r in terms of p and q. Note that we cannot simply take $r = \frac{p+q}{2}$; a simple counterexample is the case $p = -1, q = 1$ where $r = 0$ is clearly not irrational.

Since p lies in between p and q, let $r = p + c$ where $0 < c < q - p$. Since $c < q - p$, we have $c = \frac{q-p}{k}$ for some $k > 1$; to make c irrational, we take k to be irrational.

Take $r = p + \frac{q-p}{\sqrt{2}}$. We need to show r is irrational and $p < r < q$.

Part 1: $p < r < q$

Since $q < p$, $r = p + (\text{positive number}) > p$. On the other hand, $\frac{q-p}{\sqrt{2}} < q - p$ so $r < p + (q - p) = q$.

Part 2: r is irrational

We prove by contradiction. Suppose r is rational. We have $\sqrt{2} = \frac{q-p}{r-p}$. Since p, q, r are all rational (and $r - p \neq 0$), RHS is rational. This implies that LHS is rational, i.e. $\sqrt{2}$ is rational, a contradiction. □

Non-constructive proof

Exercise 10

Prove that every integer greater than 1 is divisible by a prime.

Proof. If n is prime, then we are done as $n \mid n$.

If n is not prime, then n is composite. So n has a divisor d_1 such that $1 < d_1 < n$. If d_1 is prime then we are done as $d_1 \mid n$. If d_1 is not prime then d_1 is composite, has divisor d_2 such that $1 < d_2 < n$.

If d_2 is prime, then we are done as $d_2 \mid d_1$ and $d_1 \mid n$ imply $d_2 \mid n$. If d_2 is not prime then d_2 is composite, has divisor d_3 such that $1 < d_3 < d_2$.

Continuing in this manner after k times, we will get

$$1 < d_k < d_{k-1} < \cdots < d_2 < d_1 < n$$

where $d_i \mid n$ for all i.

This process must stop after finite steps, as there can only be a finite number of d_i's between 1 and n. On the other hand, the process will stop only if there is a d_i which is a prime.

Hence we conclude that there must be a divisor d_i of n that is prime. □

Remark. This proof is also known as *proof by infinite descent*, a method which relies on the well-ordering principle of the positive integers.

Exercise 11

Prove that the equation $x^2 + y^2 = 3z^2$ has no solutions (x, y, z) in integers where $z \neq 0$.

Proof. Suppose we have a solution (x, y, z). Without loss of generality, we may assume that $z > 0$. By the least integer principle, we may also assume that our solution has z minimal. Taking remainders modulo 3, we see that

$$x^2 + y^2 \equiv 0 \pmod 3$$

Recalling that squares may only be congruent to 0 or 1 modulo 3, we conclude that

$$x^2 \equiv y^2 \equiv 0 \implies x \equiv y \equiv 0 \pmod 3$$

Writing $x = 3a$ and $y = 3b$ we obtain

$$9a^2 + 9b^2 = 3z^2 \implies 3(a^2 + b^2) = z^2 \implies 3 \mid z^2 \implies 3 \mid z$$

Now let $z = 3c$ and cancel 3's to obtain

$$a^2 + b^2 = 3c^2.$$

We have therefore constructed another solution $(a, b, c) = \left(\frac{x}{3}, \frac{y}{3}, \frac{z}{3}\right)$ to the original equation. However $0 < c < z$ contradicts the minimality of z. □

§1.2.2 Pigeonhole principle

Theorem 1.8 (Pigeonhole Principle (naive))**.** If m objects are placed into n boxes and $m > n$, then at least one box must contain more than one object.

Theorem 1.9 (Pigeonhole Principle (general))**.** If more than $k \cdot n$ objects are placed into n boxes, then at least one box must contain more than k objects.

§1.2.3 Proof by mathematical induction

Induction is an extremely powerful method of proof used throughout mathematics. It deals with infinite families of statements which come in the form of lists. The idea behind induction is in showing how each statement follows from the previous one on the list – all that remains is to kick off this logical chain reaction from some starting point.

Theorem 1.10 (Principle of Mathematical Induction (PMI))**.** Let $P(n)$ be a family of statements indexed by $\mathbf{Z}^+$. Suppose that

(i) (**base case**) $P(1)$ is true and

(ii) (**inductive step**) for all $k \in \mathbf{Z}^+$, $P(k) \implies P(k+1)$.

Then $P(n)$ is true for all $n \in \mathbf{Z}^+$.

Using logic notation, this is written as

$$\{P(1) \wedge (\forall n \in \mathbf{Z}^+)[P(k) \implies P(k+1)]\} \implies (\forall n \in \mathbf{Z}^+)P(n)$$

Induction is often visualised like toppling dominoes. The inductive step (ii) corresponds to placing each domino sufficiently close that it will be hit when the previous one falls over, and base case (i) corresponds to knocking over the first one.

$$P(1) \implies P(2) \implies \cdots \implies P(k) \implies P(k+1) \implies \cdots$$

Exercise 12

Prove that for any $n \in \mathbf{Z}^+$,

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Proof. Let $P(n) : \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Clearly $P(1)$ holds because for $n = 1$, the sum on the LHS is 1 and the expression on the RHS is also 1.

Now suppose $P(n)$ holds. Then we have

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Adding $n+1$ to both sides,

$$\begin{aligned}\sum_{k=1}^{n+1} k &= \frac{n(n+1)}{2} + (n+1)\\ &= \frac{(n+1)(n+2)}{2}\\ &= \frac{(n+1)[(n+1)+1]}{2}\end{aligned}$$

thus $P(n+1)$ is true.

By PMI, $P(n)$ is true for all $n \in \mathbf{Z}^+$. □

A corollary of induction is if the family of statements holds for $n \geq N$, rather than necessarily $n \geq 0$:

Corollary 1.11. Let N be an integer and let $P(n)$ be a family of statements indexed by integers $n \geq N$. Suppose that

(i) (**base case**) $P(N)$ is true and

(ii) (**inductive step**) for all $k \geq N$, $P(k) \implies P(k+1)$.

Then $P(n)$ is true for all $n \geq N$.

Proof. This follows directly by applying the above theorem to the statement $Q(n) = P(n+N)$ for $n \in N$. □

Strong induction

Another variant on induction is when the inductive step relies on some earlier case(s) but not necessarily the immediately previous case. This is known as *strong induction*:

Theorem 1.12 (Strong Form of Induction)**.** Let $P(n)$ be a family of statements indexed by the natural numbers. Suppose that

(i) (**base case**) $P(1)$ is true and

(ii) (**inductive step**) for all $m \in \mathbf{Z}^+$, if for integers k with $1 \leq k \leq m$, $P(k)$ is true then $P(m+1)$ is true.

Then $P(n)$ is true for all $n \in \mathbf{N}$.

Using logic notation, this is written as

$$\{P(1) \wedge (\forall m \in \mathbf{Z}^+)[P(1) \wedge P(2) \wedge \cdots \wedge P(m) \implies P(m+1)]\} \implies (\forall n \in \mathbf{Z}^+)P(n)$$

Proof. We can this it to an instance of "normal" induction by defining a related family of statements $Q(n)$.

Let $Q(n)$ be the statement "$P(k)$ holds for $k = 0, 1, \ldots, n$". Then the conditions for the strong form are equivalent to

(i) $Q(0)$ holds and

(ii) for any n, if $Q(n)$ is true then $Q(n+1)$ is also true.

It follows by induction that $Q(n)$ holds for all n, and hence $P(n)$ holds for all n. □

The following example illustrates how the strong form of induction can be useful:

> **Example 1.13** (Fundamental Theorem of Arithmetic)**.** Every natural number greater than 1 may be expressed as a product of one or more prime numbers.

Proof. Let $P(n)$ be the statement that n may be expressed as a product of prime numbers.

Clearly $P(2)$ holds, since 2 is itself prime.

Let $n \geq 2$ be a natural number and suppose that $P(m)$ holds for all $m < n$.

- If n is prime then it is trivially the product of the single prime number n.
- If n is not prime, then there must exist some $r, s > 1$ such that $n = rs$. By the inductive hypothesis, each of r and s can be written as a product of primes, and therefore $n = rs$ is also a product of primes.

Thus, whether n is prime or not, we have have that $P(n)$ holds. By strong induction, $P(n)$ is true for all natural numbers. That is, every natural number greater than 1 may be expressed as a product of one or more primes. □

Cauchy induction

Theorem 1.14 (Cauchy Induction)**.** Let $P(n)$ be a family of statements indexed by $\mathbf{Z}^+_{\geq 2}$. Suppose that

(i) (**base case**) $P(2)$ is true and

(ii) (**inductive step**) for all $k \in \mathbf{Z}^+$, $P(k) \implies P(2k)$ and $P(k) \implies (k-1)$.

Then $P(n)$ is true for all $n \in \mathbf{Z}^+_{\geq 2}$.

> **Exercise 13**
>
> Using Cauchy Induction, prove the AM–GM Inequality for n variables, which states that for positive reals $a_1, a_2, \ldots a_n$,
> $$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}.$$

Proof. Let $P(n)$ be $\frac{a_1+a_2+\cdots+a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}$.
Base case $P(2)$ is true because

$$\frac{a_1 + a_2}{2} \geq \sqrt{a_1 a_2} \iff (a_1 + a_2)^2 \geq 4a_1 a_2 \iff (a_1 - a_2)^2 \geq 0$$

Next we show that $P(n) \implies P(2n)$, i.e. if AM–GM holds for n variables, it also holds for $2n$ variables:

$$\begin{aligned}
\frac{a_1 + a_2 + \cdots + a_{2n}}{2n} &= \frac{\frac{a_1+a_2+\cdots+a_n}{n} + \frac{a_{n+1}+a_{n+2}+\cdots+a_{2n}}{n}}{2} \\
\frac{\frac{a_1+a_2+\cdots+a_n}{n} + \frac{a_{n+1}+a_{n+2}+\cdots+a_{2n}}{n}}{2} &\geq \frac{\sqrt[n]{a_1 a_2 \cdots a_n} + \sqrt[n]{a_{n+1} a_{n+2} \cdots a_{2n}}}{2} \\
\frac{\sqrt[n]{a_1 a_2 \cdots a_n} + \sqrt[n]{a_{n+1} a_{n+2} \cdots a_{2n}}}{2} &\geq \sqrt{\sqrt[n]{a_1 a_2 \cdots a_n}\,\sqrt[n]{a_{n+1} a_{n+2} \cdots a_{2n}}} \\
\sqrt{\sqrt[n]{a_1 a_2 \cdots a_n}\,\sqrt[n]{a_{n+1} a_{n+2} \cdots a_{2n}}} &= \sqrt[2n]{a_1 a_2 \cdots a_{2n}}
\end{aligned}$$

The first inequality follows from n-variable AM–GM, which is true by assumption, and the second inequality follows from 2-variable AM–GM, which is proven above.

Finally we show that $P(n) \implies P(n-1)$, i.e. if AM–GM holds for n variables, it also holds for $n-1$ variables. By n-variable AM–GM, $\frac{a_1+a_2+\cdots+a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}$ Let $a_n = \frac{a_1+a_2+\cdots+a_{n-1}}{n-1}$ Then we have

$$\frac{a_1 + a_2 + \cdots + a_{n-1} + \frac{a_1+a_2+\cdots+a_{n-1}}{n-1}}{n} = \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}$$

So,

$$\begin{aligned}
\frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} &\geq \sqrt[n]{a_1 a_2 \cdots a_{n-1} \cdot \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}} \\
\Rightarrow \left(\frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}\right)^n &\geq a_1 a_2 \cdots a_{n-1} \cdot \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} \\
\Rightarrow \left(\frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}\right)^{n-1} &\geq a_1 a_2 \cdots a_{n-1} \\
\Rightarrow \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} &\geq \sqrt[n-1]{a_1 a_2 \cdots a_{n-1}}
\end{aligned}$$

By Cauchy Induction, this proves the AM–GM inequality for n variables. □

Other variations

Apart from proving $P(n)$ indexed by $\mathbf{Z}^+$, we can also use PMI to prove statements of the form

- $(\forall n \in \mathbf{Z})P(n)$
  Base case: $P(0)$
  Inductive step: $(\forall k \in \mathbf{Z}_{\geq 0})P(k) \implies P(k+1)$ and $(\forall k \in \mathbf{Z}_{\leq 0})P(k) \implies P(k-1)$

$$\cdots \impliedby P(-n) \impliedby \cdots \impliedby P(-1) \impliedby P(0) \implies P(1) \implies \cdots \implies P(n) \implies \cdots$$

- $(\forall n \in \mathbf{Q})P(n)$
  Base case: $P(0)$
  Inductive step: $P(x) \implies P(-x)$ and $P\left(\frac{a}{b}\right) \implies P\left(\frac{a+1}{b}\right)$ and $P\left(\frac{a}{b}\right) \implies P\left(\frac{a}{b+1}\right)$

A more generalised version

Definition 1.15. A binary relation $\leq$ on X that satisfies the following conditions is called a *well-ordering* on X:

(i) for every $a, b \in X$, $a \leq b$ or $b \leq a$,

(ii) every non-empty subset S of X contains a least element wrt $\leq$.

Theorem 1.16 (Well-ordering principle)**.** Let $(X, \leq)$ be a well-ordered set, with the least element x_0. Then $P(x)$ holds for all $x \in X$ if the following conditions hold:

(i) (**base case**) $P(x_0)$ holds

(ii) (**inductive step**) $\forall x' \prec x$, $P(x') \implies P(x)$

The following principle allows us to apply induction in cases where there may not be a linear ordering.

§1.2.4 Symmetry principle

§1.2.5 Combinatorial arguments and proofs

Exercises

Some of the exercise problems here are from the “Number and Proofs” topic of H3 Mathematics, so the reader is assumed to have some basic knowledge in Number Theory, in particular modular arithmetic.

Problem 1. Let a, b be integers, not both 0. Prove that $\gcd(a+b, a-b) \leq \gcd(2a, 2b)$.

Proof. Direct proof.

Let $e = \gcd(a+b, a-b)$. Then $e \mid (a+b)$ and $e \mid (a-b)$. So

$$e \mid (a+b) + (a-b) \implies e \mid 2a$$

and

$$e \mid (a+b) - (a-b) \implies e \mid 2b$$

This implies e is a common divisor of $2a$ and $2b$. So $e \leq \gcd(2a, 2b)$. □

Problem 2 (Division Algorithm)**.** Let c and d be integers, not both 0. If q and r are integers such as $c = dq + r$, then $\gcd(c, d) = \gcd(d, r)$.

Proof. Let $m = \gcd(c, d)$ and $n = \gcd(d, r)$. To prove $m = n$, we will show $m \leq n$ and $n \leq m$.

(i) Show $n \leq m$

Since $n = \gcd(d, r)$, $n \mid d$ and $n \mid r$. There exists integers x and y such that $d = nx$ and $r = ny$.

From $c = dq + r$, we have $c = (nx)q + ny = n(xq + y)$ thus $n \mid c$. n is a common divisor of c and d, so $n \leq \gcd(c, d)$. Hence $n \leq m$.

(ii) Show $m \leq n$

This is left as an exercise.

□

Problem 3 (Euclid’s Lemma)**.** Let a, b, c be any integers. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Proof. Since $a \mid bc$, $bc = ak$ for some $k \in \mathbf{Z}$.

Since $\gcd(a, b) = 1$,

$$\begin{aligned} ax + by &= 1 \quad \text{for some } x, y \in \mathbf{Z} \\ cax + cby &= c \\ acx + aky &= c \\ a(cx + ky) &= c \end{aligned}$$

thus $a \mid c$. □

Problem 4. Let a and b be integers, not both 0. Show that $\gcd(a, b)$ is the smallest possible positive linear combination of a and b. (i.e. There is no positive integer $c < \gcd(a, b)$ such that $c = ax + by$ for some integers x and y.)

Proof. Prove by contradiction.

Suppose there is a positive integer $c < \gcd(a, b)$ such that $c = ax + by$ for some integers x and y.

Let $d = \gcd(a, b)$. Then $d \mid a$ and $d \mid b$, and hence $d \mid ax + by$. This means $d \mid c$.

Since c is positive, this implies $\gcd(a, b) = d \leq c$. This contradicts $c < \gcd(a, b)$.

Hence we conclude that there is no positive integer $c < \gcd(a, b)$ such that $c = ax + by$ for some integers x and y. □

Problem 5. Use the Unique Factorisation Theorem to prove that, if a positive integer n is not a perfect square, then $\sqrt{n}$ is irrational.

[The Unique Factorisation Theorem states that every integer $n > 1$ has a unique standard factored form, i.e. there is exactly one way to express $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ where $p_1 < p_2 < \cdots < p_t$ are distinct primes and $k_1, k_2, \ldots, k_t$ are some positive integers.]

Proof. Prove by contradiction.

Suppose n is not a perfect square and $\sqrt{n}$ is rational.

