Fons

Ryan Joo Rui An

June 11, 2024

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 June 11, 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
June 11, 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 [HKll],
4. **real analysis** which follows [Rud53; Apo57], and
5. **complex analysis** which follows [Ahl79],
6. **topology** which follows [Mun18].

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. We often say that "this is a corollary of Theorem A".
- 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.

§1.1.1 Notation

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 $P \equiv Q$, 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.

- Double negation law:
$$P \equiv \neg(\neg P)$$
- Commutative property:
$$P \wedge Q \equiv Q \wedge P, \quad P \vee Q \equiv Q \vee P$$
- Associative property for conjunction:
$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$$
- Associative property for disjunction:
$$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$$
- Distributive property for conjunction across disjunction:
$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge Q)$$
- Distributive property for disjunction across conjunction:
$$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$$
- **De Morgan's Laws**:
$$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$$
$$\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$$

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 $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$.

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 $\neg P \equiv \neg(1 < x) \equiv (x \leq 1)$ and $\neg Q \equiv \neg(x < 2) \equiv (x \geq 2)$.

Thus

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

Therefore the negation of $1 < x < 2$ is logically equivalent 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,

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

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. □

§1.1.2 If, only if, $\implies$

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).

§1.1.3 If and only if, iff, $\iff$

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'.

$$P \iff Q \equiv (P \implies Q) \wedge (Q \implies P)$$

$P \iff Q$ 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.

§1.1.4 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:

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

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

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 $(\forall x \in \mathbb{R})[x > 2 \implies x^2 > 4]$.

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

Therefore a useful denial of the statement is:

$$\text{there exists a real number } x \text{ such that } x > 2 \text{ and } x^2 \le 4.$$

□

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

§1.2.1 Direct proof

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.

§1.2.2 Proof by contrapositive

To prove $P \implies Q$, we can instead prove $\neg Q \implies \neg P$.

> **Exercise 5**
> For every integer a, prove that if $3a^2 + 1$ is even, then a is odd.

Proof. We prove this by contrapositive.

Suppose a is not odd. So $a = 2k$ for some integer k. Then

$$3a^2 + 1 = 3(2k)^2 + 1 = 2(6k^2) + 1.$$

Since $3a^2 + 1 = 2q + 1$ for some integer q, hence $3a^2 + 1$ is odd. □

> **Exercise 6**
> For $m \in \mathbb{Z}$, prove that if $3 \mid m^2$ then $3 \mid m$.

Proof. We prove this by contrapositive.

Suppose $3 \nmid m$. We shall prove $3 \nmid m^2$.

Case 1: $m = 3k + 1$

Then $m^2 = (3k + 1)^2 = 3(3k^2 + 2k) + 1$ so m^2 has remainder 1 when divided by 3, hence $3 \nmid m^2$.

Case 2: $m = 3k + 2$

This case shall be left as an exercise. □

§1.2.3 Disproof by counterexample

Providing a counterexample is the best method for refuting, or dispoving, a conjecture.

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.

The counterexample must make the hypothesis a true statement, and the conclusion a false statement.

§1.2.4 Proof by cases

You can sometimes prove a statement by:

1. Dividing the situation into cases which exhaust all the possibilities; and
2. Showing that the statement follows in all cases.

Remark. It is important to cover all the possibilities.

§1.2.5 Proof by contradiction

To prove P by contradiction, suppose that P is false, i.e. $\neg P$. Similarly, 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 7

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

Proof. We prove by contradiction. Suppose otherwise, that $\sqrt{2}$ is rational. Using the definition of rational numbers, we can write it as $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}, b \neq 0$.

We also assume that $\frac{a}{b}$ is simplified to lowest terms, since that can obviously be done with any fraction. Notice that in order for $\frac{a}{b}$ to be in simplest terms, both a and b cannot be even; one or both must be odd, otherwise we could simplify the fraction further.

Squaring both sides gives us

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

Since RHS is even, LHS must also be even. Hence it follows that a is even. Let $a = 2k$ where $k \in \mathbb{Z}$. 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 is a contradiction, as we started out assuming that $\frac{a}{b}$ was simplified to lowest terms, and now it turns out that a and b both would be even. Hence proven. □

Exercise 8

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

Proof. Suppose there is 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 $a \mid (n + 1)$. □

§1.2.6 Proof of uniqueness

$\exists!$ means "there exists a unique".

To prove uniqueness, we can do one of the following:

- Assume $\exists x, y \in S$ such that $P(x) \wedge P(y)$ is true and show $x = y$.
- Argue by assuming that $\exists x, y \in S$ are distinct such that $P(x) \wedge P(y)$, then derive a contradiction.

To prove uniqueness and existence, we also need to show that $\exists x \in S$ s.t. $P(x)$ is true.

§1.2.7 Proof of existence

To prove existential statements, we can adopt two approaches:

1. Constructive proof (direct proof)
2. Non-constructive proof (indirect proof)

Constructive 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

1. belongs to the domain X, and
2. satisfies the condition P.

Exercise 9

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 $n, n+1, n+2, \ldots, n+99$, 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 $k = 1, 2, \ldots, 99$.

Hence the existential statement is proven. □

Exercise 10

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 $x = \dfrac{p+q}{2}$ 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 $\mathbb{Q}$ is closed under addition). □

Exercise 11

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 $r = \dfrac{p+q}{2}$; 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 $c = \dfrac{q-p}{k}$ for some $k > 1$; to make c irrational, we take k to be irrational.

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

Part 1: $p < r < q$

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

Part 2: r is irrational

We prove by contradiction. Suppose r is rational. We have $\sqrt{2} = \dfrac{q-p}{r-p}$. 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

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 12**
>
> 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 13**
>
> 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. □

Exercise 14

An odd prime p may be written as a sum of two squares if and only $p \equiv 1 \pmod 4$.

Proof. We again use the method of descent, though this time *constructively*.

($\implies$) If $p = x^2 + y^2$, then both x and y are non-zero modulo p. Taking Legendre symbols, we see that

$$1 = \left(\frac{x^2}{p}\right) = \left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right) \implies p \equiv 1 \pmod 4$$

($\impliedby$) Suppose that p is a prime congruent to 1 modulo 4. We must show that there exist integers x, y such that $x^2 + y^2 = p$. We do this by descent:

1. Modulo p, the congruence $x^2 + 1 \equiv 0$ has a solution x since -1 is a quadratic residue. By taking $y = 1$, we may therefore assume the existence of a solution to an equation $x^2 + y^2 = mp$ for some integer $1 \le m < p$. If $m = 1$ we are done. Otherwise ...

2. Define
$$\begin{cases} u \equiv x \pmod m \\ v \equiv y \pmod m \end{cases} \qquad \text{such that } |u|, |v| \le \frac{m}{2}.$$
Since $xu + yv$, $xv - yu$ and $u^2 + v^2$ are all divisible by m, we may divide the identity
$$(u^2 + v^2)(x^2 + y^2) = (xu + yv)^2 + (xv - yu)^2$$
by m^2 to obtain an equation in integers:
$$kp = \left(\frac{xu + yv}{m}\right)^2 + \left(\frac{xv - yu}{m}\right)^2 \text{ where } k = \frac{u^2 + v^2}{m} \le \frac{m}{2}$$

3. We have therefore constructed an integer solution to $X^2 + Y^2 = kp$ with $k < m$. If $k \ge 2$, simply repeat the process from step 2: by descent, we must eventually reach $k = 1$.

□

§1.2.8 Pigeonhole principle

Theorem 1.2.1 (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 1.2.2 (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.

§1.2.9 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 1.2.3 (Principle of Mathematical Induction (PMI))
Let $P(n)$ be a family of statements indexed by $\mathbb{Z}^+$. Suppose that

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

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

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

Using logic notation, this is written as

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

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 15
Prove that for any $n \in \mathbb{Z}^+$,

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

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

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 $n \in \mathbb{Z}^+$. □

Remark. Do not write $P(n) = \frac{n(n+1)}{2}$, as $P(n)$ is a statement, not an expression (which does not have truth values).

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

Corollary 1.2.4

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 1.2.5 (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 $m \in \mathbb{Z}^+$, 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 $n \in \mathbb{N}$.

Using logic notation, this is written as

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

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 1.2.6 (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 1.2.7 (Cauchy Induction)

Let $P(n)$ be a family of statements indexed by $\mathbb{Z}^+_{\geq 2}$. Suppose that

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

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

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

Exercise 16

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:

$$\frac{a_1 + a_2 + \cdots + a_{2n}}{2n} = \frac{\frac{a_1+a_2+\cdots+a_n}{n} + \frac{a_{n+1}+a_{n+2}+\cdots+a_{2n}}{n}}{2}$$

$$\frac{\frac{a_1+a_2+\cdots+a_n}{n} + \frac{a_{n+1}+a_{n+2}+\cdots+a_{2n}}{n}}{2} \geq \frac{\sqrt[n]{a_1a_2\cdots a_n} + \sqrt[n]{a_{n+1}a_{n+2}\cdots a_{2n}}}{2}$$

$$\frac{\sqrt[n]{a_1a_2\cdots a_n} + \sqrt[n]{a_{n+1}a_{n+2}\cdots a_{2n}}}{2} \geq \sqrt{\sqrt[n]{a_1a_2\cdots a_n}\sqrt[n]{a_{n+1}a_{n+2}\cdots a_{2n}}}$$

$$\sqrt{\sqrt[n]{a_1a_2\cdots a_n}\sqrt[n]{a_{n+1}a_{n+2}\cdots a_{2n}}} = \sqrt[2n]{a_1a_2\cdots a_{2n}}$$

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, $\frac{a_1+a_2+\cdots+a_n}{n} \geq \sqrt[n]{a_1a_2\cdots a_n}$ 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,

$$\frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} \geq \sqrt[n]{a_1a_2\cdots a_{n-1} \cdot \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}}$$

$$\Rightarrow \left(\frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}\right)^n \geq a_1a_2\cdots a_{n-1} \cdot \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}$$

$$\Rightarrow \left(\frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}\right)^{n-1} \geq a_1a_2\cdots a_{n-1}$$

$$\Rightarrow \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} \geq \sqrt[n-1]{a_1a_2\cdots a_{n-1}}$$

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

Other variations

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

- $(\forall n \in \mathbb{Z})P(n)$

  Base case: $P(0)$

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

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

- $(\forall n \in \mathbb{Q})P(n)$

  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 1.2.8

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

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

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

Theorem 1.2.9 (Well-ordering principle)

Let $(X, \preceq)$ 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.

§1.2.10 Symmetry principle

§1.2.11 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 $k \in \mathbb{Z}$.

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

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

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

$$nb^2 = a^2. \qquad (*)$$

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 $\mathbb{Z}$ 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: $p < \dfrac{p+q}{2} < q$.

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

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

Problem 10. Given n real numbers $a_1, a_2, \ldots, a_n$. Show that there exists an a_i $(1 \le i \le n)$ 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 $\dfrac{\sqrt{2}}{a}$.

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

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

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

Then the reciprocal $\dfrac{a}{\sqrt{2}}$. Since $\sqrt{6}$ is irrational, the product $\left(\dfrac{a}{\sqrt{2}}\right)\sqrt{6} = a\sqrt{3}$ 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 $k \in \mathbb{Z}^+_{\geq 4}$

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

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

Base case: $P(2)$

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

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

Assume $P(k)$ is true for $k \geq 2, k \in \mathbb{Z}^+$, 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 $k \in \mathbb{Z}^+_{\geq 3}$

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

($\impliedby$) 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:

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

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

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

Problem 18. Let a_i where integer $1 \leq i \leq n$ 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 $n \in \mathbb{Z}^+$, prove that

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

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

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 $k \in \mathbb{Z}^+$.

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

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

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

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

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

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

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

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

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

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

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 concludes 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 $x \in Q = \{1, 2, \ldots, p-1\}$ 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 $m, n \in \mathbb{N}$, prove that

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

Proof. For $n \in \mathbb{N}$, take $P(n) : F_{n+m+1} = F_n F_m + F_{n+1} F_{m+1}$ for all $m \in \mathbb{N}$ 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 $m \in \mathbb{N}$, 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 $m \in \mathbb{N}$,

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

From our $P(n)$ assumptions and the definition of the Fibonacci numbers, LHS of (5) = Fn+m+3 = Fn+m+2 + Fn+m+1 = FnFm + Fn+1Fm+1 + Fn+1Fm + Fn+2Fm+1 = (Fn + Fn+1) Fm + (Fn+1 + Fn+2) Fm+1 = Fn+2Fm + Fn+3Fm+1 = RHS of (5). □

2 Set Theory

§2.1 Basics

§2.1.1 Notation

You should, by now, be familiar with the following definitions and notation:

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

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

  $\subseteq$ is transitive, i.e. 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

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

- 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

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

  □

- Some frequently occurring subsets of the real numbers are known as **intervals**, which can be visualised as sections of the real line:

  – Open interval
  $$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$$

  – Closed interval
  $$[a, b] = \{x \in \mathbb{R} \mid a \leq x < b\}$$

  – Half open interval
  $$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$

- 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 $(a_1, a_2, \ldots, a_n)$, 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 2.1.1.** $\mathbb{R}^2$ is the Euclidean plane, $\mathbb{R}^3$ is the Euclidean space, and $\mathbb{R}^n$ is the n-dimensional Euclidean space.
>
> $$\begin{aligned} \mathbb{R} \times \mathbb{R} = \mathbb{R}^2 &= \{(x, y) \mid x, y \in \mathbb{R}\} \\ \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3 &= \{(x, y, z) \mid x, y, z \in \mathbb{R}\} \\ \mathbb{R}^n &= \{(x_1, x_2, \ldots, x_n) \mid x_1, x_2, \ldots, x_n \in \mathbb{R}\} \end{aligned}$$

§2.1.2 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 $A \setminus B$, is the subset consisting of those elements that are in A and not in B:

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

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

Proposition 2.1.2 (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 2.1.3 (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 2.1.4 (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 17

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 18

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

§2.2.1 Definition

Definition 2.2.1

R is a **relation** between A and B if and only if R is a subset of the Cartesian product $A \times B$, i.e. $R \subseteq A \times B$.

$a \in A$ and $b \in B$ are **related** if $(a, b) \in R$, denoted by 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 2.2.2

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 2.2.3. 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 2.2.4.

- The "less than or equal to" relation $\leq$ on the set of real numbers is $\{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$. We write $x \leq y$ if (x, y) is in this set.
- The "divides" relation $\mid$ on $\mathbb{N}$ is $\{(m, n) \in \mathbb{N}^2 : m \text{ divides } n\}$. 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.

§2.2.2 Properties of relations

Let A be a set, R a relation on A, and $x, y, z \in A$. 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 2.2.5 (Less than or equal to)**.** The relation $\leq$ on R is reflexive, anti-symmetric, and transitive, but not symmetric.

Definition 2.2.6

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

Example 2.2.7 (Less than)**.** The relation $<$ on R is not reflexive, symmetric, or anti-symmetric, but it is transitive.

Example 2.2.8 (Not equal to)**.** The relation $\neq$ on R is not reflexive, anti-symmetric or transitive, but it is symmetric.

Exercise 19

Congruence modulo n Let $n \geq 2$ be an integer, and define R on $\mathbb{Z}$ 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 $a \in \mathbb{Z}$ 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.

□

§2.2.3 Equivalence relations, equivalence classes, and partitions

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 2.2.9

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 2.2.10

Given an equivalence relation $\sim$ on a set A, and given $x \in A$, the **equivalence class** of x, denoted $[x]$, is the subset

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

Example 2.2.11 (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 2.2.12

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 2.2.13

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 $i \in I$ (that is, all the subsets are non-empty),

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

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

The subsets are called the parts of the partition.

Example 2.2.14 (Odd and even natural numbers)**.** $\{\{n \in \mathbb{N} \mid n \text{ is divisible by } 2\}, \{n \in \mathbb{N} \mid n+1 \text{ is divisible by } 2\}\}$ forms a partition of the natural numbers, into evens and odds.

§2.3 Functions

§2.3.1 Definition

Definition 2.3.1

Given two sets X and Y, a **function** f from X to Y is a mapping of every element of X to some element of Y, denoted by $f : X \to Y$.

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 $f : \mathbb{R} \to \mathbb{R}$, 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 2.3.2

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 20

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

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

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

Definition 2.3.3 (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 2.3.4 (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.

§2.3.2 Injectivity, Surjectivity, Bijectivity

Definition 2.3.5

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

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

Proposition 2.3.6

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 2.3.7

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

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

□

Definition 2.3.8

$f : X \to Y$ is **surjective** if every element of Y is mapped to at least one element of X.

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

Proposition 2.3.9

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 2.3.10

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

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

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. □

Definition 2.3.11

$f : X \to Y$ 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 2.3.12 (Cantor–Schroder–Bernstein)

If $f : A \to B$ and $g : B \to A$ are both injections, then $A \sim B$.

Proof. □

§2.3.3 Composition of functions and invertibility

Definition 2.3.13

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 2.3.14 (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

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

□

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

Proposition 2.3.15

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 $X = Z = \{0\}, Y = \mathbb{R}$, with $f(0) = 0$ and $g(y) = 0$ for all $y \in \mathbb{R}$. □

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

Definition 2.3.16

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

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

An immediate concern we might have is whether there could be multiple such functions g, in which case the inverse f^{-1} would not be well-defined. This is resolved by the following result:

Proposition 2.3.17 (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 2.3.18
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 2.3.19
A function $f : X \to Y$ is invertible if and only if it is bijective.

Proof.

($\implies$) 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.

($\impliedby$) 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 2.3.20

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.

§2.3.4 Monotonic functions

Definition 2.3.21

A real valued function $f : [a, b] \to \mathbb{R}$ 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 $f(x_1) \ge f(x_2)$;

(3) **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 $[a, b]$.

§2.3.5 Convex and Concave Functions

Definition 2.3.22

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 2.3.23

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 2.3.24

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 2.3.25

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

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

§2.3.6 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 2.3.26 (Absolute value function)

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

Definition 2.3.27 (Floor function)

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

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

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

Definition 2.3.28 (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.

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

Exercise 21

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 22

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

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

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

Definition 2.4.1

Let S be a set. An **order** on S is a relation, denoted by $<$, with the following two 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. The notation $x \leq y$ indicates that $x < y$ or $x = y$, without specifying which of these two is to hold. In other words, $x \leq y$ is the negation of $x > y$.

Definition 2.4.2

An **ordered set** is a set S in which an order is defined.

Example 2.4.3. $\mathbb{Q}$ is an ordered set if $r < s$ is defined to mean that $s - r$ is a positive rational number.

Definition 2.4.4

Suppose S is an ordered set, and $E \subset S$. E is **bounded above** if there exists an **upper bound** $M \in S$ such that $x \leq M$ for all $x \in E$.

Similarly, E is **bounded below** if there exists a **lower bound** $m \in S$ such that $x \geq m$ for all $x \in E$.

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

Definition 2.4.5

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.

Then we call α the **supremum** (or *least upper bound*) of E, and we write

$$\alpha = \sup E.$$

Definition 2.4.6

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.

Then we call α the **infimum** (or *greatest lower bound*) of E, and we write

$$\alpha = \inf E.$$

Proposition 2.4.7 (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 $M \leq N$.

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 $N \leq M$.

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

Definition 2.4.8

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 2.4.9

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 2.4.10 (Comparison Theorem)

Let $S, T \subset \mathbb{R}$ 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 2.4.11

Let S, T be non-empty subsets of $\mathbb{R}$, 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 2.4.12

Let $T \subseteq \mathbb{R}$ 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 2.4.13 (Approximation Property)

Let $S \subseteq \mathbb{R}$ 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 $\{\frac{1}{n} \mid n \in \mathbb{Z}^+\}$.

(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 $\mathbb{Q}$, 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 $\mathbb{Q}$.

By ZFC, we have the Completeness Axiom, which states that any non-empty set $A \subset \mathbb{R}$ 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 $M \in \mathbb{R}$ 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 $n = \left[\frac{1}{a}\right] + 1$, 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 $\left|2k\pi + \frac{\pi}{2} - n\right| < \delta$

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 of Sets

Definition 2.5.1

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 $1, 2, \ldots, n$. Let J be the set consisting of all positive integers.

Definition 2.5.2

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 2.5.3

$2J = \{2n \mid n \in J\}$ 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 2.5.4

$\mathbb{Z}$ is countable.

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

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

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

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

□

Proposition 2.5.5

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 2.5.6

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

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

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 2.5.7

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 2.5.8 (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 2.5.9 (Principle of Inclusion and Exclusion)

Let S_i be finite sets. Then

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

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,

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

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

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

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

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

□

Theorem 2.5.10 (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 $|A| \leq |\mathcal{P}(A)|$. 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 2.5.11

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

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 $Y \in \mathbb{C}^n$ 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:

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

The equivalence classes are called congruence classes modulo n.

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

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

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

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

For any other representatives x', y' we have

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

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

□

Problem 27. Let $A = \mathbb{R}$ and for any $x, y \in A$, $x \sim y$ if and only if $x - y \in \mathbb{Z}$. 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 $\mathbb{C}$, 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)

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

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

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

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

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

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

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

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 $\mathbb{R}[x]$ denote the set of real polynomials. Define

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

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

Abstract Algebra

3 Group Theory

§3.1 Modular Arithmetic

Let n be a fixed positive integer. Define a relation on $\mathbb{Z}$ by

$$a \sim b \iff n \mid (b-a).$$

Proposition 3.1.1
$a \sim b$ is a equivalence relation.

Proof.

(1) $a \sim a$, thus the relation is reflexive.

(2) $a \sim b \implies b \sim a$ for any integers a and b, thus the relation is symmetric.

(3) If $a \sim b$ and $b \sim c$ then $n \mid (a-b)$ and $n \mid (b-c)$, so $n \mid (a-b)+(b-c) = (a-c)$, so $a \sim c$ and the relation is transitive.

□

We write $a \equiv b \pmod{n}$ (read: a is **congruent** to b mod n) if $a \sim b$.

For any $k \in \mathbb{Z}$ we denote the equivalence class of a by $\overline{a}$, called the **congruence class** (residue class) of a mod n, consisting of the integers which differ from a by an integral multiple of n; that is,

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}.$$

There are precisely n distinct equivalence classes mod n, namely

$$\overline{0}, \overline{1}, \ldots, \overline{n-1}$$

determined by the possible remainders after division by n and these residue classes partition the integers $\mathbb{Z}$. The set of equivalence classes under this equivalence relation is denoted by $\mathbb{Z}/n\mathbb{Z}$, and called the **integers modulo** n.

We can define addition and multiplication for the elements of $\mathbb{Z}/n\mathbb{Z}$, defining *modular arithmetic* as follows: for $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$,

1. (addition) $\overline{a} + \overline{b} = \overline{a+b}$
2. (multiplication) $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

This means that to compute the sum (product) of two elements $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, take any *representative* integer $a \in \overline{a}$ and any representative integer $b \in \overline{b}$, and add (multiply) integers a and b as usual in $\mathbb{Z}$, then take the equivalence class containing the result.

Theorem 3.1.2

Addition and mulltiplication on $\mathbb{Z}/n\mathbb{Z}$ are well-defined; that is, they do not depend on the choices of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\overline{a_1} = \overline{b_1}$ and $\overline{a_2} = \overline{b_2}$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$, i.e., If

$$a_1 \equiv b_1 \pmod{n}, \quad a_2 \equiv b_2 \pmod{n}$$

then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n}, \quad a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

Proof. Suppose $a_1 \equiv b_1 \pmod{n}$, i.e., $n \mid (a_1 - b_1)$. Then $a_1 = b_1 + sn$ for some integer s. Similarly, $a_2 \equiv b_2 \pmod{n}$ means $a_2 = b_2 + tn$ for some integer t.

Then $a_1 + a_2 = (b_1 + b_2) + (s+t)n$ so that $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, which shows that the sum of the residue classes is independent of the representatives chosen.

Similarly, $a_1 a_2 = (b_1 + sn)(b_2 + tn) = b_1 b_2 + (b_1 t + b_2 s + stn)n$ shows that $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ and so the product of the residue classes is also independent of the representatives chosen, completing the proof. □

An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists \overline{c} \in \mathbb{Z}/n\mathbb{Z}, \overline{a} \cdot \overline{c} = \overline{1}\}.$$

Proposition 3.1.3

$(\mathbb{Z}/n\mathbb{Z})^\times$ is also the collection of residue classes whose representatives are relatively prime to n:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}.$$

§3.2 Group Axioms

Definition 3.2.1

A **binary operation** $*$ on a set G is a function $* : G \times G \to G$. For any $a, b \in G$, we write $a * b$ for the image of (a, b) under $*$.

A binary operation $*$ on G is **associative** if, for any $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

A binary operation $*$ on G is **commutative** if, for any $a, b \in G$, $a * b = b * a$.

Example 3.2.2. The following are examples of binary operations.

- $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ respectively).
- $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ respectively).
- $-$ (usual subtraction) is a non-commutative binary operation on $\mathbb{Z}$.
- $-$ is not a binary operation on $\mathbb{Z}^+$ (nor $\mathbb{Q}^+$, $\mathbb{R}^+$) because for $a, b \in \mathbb{Z}^+$, with $a < b$, $a - b \notin \mathbb{Z}^+$; that is, $-$ does not map $\mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$.
- Taking the vector cross-product of two vectors in $\mathbb{R}^3$ is a binary operation which is not associative and not commutative.

Suppose that $*$ is a binary operation on G and $H \subseteq G$. If the restriction of $*$ to H is a binary operation on H, i.e. for all $a, b \in H$, $a * b \in H$, then H is said to be **closed** under $*$.

Remark. Observe that if $*$ is an associative (respectively, commutative) binary operation on G and $*$ is restricted to some $H \subseteq G$ is a binary operation on H, then $*$ is automatically associative (respectively, commutative) on H as well.

Definition 3.2.3 (Group)

A **group** is a pair $(G, *)$, where G is a set and $*$ is a binary operation on G satisfying the following group axioms:

(i) **(associativity)** for all $a, b, c \in G$, $a * (b * c) = (a * b) * c$.

(ii) **(identity)** there exists an identity element $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.

(iii) **(invertibility)** for all $a \in G$, there exists a unique inverse $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

G is **abelian** if the operation is commutative; it is **non-abelian** if otherwise.

Remark. The **closure** axiom (for all $a, b, c \in G$, $a * b \in G$) is implicitly implied, as a binary operation has to be closed under the set.

Notation. A group $(G, *)$ is usually simply denoted by G.

Notation. We abbreviate $a * b$ to just ab. Also, since the operation $*$ is associative, we can omit unnecessary parentheses: $(ab)c = a(bc) = abc$.

Notation. For any $a \in G$ and $n \in \mathbb{Z}^+$ we abbreviate $a^n = \underbrace{a \cdots a}_{n \text{ times}}$.

Example 3.2.4.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$ for all a.
- $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$, $\mathbb{Q}^+$, $\mathbb{R}^+$ are groups under $\times$ with $e = 1$ and $a^{-1} = \frac{1}{a}$ for all a. Note however that $\mathbb{Z} \setminus \{0\}$ is not a group under $\times$ because the element 2 (for instance) does not have an inverse in $\mathbb{Z} \setminus \{0\}$.
- For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under $+$.
- For $n \in \mathbb{Z}^+$, $(\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group under multiplication.

Definition 3.2.5 (Product group)
Let $(G, *_G)$ and $(H, *_H)$ be groups. Then the operation $*$ defined on $G \times H$ by

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

is a group operation. $(G \times H, *)$ is called the **product group** or the product of G and H.

Proof. As $*_G$ and $*_H$ are both associative binary operations then it follows easily from the definition to see that $*$ is also an associative binary operation on $G \times H$. We also note

$$e_{G\times H} = (e_G, e_H) \quad \text{and} \quad (g, h)^{-1} = (g^{-1}, h^{-1})$$

as for any $g \in G$, $h \in H$,

$$(e_G, e_H) * (g, h) = (g, h) = (g, h) * (e_G, e_H);$$

$$(g^{-1}, h^{-1}) * (g, h) = (e_G, e_H) = (g, h) * (g^{-1}, h^{-1}).$$

□

Proposition 3.2.6
Let G be a group. Then

(1) the identity of G is unique,

(2) for each $a \in G$, a^{-1} is unique,

(3) $(a^{-1})^{-1} = a$ for all $a \in G$,

(4) $(ab)^{-1} = b^{-1}a^{-1}$,

(5) for any $a_1, \ldots, a_n \in G$, $a_1 \cdots a_n$ is independent of how we arrange the parantheses (generalised associative law).

Proof.

(1) Let e_0 and e_1 both be identites, so $e_0 e_1 = e_0 = e_1$.

(2) Let c and c both be inverses to a and $e \in G$ the identity. Then $ab = e = ca$. Thus $c = ce = c(ab) = (ca)b = eb = b$.

(3) Clear.

(4) Let $c = (ab)^{-1}$ so that $(ab)c = e$, which gives $bc = a^{-1}$ and thus $c = b^{-1}a^{-1}$ by multiplying on the left.

(5) The result is trivial for $n = 1, 2, 3$. For all $k < n$ assume that any $a_1 \cdots a_k$ is independent of parantheses. Then

$$(a_1 \cdots a_n) = (a_1 \cdots a_k)(a_{k+1} \cdots a_n).$$

Then by assumption both are independent of parentheses since $k, n - k < n$ so by induction we are done.

□

Proposition 3.2.7 (Cancellation law)

Let $a, b \in G$. Then the equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, we can cancel on the left and right.

Proof. That $x = a^{-1}b$ is unique follows from the uniqueness of a^{-1} and the same for $y = ba^{-1}$. □

Definition 3.2.8 (Order)

For a group G and $x \in G$, the order of x is the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$; in this case x is said to be of order n.

If no positive power of x is the identity, the order of x is defined to be infinity, and x is said to be of infinite order.

Example 3.2.9.

- An element of a group has order 1 if and only if it is the identity.
- In the additive groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, every non-zero (i.e. non-identity) element has infinite order.
- In the multiplicative groups $\mathbb{R} \setminus \{0\}$ or $\mathbb{Q} \setminus \{0\}$, the element -1 has order 2 and all other non-identity elements have infinite order.
- In $\mathbb{Z}/9\mathbb{Z}$, the element $\overline{6}$ has order 3. (Recall that in an additive group, the powers of an element are integer multiples of the element.)
- In $(\mathbb{Z}/7\mathbb{Z})^\times$, the powers of the element $\overline{2}$ are $\overline{2}, \overline{4}, \overline{8} = \overline{1}$, the identity in this group, so 2 has order 3. Similarly, the element $\overline{3}$ has order 6, since 3^6 is the smallest positive power of 3 that is congruent to 1 mod 7.

Definition 3.2.10 (Group table)
Let $G = \{g_1, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The **group table** (multiplication table) of G is the $n \times n$ matrix whose (i, j)-entry is the group element $g_i g_j$.

For a finite group the multiplication table contains, in some sense, all the information about the group.

§3.3 Examples of Groups

An important family of groups is the dihedral groups.

Definition 3.3.1 (Dihedral group)
For $n \in \mathbb{Z}^+$, $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon.

Remark. Here "D" stands for "dihedral", meaning two-sided.

Let r be a rotation clockwise about the origin by $2\pi/n$ radians, let s be a reflection about the line of symmetry through the first labelled vertex and the origin.

Proposition 3.3.2

(1) $|r| = n$

(2) $|s| = 2$

(3) $s \neq r^i$ for all i

(4) $sr^i \neq sr^j$ for all $i \neq j$. Thus

$$D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$$

and we see that $|D_{2n}| = 2n$.

(5) $rs = sr^{-1}$

(6) $r^i s = sr^{-i}$

Proof.

(1) This is clear.

(2) So is this.

(3) And this.

(4) Just cancel on the left and use the fact that $|r| = n$. We assume that $i \not\equiv j \pmod{n}$.

(5) Omitted.

(6) By (5), this is true for $i = 1$. Assume it holds for $k < n$. Then $r^{k+1}s = r(r^k s) = rsr^{-k}$. Then $rs = sr^{-1}$ so $rsr^{-k} = sr^{-1}r^{-k} = sr^{-k-1}$ so we are done.

□

A presentation for the dihedral group with $2n$ elements is

$$D_{2n} = \{r, s \mid r^n = s^2 = 1, rs = sr^{-1}\}.$$

permutation group, subgroup, order of group, homomorphism and isomorphism

An important (if rather elementary) family of groups is the cyclic groups.

Definition 3.3.3 (Cyclic group)

A group G is called **cyclic** if there exists $g \in G$ such that

$$G = \{g^k \mid k \in \mathbb{Z}\}.$$

Such a g is called a **generator**.

As $g^i g^j = g^{i+j} = g^j g^i$ then cyclic groups are abelian.

Example 3.3.4. $\mathbb{Z}$ is cyclic and has generators 1 and -1.

Example 3.3.5. Let $n \geq 1$. The n-th cyclic group C_n is the group with elements

$$e, g, g_2, \ldots, g^{n-1}$$

which satisfy $g^n = e$. So given two elements in C_n we define

$$g_i g_j = \begin{cases} g^{i+j} & \text{if } 0 \leq i + j < n, \\ g^{i+j-n} & \text{if } n \leq i + j \leq 2n - 2. \end{cases}$$

Definition 3.3.6 (Subgroup)

Let G be a group. We say that a subset $H \subseteq G$ is a **subgroup** of G if the group operation $*$ restricts to make a group of H. That is H is a subgroup of G if:

(i) $e \in H$;

(ii) whenever $g_1, g_2 \in H$ then $g_1 g_2 \in H$.

(iii) whenever $g \in H$ then $g^{-1} \in H$.

Remark. Note that there is no need to require that associativity holds for products of elements in H as this follows from the associativity of products in G.

Example 3.3.7. The set of even integers is a subgroup of $\mathbb{Z}$; the set of odd integers is not a subgroup of $\mathbb{Z}$ because it does not even form a group, since it does not satisfy the closure axiom.

Definition 3.3.8 (Isomorphism)

An **isomorphism** $\phi : G \to H$ between two groups $(G, *_G)$ and $(H, *_H)$ is a bijection such that for any $g_1, g_2 \in G$ we have

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2).$$

Two groups are said to be **isomorphic** if there is an isomorphism between them, denoted by $G \cong H$.

Example 3.3.9 ($\mathbb{Z} \cong 10\mathbb{Z}$)**.** Consider the two groups

$$\mathbb{Z} = (\{\dots, -2, -1, 0, 1, 2, \dots\}, +)$$

and

$$10\mathbb{Z} = (\{\dots, -20, -10, 0, 10, 20, \dots\}, +).$$

These groups are "different", but only superficially so — you might even say they only differ in the names of the elements.

Formally, the map

$$\phi : \mathbb{Z} \to 10\mathbb{Z} \text{ by } x \mapsto 10x$$

is a bijection of the underlying sets which respects the group operation. In symbols,

$$\phi(x + y) = \phi(x) + \phi(y).$$

In other words, ϕ is a way of re-assigning names of the elements without changing the structure of the group.