Then $\sqrt{n} = \frac{a}{b}$ for some integers a and b. Squaring both sides and clearing denominator gives

$$nb^2 = a^2. \tag{$*$}$$

Consider the standard factored forms of n, a and b:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$$

$$a = q_1^{e_1} q_2^{e_2} \cdots q_u^{e_u} \implies a^2 = q_1^{2e_1} q_2^{2e_2} \cdots q_u^{2e_u}$$

$$b = r_1^{f_1} r_2^{f_2} \cdots r_v^{f_v} \implies b^2 = r_1^{2f_1} r_2^{2f_2} \cdots r_v^{2f_v}$$

i.e. the powers of primes in the standard factored form of a^2 and b^2 are all even integers.

This means the powers k_i of primes p_i in the standard factored form of n are also even by Unique Factorisation Theorem (UFT):

Note that all p_i appear in the standard factored form of a^2 with even power $2c_i$, because of $(*)$. By UFT, p_i must also appear in the standard factored form of nb^2 with the same even power $2c_i$.

If $p_i \nmid b$, then $k_i = 2c_i$ which is even. If $p_i \mid b$, then p_i will appear in b^2 with even power $2d_i$. So $k_i + 2d_i = 2c_i$, and hence $k_i = 2(c_i - d_i)$, which is again even.

Hence $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} = \left(p_1^{\frac{k_1}{2}} p_2^{\frac{k_2}{2}} \cdots p_t^{\frac{k_t}{2}} \right)^2$.

Since $\frac{k_i}{2}$ are all integers, $p_1^{\frac{k_1}{2}} p_2^{\frac{k_2}{2}} \cdots p_t^{\frac{k_t}{2}}$ is an integer and n is a perfect square. This contradicts the given hypothesis that n is not a perfect square.

So we conclude that when a positive integer n is not a perfect square, then $\sqrt{n}$ is irrational. □

Problem 6 (Sieve of Eratosthenes)**.** If $p > 1$ is an integer and $n \mid p$ for each integer n for which $2 \le n \le \sqrt{p}$, then p is prime.

Proof. Prove by contrapositive.

Suppose that p is not prime, so it factors as $p = mn$ for $1 < m, n < p$.

Observe that it is not the case that both $m > \sqrt{p}$ and $n > \sqrt{p}$, because if this were true the inequalities would multiply to give $mn > \sqrt{p}\sqrt{p} = p$, which contradicts $p = mn$.

Therefore $m \le \sqrt{p}$ or $n \le \sqrt{p}$. Without loss of generality, say $n \le \sqrt{p}$. Then the equation $p = mn$ gives $n \mid p$, with $1 < n \le \sqrt{p}$. Hence it is not true that $n \nmid p$ for each integer n for which $2 \le n \le \sqrt{p}$. □

Problem 7 (Euclid's proof)**.** There are infinitely many primes.

Proof. Prove by contradiction.

Suppose otherwise, that the list of primes is finite. Let $p_1, \ldots, p_r$ be our finite list of primes. We want to show this is not the full list of the primes.

Consider the number

$$N = p_1 \cdots p_r + 1.$$

Since $N > 1$, it has a prime factor p. The prime p cannot be any of $p_1, \ldots, p_r$ since N has remainder 1 when divided by each p_i. Therefore p is a prime not on our list, so the set of primes cannot be finite. □

Problem 8. If n is an integer, prove that 3 divides $n^3 - n$.

Proof. Prove by cases. This is done by partitioning **Z** according to remainders when divided by d (i.e. equivalence classes).

We prove the three cases: $n = 3k$, $n = 3k + 1$, and $n = 3k + 2$.

Case 1: $n = 3k$ for some integer k

Then
$$n^3 - n = (3k)^3 - (3k) = 3(9k^3 - k).$$

Since $9k^3 - k$ is an integer, $3 \mid n^3 - n$.

Case 2: $n = 3k + 1$ for some integer k

Then
$$n^3 - n = (3k + 1)^3 - (3k + 1) = 3(9k^3 + 9k^2 + 2k).$$

Since $9k^3 + 9k^2 + 2k$ is an integer, $3 \mid n^3 - n$.

Case 3: $n = 3k + 2$ for some integer k

The proof is similar and shall be left as an exercise. □

Problem 9. Prove that for every pair of irrational numbers p and q such that $p < q$, there is an irrational x such that $p < x < q$.

Proof. Consider the average of p and q: $p < \frac{p+q}{2} < q$.

If $\frac{p+q}{2}$ is irrational, take $x = \frac{p+q}{2}$ and we are done.

If $\frac{p+q}{2}$ is rational, call it r, take the average of p and r: $p < \frac{p+r}{2} < r < q$. Since p is irrational and r is rational, $\frac{p+r}{2}$ is irrational. In this case, we take $x = \frac{3p+q}{4}$. □

Problem 10. Given n real numbers $a_1, a_2, \ldots, a_n$. Show that there exists an a_i $(1 \leq i \leq n)$ such that a_i is greater than or equal to the mean (average) value of the n numbers.

Proof. Prove by contradiction.

Let $\bar{a}$ denote the mean value of the n given numbers. Suppose $a_i < \bar{a}$ for all a_i. Then

$$\bar{a} = \frac{a_1 + a_2 + \cdots + a_n}{n} < \frac{\bar{a} + \bar{a} + \cdots + \bar{a}}{n} = \frac{n\bar{a}}{n} = \bar{a}.$$

We derive $\bar{a} < \bar{a}$, which is a contradiction.

Hence there must be some a_i such that $a_i > \bar{a}$. □

Problem 11. Prove that the following statement is false: there is an irrational number a such that for all irrational number b, ab is rational.

Thought process: prove the negation of the statement: for every irrational number a, there is an irrational number b such that ab is irrational.

Proving technique: constructive proof (note that we can consider multiple cases and construct more than one b)

Proof. Given an irrational number a, let us consider $\frac{\sqrt{2}}{a}$.

Case 1: $\frac{\sqrt{2}}{a}$ is irrational.

Take $b = \frac{\sqrt{2}}{a}$. Then $ab = \sqrt{2}$ which is irrational.

Case 2: $\frac{\sqrt{2}}{a}$ is rational.

Then the reciprocal $\frac{a}{\sqrt{2}}$. Since $\sqrt{6}$ is irrational, the product $\left(\frac{a}{\sqrt{2}}\right)\sqrt{6} = a\sqrt{3}$ is irrational. Take $b = \sqrt{3}$, which is irrational. Then $ab = a\sqrt{3}$ which is irrational. □

Problem 12. Prove that there are infinitely many prime numbers that are congruent to 3 modulo 4.

Proof. Prove by contradiction.

Suppose there are only finitely many primes that are congruent to 3 modulo 4. Let $p_1, p_2, \ldots, p_m$ be the list of all the primes that are congruent to 3 modulo 4.

We construct an integer M by $M = (p_1 p_2 \cdots p_m)^2 + 2$.

We have the following observation:

(i) $M \equiv 3 \mod 4$.

(ii) Every p_i divides $M - 2$.

(iii) None of the p_i divides M. [Otherwise, together with (ii), this will imply p_i divides 2, which is impossible.]

(iv) M is not a prime number. [Otherwise, by (i), M is a prime number congruent to 3 modulo 4. But $M \neq p_i$ for all $1 \leq i \leq m$. This contradicts the assumption that $p_1, p_2, \ldots, p_m$ are all the prime numbers congruent to 3 modulo 4.]

From the above discussion, we know that M is a composite number by (iv). So it has a prime factorization $M = q_1 q_2 \cdots q_k$.

Since M is odd, all these prime factors q_j must be odd, and hence q_j must be congruent to either 1 or 3 modulo 4.

By (iii), q_j cannot be any of the p_i. So all q_j must be congruent to 1 modulo 4. Then M, which is the product of q_j, must also be congruent to 1 modulo 4.

This contradicts (i) that M is congruent to 3 modulo 4.

Hence we conclude that there must be infinitely many primes that are congruent to 3 modulo 4. □

Problem 13. Prove that, for any positive integer n, there is a perfect square m^2 (m is an integer) such that $n \leq m^2 \leq 2n$.

Proof. Prove by contradiction.

Suppose otherwise, that $n > m^2$ and $(m+1)^2 > 2n$ so that there is no square between n and $2n$, then

$$(m+1)^2 > 2n > 2m^2.$$

Since we are dealing with integers and the inequalities are strict, we get

$$(m+1)^2 \geq 2m^2 + 2$$

which simplifies to

$$0 \geq m^2 - 2m + 1 = (m-1)^2$$

The only value for which this is possible is $m = 1$, but you can eliminate that easily enough. □

Problem 14. Prove that for every positive integer $n \geq 4$,

$$n! > 2^n.$$

Proof. Let $P(n) : n! > 2^n$

Base case: $P(4)$

LHS: $4! = 4 \times 3 \times 2 \times 1 = 24$, RHS: $2^4 = 16 < 24$

So $P(4)$ is true.

Inductive step: $P(k) \implies P(k+1)$ for all $k \in \mathbf{Z}^+_{\geq 4}$

$$\begin{aligned} k! &> 2^k \\ (k+1)k! &> 2^k(k+1) \\ &> 2^k 2 \quad \text{since from } k \geq 4,\ k+1 \geq 5 > 2 \\ &= 2^{k+1} \end{aligned}$$

hence proven $P(k) \implies P(k+1)$ for integers $k \geq 4$.

By PMI, we have proven $P(n)$ for all integers $n \geq 4$. □

Problem 15 (H2FM TJC 2023)**.** Prove by mathematical induction, for $n \geq 2$,

$$\sqrt[n]{n} < 2 - \frac{1}{n}.$$

Proof. Let $P(n) : \sqrt[n]{n} < 2 - \frac{1}{n}$ for $n \geq 2$.

Base case: $P(2)$

When $n = 2$, $\sqrt{2} = 1.41 \cdots < 2 - \frac{1}{2} = 1.5$ which is true. Hence $P(2)$ is true.

Inductive step: $P(k) \implies P(k+1)$ for all $k \in \mathbf{Z}^+_{\geq 2}$

Assume $P(k)$ is true for $k \geq 2, k \in \mathbf{Z}^+$, i.e.

$$\sqrt[k]{k} < 2 - \frac{1}{k} \implies k < \left(2 - \frac{1}{k}\right)^k$$

We want to prove that $P(k+1)$ is true, i.e.

$$k + 1 < \left(2 - \frac{1}{k+1}\right)^{k+1}$$

Since $k > 2$, we have

$$\begin{aligned}
\left(2 - \frac{1}{k+1}\right)^{k+1} &> \left(2 - \frac{1}{k}\right)^{k+1} \quad \because k > 2 \\
&= \left(2 - \frac{1}{k}\right)^k \left(2 - \frac{1}{k}\right) \\
&> k\left(2 - \frac{1}{k}\right) \quad \text{[by inductive hypothesis]} \\
&= 2k - 1 = k + k - 1 > k - 1 \because k > 2
\end{aligned}$$

Hence $P(k+1)$ is true.

Since $P(2)$ is true and $P(k) \implies P(k+1)$, by mathematical induction $P(n)$ is true. □

Problem 16. Prove that for all integers $n \geq 3$,

$$\left(1 + \frac{1}{n}\right)^n < n$$

Proof. **Base case:** $P(3)$

On the LHS, $\left(1 + \frac{1}{3}\right)^3 = \frac{64}{27} = 2\frac{10}{27} < 3$. Hence $P(3)$ is true.

Inductive step: $P(k) \implies P(k+1)$ for all $k \in \mathbf{Z}^+_{\geq 3}$

Our inductive hypothesis is

$$\left(1 + \frac{1}{k}\right)^k < k$$

Multiplying both sides by $\left(1 + \frac{1}{k}\right)$ (to get a $k+1$ in the power),

$$\left(1 + \frac{1}{k}\right)^k \left(1 + \frac{1}{k}\right) = \left(1 + \frac{1}{k}\right)^{k+1} < k\left(1 + \frac{1}{k}\right) = k + 1$$

Since $k < k + 1 \iff \frac{1}{k} > \frac{1}{k+1}$,

$$\left(1 + \frac{1}{k}\right)^{k+1} > \left(1 + \frac{1}{k+1}\right)^{k+1}$$

The rest of the proof follows easily. □

A sequence of integers F_i, where integer $1 \leq i \leq n$, is called the *Fibonacci sequence* if and only if it is defined recursively by $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n > 2$.

Problem 17. Let F_i be the Fibonacci sequence. Prove that $3 \nmid n$ if and only if F_n is odd.

Proof. ($\Longrightarrow$) $3 \nmid n \implies F_n$ is odd

($\Longleftarrow$) F_n is odd $\implies 3 \nmid n$ (We prove the contrapositive: $3 \mid n \implies F_n$ is even)

Hence we only need to prove the following via PMI:

- $(\forall n \in \mathbf{Z}^+$ and $3 \nmid n), F_n$ is odd
  Base case: $P(1), P(2)$
  Inductive step: $P(k) \implies P(k+3)$ for all $k \geq 1$
- $(\forall n \in \mathbf{Z}^+$ and $3 \mid n), F_n$ is even
  Base case: $P(3)$
  Inductive step: $P(k) \implies P(k+3)$ for all $k \geq 3$

[Note that we have partitioned the domain into two.]

Hence to show $\forall n \in \mathbf{Z}^+ \, P(n)$,

Base case: $P(1), P(2), P(3)$

Inductive step: $\forall k \in \mathbf{Z}^+ \, P(k) \implies P(k+3)$ □

Problem 18. Let a_i where integer $1 \le i \le n$ be a sequence of integers defined recursively by initial conditions $a_1 = 1$, $a_2 = 1$, $a_3 = 3$ and the recurrence relation $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for $n > 3$.

For all $n \in \mathbf{Z}^+$, prove that

$$a_n \le 2^{n-1}.$$

Proof. Let $P(n) : a_n \le 2^{n-1}$.

Given the recurrence relation, it could be possible to use $P(k), P(k+1), P(k+2)$ to prove $P(k+3)$ for all $k \in \mathbf{Z}^+$.

Base case: $P(1), P(2), P(3)$

$P(1) : a_1 = 1 \le 2^{1-1} = 1$ is true.

$P(2) : a_2 = 1 \le 2^{2-1} = 2$ is true.

$P(3) : a_3 = 3 \le 2^{3-1} = 4$ is true.

Inductive step: $P(k) \wedge P(k+1) \wedge P(k+2) \implies P(k+3)$ for all $k \in \mathbf{Z}^+$

By inductive hypothesis, for $k \in \mathbf{Z}^+$ we have $a_k \le 2^k, a_{k+1} \le 2^{k+1}, a_{k+2} \le 2^{k+2}$.

$$\begin{aligned} a_{k+3} &= a_k + a_{k+1} + a_{k+2} \quad \text{[start from recurrence relation]} \\ &\le 2^k + 2^{k+1} + 2^{k+2} \quad \text{[use inductive hypothesis]} \\ &= 2^k(1 + 2 + 2^2) \\ &< 2^k(2^3) \quad \text{[approximation, since } 1 + 2 + 2^2 < 2^3\text{]} \\ &= 2^{k+3} \end{aligned}$$

which is precisely $P(k+3) : a_{k+3} \le 2^{k+3}$. □

Problem 19 (Bézout's lemma)**.** Let a and b be integers, not both 0. Prove that $\gcd(a,b) = ax_0 + by_0$ for some integers x_0 and y_0.

Solution. Given a and b, consider the set

$$S = \{z \in \mathbf{Z} \mid z > 0; \exists x, y \in \mathbf{Z}, z = ax + by\}.$$

S satisfies the conditions of well-ordering principle, and hence has a smallest element $c = ax_0 + by_0$. We want to show that (i) c is a common divisor of a and b; (ii) $c = \gcd(a,b)$.

(i) c is a common divisor of a and b

Suppose $c \nmid a$. By quotient-remainder theorem, $a = cq + r$ where $0 < r < c$.

Then

$$a = (ax_0 + by_0)q + r \implies r = a - (ax_0 + by_0)q \implies r = a(1 - x_0q) - b(y_0q)$$

So r is an element in S, and $r < c$. This contradicts the minimality of c in S. Hence $c \mid a$. Then $a = (ax_0 + by_0)q + r$.

Similarly, $c \mid b$.

(ii) $c = \gcd(a,b)$

Suppose otherwise, that c is not the greatest common divisor of a and b.

Let there exists some $d > c$ which satisfies $d \mid a$ and $d \mid b$.

Then $d \mid (ax + by)$ for any x and y. So d divides all elements in S. In particular, $d \mid c$, which means $d \leq c$, a contradiction.

Hence $c = \gcd(a,b)$.

This conclude the proof that $\gcd(a,b) = ax_0 + by_0$ for some integers x_0 and y_0. □

Problem 20 (Wilson's Theorem)**.** Let p be a prime number. Prove that $(p-1)!+1$ is divisible by p.

Proof. We first prove the uniqueness of inverse modulo p: for each $x \in Q = \{1,2,\dots,p-1\}$ for some prime p, there is precisely one integer y such that $xy \equiv 1 \pmod{p}$.

Proof. Suppose otherwise, that there are two distinct inverses for x modulo p; that is, $xy_1 \equiv 1 \pmod{p}$ and $xy_2 \equiv 1 \pmod{p}$. Then $x(y_1 - y_2) \equiv 0 \pmod{p}$. Since $x \nmid p$, by Euclid's lemma, $y_1 \equiv y_2 \pmod{p}$ so $y_1 = y_2 + kp$ for some integer k. But we know that $0 \le y_1, y_2 < p$, so $kp = y_1 - y_2$, $0 \le kp < p$ thus $k = 0$. Hence $y_1 = y_2$. □

If $y \neq x$, we can pair up elements of Q such that their product is congruent to 1 modulo p.

If $y = x$, then $x^2 \equiv 1 \pmod{p}$. Thus

$$p \mid x^2 = 1 \implies p \mid (x+1)(x-1) \implies p \mid x+1 \text{ or } p \mid x-1 \implies x \equiv \pm 1 \pmod{p}$$

which is $1^2 \equiv 1 \pmod{p}$ and $(p-1)^2 \equiv 1 \pmod{p}$. So aside 1 and $p-1$, all other elements can be paired up. Hence,

$$\begin{aligned}(p-1)!+1 &\equiv 1(p-1)+1 \pmod{p}\\ &\equiv p-1+1 \pmod{p}\\ &\equiv p \pmod{p}\end{aligned}$$

Hence $(p-1)!+1$ is divisible by p. □

Problem 21. For $m, n \in \mathbf{N}$, prove that

$$F_{n+m+1} = F_n F_m + F_{n+1} F_{m+1}.$$

Proof. For $n \in \mathbf{N}$, take $P(n) : F_{n+m+1} = F_n F_m + F_{n+1} F_{m+1}$ for all $m \in \mathbf{N}$ in the cases $k = n$ and $k = n + 1$. So we are using induction to progress through n and dealing with m simultaneously at each stage.

To verify $P(0)$, we note that

$$F_{m+1} = F_0 F_m + F_1 F_{m+1}$$

and

$$F_{m+2} = F_1 F_m + F_2 F_{m+1}$$

for all m, as $F_0 = 0$ and $F_1 = F_2 = 1$.

For the inductive step we assume $P(n)$, i.e. that for all $m \in \mathbf{N}$, Fn+m+1 = FnFm + Fn+1Fm+1, Fn+m+2 = Fn+1Fm + Fn+2Fm+1. To prove $P(n+1)$ it remains to show that for all $m \in \mathbf{N}$,

$$F_{n+m+3} = F_{n+2} F_m + F_{n+3} F_{m+1}.$$

From our $P(n)$ assumptions and the definition of the Fibonacci numbers,

$$\begin{aligned}
\text{LHS of (5)} &= F_{n+m+3} \\
&= F_{n+m+2} + F_{n+m+1} \\
&= F_n F_m + F_{n+1} F_{m+1} + F_{n+1} F_m + F_{n+2} F_{m+1} \\
&= (F_n + F_{n+1}) Fm + (F_{n+1} + F_{n+2}) F_{m+1} \\
&= F_{n+2} F_m + F_{n+3} F_{m+1} = \text{RHS of (5)}.
\end{aligned}$$

□

2 Set Theory

§2.1 Basics

A *set* S can be loosely defined as a collection of objects. For a set S, we write $x \in S$ to mean that x is an *element* of S, and $x \notin S$ if otherwise. A set can be defined in terms of some property $P(x)$ that the elements $x \in S$ satisfy, denoted by the following *set builder notation*:

$$\{x \in S \mid P(x)\}$$

Some basic sets (of numbers) you should be familiar with:

- $\mathbf{N} = \{0, 1, 2, 3, \dots\}$ denotes the natural numbers (non-negative integers).
- $\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ denotes the integers.
- $\mathbf{Q} = \{\frac{p}{q} \mid p, q \in \mathbf{Z}, q \neq 0\}$ denotes the rational numbers.
- $\mathbf{R}$ denotes the real numbers, which can be expressed in terms of decimal expansion.
- $\mathbf{C} = \{x + yi \mid x, y \in \mathbf{R}\}$ denotes the of complex numbers.

The *empty set* is the set with no elements, denoted by $\varnothing$.

A is a *subset* of B if every element of A is in B, denoted by $A \subseteq B$.

$$A \subseteq B \iff \forall x, x \in A \implies x \in B$$

Proposition 2.1 ($\subseteq$ is transitive)**.** If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. Let $x \in A$. Since $A \subseteq B$ and $x \in A$, $x \in B$. Since $B \subseteq C$ and $x \in B$, $x \in C$. Hence $A \subseteq C$. □

A is a *proper subset* of B if $A \subseteq B$ and $A \neq B$, denoted by $A \subset B$.

Using this definition, we have the relationship

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$$

- A and B are *equal* if and only if they contain the same elements, denoted by $A = B$.
  To prove that A and B are equal, we simply need to prove that $A \subseteq B$ and $A \subseteq B$.

  Proof. We have

$$\begin{aligned} A = B &\iff (\forall x)[x \in A \iff x \in B] \\ &\iff (\forall x)[(x \in A \implies x \in B) \land (x \in B \implies x \in A)] \\ &\iff \{(\forall x)[x \in A \implies x \in B]\} \land (\forall x)[x \in B \implies x \in A)] \\ &\iff (A \subseteq B) \land (B \subseteq A) \end{aligned}$$

□

- Some frequently occurring subsets of the real numbers are known as *intervals*, which can be visualised as sections of the real line:
  - Open interval
  $$(a,b) = \{x \in \mathbf{R} \mid a < x < b\}$$
  - Closed interval
  $$[a,b] = \{x \in \mathbf{R} \mid a \leq x < b\}$$
  - Half open interval
  $$(a,b] = \{x \in \mathbf{R} \mid a < x \leq b\}$$
- The *power set* $\mathcal{P}(A)$ of A is the set of all subsets of A (including the set itself and the empty set).
- An *ordered pair* is denoted by (a,b), where the order of the elements matters. Two pairs (a_1,b_1) and (a_2,b_2) are equal if and only if $a_1 = a_2$ and $b_1 = b_2$.

  Similarly, we have ordered triples (a,b,c), quadruples (a,b,c,d) and so on. If there are n elements it is called an n-tuple.
-

The *Cartesian product* of sets A and B, denoted by $A \times B$, is the set of all ordered pairs with the first element of the pair coming from A and the second from B:

$$A \times B = \{(a,b) \mid a \in A, b \in B\} \tag{2.1}$$

More generally, we define $A_1 \times A_2 \times \cdots \times A_n$ to be the set of all ordered n-tuples $(a_1, a_2, \dots, a_n)$, where $a_i \in A_i$ for $1 \leq i \leq n$. If all the A_i are the same, we write the product as A^n.

> **Example 2.2.** $\mathbf{R}^2$ is the Euclidean plane, $\mathbf{R}^3$ is the Euclidean space, and $\mathbf{R}^n$ is the n-dimensional Euclidean space.
>
> $$\begin{aligned} \mathbf{R} \times \mathbf{R} = \mathbf{R}^2 &= \{(x,y) \mid x,y \in \mathbf{R}\} \\ \mathbf{R} \times \mathbf{R} \times \mathbf{R} = \mathbf{R}^3 &= \{(x,y,z) \mid x,y,z \in \mathbf{R}\} \\ \mathbf{R}^n &= \{(x_1,x_2,\dots,x_n) \mid x_1,x_2,\dots,x_n \in \mathbf{R}\} \end{aligned}$$

We now disuss the algebra of sets. Given $A \subset S$ and $B \subset S$.

The *union* $A \cup B$ is the set consisting of elements that are in A or B (or both):

$$A \cup B = \{x \in S \mid x \in A \vee x \in B\}$$

The *intersection* $A \cap B$ is the set consisting of elements that are in both A and B:

$$A \cap B = \{x \in S \mid x \in A \wedge x \in B\}$$

A and B are *disjoint* if both sets have no element in common:

$$A \cap B = \varnothing$$

More generally, we can take unions and intersections of arbitrary numbers of sets, even infinitely many. If we have a family of subsets $\{A_i \mid i \in I\}$, where I is an *indexing set*, we write

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I\,(x \in A_i)\}$$

and

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I\,(x \in A_i)\}$$

The *complement* of A, denoted by A^c, is the set containing elements that are not in A:

$$A^c = \{x \in S \mid x \notin A\}$$

The *set difference*, or complement of B in A, denoted by $A \smallsetminus B$, is the subset consisting of those elements that are in A and not in B:

$$A \smallsetminus B = \{x \in A \mid x \notin B\}$$

Note that $A \smallsetminus B = A \cap B^c$.

Proposition 2.3 (Double Inclusion)**.** Let $A \subset S$ and $B \subset S$. Then

$$A = B \iff A \subseteq B \text{ and } B \subseteq A \tag{2.2}$$

Proof.

($\Longrightarrow$) If $A = B$, then every element in A is an element in B, so certainly $A \subseteq B$, and similarly $B \subseteq A$.

($\Longleftarrow$) Suppose $A \subseteq B$, and $B \subseteq A$. Then for every element $x \in S$, if $x \in A$ then $A \subseteq B$ implies that $x \in B$, and if $x \notin A$ then $B \subseteq A$ means $x \notin B$. So $x \in A$ if and only if $x \in B$, and therefore $A = B$. □

Proposition 2.4 (Distributive Laws)**.** Let $A \subset S$, $B \subset S$ and $C \subset S$. Then

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \tag{2.3}$$

$$(A \cap B) \cap C = (A \cup C) \cap (B \cup C) \tag{2.4}$$

Proof. For the first one, suppose x is in the LHS, that is $x \in A \cup (B \cap C)$. This means that $x \in A$ or $x \in B \cap C$ (or both). Thus either $x \in A$ or x is in both B and C (or x is in all three sets). If $x \in A$ then $x \in A \cup B$ and $x \in A \cup C$, and therefore x is in the RHS. If x is in both B and C then similarly x is in both $A \cup B$ and $A \cup C$. Thus every element of the LHS is in the RHS, which means we have shown $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Conversely suppose that $x \in (A \cup B) \cap (A \cup C)$. Then x is in both $A \cup B$ and $A \cup C$. Thus either $x \in A$ or, if $x \notin A$, then $x \in B$ and $x \in C$. Thus $x \in A \cup (B \cap C)$. Hence $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

By double inclusion, $(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$.

The proof of the second one follows similarly and is left as an exercise. □

Proposition 2.5 (De Morgan's Laws)**.** Let $A \subset S$ and $B \subset S$. Then

$$(A \cup B)^c = A^c \cap B^c \tag{2.5}$$

$$(A \cap B)^c = A^c \cup B^c \tag{2.6}$$

Proof. For the first one, suppose $x \in (A \cup B)^c$. Then x is not in either A or B. Thus $x \in A^c$ and $x \in B^c$, and therefore $x \in A^c \cap B^c$.

Conversely, suppose $x \in A^c \cap B^c$. Then $x \notin A$ and $x \notin B$, so x is in neither A nor B, and therefore $x \in (A \cup B)^c$.

By double inclusion, the first result holds. The second result follows similarly and is left as an exercise. □

De Morgan's laws extend naturally to any number of sets, so if $\{A_i \mid i \in I\}$ is a family of subsets of S, then

$$\left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} A_i^c \quad \text{and} \quad \left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c$$

Exercise 14

Prove the following:

1. $\left(\bigcup_{i \in I} A_i\right) \cup B = \bigcup_{i \in I} (A_i \cup B)$
2. $\left(\bigcap_{i \in I} A_i\right) \cup B = \bigcap_{i \in I} (A_i \cup B)$
3. $\left(\bigcup_{i \in I} A_i\right) \cup \left(\bigcup_{j \in J} B_j\right) = \bigcup_{(i,j) \in I \times J} (A_i \cup B_j)$
4. $\left(\bigcap_{i \in I} A_i\right) \cup \left(\bigcap_{j \in J} B_j\right) = \bigcap_{(i,j) \in I \times J} (A_i \cup B_j)$

Exercise 15

Let $S \subset A \times B$. Express the set A_S of all elements of A which appear as the first entry in at least one of the elements in S.

(A_S here may be called the projection of S onto A.)

§2.2 Relations

Definition 2.6 (Relation)**.** R is a *relation* between A and B if and only if $R \subseteq A \times B$.

$a \in A$ and $b \in B$ are *related* if $(a,b) \in R$, denoted aRb.

Remark. A relation is a set of ordered pairs.

Visually speaking, a relation is uniquely determined by a simple bipartite graph over A and B. On the bipartite graph, this is usually represented by an edge between a and b.

Definition 2.7 (Binary relation)**.** A *binary relation* in A is a relation between A and itself, i.e. $R \subseteq A \times A$.

A and B are the *domain* and *range* of R respectively, denoted by $\operatorname{dom} R$ and $\operatorname{ran} R$ respectively, if and only if $A \times B$ is the smallest Cartesian product of which R is a subset.

> **Example 2.8.** Given $R = \{(1,a),(1,b),(2,b),(3,b)\}$, then $\operatorname{dom} R = \{1,2,3\}$ and $\operatorname{ran} R = \{a,b\}$.

In many cases we do not actually use R to write the relation because there is some other conventional notation:

> **Example 2.9.**
>
> - The "less than or equal to" relation $\le$ on the set of real numbers is $\{(x,y) \in \mathbf{R}^2 \mid x \le y\}$. We write $x \le y$ if (x,y) is in this set.
> - The "divides" relation $\mid$ on $\mathbf{N}$ is $\{(m,n) \in \mathbf{N}^2 : m \text{ divides } n\}$. We write $m \mid n$ if (m,n) is in this set.
> - For a set S, the "subset" relation $\subseteq$ on $\mathcal{P}(S)$ is $\{(A,B) \in \mathcal{P}(S)^2 \mid A \subseteq B\}$. We write $A \subseteq B$ if (A,B) is in this set.

We now discuss some properties of relations. Let A be a set, R a relation on A, $x,y,z \in A$. We say that

- R is *reflexive* if xRx for all $x \in A$;
- R is *symmetric* if $xRy \implies yRx$;
- R is *anti-symmetric* if xRy and $yRx \implies x = y$;
- R is *transitive* if xRy and $yRz \implies xRz$.

> **Example 2.10** (Less than or equal to)**.** The relation $\le$ on R is reflexive, anti-symmetric, and transitive, but not symmetric.

Definition 2.11. Any relation on A that is reflexive, anti-symmetric, and transitive is called a *partial order*, denoted by $\le$. It is called a *total order* if for every $x,y \in A$, either xRy or yRx (or both).

> **Example 2.12** (Less than)**.** The relation $<$ on R is not reflexive, symmetric, or anti-symmetric, but it is transitive.

> **Example 2.13** (Not equal to)**.** The relation $\neq$ on R is not reflexive, anti-symmetric or transitive, but it is symmetric.

> **Exercise 16**
>
> Congruence modulo n Let $n \ge 2$ be an integer, and define R on $\mathbf{Z}$ by saying aRb if and only if $a - b$ is a multiple of n. Prove that R is reflexive, symmetric and transitive.

Proof.

- Reflexivity: For any $a \in \mathbf{Z}$ we have aRa as 0 is a multiple of n.
- Symmetry: If aRb then $a - b = kn$ for some integer k. So $b - a = -kn$, and hence bRa.
- Transitivity: If aRb and bRc then $a - b = kn$ and $b - c = ln$ for integers k, l. So then $a - c = (a - b) + (b - c) = (k + l)n$, and hence aRc.

□

One important type of relation is an equivalence relation. An equivalence relation is a way of saying two objects are, in some particular sense, “the same”.

Definition 2.14 (Equivalence relation)**.** A binary relation R on A is an *equivalence relation* if it is reflexive, symmetric and transitive.

Notation. We use the symbol $\sim$ to denote the equivalence relation R in $A \times A$: whenever $(a, b) \in R$ we denote $a \sim b$.

An equivalence relation provides a way of grouping together elements that can be viewed as being the same:

Definition 2.15 (Equivalence class)**.** Given an equivalence relation $\sim$ on a set A, and given $x \in A$, the *equivalence class* of x is

$$[x] \coloneqq \{y \in A \mid y \sim x\}.$$

> **Example 2.16** (Congruence modulo n)**.** For the equivalence relation of congruence modulo n, the equivalence class of 1 is the set $1 = \{\dots, -n + 1, 1, n + 1, 2n + 1, \dots\}$; that is, all the integers that are congruent to 1 modulo n.

Properties of equivalence classes:

- Every two equivalence classes are disjoint
- The union of equivalence classes form the entire set

You can translate these properties into the point of view from the elements: Every element belongs to one and only one equivalence class.

- No element belongs to two distinct classes
- All elements belong to an equivalence class

Definition 2.17. The *set of equivalence classes* (quotient sets) are the set of all equivalence classes, denoted by $A/\sim$.