§3.4 Permutation Groups

§3.5 More on Subgroups & Cyclic Groups

§3.6 Lagrange's Theorem

Definition 3.6.1 (Coset)

Let H be a subgroup of G.

Then the **left cosets** of H (or left H-cosets) are the sets

$$gH = \{gh \mid h \in H\}.$$

The **right cosets** of H (or right H-cosets) are the sets

$$Hg = \{hg \mid h \in H\}.$$

Two (left) cosets aH and bH are either disjoint or equal.

Since multiplication is injective, the cosets of H are the same size as H, and thus H partitions G into equal-sized parts.

Notation. We write G/H for the set of (left) cosets of H in G. The cardinality of G/H is called the **index** of H in G.

An important result relating the order of a group with the orders of its subgroups is Lagrange's theorem.

Theorem 3.6.2 (Lagrange's theorem)

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Groups of small order (up to order 8). Quaternions. Fermat–Euler theorem from the group-theoretic point of view.

Theorem 3.6.3 (Fermat's Little Theorem)

For every finite group G, for all $a \in G$, $a^{|G|} = e$.

Proof. Consider the subgroup H generated by a: $H = \{a^i \mid i \in \mathbb{Z}\}$. Since G is finite, the infinite sequence $a^0 = e, a^1, a^2, a^3, \ldots$ must repeat, say $a^i = a^j, i < j$. Let $k = j - i$. Multiplying both sides by $a^{-i} = (a^{-1})^i$, we get $a^{j-i} = a^k = e$. Suppose k is the least positive integer for which this holds. Then $H = \{a_0, a_1, a_2, \ldots, a^{k-1}\}$, and thus $|H| = k$. By Lagrange's Theorem, k divides $|G|$, so $a^{|G|} = (a^k)^{\frac{|G|}{k}} = e$. □

4 Ring Theory

§4.1 Definition

A ring is just a set where you can add, subtract, and multiply. In some rings you can divide, and in others you can't. There are many familiar examples of rings, the main ones falling into two camps: "number systems" and "functions".

Definition 4.1.1

A **ring** is a set R endowed with two binary operations, addition and multiplication, denoted $+$ and $\times$, with elements $0, 1 \in R$, which maps $+ : R \times R \to R$ and $\times : R \times R \to R$, subject to three axioms:

1. $(R, +)$ is an abelian group with identity 0.
2. $(R, \times)$ is a commutative semigroup, i.e. $a \times (b \times c) = (a \times b) \times c$, $a \times 1 = 1 \times a = a$, and $a \times b = b \times a$ for all $a, b, c \in R$.
3. Distributivity: $a \times (b + c) = a \times b + a \times c$ for all $a, b, c \in R$.

Example 4.1.2. Examples of rings:

- $\mathbb{Z}$: the integers $\ldots, -2, -1, 0, 1, 2, \ldots$ with usual addition and multiplication, form a ring. Note that we cannot always divide, since $1/2$ is no longer an integer.
- $2\mathbb{Z}$: the even integers $\ldots, -4, -2, 0, 2, 4, \ldots$
- $\mathbb{Z}[x]$: this is the set of polynomials whose coefficients are integers.

  It is an extension of $\mathbb{Z}$, in the sense that we allow all the integers, plus an "extra symbol" x, which we are allowed to multiply and add, giving rise to x^2, x^3, etc., as well as $2x$, $3x$, etc. Adding up various combinations of these gives all the possible integer polynomials.
- $\mathbb{Z}[x, y, z]$: polynomials in three variables with integer coefficients.

This is an extension of the previous ring. In fact you can continue adding variables to get larger and larger rings.

- $\mathbb{Z}/n\mathbb{Z}$: integers mod n.

  These are equivalence classes of the integers under the equivalence relation "congruence mod n". If we just think about addition (and subtraction), this is exactly the cyclic group of order n. However, when we call it a ring, it means we are also using the operation of multiplication.

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Ideals, homomorphisms, quotient rings, isomorphism theorems. Prime and maximal ideals. Fields. The characteristic of a field. Field of fractions of an integral domain. Factorization in rings; units, primes and irreducibles. Unique factorization in principal ideal domains, and in polynomial rings. Gauss' Lemma and Eisenstein's irreducibility criterion. Rings $\mathbb{Z}[\alpha]$ of algebraic integers as subsets of $\mathbb{C}$ and quotients of $\mathbb{Z}[x]$. Examples of Euclidean domains and uniqueness and non-uniqueness of factorization. Factorization in the ring of Gaussian integers; representation of integers as sums of two squares. Ideals in polynomial rings. Hilbert basis theorem

5 Field Theory

§5.1 Field Axioms

Definition 5.1.1

A **field** is a ring R that satisfies the following extra properties:

- $0 \neq 1$,
- every non-zero element of R has a multiplicative inverse (or reciprocal): if $r \in R$ and $r \neq 0$, then there exists $s \in R$ such that $rs = 1$; in other words: $R \setminus \{0\}$ is a group under $\times$ with identity 1.

Example 5.1.2. Examples and non-examples of fields:

- $\mathbb{Z}^+$ is not a field because, for example, 0 is not a positive integer, for no positive integer n is $-n$ a positive integer, for no positive integer n except 1 is n^{-1} a positive integer.
- $\mathbb{Z}$ is not a field because for an integer n, n^{-1} is not an integer unless $n = 1$ or $n = -1$.
- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

Proposition 5.1.3

Suppose K is a field and $X \subseteq K$ is a subset of K, with the following properties:

- $0, 1 \in X$,
- if $x, y \in X$, then $x + y, x - y, x \times y \in X$; and if $y \neq 0$, then $\frac{x}{y} \in X$.

Then X is a field.

Proof. By assumption, X is closed under addition and multiplication. Moreover, X is clearly a ring, because X inherits all the axioms from K. Finally, $0 \neq 1$, and if $0 \neq x \in X$, then $x^{-1} \in X$ by assumption. Therefore, X is a field. □ We call X a **subfield** of K.

6 Galois Theory

7 Category Theory

Part III

Linear Algebra

8 Linear Equations

§8.1 Systems of Linear Equations

Suppose F is a field. We consider tbe problem of finding n scalars (elements of F) $x_1, \ldots, x_n$ which satisfy the conditions

$$\begin{aligned} A_{11}x_1 + A_{12}x_2 + \cdots + A_{1n}x_n &= y_1 \\ A_{21}x_1 + A_{22}x_2 + \cdots + A_{2n}x_n &= y_2 \\ \vdots &= \vdots \\ A_{m1}x_1 + A_{m2}x_2 + \cdots + A_{mn}x_n &= y_m \end{aligned} \tag{8.1}$$

where $y_1, \ldots, y_m$ and $A_{ij}, 1 \le i \le m, 1 \le j \le n$ are given elements of F. We call 8.1 a **system of m linear equations in n unknowns**.

Any n-tuple $(x_1, \ldots, x_n)$ of elements of F which satisfies each of the equations in 8.1 is called a **solution** of the system.

If $y_1 = \cdots = y_m = 0$, we say that the system is **homogeneous**, or that each of the equations is homogeneous.

For the general system 8.1, suppose we select m scalars $c_1, \ldots, c_m$, multiply the j-th equation by c_j and then add up all the m equations. We obtain

$$(c_1A_{11} + \cdots + c_mA_{m1})x_1 + \cdots + (c_1A_{1n} + \cdots + c_mA_{mn})x_n = c_1y_1 + \cdots + c_my_m$$

which we call a **linear combination** of the equations in 8.1. Evidently, any soltion of the entire system of equations 8.1 will also be a solution of this new equation. This is the fundamental idea of the elimination process to find the solution(s) of a system of linear equations.

If we have another system of linear equations

$$\begin{aligned} B_{11}x_1 + B_{12}x_2 + \cdots + B_{1n}x_n &= z_1 \\ \vdots &= \vdots \\ B_{k1}x_1 + B_{k2}x_2 + \cdots + B_{kn}x_n &= z_k \end{aligned} \tag{8.2}$$

in which each of the k equations is a linear combination of the equations in 8.1, then every solution of 8.1 is a solution of this new system. Two systems of linear equations are **equivalent** if each equation in each system is a linear combination of the equations in the other system.

Theorem 8.1.1

Equivalent systems of linear equations have exactly the same equations.

§8.2 Matrices and Elementary Row Operations

Notive that there is no need to write the unknowns $x_1, \ldots, x_n$ since one actually computes only with the coefficients A_{ij} and scalars y_i. We abbreviate the system 8.1 as

$$AX = Y$$

where

$$A = \begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{m1} & \cdots & A_{mn} \end{bmatrix}, \quad X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad Y = \begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix}.$$

We call A the **matrix of coefficients** of the system. The **entries** of the matrix A are the scalars A_{ij}.

We wish now to consider operations on the rows of the matrix A which correspond to forming linear combinations of the equations in the system $AX = Y$. We restrict our attention to three **elementary row operations** on an $m \times n$ matrix A over the field F:

1.

§8.3 Row-Reduced Echelon Matrices

§8.4 Matrix Multiplication

§8.5 Invertible Matrices

Part IV

Real Analysis

9 Number Systems

§9.1 Natural Numbers $\mathbb{N}$

§9.1.1 Construction

In Peano's development, it is assumed that there is a set $\mathbb{N}$ (the natural numbers) of undefined objects with a distinguished element 1 such that

(i) 1 is a natural number; that is $1 \in \mathbb{N}$;

(ii) every $n \in \mathbb{N}$ has a successor $S(n) \in \mathbb{N}$;

(iii) for every n, $S(n) \neq 1$ (there is no number with 1 as successor)

(iv) if $S(n) = S(m)$, then $n = m$;

(v) if A is a set of natural numbers such that $1 \in A$ and

$$n \in A \implies S(n) \in A,$$

then A contains all natural numbers.

§9.1.2 Properties

Theorem 9.1.1 (Archimedean property of $\mathbb{N}$)
$\mathbb{N}$ is not bounded above.

Proof. Suppose, for a contradiction, that $\mathbb{N}$ is bounded above. Then $\mathbb{N}$ is non-empty and bounded above, so by completeness (of $\mathbb{R}$) $\mathbb{N}$ has a supremum.

By the Approximation property with $\varepsilon = \frac{1}{2}$, there is a natural number $n \in \mathbb{N}$ such that $\sup \mathbb{N} - \frac{1}{2} < n \leq \sup \mathbb{N}$.

Now $n + 1 \in \mathbb{N}$ and $n + 1 > \sup \mathbb{N}$. This is a contradiction. □

§9.2 Rational Numbers $\mathbb{Q}$

§9.2.1 Construction

Notation. $\mathbb{Z}' = \mathbb{Z} \setminus \{0\}$.

Definition 9.2.1

Let $\sim$ be the binary relation defined on $\mathbb{Z} \times \mathbb{Z}'$ by

$$(a, b) \sim (c, d) \iff ad = bc.$$

Proposition 9.2.2

$\sim$ is an equivalence on $\mathbb{Z} \times \mathbb{Z}'$.

Proof. We just check that $\sim$ is transitive. So suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then

$$ad = bc \tag{1}$$

$$cf = de \tag{2}$$

Multiplying (1) by f and (2) by b, we obtain

$$adf = bcf \tag{3}$$

$$bcf = bde \tag{4}$$

Hence $adf = bde$. Since $d \neq 0$, the Cancellation Law implies that $af = bc$. Hence $(a, b) \sim (e, f)$. □

Definition 9.2.3

The set of **rational numbers** is defined by

$$\mathbb{Q} \coloneqq \mathbb{Z} \times \mathbb{Z}' / \sim$$

i.e. $\mathbb{Q}$ is the set of $\sim$ equivalence classes.

Notation. For each $(a, b) \in \mathbb{Z} \times \mathbb{Z}'$, the corresponding equivalence class is denoted by $[(a, b)]$.

Next we want to define an addition operation on $\mathbb{Q}$. You may know that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

This suggests we make the following definition:

Definition 9.2.4

We define the binary operation $+_{\mathbb{Q}}$ on $\mathbb{Q}$ by

$$[(a, b)] +_{\mathbb{Q}} [(c, d)] = [(ad + bc, bd)].$$

Remark. Since $b \neq 0$ and $d \neq 0$, we have that $bd \neq 0$ and so $(ad + bc, bd) \in \mathbb{Z} \times \mathbb{Z}'$.

Lemma 9.2.5
$+_{\mathbb{Q}}$ is well-defined.

Theorem 9.2.6
For all $q, r, s \in \mathbb{Q}$, we have that

$$q +_{\mathbb{Q}} r = r +_{\mathbb{Q}} q$$

$$q +_{\mathbb{Q}} (r +_{\mathbb{Q}} s) = (q +_{\mathbb{Q}} r) +_{\mathbb{Q}} s.$$

Definition 9.2.7 (Identity element for $+_{\mathbb{Q}}$)
$0_{\mathbb{Q}} = [(0, 1)]$.

Proposition 9.2.8 (1) For any $q \in \mathbb{Q}$, $q +_{\mathbb{Q}} 0_{\mathbb{Q}} = q$.

(2) For any $q \in \mathbb{Q}$, there exists a unique $r \in \mathbb{Q}$ such that $q +_{\mathbb{Q}} r = 0_{\mathbb{Q}}$.

Proof.

(1) Let $q = [(a, b)]$. Then

$$\begin{aligned} q +_{\mathbb{Q}} 0Q &= [(a, b)] +_{\mathbb{Q}} [(0, 1)] \\ &= [(a \cdot 1 + 0 \cdot b, b \cdot 1)] \\ &= [(a, b)] \\ &= q. \end{aligned}$$

(2) To show that there exists at least one such element, consider $r = [(-a, b)]$. Then

$$\begin{aligned} q +_{\mathbb{Q}} r &= [(a, b)] +_{\mathbb{Q}} [(-a, b)] \\ &= [(ab + (-a)b, b^2)] \\ &= [(0, b^2)] \end{aligned}$$

Since $0 \cdot 1 = 0 \cdot b^2$, we have $(0, b^2) = (0, 1)$. Hence

$$\begin{aligned} q +_{\mathbb{Q}} r &= [(0, b^2)] \\ &= [(0, 1)] \\ &= 0_{\mathbb{Q}} \end{aligned}$$

As before, simple algebra shows that there exists at most one such element.

□

Definition 9.2.9

For any $q \in \mathbb{Q}$, $-q$ is the unique element of $\mathbb{Q}$ such that

$$q +_{\mathbb{Q}} (-q) = 0_{\mathbb{Q}}.$$

Definition 9.2.10

We define the binary operation $-_{\mathbb{Q}}$ on $\mathbb{Q}$ by

$$q -_{\mathbb{Q}} r = q +_{Q} Q(-r).$$

Next we want to define a multiplication operation on $\mathbb{Q}$. Note that

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

This suggests we make the following definition.

Definition 9.2.11

We define the binary operation $\cdot_{\mathbb{Q}}$ on $\mathbb{Q}$ by

$$[(a, b)] \cdot_{\mathbb{Q}} [(c, d)] = [(ac, bd)].$$

Remark. Since $b \neq 0$ and $d \neq 0$, we have that $bd \neq 0$ and so $(ac, bd) \in \mathbb{Z} \times \mathbb{Z}'$.

Lemma 9.2.12

$\cdot_{\mathbb{Z}}$ is well-defined.

Theorem 9.2.13

For all $q, r, s \in \mathbb{Q}$, we have that

$$q \cdot_{\mathbb{Q}} r = r \cdot_{\mathbb{Q}} q$$
$$(q \cdot_{\mathbb{Q}} r) \cdot_{\mathbb{Q}} s = q \cdot_{\mathbb{Q}} (r \cdot_{\mathbb{Q}} s)$$
$$q \cdot_{\mathbb{Q}} (r +_{\mathbb{Q}} s) = (q \cdot_{\mathbb{Q}} r) +_{\mathbb{Q}} (q \cdot_{\mathbb{Q}} s)$$

Definition 9.2.14 (Identity element for $\cdot_{\mathbb{Q}}$)

$1_{\mathbb{Q}} = [(1, 1)]$.

Theorem 9.2.15 (1) For all $q \in \mathbb{Q}$, $q \cdot_{\mathbb{Q}} 1_{\mathbb{Q}} = q$.

(2) For every $0_{\mathbb{Q}} \neq q \in \mathbb{Q}$, there exists a unique $r \in \mathbb{Q}$ such that $q \cdot_{\mathbb{Q}} r = 1_{\mathbb{Q}}$.

Proof.

(1) Let $q = [(a, b)]$. Then

$$q \cdot_{\mathbb{Q}} 1_{\mathbb{Q}}$$

□

Theorem 9.2.16

$\mathbb{Q}$ is an ordered set if $r < s$ is defined to mean that $s - r$ is a positive rational number.

§9.3 Real Numbers $\mathbb{R}$

§9.3.1 Construction: Dedekind cuts

We shall construct $\mathbb{R}$ from $\mathbb{Q}$.

Definition 9.3.1

A **Dedekind cut** $\alpha \subset \mathbb{Q}$ satisfies the following properties:

(i) $\alpha \neq \varnothing$, $\alpha \neq \mathbb{Q}$;

(ii) if $p \in \alpha$, $q \in \mathbb{Q}$ and $q < p$, then $q \in \alpha$;

(iii) if $p \in \alpha$, then $p < r$ for some $r \in \alpha$.

Note that (iii) simply says that α has no largest member; (ii) implies two facts which will be used freely:

- If $p \in \alpha$ and $q \notin \alpha$ then $p < q$.
- If $r \notin \alpha$ and $r < s$ then $s \notin \alpha$.

Example 9.3.2. Let $r \in \mathbb{Q}$ and define

$$\alpha_r \coloneqq \{p \in \mathbb{Q} \mid p < r\}.$$

We now check that this is indeed a Dedekind cut.

(1) $p = 1 + r \notin \alpha_r$ thus $\alpha_r \neq \mathbb{Q}$. $p = r - 1 \in \alpha_r$ thus $\alpha_r \neq \varnothing$.

(2) Suppose that $q \in \alpha_r$ and $q' < q$. Then $q' < q < r$ which implies that $q' < r$ thus $q' \in \alpha_r$.

(3) Suppose that $q \in \alpha_r$. Consider $\dfrac{q+r}{2} \in \mathbb{Q}$ and $q < \dfrac{q+r}{2} < r$. Thus $\dfrac{q+r}{2} \in \alpha_r$.

This example shows that every rational r corresponds to a Dedekind cut α_r.

Example 9.3.3. $\sqrt[3]{2}$ is not rational, but it is real. $\sqrt[3]{2}$ corresponds to the cut

$$\alpha = \{p \in \mathbb{Q} \mid p^3 < 2\}.$$

(1) Trivial.

(2) If $q < p$, by the monotonicity of the cubic function, this implies that $q^3 < p^3 < 2$ thus $q \in \alpha$.

(3) If $p \in \alpha$, consider $\left(p + \frac{1}{n}\right)^3 < 2$.

Definition 9.3.4

The set of real numbers, denoted by $\mathbb{R}$, is the set of all Dedekind cuts.

$$\mathbb{R} \coloneqq \{\alpha \mid \alpha \text{ is a Dedekind cut}\}$$

Proposition 9.3.5

$\mathbb{R}$ has an order.

Proof. We define $\alpha < \beta$ to mean that $\alpha \subset \beta$. Let us check if this is an order (check for transitivity and trichotomy).

(1) For $\alpha, \beta, \gamma \in \mathbb{R}$, if $\alpha < \beta$ and $\beta < \gamma$ it is clear that $\alpha < \gamma$. (A proper subset of a proper subset is a proper subset.)

(2) It is clear that at most one of the three relations

$$\alpha < \beta, \quad \alpha = \beta, \quad \beta < \alpha$$

can hold for any pair α, β.

To show that at least one holds, assume that the first two fail. Then α is not a subset of β. Hence there exists some $p \in \alpha$ with $p \in \beta$.

If $q \in \beta$, it follows that $q < p$ (since $p \notin \beta$), hence $q \in \alpha$, by (ii). Thus $\beta \subset \alpha$. Since $\beta \neq \alpha$, we conclude that $\beta < \alpha$.

Thus $\mathbb{R}$ is an ordered set. □

Proposition 9.3.6

The ordered set $\mathbb{R}$ has the least-upper-bound property.

Proof. Let $A \neq \varnothing$, $A \subset \mathbb{R}$. Assume that $\beta \in \mathbb{R}$ is an upper bound of A.

Define β to be the union of all $\alpha \in A$; in other words, $p \in \gamma$ if and only if $p \in \alpha$ for some $\alpha \in A$. We shall prove that $\gamma \in \mathbb{R}$ by checking the definition of Dedekind cuts:

(1) Since A is not empty, there exists an $\alpha_0 \in A$. This α_0 is not empty. Since $\alpha_0 \subset \gamma$, γ is not empty.

Next, $\gamma \subset \beta$ (since $\alpha \subset \beta$ for every $\alpha \in A$), and therefore $\gamma \neq \mathbb{Q}$.

(2) Pick $p \in \gamma$. Then $p \in \alpha_1$ for some $\alpha_1 \in A$. If $q < p$, then $q \in \alpha_1$, hence $q \in \gamma$.

(3) If $r \in \alpha_1$ is so chosen that $r > p$, we see that $r \in \gamma$ (since $\alpha_1 \subset \gamma$).

Next we prove that $\gamma = \sup A$.

(1) It is clear that $\alpha \leq \gamma$ for every $\alpha \in A$.

(2) Suppose $\delta < \gamma$. Then there is an $s \in \gamma$ and that $s \notin \delta$. Since $s \in \gamma$, $s \in \alpha$ for some $\alpha \in A$. Hence $\delta < \alpha$, and δ is not an upper bound of A.

□

Proposition 9.3.7

$\mathbb{R}$ is closed under addition.

Proof. Let $\alpha = (A, B)$, $\beta = (C, D)$, then $\alpha + \beta = (X, Y)$ where

$$X = \{a + c \mid a \in A, c \in C\}$$

To show that (X, Y) is a Dedekind cut, we simply need to check the conditions for Dedekind cuts.

- Property 1 is trivial.
- Property 2 is by definition.
- Property 3:

  Let $x, y \in X$ satisfy $x < y$, $y \in X$.

  Let $y = a + c$, $a \in A$, $c \in C$.

  Let $\varepsilon = y - x$.

  Let $a' = a - \dfrac{\varepsilon}{2}$, $c' = c - \dfrac{\varepsilon}{2}$.

  Then

  $$a' + c' = a + c - \varepsilon = x$$

  $a' < a, a \in A \implies a' \in A$. Similarly, $c' \in C$.
  $\therefore x = a' + c' \in X$.
- Property 4:

  $\forall a + c \in X, a \in A, c \in C$, $\exists a' \in A, c' \in C$ such that $a < a', c < c'$.

  $\therefore a' + c' \in X$ satisfies $a + c < a' + c'$.

□

We now prove that the set of real numbers satisfies the commutative, associative, and identity field axioms with respect to addition.

Proposition 9.3.8

Addition is commutative on $\mathbb{R}$: $\forall \alpha, \beta \in \mathbb{R}$,

$$\alpha + \beta = \beta + \alpha$$

Proof. We need to show that $\alpha + \beta \subseteq \beta + \alpha$ and $\beta + \alpha \subseteq \alpha + \beta$.

Let $r \in \alpha + \beta$. Then $r = a + b$ for $a \in \alpha$ and $b \in \beta$. Thus $r = b + a$ since $+$ is commutative on $\mathbb{Q}$. Hence $r \in \beta + \alpha$. Therefore $\alpha + \beta \subseteq \beta + \alpha$.

Similarly, $\beta + \alpha \subseteq \alpha + \beta$.

Therefore $\alpha + \beta = \beta + \alpha$. □

Proposition 9.3.9

Addition is associative on $\mathbb{R}$: $\forall \alpha, \beta, \gamma \in \mathbb{R}$,

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma.$$

Proof. Let $r \in \alpha + (\beta + \gamma)$. Then $r = a + (b + c)$ where $a \in \alpha, b \in \beta, c \in \gamma$. Thus $r = (a + b) + c$ by associativity of $+$ on $\mathbb{Q}$. Therefore $r \in (\alpha + \beta) + \gamma$, hence $\alpha + (\beta + \gamma) \subseteq (\alpha + \beta) + \gamma$.

Similarly, $(\alpha + \beta) + \gamma \subseteq \alpha + (\beta + \gamma)$. □

Proposition 9.3.10

Define $0^* \coloneqq \{p \in \mathbb{Q} \mid p < 0\}$. Then $\alpha + 0^* = \alpha$.

Proof. Let $r \in \alpha + 0^*$. Then $r = a + p$ for some $a \in \alpha, p \in 0^*$. Thus $r = a + p < a + 0 = a$ by ordering on $\mathbb{Q}$ and identity on $\mathbb{Q}$. Hence $\alpha + 0^* \subseteq \alpha$.

Let $r \in \alpha$. Then there exists $r' > p$ where $r' \in \alpha$. Thus $r - r' < 0$, so $r - r' \in 0^*$. We see that

$$r = \underbrace{r'}_{\in \alpha} + \underbrace{(r - r')}_{\in 0^*}.$$

Hence $\alpha \subseteq \alpha + 0*$. □

Exercise 23

Express $-\alpha$ in terms of α; show

$$\alpha + (-\alpha) = 0 = (-\alpha) + \alpha$$

Proof. We split this into two cases.

Case 1: α is a rational number, then $\alpha = (A, B)$ where $A = \{x \mid x < \alpha\}$, $B = \{x \mid x \geq \alpha\}$.

Let $-\alpha = (A', B')$, where $A' = \{x \mid x < -\alpha\}$, $B' = \{x \mid x \geq -\alpha\}$. We see that $\alpha + (-\alpha) \leq 0$ is obvious.

On the other hand, since $0 = (O, O')$, for any $\varepsilon < 0$ we have

$$\varepsilon = \left(\alpha + \frac{\varepsilon}{2}\right) + \left(-\alpha + \frac{\varepsilon}{2}\right) \in A + A'$$

Hence $\alpha + (-\alpha) = 0$.

Case 2: α is irrational, let $\alpha = (A, B)$ where B does not have a lowest value. Then $-B = \{-x \mid x \in B\}$ does not have a highest value.

We wish to define $-\alpha = (-B, -A)$, but first we need to show that this is well-defined by checking through all the conditions.

- Property 1: This is trivial.

- Property 2: Prove that $-A$ and B are disjoint.

  Note that $\forall x \in \mathbb{R}$, if $x = -y$, then exactly one out of $y \in A$ and $y \in B$ is true $\implies$ exactly one out of $x \in -B$ and $x \in -A$ is true.

- Property 3: Prove $-B$ is closed downwards.

  Suppose otherwise, that $x < y, y \in -B$ but $x \notin -B$. Then $-y \in B$, $-x \notin B$. Since A is the complement of B, $-y \notin A$, $-x \in A$. But $-y < -x$, which is a contradiction.

- Property 4 is already guaranteed by the irrationality of α.

All of these properties imply that the real numbers form a commutative group by addition. □

Negation

Given any set $X \subset \mathbb{R}$, let $-X$ denote the set of the negatives of those rational numbers. That is $x \in X$ if and only if $-x \in -X$.

If (A, B) is a Dedekind cut, then $-(A, B)$ is defined to be $(-B, -A)$.

This is pretty clearly a Dedekind cut. - proof

Signs

A Dedekind cut (A, B) is **positive** if $0 \in A$ and **negative** if $0 \in B$. If (A, B) is neither positive nor negative, then (A, B) is the cut representing 0.

If (A, B) is positive, then $-(A, B)$ is negative. Likewise, if (A, B) is negative, then $-(A, B)$ is positive. The cut (A, B) is non-negative if it is either positive or 0.

Multiplication

Let $\alpha = (A, B)$ and $\beta = (C, D)$ where α, β are both non-negative.

We define $\alpha \times \beta$ to be the pair (X, Y) where

X is the set of all products ac where $a \in A, c \in C$ and at least one of the two numbers is non-negative. Y is the set of all products bd where $b \in B, d \in D$.

§9.3.2 Properties

Theorem 9.3.11 ($\mathbb{R}$ is archimedian)

For any $x \in \mathbb{R}^+$ and $y \in \mathbb{R}^+$, there exists some $n \in \mathbb{Z}^+$ so that

$$n \cdot x > y.$$

Proof. In particular, if we take $x = 1$ from this theorem, we immediately get the following statement.

Proposition 9.3.12

For any $y \in \mathbb{R}$, there exists some positive integer n so that $n > y$.

We now give a proof of Proposition 9.3.12 directly without using Theorem 9.3.11, and then we prove Theorem 9.3.11 from Proposition 9.3.12. This shows that these two statements are in fact equivalent, though Proposition 9.3.12 looks much simpler.

Proof. Assume $n \in \mathbb{Z}^+$ does not exist; that is to say that the set of positive integers $\mathbb{Z}^+$ has an upper bound y. Then using the l.u.b. property of $\mathbb{R}$, $\sup \mathbb{Z}^+$ exists, which we denote by $x_0 \in \mathbb{R}$.

Now we look at $x_0 - 1$. This is not an upper bound by definition of x_0, which means there exists some $N \in \mathbb{Z}^+$ such that

$$x_0 - 1 < N.$$

Then it follows that $x_0 < N + 1$. Notice that $N + 1 \in \mathbb{Z}^+$. So this contradicts the assumption that x_0 is an upper bound.

Hence our original assumption cannot be true, and thus there exists $n \in \mathbb{Z}^+$ with $n > y$. □

For any $x \in \mathbb{R}^+$ and $y \in \mathbb{R}$, consider $y \cdot x^{-1} \in \mathbb{R}$. From Proposition 9.3.12, there exists some $n \in \mathbb{Z}^+$ such that

$$n > y \cdot x^{-1}.$$

Then this is equivalent to $n - yx^{-1} > 0$. Since $x > 0$, and $\mathbb{R}$ is an ordered field, we have

$$(n - y \cdot x^{-1}) \cdot x > 0.$$

This is equivalent to $n \cdot x > y$. □

Remark. The archimedian property guarantees that we can use decimals to represent real numbers.

Theorem 9.3.13 ($\mathbb{Q}$ is dense in $\mathbb{R}$)

For any $a, b \in \mathbb{R}$ with $a < b$, there exists some $x \in \mathbb{Q}$ such that $a < x < b$.

Proof. This means one can find some $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ so that

$$a < \frac{m}{n} < b,$$

which is further equivalent to finding $m \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ so that

$$an < m < bn.$$

Notice that $b - a > 0$, so by the archimedian property, there exists $n \in \mathbb{Z}^+$ so that

$$bn - an = (b - a)n > 1.$$

We now argue that there exists some integer between two real numbers, whenever their difference is larger than 1.

Lemma

For any $\alpha, \beta \in \mathbb{R}$ with $\beta - \alpha > 1$, there exists some integer m so that $\alpha < m < \beta$.

Proof. We prove this lemma by finding such m. First, using archimedian property of $\mathbb{R}$, we can find some integer $N > 0$ so that

$$-N < \alpha < \beta < N.$$

Then consider the integers which are smaller than N and greater than α, i.e., the set

$$A \coloneqq \{k \in \mathbb{Z} \mid a < k \leq N\}.$$

It is not empty since $N \in A$. Since this a subset of $\{-N+1, -N+2, \ldots, N-2, N-1, N\}$ which is a finite set, it contains only finite elements. We can pick the smallest one from it and denote it by m, i.e., $m \coloneqq \min A$. We claim this m is just the one we are looking for.

First since $m \in A$, $m > \alpha$. Then we only need to check $m < \beta$. If this is not true, i.e., $m \geq \beta$, then we consider $m - 1$. It follows

$$m - 1 \geq \beta - 1 \geq \alpha.$$

This contradicts the fact that m is the smallest integer which is greater than α.

Above all, we are done with the lemma. □

At last, apply the lemma to $\alpha = an$ and $\beta = bn$, we are done. □

Theorem 9.3.14 ($\mathbb{R}$ is closed under taking roots)

For every $y \in \mathbb{R}^+$ and every $n \in \mathbb{Z}^+$, there exists a unique $x \in \mathbb{R}^+$ so that $x^n = y$.

Proof. We first claim that such $x \in \mathbb{R}^+$, if exists, must be unique. Otherwise, assume that both $x_1, x_2 \in \mathbb{R}^+$ are solutions of the equation

$$x^n = y, \quad y \in \mathbb{R}^+, n \in \mathbb{Z}^+.$$

Assume now $x_1 < x_2$, then from the fact that $\mathbb{R}$ is an ordered field, we have $x_1^n < x_2^n$ (why?), a contradiction. Similarly, $x_1 > x_2$ also leads to a contradiction, and so $x_1 = x_2$.

Now we look for a solution for the equation. Consider a subset of $\mathbb{R}$ as

$$S \coloneqq \{a \in \mathbb{R}^+ \mid a^n < y\}.$$

Try to check that

(1) $S \neq \varnothing$;

(2) S has an upper bound.

Then using the fact that $\mathbb{R}$ has the l.u.b. property, $\sup S$ exists. Define it as x, clearly $x \in \mathbb{R}^+$. We show that x solves the equation. (The idea of the proof is similar to the proof of $\sup_{\mathbb{Q}}\{x \in \mathbb{Q} \mid x^2 \leq 2\}$ does not exist.)

First, we show that if $x^n < y$, then we can construct some $x_0 \in S$ which is greater than x, which says x is not an upper bound of S. So $x^n \geq y$.

Second, we show that if $x^n > y$, then we can find an upper bound of S which is smaller than x, which says that x is not the least upper bound. So $x^n \leq y$.

Above all, we must have $x^n = y$.

From now on, we use $y^{\frac{1}{n}}$ to denote the unique solution for the equation

$$x^n = y, \quad y \in \mathbb{R}^+, n \in \mathbb{Z}^+,$$

and call it the n-th real root of y. The property

$$(ab)^{\frac{1}{n}} = a^{\frac{1}{n}} \cdot b^{\frac{1}{n}}$$

immediately follows from the uniqueness of n-th real root. □

Theorem 9.3.15 (Completeness axiom for $\mathbb{R}$)

If non-empty $E \subset \mathbb{R}$ is bounded above, then E has a supremum.

Any set in the reals bounded from above/below must have a supremum/infimum.

Proof. We prove this using Dedekind cuts.

Let S be a real number set. We consider the rational number set $A = \{x \in \mathbb{Q} \mid \exists y \in S\}$. Set B is defined to be the complement of A in $\mathbb{Q}$.

We go through the definitions to check that $(A|B)$ is a Dedekind cut.

1. Since $S \neq \varnothing$, pick $y \in S$, then $[y] - 1$ is a real number smaller than some element in S, hence $[y] - 1 \in A$ and thus $A \neq \varnothing$.

   Since we're given that S is bounded, $\exists M > 0$ as the upper bound for S, thus $B \neq \varnothing$.