Grouping the elements of a set into equivalence classes provides a partition of the set, which we define as follows:

Definition 2.18 (Partition)**.** A *partition* of a set A is a collection of subsets $\{A_i \subseteq A \mid i \in I\}$, where I is an indexing set, with the property that

(i) $A_i \neq \varnothing$ for all $i \in I$ (all the subsets are non-empty)

(ii) $\bigcup_{i \in I} Ai = A$ (every member of A lies in one of the subsets)

(iii) $A_i \cap A_j = \varnothing$ for every $i \neq j$ (the subsets are disjoint)

The subsets are called the *parts* of the partition.

Example 2.19 (Odd and even natural numbers)**.** $\{\{n \in \mathbf{N} \mid n \text{ is divisible by } 2\}, \{n \in \mathbf{N} \mid n + 1 \text{ is divisible by } 2\}\}$ forms a partition of the natural numbers, into evens and odds.

§2.3 Functions

Definition 2.20 (Function)**.** A *function* $f : X \to Y$ is a mapping of every element of X to some element of Y.

X and Y are known as the *domain* and *codomain* of f respectively.

Remark. The definition requires that a unique element of the codomain is assigned for every element of the domain. For example, for a function $f : \mathbf{R} \to \mathbf{R}$, the assignment $f(x) = \frac{1}{x}$ is not sufficient as it fails at $x = 0$. Similarly, $f(x) = y$ where $y^2 = x$ fails because $f(x)$ is undefined for $x < 0$, and for $x > 0$ it does not return a unique value; in such cases, we say the the function is *ill-defined*. We are interested in the opposite; functions that are *well-defined*.

Definition 2.21. Given a function $f : X \to Y$, the *image* (or range) of f is

$$f(X) = \{f(x) \mid x \in X\} \subseteq Y$$

More generally, given $A \subseteq X$, the image of A under f is

$$f(A) = \{f(x) \mid x \in A\} \subseteq Y$$

Given $B \subseteq Y$, the *pre-image* of B under f is

$$f^{-1}(B) = \{x \mid f(x) \in B\} \subseteq X$$

Remark. Beware the potentially confusing notation: for $x \in X$, $f(x)$ is a single element of Y, but for $A \subseteq X$, $f(A)$ is a set (a subset of Y). Note also that $f^{-1}(B)$ should be read as "the pre-image of B" and not as "f-inverse of B"; the pre-image is defined even if no inverse function exists (in which case f^{-1} on its own has no meaning; we discuss invertibility of a function below).

Exercise 17

Prove the following statements:

(a) $f(A \cup B) = f(A) \cup f(B)$

(b) $f(A_1 \cup \cdots \cup A_n) = f(A_1) \cup \cdots \cup f(A_n)$

(c) $f(\bigcup_{\lambda \in \Lambda} A_\lambda) = \bigcup_{\lambda \in \Lambda} f(A_\lambda)$

(d) $f(A \cap B) \subset f(A) \cap f(B)$

(e) $f^{-1}(f(A)) \supset A$

(f) $f(f^{-1}(A)) \subset A$

(g) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

(h) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

(i) $f^{-1}(A_1 \cup \cdots \cup A_n) = f^{-1}(A_1) \cup \cdots \cup f^{-1}(A_n)$

(j) $f^{-1}(\bigcup_{\lambda \in \Lambda} A_\lambda) = \bigcup_{\lambda \in \Lambda} f^{-1}(A_\lambda)$

If a function is defined on some larger domain than we care about, it may be helpful to restrict the domain:

Definition 2.22 (Restriction)**.** Given a function $f : X \to Y$ and a subset $A \subseteq X$, the *restriction* of f to A is the map $f|_A : A \to Y$ defined by $f|_A(x) = f(x)$ for all $x \in A$.

The restriction is almost the same function as the original f – just the domain has changed.

Another rather trivial but nevertheless important function is the identity map:

Definition 2.23 (Identity map)**.** Given a set X, the *identity* $\mathrm{id}_X : X \to X$ is defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

Notation. If the domain is unambiguous, the subscript may be removed.

Definition 2.24 (Injectivity)**.** $f : X \to Y$ is *injective* if each element of Y has at most one element of X that maps to it.

$$\forall x_1, x_2 \in X,\ f(x_1) = f(x_2) \implies x_1 = x_2$$

Definition 2.25 (Surjectivity)**.** $f : X \to Y$ is *surjective* if every element of Y is mapped to at least one element of X.

$$\forall y \in Y,\ \exists x \in X \text{ s.t. } f(x) = y$$

Definition 2.26 (Bijectivity)**.** $f : X \to Y$ is *bijective* if it is both injective and surjective: each element of Y is mapped to a unique element of X.

Notation. Given two sets X and Y , we will write $X \sim Y$ to denote the existence of a bijection from X to Y . One easily checks that $\sim$ is transitive, i.e. if $X \sim Y$ and $Y \sim Z$, then $X \sim Z$.

Theorem 2.27 (Cantor–Schroder–Bernstein)**.** If $f : A \to B$ and $g : B \to A$ are both injections, then $A \sim B$.

Proof. □

§2.3.1 Composition and invertibility

Definition 2.28 (Composition)**.** Given two functions $f : X \to Y$ and $g : Y \to Z$, the *composition* $g \circ f : X \to Z$ is defined by

$$(g \circ f)(x) = g(f(x)) \quad (\forall x \in X)$$

The composition of functions is not commutative. However, composition is associative, as the following results shows:

Proposition 2.29 (Associativity)**.** Let $f : X \to Y$, $g : Y \to Z$, $h : Z \to W$ be three functions. Then

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Proof. Let $x \in X$. Then, by the definition of composition, we have

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x).$$

□

Proposition 2.30 (Composition preserves injectivity)**.** If $f : X \to Y$ is injective and $g : Y \to Z$ is injective, then $g \circ f : X \to Z$ is injective.

Proof. Let $f : X \to Y$ and $g : Y \to Z$ be arbitrary injective functions. We want prove that the function $g \circ f : X \to Z$ is also injective.

To do so, we will prove $\forall x, x' \in X$ that

$$(g \circ f)(x) = (g \circ f)(x') \implies x = x'$$

Suppose that $(g \circ f)(x) = (g \circ f)(x')$. Expanding out the definition of $g \circ f$, this means that $g(f(x)) = g(f(x'))$.

Since g is injective and $g(f(x)) = g(f(x'))$, we know $f(x) = f(x')$.

Similarly, since f is injective and $f(x) = f(x')$, we know that $x = x'$, as required. □

Proposition 2.31. f is injective if and only if for any set Z and any functions $g_1, g_2 : Z \to X$ we have $f \circ g_1 = f \circ g_2 \implies g_1 = g_2$.

Proof. ($\implies$) If f is injective, we ultimately wish to show that $g_1 = g_2$, so in order to do this we consider all possible inputs $z \in Z$, hoping to show that $g_1(z) = g_2(z)$.

But this is quite simple because we are given that $f \circ g_1 = f \circ g_2$ and that f is injective, so

$$f \circ g_1(z) = f \circ g_2(z) \implies g_1(z) = g_2(z)$$

($\impliedby$) We specifically pick $Z = \{1\}$, basically some random one-element set.

Then $\forall x, y \in X$, we define

$$g_1 : Z \to X, g_1(1) = x$$
$$g_2 : Z \to Y, g_2(1) = y$$

Then

$$f(x) = f(y) \implies f(g_1(1)) = f(g_2(1)) \implies g_1(1) = g_2(1) \implies x = y$$

□

Proposition 2.32 (Composition preserves surjectivity)**.** If $f : X \to Y$ is surjective and $g : Y \to Z$ is surjective, then $g \circ f : X \to Z$ is surjective.

Proof. Let $f : X \to Y$ and $g : Y \to Z$ be arbitrary surjective functions. We want to prove that the function $g \circ f : X \to Z$ is subjective.

To do so, we want to prove that for any $z \in Z$, there is some $x \in X$ such that $(g \circ f)(x) = z$. Equivalently, we want to prove that for any $z \in Z$, there is some $x \in X$ such that $g(f(x)) = z$.

Consider any $z \in Z$. Since $g : Y \to Z$ is surjective, there is some $y \in Y$ such that $g(y) = z$. Similarly, since $f : X \to Y$ is surjective, there is some $x \in X$ such that $f(x) = y$. This means that there is some $x \in X$ such that $g(f(x)) = g(y) = z$, as required. □

Proposition 2.33. f is surjective if and only if for any set Z and any functions $g_1, g_2 : Y \to Z$ we have $g_1 \circ f = g_2 \circ f \implies g_1 = g_2$.

Proof.

($\implies$) Suppose that f is surjective. Again, we wish to show that $g_1 = g_2$, so we need to consider every possible input y in Y. Then, since f is injective, we can always pick $x \in X$ such that $f(x) = y$.

Then

$$g_1 \circ f = g_2 \circ f \implies g_1 \circ f(x) = g_2 \circ f(x) \implies g_1(y) = g_2(y)$$

On the other hand, if f is not surjective, then there exists $y \in Y$ such that for all $x \in X$ we have $f(x) \neq y$. We then aim to construct set Z and $g_1, g_2 : Y \to Z$ such that

(i) $g_1(y) \neq g_2(y)$

(ii) $\forall y' \neq y, g_1(y') = g_2(y')$

Because if this is satisfied, then $\forall x \in X$, since $f(x) \neq y$ we have from (ii) that $g_1(f(x)) = g_2(f(x))$; thus $g_1 \circ f = g_2 \circ f$, and yet from (i) we have $g_1 \neq g_2$.

($\impliedby$) We construct $Z = Y \cup \{1, 2\}$ for some random $1, 2 \notin Y$.

Then we define

$$g_1 : Y \to Z, g_1(y) = 1, g_1(y') = y' \qquad\qquad g_2 : Y \to Z, g_2(y) = 2, g_2(y') = y'$$

Then when y is not in the image of f, these two functions will satisfy $g_1 \circ f = g_2 \circ f$ but not $g_1 = g_2$.

So conversely, if for any set Z and any functions $g_i : Y \to Z$ we have $g_1 \circ f = g_2 \circ f \implies g_1 = g_2$, such a value y that is in the codomain but not in the range of f cannot appear, and hence f must be surjective. □

The following proposition addresses the extent to which composition of functions preserves injectivity and surjectivity:

Proposition 2.34. Let $f : X \to Y$ and $g : Y \to Z$ be functions.

(i) If f and g are injective then so is $g \circ f$. Conversely, if $g \circ f$ is injective, then f is injective, but g need not be.

(ii) If f and g are surjective then so is $g \circ f$. Conversely, if $g \circ f$ is surjective, then g is surjective, but f need not be.

Proof. For the first part of (i), suppose $(g \circ f)(x_1) = (g \circ f)(x_2)$ for some $x_1, x_2 \in X$. From the injectivity of g we know that $g(f(x_1)) = g(f(x_2))$ implies $f(x_1) = f(x_2)$, and then from the injectivity of f we know that this implies $x_1 = x_2$. So $g \circ f$ is injective.

For the second part of (i), suppose $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X$. Then applying g gives $g(f(x_1)) = g(f(x_2))$, and by the injectivity of $g \circ f$ this means $x_1 = x_2$. So f is injective. To see that g need not be injective, a counterexample is $X = Z = \{0\}, Y = \mathbf{R}$, with $f(0) = 0$ and $g(y) = 0$ for all $y \in \mathbf{R}$. □

Recalling that id_X is the identity map on X, we can define invertibility:

Definition 2.35 (Invertibility)**.** A function $f : X \to Y$ is *invertible* if there exists $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. g is known as the *inverse* of f, denoted by $g = f^{-1}$.

Remark. Note that directly from the definition, if f is invertible then f^{-1} is also invertible, and $(f^{-1})^{-1} = f$.

Proposition 2.36 (Uniqueness of inverse)**.** If $f : X \to Y$ is invertible then its inverse is unique.

Proof. Let g_1 and g_2 be two functions for which $g_i \circ f = \mathrm{id}_X$ and $f \circ g_i = \mathrm{id}_Y$. Using the fact that composition is associative, and the definition of the identity maps, we can write

$$g_1 = g_1 \circ \mathrm{id}_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_X \circ g_2 = g_2$$

□

The following result shows how to invert the composition of invertible functions:

Proposition 2.37. Let $f : X \to Y$ and $g : Y \to Z$ be functions. If f and g are invertible, then $g \circ f$ is invertible, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. Making repeated use of the fact that function composition is associative, and the definition of the inverses f^{-1} and g^{-1}, we note that

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= ((f^{-1} \circ g^{-1}) \circ g) \circ f \\ &= (f^{-1} \circ (g^{-1} \circ g)) \circ f \\ &= (f^{-1} \circ \mathrm{id}_Y) \circ f \\ &= f^{-1} \circ f \\ &= \mathrm{id}_X\end{aligned}$$

and similarly,

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ (f \circ (f^{-1} \circ g^{-1})) \\ &= g \circ ((f \circ f^{-1}) \circ g^{-1}) \\ &= g \circ (\mathrm{id}_Y \circ g^{-1}) \\ &= g \circ g^{-1} \\ &= \mathrm{id}_Z\end{aligned}$$

which shows that $f^{-1} \circ g^{-1}$ satisfies the properties required to be the inverse of $g \circ f$. □

The following result provides an important and useful criterion for invertibility:

Theorem 2.38. A function $f : X \to Y$ is invertible if and only if it is bijective.

Proof.

($\Longrightarrow$) Suppose f is invertible, so it has an inverse $f^{-1} : Y \to X$. To show f is injective, suppose that for some $x_1, x_2 \in X$ we have $f(x_1) = f(x_2)$. Then applying f^{-1} to both sides and noting that by definition $f^{-1} \circ f = \mathrm{id}_X$, we see that $x_1 = f^{-1}(f(x_1)) = f^{-1}(f(x_2)) = x_2$. So f is injective. To show that f is surjective, let $y \in Y$, and note that $f^{-1}(y) \in X$ has the property that $f(f^{-1}(y)) = y$. So f is surjective. Therefore f is bijective.

($\Longleftarrow$) Suppose f is bijective, we aim to show that there is a well-defined $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. Since f is surjective, we know that for any $y \in Y$, there is an $x \in X$ such that $f(x) = y$. Furthermore, since f is injective, we know that this x is unique. So for each $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$. This recipe provides a well-defined function $g(y) = x$, for which we have $g(f(x)) = x$ for any $x \in X$ and $f(g(y)) = y$ for any $y \in Y$. So g satisfies the property required to be an inverse of f and therefore f is invertible. □

It is also possible to define left-inverse and right-inverse functions as functions that partially satisfy the definition of the inverse:

Definition 2.39. A function $f : X \to Y$ is *left invertible* if there exists a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$, and is *right invertible* if there exists a function $h : Y \to X$ such that $f \circ h = \mathrm{id}_Y$.

As may be somewht apparent from the previous proof, being left- and right-invertible is equivalent to being injective and surjective, respectively. We leave this as an exercise to show.

§2.3.2 Monotonicity

Definition 2.40. $f:[a,b]\to\mathbf{R}$ is called

(1) *increasing*, if any $a<x_1\le x_2<b$, there is $f(x_1)\le f(x_2)$;

(2) *decreasing*, if any $a<x_1\le x_2<b$, there is $f(x_1)\ge f(x_2)$;

f is *monotonic* if it is increasing or decreasing.

Suppose $f(x)$ is continuous in $[a,b]$. To locate the roots of $f(x)=0$:

- If $f(a)$ and $f(b)$ have *opposite* signs, i.e. $f(a)f(b)<0$, then there is an odd number of real roots (counting repeated) in $[a,b]$.

  Furthermore, if f is either strictly increasing or decreasing in $[a,b]$, then $f(x)=0$ has *exactly one real root* in $[a,b]$.
- If $f(a)$ and $f(b)$ have *same* signs, i.e. $f(a)f(b)>0$, then there is an even number of roots (counting repeated) in $[a,b]$.

§2.3.3 Convexity and concavity

Definition 2.41. A function f is *convex* if for all $x_1,x_2\in D_f$ and $0\le t\le 1$, we have

$$f(tx_1+(1-t)x_2)\le tf(x_1)+(1-t)f(x_2).$$

Note that equality holds when $x_1=x_2$.

Definition 2.42. A function f is *strictly convex* if for all $x_1,x_2\in D_f$ with $x_1\ne x_2$ and $0<t<1$, we have

$$f(tx_1+(1-t)x_2)<tf(x_1)+(1-t)f(x_2).$$

Definition 2.43. A function f is *concave* if for all $x_1,x_2\in D_f$ and $0\le t\le 1$, we have

$$f(tx_1+(1-t)x_2)\ge tf(x_1)+(1-t)f(x_2).$$

Note that equality holds when $x_1=x_2$.

Definition 2.44. A function f is *strictly concave* if for all $x_1,x_2\in D_f$ with $x_1\ne x_2$ and $0<t<1$, we have

$$f(tx_1+(1-t)x_2)>tf(x_1)+(1-t)f(x_2).$$

§2.3.4 Other functions

Piecewise Functions

A function that has its domain divided into *separate partitions* and each partition of the domain given a different formula or rule is known as a *piecewise funtion*, i.e. a function defined "piece-wise".