   (Note that an upper bound is simply a number that is bigger than anything from the set, and is not the supremum

2. We defined B to be the complement of A in $\mathbb{Q}$, so this condition is trivial.

3. For any $x, y \in A$, if $x < y$ and $y \in A$, then $\exists z \in S$ such that $y < z \implies x < z \implies x \in A$.

4. Suppose otherwise that $x \in A$ is the largest element in A, then $\exists y \in S$ such that $x < y$ We then pick a rational number z between x and y. Since we still have $z < y$, we have $z \in A$ but $z > x$, contradictory to z being the largest.

   Now there's actually an issue with the proof for property 4 here How exactly are we finding z?

   First $x \in \mathbb{Q}$. Then $y \in \mathbb{R}$ so we rewrite it as $y = (C|D)$ via definition.

   $x < y$ translates to the fact that $x \in C$.

   Since y is real, by definition we know that C must not have a largest element.

   In particular, x is not largest and we can pick $z \in C$ such that $z > x$. This is in fact the z that we need

Now that all the properties of a real number are validated, we may finally conclude that $\alpha = (A|B)$ is indeed a real number.

Now we need to show that $\alpha = \sup S$.

Let $x \in S$. If x is not the maximum value of S, i.e. $\exists y \in S, x < y$, then $x \in A$ and thus $x < \alpha$.

If x is the maximum value of S, then for any rational number $y < x$ we have $y \in A$, and for any rational number $y \geq x$ we have $y \in B$. Thus $x = (A|B) = \alpha$.

In conclusion, $x \leq \alpha$ for all $x \in S$.

For any upper bound x of S, since $\forall y \in S, x \geq y$ we have $x \in B$ and thus $x \geq \alpha$.

$\therefore \alpha$ is the smallest upper bound of S and thus $\sup S = \alpha$ exists. □

§9.3.3 Extended real number system

Definition 9.3.16

We add $\pm\infty$ to $\mathbb{R}$, and call the union $\mathbb{R} \cup \{\pm\infty\}$ the **extended real number system**. Now any non-empty set $E \subset \mathbb{R}$ has a supremum and infimum, since we can define

$$\sup E = +\infty, \quad \text{if } E \text{ has no upper bound in } \mathbb{R}$$

and

$$\inf E = -\infty, \quad \text{if } E \text{ has no lower bound in } \mathbb{R}.$$

The extended real number system does not form a field, but it is customary to make the following conventions:

(1) If x is real then

$$x + \infty = +\infty, \quad x - \infty = -\infty, \quad \frac{x}{+\infty} = \frac{x}{-\infty} = 0.$$

(2) If $x > 0$ then $x \cdot (+\infty) = +\infty$, $x \cdot (-\infty) = -\infty$.

(3) If $x < 0$ then $x \cdot (+\infty) = -\infty$, $x \cdot (-\infty) = +\infty$.

When it is desired to make the distinction between real numbers on the one hand and the symbols $+\infty$ and $-\infty$ on the other quite explicit, the former are called *finite*.

§9.4 Euclidean Plane $\mathbb{R}^2$

We consider the Cartesian product of $\mathbb{R}$ with $\mathbb{R}$; that is,

$$\mathbb{R}^2 \coloneqq \mathbb{R} \times \mathbb{R} \coloneqq \{(x_1, x_2) \mid x_1, x_2 \in \mathbb{R}\}.$$

Over $\mathbb{R}^2$, we can define operations

- Addition $+$: $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$;
- Scalar multiplication $\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$: $c \cdot (x_1, x_2) = (c \cdot x_1, c \cdot x_2)$.

This two operations make $\mathbb{R}^2$ a 2-dimensional vector space (linear space) over the real field $\mathbb{R}$. We also say $\mathbb{R}^2$ is a $\mathbb{R}$-linear space of real dimension 2. For example, $\{(1,0),(0,1)\}$ form a basis of $\mathbb{R}^2$.

Moreover, over the linear space $\mathbb{R}^2$, one can define an inner product as

$$\langle (x_1, x_2), (y_1, y_2) \rangle = x_1 y_1 + x_2 y_2.$$

The inner product induces a norm

$$|(x_1, x_2)| = \sqrt{\langle (x_1, x_2), (x_1, x_2) \rangle} = \sqrt{x_1^2 + x_2^2}.$$

From now on, we use $\vec{x}$ to denote (x_1, x_2).

Proposition 9.4.1

- $|\vec{x}| \geq 0$, where equality holds if and only if $\vec{x} = \vec{0}$.
- $|c \cdot \vec{x}| = |c||\vec{x}|$
- $|\vec{x} + \vec{y}| \leq |\vec{x}| + |\vec{y}|$
- $|\langle \vec{x}, \vec{y} \rangle| \leq |\vec{x}||\vec{y}|$

All constructions here can be easily generalised to any $\mathbb{R}^n$ with $n \in \mathbb{Z}^+$.

§9.5 Complex Numbers $\mathbb{C}$

Over $\mathbb{R}^2$, we can define a multiplication $\cdot$ as

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

If we identity $\mathbb{R}^2$ with

$$\mathbb{C} \coloneqq \{x + yi \mid x, y \in \mathbb{R}\}$$

via $(x, y) \mapsto x + yi$, then all structures defined above are induced to $\mathbb{C}$. In particular, the multiplication is induced to $\mathbb{C}$ via requiring $i^2 = -1$. A nontrivial fact is that $(\mathbb{C}, +, \cdot)$ is a field. A element in $\mathbb{C}$ is called a complex number. Usually, people prefer to use $z = x + yi$, $x, y \in \mathbb{R}$, to denote a complex number. Here x is called the real part of z and y is called the imaginary part of z. We use $|z|$ to denote its norm.

§9.6 Euclidean Spaces

For each positive integer n, let $\mathbb{R}^n$ be the set of all ordered n-tuples

$$\mathbf{x} = (x_1, x_2, \ldots, x_n),$$

where $x_1, \ldots, x_n$ are real numbers, called the *coordinates* of $\mathbf{x}$. The elements of $\mathbb{R}^n$ are called points, or vectors, especially when $n > 1$. We shall denote vectors by boldfaced letters.

Since $\mathbb{R}^n$ is a vector space (over $\mathbb{R}$), $\mathbb{R}^n$ has the following extra properties

- For any two vectors $\mathbf{x}$ and $\mathbf{y}$ we may perform addition:

  $$\mathbf{x} + \mathbf{y} = (x_1 + y_1, \ldots, x_n + y_n)$$

  Properties of addition:

  1. $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$
  2. $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$
  3. Zero vector $\mathbf{0} = (0, \ldots, 0)$ satisfies $\mathbf{x} + \mathbf{0} = \mathbf{0} + \mathbf{x} = \mathbf{x}$
  4. For any vector $\mathbf{x}$, its negative $-\mathbf{x}$ satisfies $\mathbf{x} + (-\mathbf{x}) = (-\mathbf{x}) + \mathbf{x} = \mathbf{0}$

- For any vector $\mathbf{x}$ and scalar $k \in \mathbb{R}$ we may perform scalar multiplication:

  $$k\mathbf{x} = (kx_1, \ldots, kx_n)$$

  Properties of scalar multiplication:

  1. $0 \cdot \mathbf{x} = \mathbf{0}, 1 \cdot \mathbf{x} = \mathbf{x}$
  2. $(kl)\mathbf{x} = k(l\mathbf{x}) = l(k\mathbf{x})$
  3. $k(\mathbf{x} + \mathbf{y}) = k\mathbf{x} + k\mathbf{y}$
  4. $(k + l)\mathbf{x} = k\mathbf{x} + l\mathbf{x}$

We define the **inner product** (or scalar product) of $\mathbf{x}$ and $\mathbf{y}$ by

$$\mathbf{x} \cdot \mathbf{y} \coloneqq \sum_{i=1}^{n} x_i y_i.$$

The Euclidean space builds upon the vector space $\mathbb{R}^n$; specifically speaking, it is $\mathbb{R}^n$ endowed with two extra notions:

- The **norm** of the Euclidean space $\|\cdot\|$ is a real-valued function $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$. Given a vector $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{R}^n$, the norm of $\mathbf{x}$ is defined as

  $$\|\mathbf{x}\| \coloneqq \sqrt{\mathbf{x} \cdot \mathbf{x}} = \sqrt{\sum_{i=1}^{n} x_i^2} = \sqrt{x_1^2 + \cdots + x_n^2}.$$

- The **metric** d of the Euclidean space is a real-valued function $d : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. Given two vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$, the distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$d(\mathbf{x}, \mathbf{y}) \coloneqq \|\mathbf{x} - \mathbf{y}\| = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}.$$

Remark. The norm is something like the length of the vector itself (distant to the origin); the metric refers to the distance function which measures the length between two points in $\mathbb{R}^n$ (determined by their positional vectors $\mathbf{x}$ and $\mathbf{y}$). Essentially, the metric is a much more general notion than the norm: the norm can only be defined on vector spaces; the metric can literally be defined on any set.

Norms are required to satisfy the following properties:

(1) (**positive definiteness**) for any vector $\mathbf{x}$, $\|\mathbf{x}\| \geq 0$, and equality holds if and only if $\mathbf{x} = \mathbf{0}$.

(2) (**absolute homogeneity**) for any vector $\mathbf{x}$ and scalar a, $\|a\mathbf{x}\| = |a|\|\mathbf{x}\|$.

(3) (**triangle inequality**) for any two vectors $\mathbf{x}$ and $\mathbf{y}$, $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$.

Metrics are required to satisfy the following properties:

(1) (**positive definiteness**) for any two elements $\mathbf{x}$ and $\mathbf{y}$, $d(\mathbf{x}, \mathbf{y}) \geq 0$, equality holds if and only if $\mathbf{x} = \mathbf{y}$.

(2) (**symmetry**) for any two elements $\mathbf{x}$ and $\mathbf{y}$, $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.

(3) (**triangle inequality**) for any three elements $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$, $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

Generally, if there is a norm $\|\cdot\|$ on some vector space, then this norm naturally determines a metric $d(x, y) = \|x - y\|$, which is precisely the case for Euclidean spaces.

Definition 9.6.1

$E \subset \mathbb{R}^n$ is **bounded** if there exists $M > 0$ such that $\|x\| \leq M$ for all $x \in E$.

Exercise 24

Given E and F in $\mathbb{R}^n$ and real number k, define

$$kE = \{kx \mid x \in E\}$$

$$E + F = \{x + y \mid x \in E, y \in F\}$$

(a) Show that if E is bounded, then kE is bounded;

(b) Show that if E and F are bounded, then $E + F$ is bounded.

Definition 9.6.2

The **diameter** of $E \subset \mathbb{R}^n$ is defined as

$$\operatorname{diam} E \coloneqq \sup_{x,y \in E} d(x,y).$$

Exercise 25

Find the diameter of the open unit ball in $\mathbb{R}^n$ given by

$$B = \{x \in \mathbb{R}^n \mid \|x\| < 1\}.$$

Solution. First note that

$$d(x,y) = \|x-y\| \le \|x\| + \|-y\| = \|x\| + \|y\| < 1 + 1 = 2.$$

On the other hand, for any $\varepsilon > 0$, we pick

$$x = \left(1 - \frac{\varepsilon}{4}, 0, \ldots, 0\right), \quad y = \left(-\left(1 - \frac{\varepsilon}{4}\right), 0, \ldots, 0\right).$$

Then $d(x,y) = 2 - \dfrac{\varepsilon}{2} > 2 - \varepsilon$.

Therefore $\operatorname{diam} B = 2$. □

Exercise 26

Given a set E in $\mathbb{R}^n$, show that E is bounded if and only if $\operatorname{diam} E < +\infty$.

Proof.

($\Longrightarrow$) If E is bounded, then there exists $M > 0$ such that $\|x\| \le M$ for all $x \in E$.

Thus for any $x, y \in E$,

$$d(x,y) = \|x-y\| \le \|x\| + \|y\| \le 2M.$$

Thus $\operatorname{diam} E = \sup d(x,y) \le 2M < +\infty$.

($\Longleftarrow$) Suppose that $\operatorname{diam} E = r$. Pick a random point $x \in E$, suppose that $\|x\| = R$.

Then for any other $y \in E$,

$$\|y\| = \|x + (y-x)\| \le \|x\| + \|y-x\| \le R + r.$$

Thus, by picking $M = R + r$, we obtain $\|y\| \le M$ for all $y \in E$, and we are done.

Remark. Basically you use x to confine E within a ball, which is then confined within an even bigger ball centered at the origin. □

Definition 9.6.3

The **distance between sets** $E \subset \mathbb{R}^n$ and $F \subset \mathbb{R}^n$ is defined as

$$d(E,F) \coloneqq \inf_{x \in E, y \in F} \|x-y\|.$$

Obviously $d(E, F) > 0$ implies that E and F are disjoint, but E and F may still be disjoint even if $d(E, F) = 0$. For example, the closed intervals $E = (-1, 0)$ and $F = (0, 1)$.

Exercise 27

Suppose that E and F are sets in $\mathbb{R}^n$ where E and F is finite. Prove that E and F are disjoint if and only if $d(E, F) > 0$.

10 Basic Topology

§10.1 Metric Space

Definition 10.1.1

A set X, whose elements we shall call *points*, is a **metric space** if for any two points $p, q \in X$ there is associated a real value function (called distance function or *metric*) $d : X \times X \to \mathbb{R}$ which satisfies the following properties:

(i) (**positive definitiveness**) $d(p,q) \geq 0$, where equality holds if and only if $x = y$;

(ii) (**symmetry**) $d(p,q) = d(q,p)$;

(iii) (**triangle inequality**) $d(p,q) \leq d(p,r) + d(r,q)$ for any $r \in X$.

Example 10.1.2. Take $X = \mathbb{R}^n$. Then each of the following functions define metrics on X.

$$d_1(x,y) = \sum_{i=1}^{n} |x_i - y_i|;$$

$$d_2(x,y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)}$$

$$d_\infty(x,y) = \max_{i \in \{1,2,\ldots,n\}} |x_i - y_i|.$$

These are called the ℓ^1-("ell one"), ℓ^2- (or Euclidean) and ℓ^∞-distances respectively. Of course, the Euclidean distance is the most familiar one.

The proof that each of d_1, d_2, d_∞ is a metric is mostly very routine, with the exception of proving that d_2, the Euclidean distance, satisfies the triangle inequality. To establish this, recall that the Euclidean norm $\|x\|_2$ of a vector $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ is

$$\|x\|_2 := \left(\sum_{i=1}^{n} {x_i}^2 \right)^{\frac{1}{2}} = \langle x, x \rangle^{\frac{1}{2}},$$

where the inner product is given by

$$\langle x, y\rangle \coloneqq \sum_{i=1}^{n} x_i y_i.$$

Then $d_2(x,y) = \|x-y\|_2$, and so the triangle inequality is the statement that

$$\|w-y\|_2 \le \|w-x\|_2 + \|x-y\|_2 .$$

This follows immediately by taking $u = w-x$ and $v = x-y$ in the following lemma.

Lemma 10.1.3

If $u, v \in \mathbb{R}^n$ then $\|u+v\|_2 \le \|u\|_2 + \|v\|_2$.

Proof. Since $\|u\|_2 \ge 0$ for all $u \in \mathbb{R}^n$, the desired inequality is equivalent to

$$\|u+v\|_2^2 \le \|u\|_2^2 + 2\|u\|_2\|v\|_2 + \|v\|_2^2 .$$

But since $\|u+v\|_2^2 = \langle u+v, u+v\rangle = \|u\|_2^2 + 2\langle u, v\rangle + \|v\|_2^2$, this inequality is immediate from the Cauchy–Schwarz inequality, that is to say the inequality $|\langle u, v\rangle| \le \|u\|_2\|v\|_2$. □

Example 10.1.4 (Discrete metric)**.** Let X be an arbitrary set. The **discrete metric** on a set X is defined as follows:

$$d(x,y) = \begin{cases} 1 & \text{if } x \neq y, \\ 0 & \text{if } x = y. \end{cases}$$

Exercise 28

Prove that this is indeed a metric.

A metric space (X, d) naturally induces a metric on any of its subsets.

Definition 10.1.5

For any $x \in X$, $r > 0$, the **open ball** centred at x with radius r is defined as

$$B_r(x) \coloneqq \{y \in X \mid d(x,y) < r\}.$$

Similarly, the **closed ball** centred at x with radius r is defined as

$$\bar{B}_r(x) \coloneqq \{y \in X \mid d(x,y) \le r\}.$$

The **punctured ball** is defined as

$$B_r(x) \setminus \{x\} = \{y \in X \mid 0 < d(x,y) < r\}.$$

Definition 10.1.6 (Neighbourhood)
A set $N \subset X$ is called a **neighbourhood** of $x \in X$ if it contains a ball $B_r(x)$ for some $r > 0$.

Example 10.1.7. An open (closed) ball in $\mathbb{R}$ is equivalent to a finite open (closed) interval, i.e. (a, b) ($[a, b]$), $a, b \in \mathbb{R}$.

Definition 10.1.8 (1) p is a **limit point** of E if every neighborhood of p contains $q \neq p$ such that $q \in E$:

$$\forall r > 0, \exists q \in E, q \neq p \text{ s.t. } q \in B_r(p).$$

The **induced set** of E, denoted by E', is the set of all limit points of E in X.

(2) p is an **isolated point** of E if it not a limit point of E.

(3) E is **closed** if every limit point of E is a point of E, i.e $\bar{E} = E$.
The **closure** of E, denoted by $\bar{E}$, is the union set $E \cup E'$.

(4) p is an **interior point** of E if there is a neighborhood N of p such that $N \subset E$:

$$\exists r > 0 \text{ s.t. } B_r(p) \subset E.$$

The **interior** of E, denoted by E°, is the set of all interior points in E:

$$E^\circ \coloneqq \{p \in X \mid \exists r > 0 \text{ s.t. } B_r(p) \subset E\}$$

A point x is an **exterior point** of A if it is an interior point of A^c.

(5) E is **open** if every point of E is an interior point of E, i.e. $E^\circ = E$.

(6) E is **perfect** if E is closed and if every point of E is a limit point of E.

(7) E is **bounded** if

$$\exists M \in \mathbb{R}, q \in X \text{ s.t. } \forall p \in E, d(p, q) < M.$$

The **boundary** of E, denoted by ∂E, is the set difference $\bar{E} \setminus E^\circ$.
p is a **boundary point** of E if $p \in \partial E$.
E is compact if it is a bounded closed set.

(8) E is **dense** in X if every point of X is a limit point of E, or a point of E (or both).
A subset $B \subset A$ is a dense subset of A if $\bar{B} = A$.
E is **nowhere dense** its closure has no interior, i.e. $(\bar{E})^\circ = \varnothing$.

Definition 10.1.9 (Open set)

E is **open** if it is a neighbourhood of each of its elements, i.e., for every $x \in E$ there exists some open ball $B_r(x) \subset E$ for some $r > 0$.

Proposition 10.1.10

Any open ball is open.

Proof. Assume $B_r(x)$ is an open ball in a metric space (X, d). Then for any point $y \in B_r(x)$, there is

$$d(y, x) < r.$$

Now we define $r' \coloneqq r - d(y, x)$, which is positive.

Consider the ball $B_{r'}(y)$. We shall show it lives in $B_r(x)$. For this, take any point $z \in B_{r'}(y)$. Using the triangle inequality of a metric, we have

$$\begin{aligned} d(z, x) &\leq d(z, y) + d(y, x) \\ &< r' + d(y, x) \\ &= r. \end{aligned}$$

Hence $z \in B_r(x)$, and $B_{r'}(y) \subset B_r(x)$. □

Proposition 10.1.11 (1) Both $\varnothing$ and X are open.

(2) If E_1, E_2 are open, then $E_1 \cap E_2$ is open.

(3) If E_i is open for $i \in I$, then $\bigcup_{i \in I} E_i$ is open.

An arbitrary union of open sets is open; a finite intersection of open sets is open.

Proof.

(1) Obvious by definition.

(2) Take a point $x \in E_1 \cap E_2$, we need to find an open ball with radius $r > 0$ such that $x \in B_r(x) \subset E_1 \cap E_2$.

To find such $r > 0$, notice that since both E_1 and E_2 are open, there are open balls

$$\begin{aligned} x \in B_{r_1}(x) \subset E_1 \\ x \in B_{r_2}(x) \subset E_2 \end{aligned}$$

Take $r \coloneqq \min\{r_1, r_2\}$. Then $B_r(x) \subset B_{r_1}(x) \subset E_1$ and $B_r(x) \subset B_{r_2}(x) \subset E_2$, and hence $B_r(x) \subset E_1 \cap E_2$.

(3) Take a point $x \in \bigcup_{i \in I} E_\alpha$, then we can assume x lives in some E_k, $k \in I$. Since E_k is open, take an open ball

$$B_r(x) \subset E_k.$$

It follows

$$B_r(x) \subset E_k \subset \bigcup_{i \in I} E_i.$$

Hence $\bigcup_{i \in I} E_i$ is open.

□

Example 10.1.12. We know $I_n \coloneqq \left(-\frac{1}{n}, \frac{1}{n}\right) \subset \mathbb{R}$ is open for any $n \in \mathbb{Z}^+$. However, $\bigcap_{n\in\mathbb{Z}^+} I_n = \{0\}$ is not open.

Definition 10.1.13 (Closed set)

E is **closed** if its complement E^c is open.

Example 10.1.14. The closed interval $[a, b]$, $a \le b$ is closed in $\mathbb{R}$.

Proposition 10.1.15

Any closed ball is closed.

Proof. To prove that $\bar{B}_r(x) = \{y \in X \mid d(x, y) \le r\}$ is closed, we need to show that its complement $\bar{B}_r(x)^c = \{y \in X \mid d(x, y) > r\}$ is open.

Let $z \in \bar{B}_r(x)^c$. Choose $r' > 0$ such that $r + r' < d(x, z)$; that is, $r' < d(x, z) - r$.

We claim that $B_{r'} \subseteq \bar{B}_r(x)^c$. Pick $y \in B_{r'}(z)$. Then $d(y, z) < r'$. But $r + d(y, z) < d(x, z)$ so $r < d(x, z) - d(y, z) \le d(x, y)$ by triangle inequality. Hence we have $r < d(x, y)$, thus $y \in \bar{B}_r(x)^c$. Therefore $\bar{B}_r(x)^c$ is open, so $\bar{B}_r(x)$ is closed. □

Proposition 10.1.16 (1) Both $\varnothing$ and X are closed.

(2) If E_1 and E_2 are closed, then $E_1 \cup E_2$ is closed.

(3) If E_i is closed for $i \in I$, then $\bigcap_{i\in I} E_i$ is closed.

An arbitrary intersection of closed sets is closed; a finite union of closed sets is closed.

Proof.

(1) It follows immediately from $\varnothing = X^c$ and $X = \varnothing^c$.

(2) It follows from above that

$$(E_1 \cup E_2)^c = {E_1}^c \cap {E_2}^c$$

is open (de Morgan's law applied), and hence $E_1 \cup E_2$ is closed.

(3) It follows from above that

$$\left(\bigcap_{i\in I} E_i\right)^c = \bigcup_{i\in I} {E_i}^c$$

is open (de Morgan's law applied), and hence $\bigcap_{i\in I} E_i$ is closed.

□

Example 10.1.17. Consider a sequence of closed sets $\left[-1+\frac{1}{n}, 1-\frac{1}{n}\right]$, $n \in \mathbb{Z}^+$, of $\mathbb{R}$. Take their union

$$\bigcup_{n\in\mathbb{Z}^+}\left[-1+\frac{1}{n}, 1-\frac{1}{n}\right] = (-1,1)$$

which is open, not closed.

Definition 10.1.18 (Limit point)

p is a **limit point** of E if every neighborhood of p contains $q \neq p$ such that $q \in E$:

$$\forall r > 0, \exists q \in E, q \neq p \text{ s.t. } q \in B_r(p).$$

The **induced set** of E, denoted by E', is the set of all limit points of E in X.

The **closure** of E, denoted by $\bar{E}$, is the union set $E \cup E'$.

Example 10.1.19.

- Consider the metric space $\mathbb{R}$, a and b are limit points $(a,b]$. The limit point set of $(a,b]$ is $[a,b]$, which is also the closure $(a,b]$.
- Consider the metric space $\mathbb{R}^2$. The limit point set of any open ball $B_r(x)$ is the closed ball $\bar{B}_r(x)$, which is also the closure of $B_r(x)$.
- Consider $\mathbb{Q} \subset \mathbb{R}$. $\mathbb{Q}' = \bar{\mathbb{Q}} = \mathbb{R}$.

Proposition 10.1.20

If p is a limit point of E, then every neighbourhood of p contains infinitely many points of E.

Proof. Prove by contradiction. Suppose there is a neighborhood $B_r(p)$ which contains only a finite number of points of E: $q_1, \ldots, q_n$, which are distinct from p. Define

$$r = \min_{1\leq m\leq n} d(p, q_m).$$

The minimum of a finite set of positive numbers is clearly positive, so that $r > 0$.

The neighborhood $B_r(p)$ contains no point $q \in E, q \neq p$ so that p is not a limit point of E, a contradiction. □

Corollary 10.1.21

A finite point set has no limit points.

Definition 10.1.22

E is called **dense** if $\bar{E} = X$.

Proposition 10.1.23 (1) A is a dense set in X if and only if A intersects with all open sets in X.

(2) If A is dense in X and B is dense in A, then B is dense in X.

(3) If A and B are dense in X where A is open, then $A \cap B$ is dense in X.

Proposition 10.1.24 (1) $\bar{E}$ is closed;

(2) $E = \bar{E}$ if and only if E is closed;

(3) $\bar{E} \subset F$ for every closed set $F \subset X$ such that $E \subset F$.

By (1) and (3), $\bar{E}$ is the *smallest* closed subset of X that contains E.

Proof.

(1)

(2)

(3)

□

Proposition 10.1.25 (1) E° is open.

(2) E is open if and only if $E = E^\circ$.

(3) If $G \subset E$ and G is open, then $G \subset E^\circ$.

Proof.

(1) If $p \in E^\circ$ then $B_r(p) \subset E$ for some $r > 0$ and if $q \in B_r(p)$ then by triangle inequality, $B_{r-d(p,q)}(q) \subset E$ so $B_r(p) \subset E^\circ$ and hence E° is open.

(2) Certainly if E is open then $E = E^\circ$ since for each $p \in E$ there exists $r > 0$ such that $B_r(p) \subset E$.

Conversely if $E^\circ = E$ then this holds for each $p \in E$ so E is open.

(3) If $G \subset E$ is open then for each $p \in G$ there exists $r > 0$ such that $B_r(p) \subset G$, hence $B_r(p) \subset E$ so $p \in E^\circ$ and it follows that $G \subset E^\circ$.

□

Proposition 10.1.26

The set of exterior points, $(A^c)^\circ$ is the same as $(\bar{A})^c$.

Proof.

$$\begin{aligned} x \in (A^c)^\circ &\iff \exists \varepsilon > 0 \text{ such that } B(x,\varepsilon) \subset A^c \\ &\iff B(x,\varepsilon) \cap A = \varnothing \\ &\iff x \notin A \text{ and } B_0(x,\varepsilon) \cap A = \varnothing \\ &\iff x \notin A \cup A' = \bar{A} \\ &\iff x \in (\bar{A}^c) \end{aligned}$$

□

Proposition 10.1.27 (1) A' is closed.

(2) $\bar{A}$ is closed, i.e. $\bar{\bar{A}} = \bar{A}$

Proof.

(1) In order to show that A' is closed, we need to show that if x is a limit point of A', then $x \in A'$, i.e. x is a limit point of A.

So we need to show that limit points of A' are always limit points of A: Let x be a limit point of A', then for all $\varepsilon > 0$, $B_0(x, \varepsilon/2)$ intersects with A' and we may pick $y \in B_0(x,\varepsilon/2) \cap A'$

Now here's the tricky part Since $y \in A'$, y is a limit point of A, hence $B_0(y, |y-x|)$ intersects with A and thus we may pick $z \in B_0(y, |y-x|) \cap A$.

We show that $z \in B_0(x,\varepsilon)$:

$$|z-x| \le |z-y| + |y-x| < 2|y-x| < \varepsilon,$$

hence $z \in B(x,\varepsilon)$.

$$|z-y| < |x-y|,$$

hence $z \neq x$

$\therefore z \in B_0(x,\varepsilon)$

(2)

□

Theorem 10.1.28 (Cantor's Intersection Theorem)

Given a decreasing sequence of compact sets $A_1 \supset A_2 \supset \cdots$, there exists a point $x \in \mathbb{R}^n$ such that x belongs to all A_i. In other words, $\bigcap_{i=1}^{\infty} A_i \neq \varnothing$. Moreover, if for all $i \in \mathbb{N}$ we have $\operatorname{diam} A_{i+1} \le c \cdot \operatorname{diam} A_k$ for some constant $c < 1$, then such a point must be unique, i.e. $\bigcap_{i=1}^{\infty} A_k = \{x\}$ for some $x \in \mathbb{R}^n$.

Theorem 10.1.29 (Heine–Borel Theorem)

A set $A \subset \mathbb{R}^n$ is compact if and only if every open covering has a finite subcover, i.e. for any family of open sets $\mathscr{U} = \{U_i\}_{i \in I}$ satisfying $A \subset \bigcup_{i \in I} U_i$, there exists $\{U_1, \ldots, U_n\} \subset \mathscr{U}$ such that $A \subset \bigcup_{i=1}^{n} U_i$.

Theorem 10.1.30 (Bolzano–Weierstrass Theorem)
Infinite bounded sets in $\mathbb{R}^n$ must contain limit points.

We will follow a very specific sequence of steps to prove these three theorems:

(a) Cantor Intersection for $n = 1$

(b) Bolzano–Weierstrass for $n = 1$

(c) Bolzano–Weierstrass for general n

(d) Cantor Intersection for general n

(e) Heine–Borel for general n

Proof.

(a) Suppose that there is a decreasing sequence of compact sets $A_1, A_2, \ldots$ in the real numbers

Since A_k are bounded, we may let $a_k = \inf A_k$ Also since A_k are closed, $a_k \in A_k$

Note that since A_k is a decreasing sequence of sets we have $a_1 \leq a_2 \leq \ldots$

Also, whenever we have $n > k$, we have $a_n \in A_n$, but $A_n \subset A_k$ and thus $a_n \in A_k$.

Let $b_1 = \sup A_1$, then $a_k \in A_1$ and thus $a_k \leq b_1$ for all k.

This tells us that the sequence $\{a_k\}$ is bounded above, and thus we may let $a = \sup a_k$.

Our goal is to show that the number a appears in all A_k, thus showing that the entire intersection $\bigcap A_k$ contains a and thus must be non-empty.

Now we split this in two cases, which asks whether a is simply made from isolated points, or if it is actually some nontrivial point obtained from the boundaries of A_k

Case 1: $a_k = a$ for some k In this case we see that $a_k \leq a_n \leq a$ for all $n > k$ and thus $a_n = a$ in this case, therefore a is an element in A_n for all n

In this case you can imagine that there is a possibility where a is an isolated minimum point of A_n which stays there forever in the decreasing sequence of sets

Case 2: $a_k < a$ for all k; in this case we see that a is the limit point of the increasing sequence $\{a_k\}$

Exercise 1: Show that a is a limit point of each A_k.

Note that a_n is in A_k for each $n > k$, and since $a = \sup\{a_k\}$ where a_k is increasing, we can actually show that a is a limit point of $\{a_n \mid n \leq k\}$: For every $\varepsilon > 0$, we pick n_0 such that $0 < a - a_{n_0} < \varepsilon$ Pick $n\prime > \max\{k, n_0\}$, then $a_{n'} \geq a_{n_0}$ and so

$$0 < a - a_n\prime \leq a_{n_0} < \varepsilon$$

This shows that there exists a'_n in $B_0(a, \varepsilon) \cap \{a_n \mid n > k\}$ for all ε, and so a is a limit point of $\{a_n \mid n > k\}$.

Now since $\{a_n | n \geq k\}$ is a subset of A_k we also see that a is a limit point of A_k Finally, since A_k is closed, we conclude that a is in A_k for all k, and we are done

Wait hold on, I forgot about the second part

Now we consider a decreasing sequence of compact sets $A_1, A_2, \ldots$ such that $\operatorname{diam} A_{k+1} \leq c \operatorname{diam} A_k$ for $c < 1$.

Suppose otherwise that there exists x, y in $\bigcap A_k$

You can imagine that this will form a fixed distance between two points, and thus there is a constant positive lower bound for the diameters:

$$\operatorname{diam} A_k \geq |x - y| > 0 \forall k$$

But this cannot be true because $\operatorname{diam} A_{k+1} \leq c \operatorname{diam} A_k$ and so the diameter is controlled by a decreasing geometric sequence:

$$\operatorname{diam} A_{k+1} \leq c^k \operatorname{diam} A_1$$

So we can simply pick a natural number k such that

$$k > \log_c \frac{|x - y|}{\operatorname{diam} A_1}$$

(b) We consider an infinite bounded set A in the real numbers. Since A is bounded, we can pick a closed interval $[a_1, b_1]$ containing A.

We then perform a series of binary cuts: Consider the two halves of $[a_1, b_1]$. We know that at least one of these two must contain infinitely many elements in A, otherwise A cannot be infinite. We pick this half of the interval and denote it by $[a_2, b_2]$. We continue this to pick a decreasing sequence of closed intervals $[a_n, b_n]$.

Now $\operatorname{diam}[a_{n+1}, b_{n+1}] = \frac{1}{2} \operatorname{diam}[a_n, b_n]$, so by the Cantor Intersection Theorem, there exists a unique real number c in the intersection $\bigcap [a_n, b_n]$.

We show that this c is in fact a limit point of A.

For any $\varepsilon > 0$, we need to show that $B_0(c, \varepsilon) \cap A \neq \varnothing$, i.e. we need to find an element $x \neq c$ in A that is less than ε apart from c.

We then realize that we can simply exploit the decreasing sequence $[a_n, b_n]$ Since $\operatorname{diam}[a_n, b_n]$ is controlled by a decreasing sequence:

$$\operatorname{diam}[a_{n+1}, b_{n+1}] \leq 1/2^n \operatorname{diam}[a_1, b_1]$$

We take a sufficiently large n so that $b_n - a_n < \varepsilon$ Since c is in $[a_n, b_n]$, for all x in $[a_n, b_n]$ we have $|x - c| \leq b_n - a_n < \varepsilon$ and therefore $[a_n, b_n]$ is within $B(c, \varepsilon)$.

Here's the funny part: $[a_n, b_n]$ contains infinitely many elements of A, so it must contain at least one element in A that is not c.

Therefore this element $x \neq c$ is in $B_0(c, \varepsilon)$.

(c) Now we have an infinte bounded set A in $\mathbb{R}^n$

The idea here is to consecutively come up with better and better sequences of points in A. We denote x_i to be the i-th coordinate in $\mathbb{R}^n$.