Definition 2.45 (Absolute value function)**.**

$$f(x)=|x|=\begin{cases}-x & x<0,\\ x & x\ge 0.\end{cases}$$

Definition 2.46 (Floor function)**.** The *floor function* $f(x)=\lfloor x\rfloor$ is defined as the greatest integer smaller than or equal to x.

For $x\in\mathbf{R}$ and $n\in\mathbf{Z}$,

$$\lfloor x\rfloor=n\iff n\le x<n+1.$$

Definition 2.47 (Ceiling function)**.** The ceiling function $f(x) = \lceil x \rceil$ is the direct opposite of the floor function; it maps all real numbers in the domain to the smallest integer not smaller than it.

$$\lceil x \rceil = \begin{cases} \lfloor x \rfloor + 1 & x \notin \mathbf{Z} \\ \lfloor x \rfloor & x \in \mathbf{Z} \end{cases}$$

Exercise 18

Prove that

(a) $\lfloor \sqrt{x} \rfloor = \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor$

(b) $\lceil \sqrt{x} \rceil = \left\lceil \sqrt{\lceil x \rceil} \right\rceil$

Solution.

(a)

$$\begin{aligned} & \lfloor \sqrt{x} \rfloor = n \\ \iff & n \le \sqrt{x} < n+1 \quad \text{[by definition of floor function]} \\ \iff & n^2 \le x < (n+1)^2 \quad \text{[square both sides]} \\ \iff & n^2 \le \lfloor x \rfloor \le x < (n+1)^2 \\ \iff & n \le \sqrt{\lfloor x \rfloor} < n+1 \quad \text{[take square root throughout]} \\ \iff & \left\lfloor \sqrt{\lfloor x \rfloor} \right\rfloor = n \quad \text{[by definition of floor function]} \end{aligned}$$

(b)

$$\begin{aligned} & \lceil \sqrt{x} \rceil = n+1 \\ \iff & n < \sqrt{x} \le n+1 \quad \text{[by definition of ceiling function]} \\ \iff & n^2 < x \le (n+1)^2 \quad \text{[square both sides]} \\ \iff & n^2 < x \le \lceil x \rceil \le (n+1)^2 \\ \iff & n < \sqrt{\lceil x \rceil} \le n+1 \quad \text{[take square root throughout]} \\ \iff & \left\lceil \sqrt{\lceil x \rceil} \right\rceil = n+1 \quad \text{[by definition of ceiling function]} \end{aligned}$$

□

Symmetrical Functions

There are special functions with some form of geometric symmetry.

- Even Functions

  f is *even* if $f(-x) = f(x)$ for every $x \in D_f$.

  The graph of an even function is symmetric about the y-axis.

- Odd Functions

  f is *odd* if $f(-x) = -f(x)$ for every $x \in D_f$.

  The graph of an odd function is symmetric about the origin.

- Periodic Functions

  f is *periodic* if $f(x+p) = f(x)$ for every $x \in D_f$, where p is a positive constant. The smallest such p is known as the period.

Exercise 19

For a triangle ABC with corresponding angles a, b and c, show that

$$\sin a + \sin b + \sin c \leq \frac{3\sqrt{3}}{2}$$

and determine when equality holds. (Hint: $y = \sin x$ is concave)

Solution. Since $f(x) = \sin x$ is strictly concave on $[0, \pi]$,

$$\begin{aligned}
&\frac{1}{3}f(a) + \frac{1}{3}f(b) + \frac{1}{3}f(c) \\
&= \frac{1}{3}f(a) + \frac{2}{3}\left(\frac{1}{2}f(b) + \frac{1}{2}f(c)\right) \\
&\leq \frac{1}{3}f(a) + \frac{2}{3}\left(f\left(\frac{b}{2} + \frac{c}{2}\right)\right) \quad \text{[Concavity Inequality]} \\
&\leq f\left(\frac{a}{3} + \frac{2}{3}\left(\frac{b+c}{2}\right)\right) \quad \text{[Concavity Inequality]} \\
&= f\left(\frac{a+b+c}{3}\right)
\end{aligned}$$

Hence

$$\sin a + \sin b + \sin c = f(a) + f(b) + f(c) \leq 3f\left(\frac{a+b+c}{3}\right) = 3\sin\frac{\pi}{3} = \frac{3\sqrt{3}}{2}.$$

Equality holds when $a = b = c$, i.e. when ABC is an equilateral triangle. □

§2.4 Boundedness

Let S be a set.

Definition 2.48 (Order)**.** An *order* on S is a relation, denoted by $<$, with the following properties:

(i) (**trichotomy**) $\forall x, y \in S$, one and only one of the statements

$$x < y, \quad x = y, \quad y < x$$

is true.

(ii) (**transitivity**) $\forall x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.

Notation. $x \le y$ indicates that $x < y$ or $x = y$, without specifying which of these two is to hold. In other words, $x \le y$ is the negation of $x > y$.

Definition 2.49 (Ordered set)**.** An *ordered set* is a set S in which an order is defined.

> **Example 2.50.** $\mathbf{Q}$ is an ordered set if $r < s$ is defined to mean that $s - r$ is a positive rational number.

Definition 2.51. Suppose S is an ordered set, and $E \subset S$.

(1) $M \in S$ is an *upper bound* of E if $x \le M$ for all $x \in E$.
E is *bounded above* if there exists an upper bound $M \in S$.

(2) $m \in S$ is a *lower bound* of E if $x \ge m$ for all $x \in E$.
E is *bounded below* if there exists a lower bound $m \in S$.

(3) E is *bounded* in S if it is bounded above and below.

Definition 2.52 (Supremum)**.** Suppose S is an ordered set, $E \subset S$, and E is bounded above. Suppose there exists $\alpha \in S$ with the following properties:

(i) α is an upper bound for E;

(ii) if $\beta < \alpha$ then β is not an upper bound of E, i.e. $\exists x \in S$ s.t. $x > \beta$ (least upper bound).

Then we call α the *supremum* of E, and we write $\alpha = \sup E$.

Definition 2.53 (Infimum)**.** Suppose there exists $\alpha \in S$ with the following properties:

(i) α is a lower bound for E;

(ii) if $\beta > \alpha$ then β is not a lower bound of E, i.e. $\exists x \in S$ s.t. $x < \beta$ (greatest lower bound).

Then we call α the *infimum* of E, and we write $\alpha = \inf E$.

Proposition 2.54 (Uniqueness of suprenum)**.** If E has a supremum, then it is unique.

Proof. Assume that M and N are suprema of E.

Since N is a supremum, it is an upper bound for E. Since M is a supremum, then it is the least upper bound and thus $M \le N$.

Similarly, since M is a supremum, it is an upper bound for E; since N is a supremum, it is a least upper bound and thus $N \le M$.

Since $N \le M$ and $M \le N$, thus $M = N$. Therefore, a supremum for a set is unique if it exists. □

Definition 2.55. An ordered set S is said to have the *least-upper-bound property* (l.u.b.) if the following is true: if non-empty $E \subset S$ is bounded above, then $\sup E$ exists in S.

We shall now show that there is a close relation between greatest lower bounds and least upper bounds, and that every ordered set with the least-upper-bound property also has the greatest-lower-bound property.

Theorem 2.56. Suppose S is an ordered set with the least-upper-bound property, $B \subset S$, B is not empty, and B is bounded below. Let L be the set of all lower bounds of B. Then

$$\alpha = \sup L$$

exists in S, and $\alpha = \inf B$.

In particular, $\inf B$ exists in S.

Proof. Since B is bounded below, L is not empty. Since L consists of exactly those $y \in S$ which satisfy the inequality $y \leq x$ for every $x \in B$, we see that every $x \in B$ is an upper bound of L. Thus L is bounded above. Our hypothesis about S thus implies that L has a supremum in S; call it α.

If $\gamma < \alpha$ then γ is not an upper bound of L, hence $\gamma \notin B$. It follows that $\alpha \leq x$ for every $x \in B$. Thus $\alpha \in L$.

If $\alpha < \beta$ then $\beta \notin L$, since α is an upper bound of L.

We have shown that $\alpha \in L$ but $\beta \notin L$ if $\beta > \alpha$. In other words, α is a lower bound of B, but β is not if $\beta > \alpha$. This means that $\alpha = \inf B$. □

Theorem 2.57 (Comparison Theorem)**.** Let $S, T \subset \mathbf{R}$ be non-empty sets such that $s \leq t$ for every $s \in S$ and $t \in T$. If T has a supremum, then so does S, and $\sup S \leq \sup T$.

Proof. Let $\tau = \sup T$. Since τ is a supremum for T, then $t \leq \tau$ for all $t \in T$. Let $s \in S$ and choose any $t \in T$. Then, since $s \leq t$ and $t \leq \tau$, then $s \leq t$. Thus, τ is an upper bound for S.

By the Completeness Axiom, S has a supremum, say $\sigma = \sup S$. We will show that $\sigma \leq \tau$. Notice that, by the above, τ is an upper bound for S. Since σ is the least upper bound for S, then $\sigma \leq \tau$. Therefore,

$$\sup S \leq \sup T.$$

□

Let's explore some useful properties of sup and inf.

Proposition 2.58. Let S, T be non-empty subsets of $\mathbf{R}$, with $S \subseteq T$ and with T bounded above. Then S is bounded above, and $\sup S \leq \sup T$.

Proof. Since T is bounded above, it has an upper bound, say b. Then $t \leq b$ for all $t \in T$, so certainly $t \leq b$ for all $t \in S$, so b is an upper bound for S.

Now S, T are non-empty and bounded above, so by completeness each has a supremum. Note that $\sup T$ is an upper bound for T and hence also for S, so $\sup T \geq \sup S$ (since $\sup S$ is the least upper bound for S). □

Proposition 2.59. Let $T \subseteq \mathbf{R}$ be non-empty and bounded below. Let $S = \{-t \mid t \in T\}$. Then S is non-empty and bounded above. Furthermore, $\inf T$ exists, and $\inf T = -\sup S$.

Proof. Since T is non-empty, so is S. Let b be a lower bound for T, so $t \geq b$ for all $t \in T$. Then $-t \leq -b$ for all $t \in T$, so $s \leq -b$ for all $s \in S$, so $-b$ is an upper bound for S.

Now S is non-empty and bounded above, so by completeness it has a supremum. Then $s \leq \sup S$ for all $s \in S$, so $t \geq -\sup S$ for all $t \in T$, so $-\sup S$ is a lower bound for T.

Also, we saw before that if b is a lower bound for T then $-b$ is an upper bound for S. Then $-b \geq \sup S$ (since $\sup S$ is the least upper bound), so $b \leq -\sup S$. So $-\sup S$ is the greatest lower bound.

So $\inf T$ exists and $\inf T = -\sup S$. □

Proposition 2.60 (Approximation Property)**.** Let $S \subseteq \mathbf{R}$ be non-empty and bounded above. For any $\varepsilon > 0$, there is $s_\varepsilon \in S$ such that $\sup S - \varepsilon < s_\varepsilon \leq \sup S$.

Proof. Take $\varepsilon > 0$.

Note that by definition of the supremum we have $s \leq \sup S$ for all $s \in S$. Suppose, for a contradiction, that $\sup S - \varepsilon \geq s$ for all $s \in S$.

Then $\sup S - \varepsilon$ is an upper bound for S, but $\sup S - \varepsilon < \sup S$, which is a contradiction.

Hence there is $s_\varepsilon \in S$ with $\sup S - \varepsilon < s_\varepsilon$. □

Problem 22. Consider the set $\{\frac{1}{n} \mid n \in \mathbf{Z}^+\}$.

(a) Show that $\max S = 1$.

(b) Show that if d is a lower bound for S, then $d \leq 0$.

(c) Use (b) to show that $0 = \inf S$.

Proof. □

If we are dealing with rational numbers, the sup/inf of a set may not exist. For example, a set of numbers in $\mathbf{Q}$, defined by $\{[\pi \cdot 10^n]/10^n\}$. 3,3.1,3.14,3.141,3.1415,3.14159,... But this set does not have an infimum in $\mathbf{Q}$.

By ZFC, we have the Completeness Axiom, which states that any non-empty set $A \subset \mathbf{R}$ that is bounded above has a supremum; in other words, if A is a non-empty set of real numbers that is bounded above, there exists a $M \in \mathbf{R}$ such that $M = \sup A$.

Problem 23. Find, with proof, the supremum and/or infimum of $\{\frac{1}{n}\}$.

Proof. For the suprenum,

$$\sup\left\{\frac{1}{n}\right\} = \max\left\{\frac{1}{n}\right\} = 1.$$

For the infinum, for all positive a we can pick $n = [\frac{1}{a}] + 1$, then $a > \frac{1}{n}$. Hence

$$\inf\left\{\frac{1}{n}\right\} = 0.$$

□

Problem 24. Find, with proof, the supremum and/or infimum of $\{\sin n\}$.

Proof. The answer is easy to guess: ±1

For the supremum, we need to show that 1 is the smallest we can pick, so for any $a = 1 - \varepsilon < 1$ we want to find an integer n close enough to $2k\pi + \dfrac{\pi}{2}$ so that $\sin n > a$.

Whenever we want to show the approximations between rational and irrational numbers we should think of the **pigeonhole principle**.

$$2k\pi + \frac{\pi}{2} = 6k + (2\pi - 6)k + \frac{\pi}{2}$$

Consider the set of fractional parts $\{(2\pi - 6)k\}$. Since this an infinite set, for any small number δ there is always two elements $\{(2\pi - 6)a\} < \{(2\pi - 6)b\}$ such that

$$|\{(2\pi - 6)b\} - \{(2\pi - 6)a\}| < \varepsilon$$

Then $\{(2\pi - 6)(b - a)\} < \delta$

We then multiply by some number m (basically adding one by one) so that

$$0 \leq \{(2\pi - 6) \cdot m(b - a)\} - \left(2 - \frac{\pi}{2}\right) < \delta$$

Picking $k = m(b - a)$ thus gives

$$\begin{aligned} 2k\pi + \frac{\pi}{2} &= 6k + (2\pi - 6)k + \frac{\pi}{2} \\ &= 6k + [(2\pi - 6)k] + 2 + (2\pi - 6)k - \left(2 - \frac{\pi}{2}\right) \end{aligned}$$

Thus $n = 6k + [(2\pi - 6)k] + 2$ satisfies $\left|2k\pi + \dfrac{\pi}{2} - n\right| < \delta$

Now we're not exactly done here because we still need to talk about how well $\sin n$ approximates to 1.

We need one trigonometric fact: $\sin x < x$ for $x > 0$. (This simply states that the area of a sector in the unit circle is larger than the triangle determined by its endpoints.)

$$\begin{aligned}\sin n &= \sin\left(n - \left(2k\pi + \frac{\pi}{2}\right) + \left(2k\pi + \frac{\pi}{2}\right)\right)\\ &= \cos\left(n - \left(2k\pi + \frac{\pi}{2}\right)\right)\\ &= \cos\theta\end{aligned}$$

$$1 - \sin n = 2\sin^2\frac{\theta}{2} = 2\sin^2\left|\frac{\theta}{2}\right| \leq \frac{\theta^2}{2} < \delta$$

Hence we simply pick $\delta = \varepsilon$ to ensure that $1 - \sin n < \varepsilon$, and we're done. □

§2.5 Cardinality

Definition 2.61. If there exists a bijective mapping of A onto B, we say that A and B can be put in *1-1 correspondence*, or that A and B have the same **cardinal number**, or, briefly, that A and B are *equivalent*, denoted by $A \sim B$ (an equivalence relation).

Notation. For any positive integer n, let J_n be the set whose elements are the integers $1, 2, \dots, n$. Let J be the set consisting of all positive integers.

Definition 2.62. For any set A, we say

- A is **finite** if $A \sim J_n$ for some n (the empty set is also considered to be finite)
- A is **infinite** if A is not finite.
- A is **countable** if $A \sim J$.
- A is **uncountable** if A is neither finite nor countable.
- A is **at most countable** if A is finite or countable.

For two finite sets A and B, we evidently have $A \sim B$ if and only if A and B contain the same number of elements.

For infinite sets, however, the idea of "having the same number of elements" becomes quite vague, whereas the notion of bijectivity retains its clarity.

Proposition 2.63. $2J = \{2n \mid n \in J\}$ is countable.

Proof. We can find the function $f: J \to 2J$ given by

$$f(n) = 2n$$

which is bijective. Thus there is a 1-1 correspondence between J and $2J$. □

Proposition 2.64. $\mathbf{Z}$ is countable.

Proof. Consider the following arrangement of the sets $\mathbf{Z}$ and J:

$$\begin{aligned} \mathbf{Z}: &\quad 0, 1, -1, 2, -2, 3, -3, \dots \\ J: &\quad 1, 2, 3, 4, 5, 6, 7, \dots \end{aligned}$$

We can even give an explicit formula for a bijective function $f: J \to \mathbf{Z}$:

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even,} \\ -\dfrac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

□

Proposition 2.65. Every infinite subset of a countable set A is countable.

Proof. Suppose $E \subset A$, and E is infinite. Arrange the elements $x \in A$ in a sequence $\{x_n\}$ of distinct elements.