Our first wish is to pick some elements in A so that they sort of converge at x_1.

Because such considerations of 'restricting to a single coordinate' is important here, we define the projection map to the i-th coordinate by

$$f_i(x_1, \dots, x_n) = x_i$$

So, we look at $f_i(A)$ and try to apply BW for the case where $n = 1$.

However, the problem is that $f_i(A)$ need not be infinite. For example, the set $\{(0,0),(0,1),(0,2),\dots\}$ projected onto the first coordinate is simply $\{0\}$.

This forces us to consider two cases

Exercise 2: Show that $f_i(A)$ is bounded This is simple 1. $f_1(A)$ is infinite, then we can apply BW(n=1) to find a real number c_1 which is a limit point in $f_1(A)$

Here we can construct a sequence of points

$$\{x^{(1),1}, x^{(1),2}, ...\}$$

so that their first coordinates satisfy

$$|x_1^{(1),n} - c_1| < 1/n$$

for all natural number n (I know this notation is cumbersome but the problem is that we need multiple sequences for this proof)

2. $f_1(A)$ is finite, then by the Pigeonhole Principle there exists a real number c_1 such that its preimage $f_1^{-1}(c_1)$ in A is infinite

In this case we can randomly pick a sequence $\{x^{(1),1}, x^{(1),2}, \dots\}$ in A so that their first coordinate is equal to c_1

I forgot to mention something that is implied, but we actually do have the need to emphasize that the sequence $\{x^{(1),1}, x^{(1),2}, \dots\}$ can be chosen to contain mutually distinct entries

Now that we have a sequence that behaves nice on the first coordinate, we may then move on to the second coordinate

Let $A_1 = \{x^{(1),1}, x^{(1),2}, \dots\}$ We again consider $f_2(A_1)$ in two cases, infinite or finite

In any case, we are able to find a subsequence $\{x^{(2),1}, x^{(2),2}, \dots\}$, where $x^{(2),k} = x^{(1),n_k}$ for some strictly increasing sequence of natural numbers n_k

So that, for the limit point/point with infinite preimage c_2, this sequence satisfies

$$|f_2(x^{(2),n}) - c_2| < \frac{1}{n}$$

Note that the property we have for the second case (we in fact have $f_2(x^{(2),n}) = c_2$) is just a better version of this.

Now, take note that picking this subsequence does no harm whatsoever towards the first coordinate (if anything it would turn out to be better) since

$$|f_1(x^{(2),k}) - c_1| = |f_1(x^{(1),n_k} - c_1| < \frac{1}{n_k} \leq \frac{1}{k}$$

($n_1 < \cdots < n_k$ is a strictly increasing sequence of natural numbers so $n_k \geq k$)

This continues on until we obtain a sequence of points $\{x^{(n),1}, x^{(n),2}, \dots\}$ in A so that

$$|f_i(x^{(n),k} - c_i| < \frac{1}{k} \quad \forall i, k$$

As we can see, the point $c = (c_1, \dots, c_n)$ is in fact a limit point of A as we can always choose a big enough k so that $x^{(n),k}$ is in $B(c, \varepsilon) \cap A$.

Since $\{x^{(n),k}\}$ was always chosen to be a sequence of distinct entries, there is no danger for this sequence to always be c, and so c must be a limit point of A.

(d) We may now return to the general case of Cantor.

Suppose that there is a sequence of decreasing compact sets $A_1, A_2, \dots$ in $\mathbb{R}^n$. Note that every point is contained in A_1, so boundedness will never be an issue here.

Since A_k are all nonempty, we can simply pick any element a_k from A_k.

For the uncannily specific case that there are only finitely many $\{a_k\}$ chosen, we simply note that, again by Pigeonhole Principle, one of the a_k appears infinitely often; thus for each A_n we simply pick $n_k > n$ so that A_{n_k} contains a_k, then a_k is in A_{n_k} which is a subset of A_n.

Otherwise, we can then note that $\{a_k\}$ is an infinite bounded set of points, so there must exist a limit point a of $\{a_k\}$.

We can now see that a is always an element of A_k: Using the same technique as Exercise 1, we see that a is a limit point of $\{a_n \mid n > k\}$ and so is a limit point of A_k, therefore a is in A_k as A_k is closed.

This proves the first part of the statement The second part is completely identical to the second part of the $n = 1$ case so we don't need to waste our time there either

(e) We now consider a compact set A with some open covering $\mathscr{U}$.

This theorem is proved by contradiction: Suppose otherwise that set A cannot be covered by any finite collection of open sets in $\mathscr{U}$

Since A is compact, we may enclose it in a closed cube Q_1 (whose edges are parallel to the axes)

Now, for each step, we partition Q into 2^n cubes by cutting it in half from each direction.

Then, starting from Q_1, there must exist one of these smaller cubes, denoted by Q_2, such that $A \cap Q_2$ cannot be covered by a finite collection of open sets in $\mathscr{U}$. Otherwise, if each $A \cap Q$ has a finite cover, then we simply collect all of these open sets together to form a finite cover of A, which violates our assumption.

We continue on to partition Q_n and pick Q_{n+1} so that A_{n+1} has no finite cover (denote $A_n = A \cap Q_n$).

Note that A and Q_n are both compact, so A_n is compact Also we see that there is a decreasing sequence $A_1, A_2, \ldots$ (we can't exactly obtain a relation between $\operatorname{diam} A_n$ and $\operatorname{diam} A_{n+1}$ here)

By Cantor Intersection Theorem we can always find a point x in A located in the intersection $\bigcap A_k$.

Now, since $\mathscr{U}$ is an open covering of A, there exists an open set U in $\mathscr{U}$ such that $x \in U$.

The final key step is to exploit the sequence of decreasing cubes Q_n. So even though there isn't a clear cut way to control the sizes of $\operatorname{diam} A_n$, we do in fact have the property that $\operatorname{diam} Q_{n+1} = \frac{1}{2^n} \operatorname{diam} Q_1$.

Therefore, by picking a sufficiently large n, we can obtain Q_n that is contained in U.

But this is a contradiction. This is because we've specifically chosen the sequence A_n to be sets that do not possess any finite cover $\{U_1, ..., U_n\}$ in $\mathscr{U}$. But here A_n simply would have a one-element cover $\{U\}$.

This completes our proof.

□

Proposition 10.1.31

Suppose $Y \subset X$. A subset E of Y is open relative to Y if and only if $E = Y \cap G$ for some open subset G of X.

Proof.

($\Longrightarrow$) Suppose E is open relative to Y. Thus for each $p \in E$ there exists $r_p > 0$ such that $d(p, q) < r_p$, $q \in Y$ imply $q \in E$.

Let V_p be the set of all $q \in X$ such that $d(p, q) < r_p$, and define

$$G := \bigcup_{p \in E} V_p.$$

Then G is an open subset of X, by

($\Longleftarrow$) □

§10.2 Compactness

Definition 10.2.1

By an **open cover** of a set E in a metric space X we mean a collection $\{G_i \mid i \in I\}$ of open subsets of X such that

$$E \subset \bigcup_{i \in I} G_i.$$

For $I' \subset I$, if the subcollection $\{G_i \mid i \in I'\}$ is also an open cover of S; that is,

$$E \subset \bigcup_{i \in I'} G_\alpha,$$

then $\{G_i \mid i \in I'\}$ is called a **subcover**. If moreover, I' is finite, then it is called a **finite subcover**.

Definition 10.2.2 (Compactness)

A subset K of metric space X is said to be **compact** if every open cover of K contains a finite subcover.

Proposition 10.2.3

Suppose $K \subset Y \subset X$. Then K is compact relative to X if and only if K is compact relative to Y.

Proof.

($\Longrightarrow$) Suppose K is compact relative to X. Let $\{V_i \mid i \in I\}$ be a collection of sets open relative to Y, such that $K \subset \bigcup_{i \in I} V_i$. By □

sequential compactness A set K is compact if and only if every sequence of points in K has a subsequence that converges to a point in K.

Any continuous function defined on a compact set is bounded.

extreme value theorem

§10.3 Perfect Sets

§10.4 Connected Sets

Definition 10.4.1

Two subsets A and B of a metric space X are said to be **separated** if both $A \cap \bar{B}$ and $\bar{A} \cap B$ are empty, i.e. no point of A lies in the closure of B and no point of B lies in the closure of A.

A set $E \subset X$ is said to be **connected** if E is not a union of two non-empty separated sets.

Remark. Separated sets are of course disjoint, but disjoint sets need not be separated. For example, the interval $[0,1]$ and the segment $(1,2)$ are not separated, since 1 is a limit point of $(1,2)$. However, the segments $(0,1)$ and $(1,2)$ are separated.

The connected subsets of the line have a particularly simple structure:

Proposition 10.4.2

A subset $E \subset \mathbb{R}^1$ is connected if and only if it has the following property: if $x, y \in E$ and $x < z < y$, then $z \in E$.

Proof. ($\Longleftarrow$) If there exists $x, y \in E$ and some $z \in (x,y)$ such that $z \notin E$, then $E = A_z \cup B_z$ where

$$A_z = E \cap (-\infty, z), \quad B_z = E \cap (z, \infty).$$

Since $x \in A_z$ and $y \in B_z$, A and B are non-empty. Since $A_z \subset (-\infty, z)$ and $B_z \subset (z, \infty)$, they are separated. Hence E is not connected.

($\Longrightarrow$) Suppose E is not connecetd. Then there are non-empty separated sets A and B such that $A \cup B = E$. Pick $x \in A$, $y \in B$, and WLOG assume that $x < y$. Define

$$z \coloneqq \sup(A \cap [x,y].)$$

By $\square$

11 Numerical Sequences and Series

§11.1 Convergent Sequences

Definition 11.1.1

A sequence $\{x_n\}$ in metric space X **converges** if there exists some $x \in X$ such that $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$, $\forall n \geq N$, $d(x_n, x) < \varepsilon$.

We call x the **limit** of $\{x_n\}$, and write $x_n \to x$, or

$$\lim_{n\to\infty} x_n = x.$$

If $\{x_n\}$ does not converge, it is said to **diverge**.

Remark. Take note of the use of logical statements:

- ε is independent, so it is literally for all $\varepsilon > 0$.
- N is dependent on ε; if ε is very small we would expect the sequence $\{x_n\}$ to get close enough to x further down the line.
- The order of the quantifiers matters.

Example 11.1.2. $\dfrac{1}{n} \to 0$ as $n \to \infty$. The proof is fairly straighforward: $\forall \varepsilon > 0$, pick $N = \frac{1}{\varepsilon} + 1$. Then $\forall n > N$,

$$\frac{1}{n} < \frac{1}{N} = \frac{1}{\frac{1}{\varepsilon} + 1} < \frac{1}{\frac{1}{\varepsilon}} = \varepsilon.$$

We now outline some important properties of convergent sequences in metric spaces.

Proposition 11.1.3

Let $\{x_n\}$ be a sequence in metric space X.

(1) $\{x_n\}$ converges to $x \in X$ if and only every neighbourhood of x contains x_n for all but finitely many n.

(2) (uniqueness of the limit) If $x \in X$, $x' \in X$, and if $\{x_n\}$ converges to x and to x', then $x' = x$.

(3) (boundedness of convergent sequences) If $\{x_n\}$ converges, then $\{x_n\}$ is bounded.

(4) For $E \subset X$, x is a limit point of E, if and only if there exists a sequence $\{x_n\}$ in $E \setminus \{x\}$ such that $x_n \to x$.

Proof.

(1) ($\Longrightarrow$) Suppose $x_n \to x$. We want to prove that any neighbourhood U of x eventually contains all x_n.

Since U is a neighbourhood of x, pick a ball $B_\varepsilon(x) \subset U$. Corresponding to this ε, there exists $N \in \mathbb{N}$ such that $n \geq N$ implies $d(x_n, x) < \varepsilon$. Thus $n \geq N$ implies $x_n \in U$.

($\Longleftarrow$) Suppose every neighbourhood of x contains all but finitely many of the x_n. Fix $\varepsilon > 0$, pick a ball $B_\varepsilon(x)$. Since $B_\varepsilon(x)$ is a neighbourhood of x, it will also eventually contain all x_n. By assumption, there eists $N \in \mathbb{N}$ such that $x_n \in B_\varepsilon(x)$ if $n \geq N$. Thus $d(x_n, x) < \varepsilon$ if $n \geq N$, hence $x_n \to x$.

(2) Let $\varepsilon > 0$ be given. There exists $N, N' \in \mathbb{N}$ such that

$$n \geq N \implies d(x_n, x) < \frac{\varepsilon}{2}$$

and

$$n \geq N' \implies d(x_n, x') < \frac{\varepsilon}{2}.$$

Take $N_1 \coloneqq \max\{N, N'\}$. Hence if $n \geq N_1$ we have $d(x_n, x) < \frac{\varepsilon}{2}$ and $d(x_n, x') < \frac{\varepsilon}{2}$ at the same time. By triangle inequality,

$$d(x, x') \leq d(x, x_n) + d(x_n, x') < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Since ε was arbitrary (i.e. holds for all $\varepsilon > 0$), we must have $d(x, x') = 0$ and thus $x = x'$.

(3) Suppose $x_n \to x$. Then there exists $N \in \mathbb{N}$ such that $n > N$ implies $d(x_n, x) < 1$. Take

$$r \coloneqq \max\{1, d(x_1, x), \ldots, d(x_N, x)\}.$$

Then $d(x_n, x) \leq r$ for $n = 1, 2, \ldots, N$, so $\{x_n\}$ is in $B_r(x)$.

(4) ($\Longrightarrow$) If x is a limit point, then for all $\varepsilon > 0$, $B_\varepsilon \setminus \{x\}(x)$ contains points in E. We then construct such a sequence $\{x_n\}$ in $E \setminus \{x\}$: pick any $x_n \in E$ so that x_n is contained in $B_{\frac{1}{n}} \setminus \{x\}(x)$. Then it is easy to show that $\{x_n\}$ is a sequence in $E \setminus \{x\}$ which converges to x.

($\Longleftarrow$) Suppose that there exists a sequence $\{x_n\}$ in $E \setminus \{x\}$ such that $x_n \to x$. We wish to show that $B_\varepsilon \setminus \{x\}(x)$ contains points in E for all $\varepsilon > 0$.

Since $\{x_n\}$ converges to x, for all $\varepsilon > 0$ the sequence is eventually contained in $B_\varepsilon(x)$. However because we have the precondition that $\{x_n\}$ has to be in $E \setminus \{x\}$, the sequence is in fact eventually contained in $B_\varepsilon \setminus \{x\}(x)$.

□

§11.2 Subsequences

Definition 11.2.1

Given a sequence $\{x_n\}$, consider a sequence $\{n_k\}$ of positive integers such that $n_1 < n_2 < \dots$. Then $\{x_{n_i}\}$ is called a **subsequence** of $\{x_n\}$. If $\{x_{n_i}\}$ converges, its limit is called a **subsequential limit** of $\{x_n\}$.

Proposition 11.2.2

$\{x_n\}$ converges to x if and only if every subsequence of $\{x_n\}$ converges to x.

Proof. ($\Longrightarrow$) Every subsequence of $\{x_n\}$ can be written in the form $\{x_{n_i}\}$ where $n_1 < n_2 < \dots$ is a strictly increasing sequence of positive integers.

Intuitively, if every neighbourhood of x eventually contains all x_n, then since $\{x_{n_i}\}$ is a subset of $\{x_n\}$ they should all be contained in the neighbourhood eventually as well.

Given that $\{x_n\}$ converges to x, we have $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$, $\forall n > N$, $d(x_n, x) < \varepsilon$.

Pick M such that $n_M > N$, then $\forall i > M$, $d(x_{n_i}, x) < \varepsilon$. □

Proposition 11.2.3

Subsequential limits of a sequence are precisely the limit points of the sequence (viewed as a set)

Proof. This is just part (d) of the previous section.

Again, to make this work, we need to assume that nothing funny is going on at subsequential limits If the limits appear due to eventually constant subsequences, then they need not be limit points of the original sequence when viewed as a set

3.6, 3.7 are precisely the statements we've prepared for last week □

Proposition 11.2.4

If $\{x_n\}$ is a sequence in a compact set (bounded closed set), then there exists a convergent subsequence of $\{x_n\}$

Proof. This is Weierstrass-Bolzano together with part (b)

Ah yes, regarding compact sets I need to emphasize this again, but the definition that we are currently using for compact sets is not the actual definition

I've sent a video before the lesson which talks about the real definition for compact sets Essentially, compact sets satisfies the property akin to the statement in Heine-Borel: Given a topological space (X, τ), a compact set K in X is a set satisfying that, given any open covering $\{U_i\}$ of X, there exists a finite open cover $\{U_1, \dots, U_n\}$ of X

This is difficult to process at this stage Since we're currently only working with Euclidean spaces it would be more beneficial if you consider the Heine-Borel Theorem as a property first It would be a lot easier to accept the definition after you're more accustomed to applying the theorem □

Proposition 11.2.5

(Rudin 3.7) Subsequential limits form a closed subset

Proof. Actually we've done this two weeks before, it is simply saying that A" is a subset of A'.

(A" is not always A'; consider the set in R^2 given by (1/n,1/m)|n,m in N Then (1,0),(0,1) are in A' but not in A" □

§11.3 Cauchy Sequences

This is a very helpful way to determine whether a sequence is convergent or divergent, as it does not require the limit to be known. In the future you will see many instances where the convergence of all sorts of limits are compared with similar counterparts; generally we describe such properties as *Cauchy criteria*.