Construct a sequence $\{n_k\}$ as follows: Let n_1 be the smallest positive integer such that $x_{n_1} \in E$. Having chosen $n_1, \dots, n_{k-1}$ $(k = 2, 3, 4, \dots)$, let n_k be the smallest integer greater than n_{k-1} such that $x_{n_k} \in E$.

Putting $f(k) = x_{n_k}$ $(k = 1, 2, 3, \dots)$, we obtain a 1-1 correspondence between E and J. □

This shows that countable sets represent the "smallest" infinity: No uncountable set can be a subset of a countable set.

Proposition 2.66. Let $\{E_n \mid n \in J\}$ be a sequence of countable sets, and put

$$S = \bigcup_{n=1}^{\infty} E_n.$$

Then S is countable.

Proof. Let every set E_n be arranged in a sequence $\{x_{n_k}\}$ $(k = 1, 2, 3, \dots)$, and consider the infinite array

$$\begin{array}{ccccc} x_{11} & x_{12} & x_{13} & x_{14} & \cdots \\ x_{21} & x_{22} & x_{23} & x_{24} & \cdots \\ x_{31} & x_{32} & x_{33} & x_{34} & \cdots \\ x_{41} & x_{42} & x_{43} & x_{44} & \cdots \\ \vdots & & & & \end{array}$$

in which the elements of E_n form the n-th row. The array contains all elements of S. These elements can be arranged in a sequence

$$x_{11}, x_{21}, x_{12}, x_{31}, x_{22}, x_{13}, x_{41}, x_{32}, x_{23}, x_{14}, \dots$$

□

Proposition 2.67. Let A and B be finite sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof. The proof is left as an exercise. □

Proposition 2.68 (Subsets of a finite set)**.** If a set A is finite with $|A| = n$, then its power set has $|\mathcal{P}(A)| = 2^n$.

Proof. We use induction. For the initial step, note that if $|A| = 0$ then $A = \varnothing$ has no elements, so there is a single subset $\varnothing$, and therefore $|\mathcal{P}(A)| = 1 = 2^0$.

Now suppose that $n \geq 0$ and that $|P(S)| = 2^n$ for any set S with $|S| = n$. Let A be any set with $|A| = n + 1$. By definition, this means that there is an element a and a set $A_0 = A \setminus \{a\}$ with $|A_0| = n$. Any subset of A must either contain the element a or not, so we can partition $\mathcal{P}(A) = P(A_0) \cup \{S \cup \{a\} \mid S \in P(A_0)\}$. These two sets are disjoint, and each of them has cardinality $|P(A_0)| = 2^n$ by the inductive hypothesis. Hence $|\mathcal{P}(A)| = 2^n + 2^n = 2^{n+1}$.

Thus, by induction, the result holds for all n. □

Another way to see this is through combinatorics: Consider the process of creating a subset. We can do this systematically by going through each of the $|A|$ elements in A and making the yes/no decision whether to put it in the subset. Since there are $|A|$ such choices, that yields $2^{|A|}$ different combinations of elements and therefore $2^{|A|}$ different subsets.

Theorem 2.69 (Principle of Inclusion and Exclusion)**.** Let S_i be finite sets. Then

$$\left|\bigcup_{i=1}^{n} S_i\right| = \sum_{i=1} |S_i| - \sum_{1 \leq i < j \leq n} |S_i \cap S_j| + \sum_{1 \leq i < j < k \leq n} |S_i \cap S_j \cap S_k| + \cdots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} S_i\right|. \tag{2.7}$$

Proof. By induction. □

The following more elegant proof was presented to the author by Dr. Ho Weng Kin during a H3 Mathematics lecture in 2024.

Proof. Let U be a finite set (interpreted as the universal set), and $S \subseteq U$. Define the characteristic/indicator function of S by

$$\chi_S(x) = \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{if } x \notin S. \end{cases}$$

In other words,

$$x \in S \iff \chi_S(x) = 1$$

and equivalently,

$$x \notin S \iff \chi_S(x) = 0.$$

Let $S_1, S_2 \subseteq U$ be given. Then for any $x \in U$ it holds that

$$\chi_{S_1 \cap S_2}(x) = \chi_{S_1}(x) \cdot \chi_{S_2}(x)$$

where $\cdot$ denotes ordinary multiplication.

Similarly,

$$\chi_{S_1 \cup S_2}(x) = 1 - \left(1 - \chi_{S_1}(x)\right) \cdot \left(1 - \chi_{S_2}(x)\right).$$

In general, for any $x \in U$ it holds that

$$\chi_{S_1 \cup \cdots \cup S_n}(x) = 1 - \left(1 - \chi_{S_1}(x)\right) \cdots \left(1 - \chi_{S_n}(x)\right)$$

for any $S_1, \ldots, S_n \subset U$.

Since $x \in S$ if and only if $\chi_S(x) = 1$, it follows that

$$|S| = \sum_{x \in U} \chi_S(x).$$

To prove the PIE, we calculate

$$\begin{aligned}
&|S_1 \cup \cdots \cup S_n| \\
&= \sum_{x \in U} \chi_{S_1 \cup \cdots \cup S_n}(x) \\
&= \sum_{x \in U} 1 - \left(1 - \chi_{S_1}(x)\right) \cdots \left(1 - \chi_{S_n}(x)\right) \\
&= \left(\chi_{S_1}(x) + \cdots + \chi_{S_n}(x)\right) - \left(\chi_{S_1}(x)\chi_{S_2}(x) + \cdots + \chi_{S_{n-1}}(x)\chi_{S_n}(x)\right) + \cdots + (-1)^{n+1}\chi_{S_1}(x)\cdots\chi_{S_n}(x) \\
&= \left(\chi_{S_1}(x) + \cdots + \chi_{S_n}(x)\right) - \left(\chi_{S_1 \cap S_2}(x) + \cdots + \chi_{S_{n-1} \cap S_n}(x)\right) + \cdots + (-1)^{n+1}\chi_{S_1 \cap \cdots \cap S_n}(x) \\
&= \sum_{i=1}^{n} |S_i| - \sum_{J \subseteq \{1,\ldots,n\}, |J|=2} \left|\bigcap_{j \in J} S_j\right| + \cdots + (-1)^{k+1} \sum_{J \subseteq \{1,\ldots,n\}, |J|=k} \left|\bigcap_{j \in J} S_j\right| + \cdots + (-1)^{n+1} \left|\bigcap_{i=1}^{n} S_i\right|.
\end{aligned}$$

□

Theorem 2.70 (Cantor)**.** For a set A, $|A| < |\mathcal{P}(A)|$.

Proof. Define the function $f : A \to \mathcal{P}(A)$ by $f(x) = \{x\}$. Then, f is injective as $\{x\} = \{y\} \implies x = y$. Thus $|A| \le |\mathcal{P}(A)|$. To finish the proof now all we need to show is that $|A| \neq |\mathcal{P}(A)|$. We will do so through contradiction. Suppose that $|A| = |\mathcal{P}(A)|$. Then, there exists a surjection $g : A \to \mathcal{P}(A)$. We define the set B as

$$B := \{x \in A \mid x \notin g(x)\} \in \mathcal{P}(A)$$

Since g is surjective, there exists a $b \in A$ such that $g(b) = B$. There are two cases:

1. $b \in B$. Then $b \notin g(b) = B \implies b \notin B$.
2. $b \notin B$. Then $b \notin g(b) = B \implies b \in B$.

In either case we obtain a contradiction. Thus, g is not surjective so $|A| \neq |\mathcal{P}(A)|$. □

Corollary 2.71. For all $n \in \mathbf{N} \cup \{0\}$, $n < 2^n$.

Proof. This can be easily proven through induction. □

Exercises

Problem 25. Let A be the set of all complex polynomials in n variables. Given a subset $T \subset A$, define the *zeros* of T as the set

$$Z(T) = \{P = (a_1, \dots, a_n) \mid f(P) = 0 \text{ for all } f \in T\}$$

A subset $Y \in \mathbf{C}^n$ is called an algebraic set if there exists a subset $T \subset A$ such that $Y = Z(T)$.

Prove that the union of two algebraic sets is an algebraic set.

Proof. We would like to consider $T = \{f_1, f_2, \dots\}$ expressed as indexed sets $T = \{f_i\}$. Then $Z(T)$ can also be expressed as $\{P \mid \forall i, f_i(P) = 0\}$.

Suppose that we have two algebraic sets X and Y. Let $X = Z(S)$, $Y = Z(T)$ where S, T are subsets of A (basically, they are certain sets of polynomials). Then

$$X = \{P \mid \forall f \in S, f(P) = 0\}$$

$$Y = \{P \mid \forall g \in T, g(P) = 0\}$$

We imagine that for $P \in X \cap Y$, we have $f(P) = 0$ or $g(P) = 0$. Hence we consider the set of polynomials

$$U = \{f \cdot g \mid f \in S, g \in T\}$$

For any $P \in X \cup Y$ and for any $fg \in U$ where $f \in S$ and $f \in g$, either $f(P) = 0$ or $g(P) = 0$, hence $fg(P) = 0$ and thus $P \in Z(U)$.

On the other hand if $P \in Z(U)$, suppose otherwise that P is not in $X \cup Y$, then P is neither in X nor in Y. This means that there exists $f \in S, g \in T$ such that $f(P) \neq 0$ and $g(P) \neq 0$, hence $fg(P) \neq 0$. This is a contradiction as $P \in Z(U)$ implies $fg(P) = 0$. Hence we have $X \cup Y = Z(U)$ and thus $X \cup Y$ is an algebraic set.

Now the other direction is simpler and can actually be generalised: The intersection of arbitrarily many algebraic sets is algebraic.

The basic result is that if $X = Z(S)$ and $Y = Z(T)$ then $X \cap Y = Z(S \cup T)$. □

Problem 26 (Modular Arithmetic)**.** Define the ring of integers modulo n:

$$\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}/\sim \quad \text{where } x \sim y \iff x - y \in n\mathbf{Z}.$$

The equivalence classes are called congruence classes modulo n.

(a) Define the sum of two congruence classes modulo n, $[x], [y] \in \mathbf{Z}/n\mathbf{Z}$, by

$$[x] + [y] = [x + y]$$

Show that the above definition is well-defined.

(b) Define the product of two congruence classes modulo n and show that such a definition is well-defined.

Solution.

(a) We often define such concepts by considering the **representatives** of the equivalence classes.

For example, here we define $[x] + [y] = [x + y]$ for two elements $[x]$ and $[y]$ in $\mathbf{Z}/n\mathbf{Z}$. So what we know here are the classes $[x]$ and $[y]$. But what exactly are x and y? They are just some element in the equivalence classes that was arbitrarily picked out. We then perform the sum $x + y$, and consequently, we used this to point towards the class $[x + y]$.

However, x and y are arbitrarily picked. We want to show that, regardless of which representatives are chosen from the equivalence classes $[x]$ and $[y]$, we will always obtain the same result.

In the definition itself, we have defined that, for the two representatives x and y we define $[x]+[y] = [x + y]$. So now, let's say that we take two other arbitrary representatives, $x' \in [x]$ and $y' \in [y]$. Then by definition, we have

$$[x] + [y] = [x' + y']$$

Thus, our goal is to show that $x' + y'] = [x + y]$. This expression means that the two sides of the equation are referring to the same equivalence class. Therefore, the expression above is completely equivalent to the condition.

$$x' + y' \sim x + y$$

We then check that this final expression is indeed true: Since $x' \in [x]$ and $y' \in [y]$, we have

$$\begin{aligned} & x' \sim x \text{ and } y' \sim y \\ \implies & x' - x, y' - y \in n\mathbf{Z} \\ \implies & (x' + y') - (x + y) = (x' - x) + (y' - y) \in n\mathbf{Z} \end{aligned}$$

(b) The product of two congruence classes is defined by

$$[x][y] = [xy]$$

For any other representatives x', y' we have

$$\begin{aligned} & x'y' - xy \\ & = x'y' - xy' + xy' - xy \\ & = (x' - x)y' + x(y' - y) \in n\mathbf{Z} \end{aligned}$$

Thus $[x'y'] = [xy]$ and the product is well-defined.

□

Problem 27. Let $A = \mathbf{R}$ and for any $x, y \in A$, $x \sim y$ if and only if $x - y \in \mathbf{Z}$. For any two equivalence classes $[x], [y] \in A/\sim$, define

$$[x] + [y] = [x + y] \text{ and } -[x] = [-x]$$

(a) Show that the above definitions are well-defined.

(b) Find a one-to-one correspondence $\phi : X \to Y$ between $X = A/\sim$ and $Y : |z| = 1$, i.e. the unit circle in $\mathbf{C}$, such that for any $[x_1], [x_2] \in X$ we have

$$\phi([x_1])\phi([x_2]) = \phi([x_1 + x_2])$$

(c) Show that for any $[x] \in X$,

$$\phi(-[x]) = \phi([x])^{-1}$$

Solution.

(a)

$$(x' + y') - (x + y) = (x' - x) + (y' - y) \in \mathbf{Z}$$

Thus $[x' + y'] = [x + y]$

$$(-x') - (-x) = -(x' - x) \in \mathbf{Z}$$

Thus $[-x'] = [-x]$.

(b) Complex numbers in the polar form: $z = re^{i\theta}$

Then the correspondence is given by $\phi([x]) = e^{2\pi i x}$

$$[x] = [y] \iff x - y \in \mathbf{Z} \iff e^{2\pi i(x-y)} = 1 \iff e^{2\pi ix} = e^{2\pi iy}$$

Hence this is a bijection.

Before that, we also need to show that ϕ is well-defined, which is almost the same as the above.

If we choose another representative x' then

$$\phi([x]) = e^{2\pi ix'} = e^{2\pi ix} \cdot e^{2\pi i(x'-x)} = e^{2\pi ix}$$

(c) You can either refer to the specific correspondence $\phi([x]) = e^{2\pi ix}$ or use its properties.

$$\phi(-[x])\phi([x]) = \phi([-x])\phi([x]) = \phi([-x + x]) = \phi([0]) = 1$$

□

Problem 28 (Complex Numbers)**.** Let $\mathbf{R}[x]$ denote the set of real polynomials. Define

$$\mathbf{C} = \mathbf{R}[x]/(x^2+1)\mathbf{R}[x]$$

where

$$f(x) \sim g(x) \iff x^2+1 \text{ divides } f(x)-g(x).$$

The complex number $a+bi$ is defined to be the equivalence class of $a+bx$.

(a) Define the sum and product of two complex numbers and show that such definitions are well-defined.

(b) Define the reciprocal of a complex number.

Part II

Linear Algebra

3 Vector Spaces

§3.1 Definition of Vector Space

Notation. $\mathbf{F}$ denotes $\mathbf{R}$ or $\mathbf{C}$.

Notation. $\mathbf{F}^n$ is the set of n-tuples whose elements belong to $\mathbf{F}$:

$$\mathbf{F}^n \coloneqq \{(x_1, \dots, x_n) \mid x_i \in \mathbf{F}\}$$

For $(x_1, \dots, x_n) \in \mathbf{F}^n$ and $i = 1, \dots, n$, we say that x_i is the i-th coordinate of $(x_1, \dots, x_n)$.

Definition 3.1 (Vector space)**.** V is a *vector space* over $\mathbf{F}$ if the following properties hold:

(i) Addition is commutative: $u + v = v + u$ for all $u, v \in V$

(ii) Addition is associative: $(u + v) + w = u + (v + w)$ for all $u, v, w \in V$
Multiplication is associative: $(ab)v = a(bv)$ for all $v \in V$, $a, b \in \mathbf{F}$

(iii) Additive identity: there exists $\mathbf{0} \in V$ such that $v + \mathbf{0} = v$ for all $v \in V$

(iv) Additive inverse: for every $v \in V$, there exists $w \in V$ such that $v + w = \mathbf{0}$

(v) Multiplicative identity: $1v = v$ for all $v \in V$

(vi) Distributive properties: $a(u + v) = au + av$ and $(a + b)v = av + bv$ for all $a, b, \in \mathbf{F}$ and $u, v \in V$

Notation. For the rest of this text, V denotes a vector space over $\mathbf{F}$.

Example 3.2. $\mathbf{R}^n$ is a vector space over $\mathbf{R}$, $\mathbf{C}^n$ is a vector space over $\mathbf{C}$.

Elements of a vector space are called *vectors* or *points*.

The scalar multiplication in a vector space depends on $\mathbf{F}$. Thus when we need to be precise, we will say that V is a vector space over $\mathbf{F}$ instead of saying simply that V is a vector space. For example, $\mathbf{R}^n$ is a vector space over $\mathbf{R}$, and $\mathbf{C}^n$ is a vector space over $\mathbf{C}$. A vector space over $\mathbf{R}$ is called a *real vector space*; a vector space over $\mathbf{C}$ is called a *complex vector space*.

Proposition 3.3 (Uniqueness of additive identity)**.** A vector space has a unique additive identity.

Proof. Suppose otherwise, then $\mathbf{0}$ and $\mathbf{0}'$ are additive identities of V. Then

$$\mathbf{0}' = \mathbf{0}' + \mathbf{0} = \mathbf{0} + \mathbf{0}' = \mathbf{0}$$

where the first equality holds because $\mathbf{0}$ is an additive identity, the second equality comes from commutativity, and the third equality holds because $\mathbf{0}'$ is an additive identity. Thus $\mathbf{0}' = \mathbf{0}$. □

Proposition 3.4 (Uniqueness of additive inverse)**.** Every element in a vector space has a unique additive inverse.

Proof. Suppose otherwise, then for $v \in V$, w and w' are additive inverses of v. Then

$$w = w + \mathbf{0} = w + (v + w') = (w + v) + w' = \mathbf{0} + w' = w'.$$

Thus $w = w'$. □

Because additive inverses are unique, the following notation now makes sense.

Notation. Let $v, w \in V$. Then $-v$ denotes the additive inverse of v; $w - v$ is defined to be $w + (-v)$.

Proposition 3.5 (The number 0 times a vector)**.** For every $v \in V$, $0v = \mathbf{0}$.

Proof. For $v \in V$, we have

$$0v = (0 + 0)v = 0v + 0v.$$

Adding the additive inverse of $0v$ to both sides of the equation gives $\mathbf{0} = 0v$. □

Proposition 3.6 (A number times the vector 0)**.** For every $a \in \mathbf{F}$, $a\mathbf{0} = \mathbf{0}$.

Proof. For $a \in \mathbf{F}$, we have

$$a\mathbf{0} = a(\mathbf{0} + \mathbf{0}) = a\mathbf{0} + a\mathbf{0}.$$

Adding the additive inverse of $a\mathbf{0}$ to both sides of the equation gives $\mathbf{0} = a\mathbf{0}$. □

Now we show that if an element of V is multiplied by the scalar 1, then the result is the additive inverse of the element of V.

Proposition 3.7 (The number -1 times a vector)**.** For every $v \in V$, $(-1)v = -v$.

Proof. For $v \in V$, we have

$$v + (-1)v = 1v + (-1)v = (1 + (-1))v = 0v = \mathbf{0}.$$

Since $v + (-1)v = \mathbf{0}$, $(-1)v$ is the additive inverse of v. □

Example 3.8. $\mathbf{F}^\infty$ is defined to be the set of all sequences of elements of $\mathbf{F}$:

$$\mathbf{F}^\infty \coloneqq \{(x_1, x_2, \dots) \mid x_i \in \mathbf{F}\}$$

Addition and scalar multiplication on $\mathbf{F}^\infty$ are defined as expected:

$$\begin{aligned}(x_1, x_2, \dots) + (y_1, y_2, \dots) &= (x_1 + y_1, x_2 + y_2, \dots)\\ \lambda(x_1, x_2, \dots) &= (\lambda x_1, \lambda x_2, \dots)\end{aligned}$$

With these definitions, $\mathbf{F}^\infty$ becomes a vector space over $\mathbf{F}$, as you should verify. The additive identity in this vector space is $\mathbf{0} = (0, 0, \dots)$.

Our next example of a vector space involves a set of functions.

Notation. If S is a set, $\mathbf{F}^S \coloneqq \{f \mid f : S \to \mathbf{F}\}$.

For $f, g \in \mathbf{F}^S$, the sum $f + g \in \mathbf{F}^S$ is the function defined by

$$(f + g)(x) = f(x) + g(x) \quad (\forall x \in S)$$

For $\lambda \in \mathbf{F}$, $f \in \mathbf{F}^S$, the product $\lambda f \in \mathbf{F}^S$ is the function defined by

$$(\lambda f)(x) = \lambda f(x) \quad (\forall x \in S)$$

Example 3.9. If $S = [0, 1]$ and $\mathbf{F} = \mathbf{R}$, then $\mathbf{R}^{[0,1]}$ is the set of real-valued functions on the interval $[0, 1]$.

Example 3.10. If S is a non-empty set, then $\mathbf{F}^S$ (with the operations of addition and scalar multiplication as defined above) is a vector space over $\mathbf{F}$.

Additive identity of $\mathbf{F}^S$ is the function $0 : S \to \mathbf{F}$ defined by

$$0(x) = 0 \quad (\forall x \in S)$$

For $f \in \mathbf{F}^S$, additive inverse of f is the function $-f : S \to \mathbf{F}$ defined by

$$(-f)(x) = -f(x) \quad (\forall x \in S)$$

It is easy to see that $\mathbf{F}^n$ and $\mathbf{F}^\infty$ are special cases of the vector space $\mathbf{F}^S$ because a list of length n of numbers in $\mathbf{F}$ can be thought of as a function from $\{1, 2, \dots, n\}$ to $\mathbf{F}$ and a sequence of numbers in $\mathbf{F}$ can be thought of as a function from the set of positive integers to $\mathbf{F}$. In other words, we can think of $\mathbf{F}^n$ as $\mathbf{F}^{\{1,2,\dots,n\}}$ and we can think of $\mathbf{F}^\infty$ as $\mathbf{F}^{\{1,2,\dots\}}$.

§3.2 Subspaces

Definition 3.11 (Subspace)**.** $U \subset V$ is a *subspace* of V if U is also a vector space (with the same addition and scalar multiplication as on V).

Lemma 3.12 (Conditions for a subspace)**.** $U \subset V$ is a subspace of V if and only if U satisfies the following conditions:

(i) Additive identity: $\mathbf{0} \in U$

(ii) Closed under addition: $u + w \in U$ for all $u, w \in U$

(iii) Closed under scalar multiplication: $\lambda u \in U$ for all $\lambda \in \mathbf{F}$, $u \in U$

Proof. If U is a subspace of V, then U satisfies the three conditions above by the definition of vector space.

Conversely, suppose U satisfies the three conditions above. (i) ensures that the additive identity of V is in U. (ii) ensures that addition makes sense on U. (iii) ensures that scalar multiplication makes sense on U.

If $u \in U$, then $-u = (-1)u \in U$ by (iii). Hence every element of U has an additive inverse in U.

The other parts of the definition of a vector space, such as associativity and commutativity, are automatically satisfied for U because they hold on the larger space V. Thus U is a vector space and hence is a subspace of V. □

Remark. The three conditions in Lemma 3.12 usually enable us to determine quickly whether a given subset of V is a subspace of V.

Definition 3.13 (Sum of subsets)**.** Suppose $U_1, \dots, U_n \subset V$. The *sum* of $U_1, \dots, U_n$ is the set of all possible sums of elements of $U_1, \dots, U_n$:

$$U_1 + \dots + U_n \coloneqq \{u_1 + \dots + u_n \mid u_i \in U_i\}.$$

Example 3.14. Suppose that $U = \{(x, 0, 0) \in \mathbf{F}^3 \mid x \in F\}$ and $W = \{(0, y, 0) \in \mathbf{F}^3 \mid y \in \mathbf{F}\}$. Then

$$U + W = \{(x, y, 0) \mid x, y \in \mathbf{F}\}.$$

Example 3.15. Suppose that $U = \{(x, x, y, y) \in \mathbf{F}^4 \mid x, y \in \mathbf{F}\}$ and $W = \{(x, x, x, y) \in \mathbf{F}^4 \mid x, y \in \mathbf{F}\}$. Then

$$U + W = \{(x, x, y, z) \in \mathbf{F}^4 \mid x, y, z \in \mathbf{F}\}.$$

The next result states that the sum of subspaces is a subspace, and is in fact the smallest subspace containing all the summands.

Proposition 3.16. Suppose $U_1, \dots, U_n$ are subspaces of V. Then $U_1 + \dots + U_n$ is the smallest subspace of V containing $U_1, \dots, U_n$.

Proof. It is easy to see that $\mathbf{0} \in U_1 + \dots + U_n$ and that $U_1 + \dots + U_n$ is closed under addition and scalar multiplication. Hence $U_1 + \dots + U_n$ is a subspace of V.

Clearly $U_1, \dots, U_n$ are all contained in $U_1 + \dots + U_n$ (to see this, consider sums $u_1 + \dots + u_n$ where all except one of the u's are $\mathbf{0}$). Conversely, every subspace of V containing $U_1, \dots, U_n$ contains $U_1 + \dots + U_n$ (because subspaces must contain all finite sums of their elements). Thus $U_1 + \dots + U_n$ is the smallest subspace of V containing $U_1, \dots, U_n$. □

Remark. Sums of subspaces in the theory of vector spaces are analogous to unions of subsets in set theory. Given two subspaces of a vector space, the smallest subspace containing them is their sum. Analogously, given two subsets of a set, the smallest subset containing them is their union.

Definition 3.17 (Direct sum)**.** Suppose $U_1, \dots, U_n$ are subspaces of V. The sum $U_1 + \dots + U_n$ is called a *direct sum* if each element of $U_1 + \dots + U_n$ can be written in only one way a sum of $u_1 + \dots + u_n$, $u_i \in U_i$. In this case, we denote the sum as

$$U_1 \oplus \dots \oplus U_n.$$

Example 3.18. Suppose that $U = \{(x,y,0) \in \mathbf{F}^3 \mid x,y \in \mathbf{F}\}$ and $W = \{(0,0,z) \in \mathbf{F}^3 \mid z \in \mathbf{F}\}$. Then $\mathbf{F}^3 = U \oplus W$.

Example 3.19. Suppose U_i is the subspace of $\mathbf{F}^n$ of those vectors whose coordinates are all 0 except for the i-th coordinate; that is, $U_i = \{(0,\dots,0,x,0,\dots,0) \in \mathbf{F}^n \mid x \in \mathbf{F}\}$. Then $\mathbf{F}^n = U_1 \oplus \dots \oplus U_n$.

Lemma 3.20 (Condition for direct sum)**.** Suppose $V_1, \dots, V_n$ are subspaces of V, $W = V_1 + \dots + V_n$. Then the following are equivalent:

(i) Any element in W can be uniquely expressed as the sum of vectors in $V_1, \dots, V_n$.

(ii) If $v_i \in V_i$ satisfies $v_1 + \dots + v_n = \mathbf{0}$, then $v_1 = \dots = v_n = \mathbf{0}$.

(iii) For $k = 2, \dots, n$, $(V_1 + \dots + V_{k-1}) \cap V_k = \{\mathbf{0}\}$.

Proof.

(i) $\Longleftrightarrow$ (ii) First suppose W is a direct sum. Then by the definition of direct sum, the only way to write $\mathbf{0}$ as a sum $u_1 + \dots + u_n$ is by taking $u_i = \mathbf{0}$.

Now suppose that the only way to write $\mathbf{0}$ as a sum $v_1 + \dots + v_n$ by taking $v_1 = \dots = v_n = \mathbf{0}$. For $v \in V_1 + \dots + V_n$, suppose that there is more than one way to represent v:

$$v = v_1 + \dots + v_n$$
$$v = v_1' + \dots + v_n'$$

for some $v_i, v_i' \in V_i$. Substracting the above two equations gives

$$\mathbf{0} = (v_1 - v_1') + \dots + (v_n - v_n').$$

Since $v_i - v_i' \in V_i$, we have $v_i - v_i' = \mathbf{0}$ so $v_i = v_i'$. Hence there is only one unique way to represent $v_1 + \dots + v_n$, thus W is a direct sum.

(ii) $\Longleftrightarrow$ (iii) First suppose if $v_i \in V_i$ satisfies $v_1 + \dots + v_n = \mathbf{0}$, then $v_1 = \dots = v_n = \mathbf{0}$. Let $v_k \in (V_1 + \dots + V_{k-1}) \cap V_k$. Then $v_k = v_1 + \dots + v_{k-1}$ where $v_i \in V_i$ $(1 \le i \le k-1)$. Thus

$$v_1 + \dots + v_{k-1} - v_k = \mathbf{0}$$
$$v_1 + \dots + v_{k-1} + (-v_k) + \mathbf{0} + \dots + \mathbf{0} = \mathbf{0}$$

by taking $v_{k+1} = \dots = v_n = \mathbf{0}$. Then $v_1 = \dots = v_k = \mathbf{0}$.

Now suppose that for $k = 2, \dots, n$, $(V_1 + \dots + V_{k-1}) \cap V_k = \{\mathbf{0}\}$.

$$\begin{aligned} v_1 + \dots + v_n &= \mathbf{0} \\ v_1 + \dots + v_{n-1} &= -v_n \end{aligned}$$

where $v_1 + \dots + v_{n-1} \in V_1 + \dots + V_{n-1}$, $-v_n \in V_n$. Thus

$$v_1 + \dots + v_{n-1} = -v_n \in (V_1 + \dots + V_{n-1}) \cap V_n = \{\mathbf{0}\}$$

so $v_1 + \dots + v_{n-1} = \mathbf{0}$, $v_n = \mathbf{0}$. Induction on n gives $v_1 = \dots = v_{n-1} = v_n = \mathbf{0}$. □

Proposition 3.21. Suppose U and W are subspaces of V. Then $U + W$ is a direct sum if and only if $U \cap W = \{\mathbf{0}\}$.

Proof. First suppose that $U + W$ is a direct sum. If $v \in U \cap W$, then $\mathbf{0} = v + (-v)$, where $v \in U$, $-v \in W$. By the unique representation of $\mathbf{0}$ as the sum of a vector in U and a vector in W, we have $v = \mathbf{0}$. Thus $U \cap W = \{\mathbf{0}\}$.

Now suppose $U \cap W = \{\mathbf{0}\}$. To prove that $U + W$ is a direct sum, suppose $u \in U$, $w \in W$, and

$$0 = u + w.$$

$u = -w \in W$, thus $u \in U \cap W$, so $u = w = \mathbf{0}$. By Lemma 3.20, $U + W$ is a direct sum. □

Exercises

Problem 29. Suppose W is a vector space over $\mathbf{F}$, V_1 and V_2 are subspaces of W. Show that $V_1 \cap V_2$ is a vector space over $\mathbf{F}$ if and only if $V_1 \subset V_2$ or $V_2 \subset V_1$.

Solution. The backward direction is trivial. We focus on proving the forward direction.

Supppse otherwise, then $V_1 \setminus V_2 \neq \varnothing$ and $V_2 \setminus V_1 \neq \varnothing$. Pick $v_1 \in V_1 \setminus V_2$ and $v_2 \in V_2 \setminus V_1$. Then

$$\begin{aligned} v_1, v_2 \in V_1 \cup V_2 &\implies v_1 + v_2 \in V_1 \cup V_2 \\ &\implies v_2, v_1 + v_2 \in V_2 \\ &\implies v_1 = (v_1 + v_2) - v_2 \in V_2 \end{aligned}$$

which is a contradiction. □

Problem 30. Suppose W is a vector space over $\mathbf{F}$, V_1, V_2, V_3 are subspaces of W. Then $V_1 \cup V_2 \cup V_3$ is a vector space over $\mathbf{F}$ if and only if one of the V_i contains the other two.

Solution. We prove the forward direction. Suppose otherwise, then $v_1 \in V_1 \setminus (V_2 + V_3)$, $v_2 \in V_2 \setminus (V_1 + V_3)$, $v_3 \in V_3 \setminus (V_1 + V_2)$. Consider

$$\{v_1 + v_2 + v_3, v_1 + v_2 + 2v_3, v_1 + 2v_2 + v_3, v_1 + 2v_2 + 2v_3\} \subset V_1 \cup V_2 \cup V_3$$

Then

$$\begin{aligned} &(v_1 + v_2 + 2v_3) - (v_1 + v_2 + v_3) = v_3 \notin V_1 + V_2 \\ \implies &v_1 + v_2 + v_3 \notin V_1 + V_2 \quad \text{or} \quad v_1 + v_2 + 2v_3 \notin V_1 + V_2 \\ \implies &v_1 + v_2 + v_3 \in V_3 \quad \text{or} \quad v_1 + v_2 + 2v_3 \in V_3 \\ \implies &v_1 + v_2 \in V_3 \end{aligned}$$

Similarly,

$$\begin{aligned} &(v_1 + 2v_2 + 2v_3) - (v_1 + 2v_2 + v_3) = v_3 \notin V_1 + V_2 \\ \implies &v_1 + 2v_2 + v_3 \notin V_1 + V_2 \quad \text{or} \quad v_1 + 2v_2 + 2v_3 \notin V_1 + V_2 \\ \implies &v_1 + 2v_2 + v_3 \in V_3 \quad \text{or} \quad v_1 + 2v_2 + 2v_3 \in V_3 \\ \implies &v_1 + 2v_2 \in V_3 \end{aligned}$$

This implies $(v_1 + 2v_2) - (v_1 + v_2) = v_2 \in V_3$, a contradiction. □

4 Finite-Dimensional Vector Spaces

§4.1 Span and Linear Independence

Definition 4.1 (Linear combination)**.** A *linear combination* of vectors $\{v_1,\dots,v_n\}$ in V is a vector of the form

$$a_1v_1 + \cdots + a_nv_n$$

where $a_i \in \mathbf{F}$.

Definition 4.2 (Span)**.** The *span* of $\{v_1,\dots,v_n\}$ is the set of all linear combinations of $v_1,\dots,v_n$:

$$\operatorname{span}\{v_1,\dots,v_n\} = \{a_1v_1 + \cdots + a_nv_n \mid a_i \in \mathbf{F}\}.$$

The span of the empty list $(\,)$ is defined to be $\{\mathbf{0}\}$.

We say that $v_1,\dots,v_n$ *spans* V if $\operatorname{span}\{v_1,\dots,v_n\} = V$.

Proposition 4.3. $\operatorname{span}\{v_1,\dots,v_n\}$ in V is the smallest subspace of V containing $v_1,\dots,v_n$.

Proof. First we show that $\operatorname{span}\{v_1,\dots,v_n\}$ is a subspace of V.

(i) Additive identity $\mathbf{0} = 0v_1 + \cdots + 0v_n \in \operatorname{span}\{v_1,\dots,v_n\}$

(ii) $(a_1v_1 + \cdots + a_nv_n) + (c_1v_1 + \cdots + c_nv_n) = (a_1 + c_1)v_1 + \cdots + (a_n + c_n)v_n \in \operatorname{span}\{v_1,\dots,v_n\}$, so $\operatorname{span}\{v_1,\dots,v_n\}$ is closed under addition.

(iii) $\lambda(a_1v_1 + a_nv_n) = (\lambda a_1)v_1 + \cdots + (\lambda a_n)v_n \in \operatorname{span}\{v_1,\dots,v_n\}$, so $\operatorname{span}\{v_1,\dots,v_n\}$ is closed under scalar multiplication.

Thus $\operatorname{span}\{v_1,\dots,v_n\}$ is a subspace of V.

Each v_i is a linear combination of $v_1,\dots,v_n$:

$$v_i = 0v_1 + \cdots + 0v_{i-1} + 1v_i + 0v_{i+1} + \cdots + 0v_n.$$

Thus $v_i \in \operatorname{span}\{v_1,\dots,v_n\}$. Conversely, since subspaces are closed under scalar multiplication and addition, every subspace of V containing each v_i contains $\operatorname{span}\{v_1,\dots,v_n\}$.

Hence $\operatorname{span}\{v_1,\dots,v_n\}$ is the smallest subspace of V containing $v_1,\dots,v_n$. □

Definition 4.4 (Finite-dimensional vector space)**.** V is *finite-dimensional* if there exists $v_1,\dots,v_n$ that spans V; otherwise, it is infinite-dimensional.

> **Example 4.5.** $\mathbf{F}^3$ is finite-dimensional because $\mathbf{F}^3 = \operatorname{span}\{(1,0,0),(0,1,0),(0,0,1)\}$; $\mathbf{F}^\infty$ is infinite-dimensional.

Otherwise mentioned, all subsequent vector spaces are finite-dimensional.

Definition 4.6 (Polynomial)**.** A function $p : \mathbf{F} \to \mathbf{F}$ is a *polynomial* with coefficients in $\mathbf{F}$ if there exist $a_i \in \mathbf{F}$ such that

$$p(z) = a_0 + a_1 z + \cdots + a_n z^n$$

for all $z \in \mathbf{F}$.

We denote the set of all polynomials with coefficients in $\mathbf{F}$ by $\mathcal{P}(\mathbf{F})$.

A polynomial $p \in \mathcal{P}(\mathbf{F})$ is has degree n if there exist scalars $a_0, a_1, \dots, a_n \in \mathbf{F}$ with $a_n \neq 0$ such that $p(z) = a_0 + a_1 z + \cdots + a_n z^n$ for all $z \in \mathbf{F}$; if p has degree n, we write $\deg p = n$.

For non-negative integer n, $\mathcal{P}^n(\mathbf{F})$ denotes the set of all polynomials with coefficients in $\mathbf{F}$ and degree at most n.

Definition 4.7 (Linear independence)**.** $\{v_1, \dots, v_n\}$ is *linearly independent* in V if the only choice of $a_1, \dots, a_n \in \mathbf{F}$ that makes $a_1 v_1 + \cdots + a_n v_n = \mathbf{0}$ is $a_1 = \cdots = a_n = 0$; otherwise, it is *linearly dependent*.

Lemma 4.8 will often be useful; it states that given a linearly dependent list of vectors, one of the vectors is in the span of the previous ones and furthermore we can throw out that vector without changing the span of the original list.

Lemma 4.8 (Linear dependence lemma)**.** Suppose $\{v_1, \dots, v_n\}$ is linearly dependent in V. Then there exists v_k such that the following hold:

(i) $v_k \in \operatorname{span}\{v_1, \dots, v_{k-1}\}$

(ii) $\operatorname{span}\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\} = \operatorname{span}\{v_1, \dots, v_n\}$

Proof. Since $\{v_1, \dots, v_n\}$ is linearly dependent, there exists $a_1, \dots, a_n \in \mathbf{F}$, not all 0, such that

$$a_1 v_1 + \cdots + a_n v_n = 0.$$

Let $k = \max\{1, \dots, n\}$ such that $a_k \neq 0$. Then

$$v_k = -\frac{a_1}{a_k} v_1 - \cdots - \frac{a_{k-1}}{a_k} v_{k-1},$$

proving (i).

To prove (ii), suppose $u \in \operatorname{span}\{v_1, \dots, v_n\}$. Then there exists $c_1, \dots, c_n \in \mathbf{F}$ such that

$$u = c_1 v_1 + \cdots + c_n v_n.$$

□

Proposition 4.9 says that no linearly independent list in V is longer than a spanning list in V.

Proposition 4.9. The length of every linearly independent list of vectors is less than or equal to the length of every spanning list of vectors.

Proof. □

§4.2 Bases

Definition 4.10 (Basis)**.** $\{v_1 \dots, v_n\}$ is a *basis* of V if it is linearly independent and spans V.

> **Example 4.11.** Let $\mathbf{e}_i = (0, \dots, 0, 1, 0, \dots, 0)$ where the i-th coordinate is 1. $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is a basis of $\mathbf{F}^n$, called the *standard basis* of $\mathbf{F}^n$.

Example 4.12. $\{1, z, \dots, z^n\}$ is a basis of $\mathcal{P}^n(\mathbf{F})$.

Lemma 4.13 (Criterion for basis)**.** The following are equivalent:

(i) $\{v_1, \dots, v_n\}$ is a basis of V.

(ii) Every $v \in V$ is uniquely expressed as a linear combination of $v_1, \dots, v_n$.

(iii) $v_i \neq 0$, $V = Fv_1 \oplus \cdots \oplus Fv_n$.

Proof. □

Proposition 4.14. Every spanning list in a vector space can be reduced to a basis of the vector space.

Proposition 4.15. Every finite-dimensional vector space has a basis.

Proof. By definition, a finite-dimensional vector space has a spanning list. The previous result tells us that each spanning list can be reduced to a basis. □

Proposition 4.16. Every linearly independent list of vectors in a finite-dimensional vector space can be extended to a basis of the vector space.

Proposition 4.17. Suppose U is a subspace of V. Then there exists a subspace W of V such that $V = U \oplus W$.

Proof. □

§4.3 Dimension

Definition 4.18 (Dimension)**.** The *dimension* of V is the length of any basis of V, denoted by $\dim V$.

Proposition 4.19. Suppose U is a subspace of V, then $\dim U \leq \dim V$.

Proposition 4.20. Every linearly independent list of vectors in V with length $\dim V$ is a basis of V.

Proposition 4.21. Every spanning list of vectors in V with length $\dim V$ is a basis of V.

Lemma 4.22 (Dimension of a sum)**.** Suppose U_1 and U_2 are subspaces of V, then

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2).$$

5 Linear Maps

§5.1 Vector Space of Linear Maps

Definition 5.1 (Linear map)**.** A *linear map* from V to W is a function $T : V \to W$ with the following properties:

(i) Additivity: $T(v + w) = Tv + Tw$ for all $v, w \in V$

(ii) Homogeneity: $T(\lambda v) = \lambda T(v)$ for all $\lambda \in \mathbf{F}$, $v \in V$

Notation. The set of all linear maps from V to W is denoted $\mathcal{L}(V, W)$; the set of linear transformations on V is denoted $\mathcal{L}(V)$.

Proposition 5.2 (Linear map lemma)**.** Suppose $\{v_1, \dots, v_n\}$ is a basis of V and $w_1, \dots, w_n \in W$. Then there exists a unique linear map $T : V \to W$ such that

$$Tv_i = w_i \quad (i = 1, \dots, n)$$

Proof. First we show the existence of a linear map T with the desired property. Define $T : V \to W$ by

$$T(c_1 v_1 + \cdots + c_n v_n) = c_1 w_1 + \cdots + c_n w_n,$$

for some $c_i \in \mathbf{F}$. Since $\{v_1, \dots, v_n\}$ is a basis of V, by Lemma 4.13, each $v \in V$ can be uniquely expressed as a linear combination of $v_1, \dots, v_n$, thus the equation above does indeed define a function $T : V \to W$. For $i = 1, \dots, n$, take $c_i = 1$ and the other c's equal to 0 to show that $Tv_i = w_i$.

We now show that $T : V \to W$ is a linear map:

(i) If $u, v \in V$ with $u = a_1 v_1 + \cdots + a_n v_n$ and $c_1 v_1 + \cdots + c_n v_n$, then

$$\begin{aligned} T(u + v) &= T\big((a_1 + c_1)v_1 + \cdots + (a_n + c_n)v_n\big) \\ &= (a_1 + c_1)w_1 + \cdots + (a_n + c_n)w_n \\ &= (a_1 w_1 + \cdots + a_n w_n) + (c_1 w_1 + \cdots + c_n w_n) \\ &= Tu + Tv \end{aligned}$$

so T satisfies additivity.

(ii) If $\lambda \in \mathbf{F}$ and $v = c_1 v_1 + \cdots + c_n v_n$, then

$$\begin{aligned} T(\lambda v) &= T(\lambda c_1 v_1 + \cdots + \lambda c_n v_n) \\ &= \lambda c_1 w_1 + \cdots + \lambda c_n w_n \\ &= \lambda(c_1 w_1 + \cdots + c_n w_n) \\ &= \lambda Tv \end{aligned}$$

so T satisfies homogeneity.

To prove uniqueness, now suppose that $T \in \mathcal{L}(V,W)$ and $Tv_i = w_i$ for $i = 1, \dots, n$. Let $c_i \in \mathbf{F}$. The homogeneity of T implies that $T(c_i v_i) = c_i w_i$. The additivity of T now implies that

$$T(c_1 v_1 + \cdots + c_n v_n) = c_1 w_1 + \cdots + c_n w_n.$$

Thus T is uniquely determined on $\operatorname{span}\{v_1, \dots, v_n\}$. Since $\{v_1, \dots, v_n\}$ is a basis of V, this implies that T is uniquely determined on V. □

Proposition 5.3. $\mathcal{L}(V,W)$ is a vector space, with the operations addition and scalar multiplication defined as follows: suppose $S, T \in \mathcal{L}(V,W)$, $\lambda \in \mathbf{F}$,

(i) $(S+T)(v) = Sv + Tv$

(ii) $(\lambda T)(v) = \lambda(Tv)$

for all $v \in V$.

Definition 5.4 (Product of linear maps)**.** $T \in \mathcal{L}(U,V)$, $S \in \mathcal{L}(V,W)$, then the *product* $ST \in \mathcal{L}(U,W)$ is defined by

$$(ST)(u) = S(Tu) \quad (\forall u \in U)$$

Remark. In other words, ST is just the usual composition $S \circ T$ of two functions.

Remark. ST is defined only when T maps into the domain of S.

Proposition 5.5 (Algebraic properties of products of linear maps)**.**

(i) Associativity: $(T_1 T_2) T_3 = T_1 (T_2 T_3)$ for all linear maps T_1, T_2, T_3 such that the products make sense (meaning that T_3 maps into the domain of T_2, T_2 maps into the domain of T_1)

(ii) Iidentity: $TI = IT = T$ for all $T \in \mathcal{L}(V,W)$ (the first I is the identity map on V, and the second I is the identity map on W)

(iii) Distributive: $(S_1 + S_2)T = S_1 T + S_2 T$ and $S(T_1 + T_2) = ST_1 + ST_2$ for all $T, T_1, T_2 \in \mathcal{L}(U,V)$ and $S, S_1, S_2 \in \mathcal{L}(V,W)$

Proposition 5.6. $T \in \mathcal{L}(V,W)$. Then $T(0) = 0$.

Proof. By additivity, we have

$$T(0) = T(0+0) = T(0) + T(0).$$

Add the additive inverse of $T(0)$ to each side of the equation above to conclude that $T(0) = 0$. □

§5.2 Kernel and Image

Definition 5.7 (Kernel)**.** For $T \in \mathcal{L}(V,W)$, the *kernel* of T is the subset of V consisting of those vectors that T maps to 0:

$$\ker T \coloneqq \{v \in V \mid Tv = 0\}.$$

Proposition 5.8. $T \in \mathcal{L}(V,W)$, $\ker T$ is a subspace of V.

Proof. By Lemma 3.12, we check the conditions of a subspace:

(i) $T(0) = 0$ by Proposition 5.6, so $0 \in \ker T$.

(ii) For all $v, w \in \ker T$,

$$T(v+w) = Tv + Tw = 0 \implies v + w \in \ker T$$

so $\ker T$ is closed under addition.

(iii) For all $v \in \ker T$, $\lambda \in \mathbf{F}$,

$$T(\lambda v) = \lambda T v = 0 \implies \lambda v \in \ker T$$

so $\ker T$ is closed under scalar multiplication.

□

Definition 5.9 (Injectivity)**.** $T : V \to W$ is *injective* if

$$Tu = Tv \implies u = v.$$

Proposition 5.10. $T \in \mathcal{L}(V, W)$, T is injective if and only if $\ker T = 0$.

Proof. □

Definition 5.11 (Image)**.** For $T : V \to W$, the *image* of T is the subset of W consisting of those vectors that are of the form Tv for some $v \in V$:

$$\operatorname{im} T \coloneqq \{Tv \mid v \in V\}.$$

Proposition 5.12. $T \in \mathcal{L}(V, W)$, $\operatorname{im} T$ is a subspace of W.

Proof. □

Definition 5.13 (Surjectivity)**.** $T : V \to W$ is *surjective* if $\operatorname{im} T = W$.

Theorem 5.14 (Fundamental Theorem of Linear Maps)**.** $T \in \mathcal{L}(V, W)$, then $\operatorname{im} T$ is finite-dimensional and

$$\dim V = \dim \ker T + \dim \operatorname{im} T.$$

§5.3 Matrices

Definition 5.15 (Matrix)**.** A $m \times n$ *matrix* A is a rectangular array with m rows and n columns:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

where $a_{ij} \in \mathbf{F}$.

Definition 5.16 (Matrix of a linear map)**.** $T \in \mathcal{L}(V, W)$, $\{v_1, \dots, v_n\}$ is a basis of V, $\{w_1, \dots, w_m\}$ is a basis of W. The *matrix* of T with respect to these bases of the $m \times n$ matrix $M(T)$ whose entries a_{ij} are defined by

§5.4 Invertibility and Isomorphism

Definition 5.17 (Invertibility)**.** $T \in \mathcal{L}(V, W)$ is *invertible* if there exists $S \in \mathcal{L}(W, V)$ such that $ST = I_V$, $TS = I_W$, where I_V and I_W are the *identity maps* on V and W respectively; S is known as the *inverse* of T.

Proposition 5.18 (Uniqueness of inverse)**.** An invertible linear map has a unique inverse.

Proof. Suppose $T \in \mathcal{L}(V, W)$ is invertible. S_1 and S_2 are inverses of T. Then

$$S_1 = S_1 I = S_1(TS_2) = (S_1T)S_2 = IS_2 = S_2.$$

Thus $S_1 = S_2$. □

Now that we know that the inverse is unique, we can give it a notation.

Bibliography

[Ahl79] L. V. Ahlfors. *Complex Analysis.* McGraw-Hill, 1979.

[Apo57] T. M. Apostol. *Mathematical Analysis.* Addison-Wesley, 1957.

[Axl15] S. Axler. *Linear Algebra Done Right.* Springer International Publishing, 2015.

[DF04] D. S. Dummit and R. M. Foote. *Abstract Algebra.* John Wiley & Sons, 2004.

[Mun18] J. R. Munkres. *Topology.* Pearson Education Limited, 2018.

[Pól45] G. Pólya. *How to Solve It.* Princeton University Press, 1945.

[Rud53] W. Rudin. *Principles of Mathematical Analysis.* McGraw-Hill, 1953.

[Sch92] A. H. Schoenfeld. “Learning to think mathematically: Problem solving, metacognition, and sense-making in mathematics”. In: *Handbook for Research on Mathematics Teaching and Learning.* Macmillan, 1992, pp. 334–370.

[Spi08] M. Spivak. *Calculus.* Publish or Perish, Inc., 2008.

[Ste08] J. Stewart. *Calculus Early Transcendentals.* Thomson Learning, Inc., 2008.