Definition 11.3.1

A sequence $\{x_n\}$ in a metric space X is said to be a **Cauchy sequence** if $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$, $\forall n, m \geq N$,

$$d(x_n, x_m) < \varepsilon.$$

Remark. This simply means that the distances between any two terms is sufficiently small after a certain point.

It is easy to prove that a converging sequence is Cauchy using the triangle inequality. The idea is that, if all the points are becoming arbitrarily close to a given point x, then they are also becoming close to each other. The converse is not always true, however.

Proposition 11.3.2

A sequence $\{x_k\}$ in $\mathbb{R}^n$ is convergent if and only if it is Cauchy.

Proof.

($\Longrightarrow$) Suppose that $\{x_k\}$ converges to x, then there exists N such that for $k > N$, $|x_k - x| < \dfrac{\varepsilon}{2}$ Then for $k, l > N$,

$$|x - k - x_l| \leq |x_k - x| + |x_l - x| < \varepsilon$$

($\Longleftarrow$) First, we show that $\{x_k\}$ must be bounded. Pick N such that for all $k, l > N$ we have $|x_k - x_l| < 1$. Centered at x_k, we show that $\{x_k\}$ is bounded; to do this we pick

$$r = \max\{1, |x_k - x_1|, \ldots, |x_k - x_N|\}$$

Then the sequence x_k is in $B(x_k, r)$ and thus is bounded.

Since $\{x_k\}$ is bounded, by the collolary of Bolzano-Weierstrass we know that $\{x_k\}$ contains a subsequence $\{x_{k_i}\}$ that converges to a limit x.

Then for all $\varepsilon > 0$, pick N_1 such that for all $k, l > N$, $|x_k - x_l| < \dfrac{\varepsilon}{2}$. Simultaneously, since $\{x_{k_i}\}$ converges to x, pick M such that for $i > M$, $|x_{k_i} - x| < \dfrac{\varepsilon}{2}$.

Now, since $k_1 < k_2 < \ldots$ is a sequence of strictly increasing natural numbers, we can pick $i > M$ such that $k_i > N$. Then for all $k > N$, by setting $l = k_i$ we obtain

$$|x_k - x_{k_i}| < \frac{\varepsilon}{2}, \quad |x_{k_i} - x| < \frac{\varepsilon}{2}$$

and hence

$$|x_k - x| \leq |x_k - x_{k_i}| + |x_{k_i} - x| < \varepsilon$$

□

Definition 11.3.3

Let nonempty $E \subseteq X$. Let S be the set of all real numbers of the form $d(x, y)$, with $x, y \in E$. Then the **diameter** of E is

$$\operatorname{diam} E \coloneqq \sup S.$$

§11.4 Upper and Lower Limits

§11.4.1 Limits of Multiple Sequences

We shall cover some of the more basic aspects of limits in this section.

Inequalities

First let's consider two converging sequences $\{a_n\}$ and $\{b_n\}$

If $a_n \le b_n$, then $\lim a_n \le \lim b_n$.

Remark. One important thing to take note for limits is that, even if you have $a_n < b_n$, you cannot say that $\lim a_n < \lim b_n$; for example, $\frac{1}{n} > -\frac{1}{n}$ but their limits are both 0.

Proof. Let's say that $A = \lim a_n$ and $B = \lim b_n$. Suppose otherwise that $A > B$, then we try to cause some chaos with $\varepsilon = A - B > 0$.

Since $\frac{\varepsilon}{2} > 0$, then there exists N_1 such that for $n > N_1$ we have $|a_n - A| < \frac{\varepsilon}{2}$; and there exists N_2 such that for $n > N_2$ we have $|b_n - B| < \frac{\varepsilon}{2}$.

Let $N = \max\{N_1, N_2\}$, then for any $n > N$, the two inequalities above will hold simultaneously But then we would have

$$a_n > A - \frac{\varepsilon}{2}, b_n < B + \frac{\varepsilon}{2}$$

and thus

$$a_n - b_n > A - B - \varepsilon = 0,$$

so $a_n > b_n$, a contradiction □

A corollary is that limits essentially preserve signs, if you include 0 in your consideration

A converging sequence of nonnegative numbers will always be nonnegative, and same goes to nonpositive numbers : Now as we can see in the proof above, there is actually a place where the restrictions of limits overpower the statement itself : What I mean by that is, suppose that you want to form a proof by contradiction : What you need here is just one term $a_n > b_n$ But you actually have $a_n > b_n$ eventually for all terms in the sequence : In fact, a better exercise would have been to show that limsups and liminfs also preserves inequalities

I'll just use limsups for example If $a_n \le b_n$, let $A = \limsup a_n$, $B = \limsup b_n$. Suppose otherwise that $A > B$. Let $\varepsilon = A - B > 0$; since $\frac{\varepsilon}{2} > 0$, then for all N_1, there exists $n > N_1$ such that $a_n > A - \frac{\varepsilon}{2}$; and there exists N_2 such that for all $n > N_2$, $b_n < B + \frac{\varepsilon}{2}$.

Now we arrange our thoughts logically First, we pick $N_2 = N$ such that for all $n > N$, $b_n < B + \frac{\varepsilon}{2}$. Then we may fix $N_1 = N$.

Due to the first condition, we see that it is possible to pick $n_0 > N$ such that $a_{n_0} > A - \frac{\varepsilon}{2}$. Now due to the second condition, since $n_0 > N$, this exact same n_0 would satisfy $b_{n_0} < B + \frac{\varepsilon}{2}$.

Therefore, n_0 satisfies $a_{n_0} - b_{n_0} > A - B - \varepsilon = 0$ and we are done.

Sandwich Theorem

Theorem 11.4.1 (Sandwich Theorem)

Let $a_n \le c_n \le b_n$ where $\{a_n\}, \{b_n\}$ are converging sequences such that $\lim a_n = \lim b_n = L$, then $\{c_n\}$ is also a converging sequence and $\lim c_n = L$.

Now, one very very very important thing about this theorem

The purpose of this theorem is to investigate some difficult sequence $\{c_n\}$ with two simpler sequences $\{a_n\}$ and $\{b_n\}$ which bounds it from below and from above respectively If you look closely at the statement, you may realize that we're only working under the condition that $\{a_n\}$ and $\{b_n\}$ are converging sequences

In other words, at this point we don't know whether $\{c_n\}$ is convergent.

In fact, this is supposed to be the main implication

Of course, $\lim c_n = L$ is proven at the exact same time, so both implications constitute the two parts of the conclusion

What I want to say is that you cannot simply take lim over $a_n \le c_n \le b_n$ and say that lim preserves inequalities, because in order to apply this inequality-preserving property, you need to ensure that all sequences are converging before you can apply it; clearly, this does not work here since we have not shown that c_n is convergent, therefore this idea does not work.

There are two ways to circumvent this One is to use $\varepsilon - N$; basically, just do it

But if you're really lazy, then the second method is to use the idea above except you first take limsup and liminf

The advantage of these two is that you don't need the original sequences to be convergent in order to apply them, and that they preserve inequalities even if the original sequences show no signs of convergence

So basically,

$$\limsup a_n \le \limsup c_n \le \limsup b_n,$$

and

$$\liminf a_n \le \liminf c_n \le \liminf b_n.$$

Then since $\{a_n\}$ and $\{b_n\}$ actually converge to L, all the liminfs and limsups of a_n and b_n are L, so we obtain $\limsup c_n = L$ and $\liminf c_n = L$.

In particular, $\limsup c_n = \liminf c_n$, thus c_n is convergent and it follows that $\lim c_n = L$.

Arithmetic properties

Proposition 11.4.2

For convergent $\{a_n\}$ and $k \in \mathbb{R}$,

$$\lim_{n\to\infty} ka_n = k \lim_{n\to\infty} a_n. \tag{11.1}$$

Proof. The proof is left as an exercise. You will need to k into cases where it is positive, negative or 0. □

Proposition 11.4.3

If $\{a_n\}$ and $\{b_n\}$ convergent sequences of real numbers, then

$$\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n. \tag{11.2}$$

Proof. Let $A = \lim_{n\to\infty} a_n$ and $B = \lim_{n\to\infty} b_n$.

$\forall \varepsilon > 0,\ \exists N_1 \in \mathbb{N},\ \forall n > N_1$

$$|a_n - A| < \frac{\varepsilon}{2}.$$

$\forall \varepsilon > 0,\ \exists N_2 \in \mathbb{N},\ \forall n > N_2,$

$$|b_n - B| < \frac{\varepsilon}{2}.$$

Let $N = \max\{N_1, N_2\}$, then for all $n > N$, by the triangle inequality we have

$$\big|(a_n + b_n) - (A + B)\big| \le |a_n - A| + |b_n - B| < \varepsilon.$$

□

Corollary 11.4.4

If $\{a_n\}$ and $\{b_n\}$ are convergent sequences of real numbers, then

$$\lim_{n\to\infty}(a_n - b_n) = \lim_{n\to\infty} a_n - \lim_{n\to\infty} b_n.$$

Proposition 11.4.5

If $\{a_n\}$ and $\{b_n\}$ are convergent, then

$$\lim_{n\to\infty}(a_n b_n) = \lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} b_n. \tag{11.3}$$

Proof. Let $A = \lim_{n\to\infty} a_n$ and $B = \lim_{n\to\infty} b_n$.

Consider the limit $\lim(a_n b_n - AB)$, as it would be sufficient to prove that this is equal to 0.

Now we will use a common technique to deal with such products:

$$\lim(a_n b_n - AB) = \lim(a_n b_n - A b_n + A b_n - AB)$$

The idea is to show that this is equal to

$$\lim(a_n b_n - A b_n) + \lim(A b_n - AB)$$

(Note that we cannot write this yet because we have not shown that these two sequences are convergent)

So let's examine these two sequences. The second one is easier since we have proved proposition 11.4.3:

$$\lim b_n = B \implies \lim(b_n - B) = 0$$

Thus $\lim(Ab_n - AB) = A\lim(b_n - B) = 0$.

As for the first one, we want to show that $\lim(a_n - A)b_n = 0$. Since we know that b_n is itself a converging sequence, thus in particular b_n is bounded, so suppose that $M > 0$ is a bound of b_n, i.e. for all natural number n, $|b_n| \leq M$.

Since $\lim a_n = a$, for all $\varepsilon > 0$, there exists N such that for all $n > N$, $|a_n - a| < \frac{\varepsilon}{M}$.

Combining the two above, we then conclude that for all $\varepsilon > 0$, there exists N such that for all $n > N$,

$$|a_n b_n - Ab_n| = |(a_n - A)b_n| < \frac{\varepsilon}{M} \cdot M = \varepsilon.$$

Therefore, this implies that $\lim(a_n b_n - Ab_n) = 0$.

Since we have shown that the two parts are equal to 0, we can conclude that $\lim(a_n b_n - AB) = 0$. □

Proposition 11.4.6

If $\{a_n\}$ and $\{b_n\}$ are converging, b_n is never 0 and $\lim b_n \neq 0$, then

$$\lim \frac{a_n}{b_n} = \frac{\lim a_n}{\lim b_n}.$$

Proof. Since we already have third proposition, it is sufficient for us to show that $\lim \frac{1}{b_n} = \frac{1}{\lim b_n}$.

Let $b = \lim b_n$, then we consider the limit

$$\lim\left(\frac{1}{b_n} - \frac{1}{b}\right) = \lim\left(\frac{b - b_n}{b_n b}\right).$$

Again, the important term here is $b - b_n$, but there is an extra term of $\frac{1}{b_n b}$, so we'll need to control this.

Since we need this to be bounded, we actually cannot have b_n to be close to 0. The good thing here is that $b \neq 0$, so we can restrict b_n to be close enough to b so that it stays away from 0.

So we can first pick N_1 such that for all $n > N_1$,

$$|b_n - b| < \frac{|b|}{2}.$$

Then

$$|b_n b - b^2| < \frac{b^2}{2}$$
$$\frac{b^2}{2} < b_n b < \frac{3b^2}{2}$$

This show that if $n > N_1$, $b_n b$ would always be positive, and $\frac{1}{b_n b} < \frac{2}{b^2}$.

Let $M = \frac{2}{b^2}$, then we may refer back to the original statement

$$\left|\frac{b - b_n}{b_n b}\right| < M|b - b_n|$$

We pick N_2 such that for all $n > N_2$, $|b_n - b| < \frac{\varepsilon}{M}$.

Let $N = \max\{N_1, N_2\}$, then for all $n > N$,

$$\left|\frac{b - b_n}{b_n b}\right| < M \cdot \frac{\varepsilon}{M} = \varepsilon.$$

□

Now let's talk a little bit about the arithmetic properties of limsups and liminfs : There are quite a number of differences for this; essentially the arithmetical properties aren't as well-behaved as the more specific case of limits : (i) $\limsup ka_n = k \limsup a_n$ holds if $k > 0$ However, if $k < 0$, then $\limsup ka_n = k \liminf a_n$.

(ii) $\limsup(a_n + b_n)$ is in general not equal to $\limsup a_n + \limsup b_n$ However, we do have the following:

$$\limsup(a_n + b_n) \leq \limsup a_n + \limsup b_n$$

Moreover, $\limsup(a_n + b_n)$ may be bounded from below as follows:

$$\limsup(a_n + b_n) \geq \limsup a_n + \liminf b_n$$

Your homework for today is to write down the analogous properties for liminf, and to prove (i) and (ii)

Now you should try to prove (i) for liminf as well; as for (ii), try to explain why properties (i),(ii) for limsup and property (i) for liminf would imply property (ii) for $\liminf$

Problem 29. Let $\{x_n\}$ be a sequence of real numbers and let $\alpha \geq 2$ be a constant. Define the sequence $\{y_n\}$ as follows:

$$y_n = x_n + \alpha x_{n+1}, n = 1, 2, \ldots$$

Show that if $\{y_n\}$ is convergent, then $\{x_n\}$ is also convergent.

§11.5 Series

Definition 11.5.1

Given a sequence $\{a_n\}$ we associate a sequence $\{s_n\}$, where

$$s_n = \sum_{k=1}^{n} a_k$$

which we call a **series**. The numbers s_n are called the **partial sums** of the series.

If $\{s_n\}$ converges to s, we say that the series **converges**, and write

$$\sum_{n=1}^{\infty} a_n = s;$$

s is called the sum of the series – the limit of a sequence of sums.

If $\{s_n\}$ diverges, the series is said to diverge.

The Cauchy criterion can

Proposition 11.5.2

12 Continuity

§12.1 Limit of Functions

Assume (X, d_X) is metric space and $E \subset X$ is a subset of X. Then the metric d_X induces a metric on E. We now consider another metric space (Y, d_Y). A map $f : E \to Y$ is also called a function over E with values in Y. In particular, if $Y = \mathbb{R}$, then f is called a real-valued function; and if $Y = \mathbb{C}$, f is called a complex-valued function.

Definition 12.1.1

Consider a limit point $p \in E$ and a point $q \in Y$. We say the **limit** of the funcion $f(x)$ at p is q, denoted as

$$\lim_{x \to p} f(x) = q$$

if $\forall \varepsilon > 0$, $\exists \delta > 0$ s.t. $\forall x \in E$ with $0 < d_X(x, p) < \delta$, there is

$$d_Y\big(f(x), q\big) < \varepsilon.$$

We can recast this definition in terms of limits of sequences:

Proposition 12.1.2

Let X, Y, E, f, p be as in Definition 12.1.1. Then $\lim_{x \to p} f(x) = q$ if and only if

$$\lim_{n \to \infty} f(p_n) = q$$

for every sequence $\{p_n\}$ in E such that $p_n \neq p$ and $\lim_{n \to \infty} p_n = p$.

Proof.

($\Longrightarrow$) Suppose $\lim_{x \to p} f(x) = q$. Choose $\{p_n\}$ in E satisfying $p_n \neq p$ and $\lim_{n \to \infty} p_n = p$.

Let $\varepsilon > 0$ be given. Then there exists $\delta > 0$ such that $d_Y\big(f(x), q\big) < \varepsilon$ if $x \in E$ and $0 < d_X(x, p) < \delta$.

Also, there exists $N \in \mathbb{N}$ such that $n > N$ implies $0 < d_X(p_n, p) < \delta$. Thus for $n > N$, we have $d_Y\big(f(p_n), q\big) < \varepsilon$, which shows that $\lim_{n \to \infty} f(p_n) = q$.

($\Longleftarrow$) □

By the same proofs as for sequences, limits are unique, and in $\mathbb{R}$ they add/multiply/divide as expected.

Definition 12.1.3

f is **continuous** at p if

$$\lim_{x \to p} f(x) = f(p).$$

In the case where p is not a limit point of the domain E, we say f is continuous at p. If f is continuous at all points of E, then we say f is continuous on E.

The sequential definition of continuity follows almost directly from the sequential definition of limits: f is continuous at p if for every sequence x_n converging to p, the sequence $f(x_n)$ converges to $f(p)$.

§12.2 Continuous Functions

§12.3 Continuity and Compactness

§12.4 Continuity and Connectedness

§12.5 Discontinuities

§12.6 Monotonic Functions

§12.7 Infinite Limits and Limits at Infinity

13 Differentiation

§13.1 The Derivative of a Real Function

Definition 13.1.1

A function $f : [a, b] \to \mathbb{R}$ is called **differentiable** at $x_0 \in [a, b]$, if the limit of the function

$$\phi(t) \coloneqq \frac{f(t) - f(x_0)}{t - x_0}, \quad a < t < b, t \neq x_0$$

exists as $t \to x_0$. For this case, we write

$$f'(x_0) = \lim_{t \to x_0} \phi(t) = \lim_{t \to x_0} \frac{f(t) - f(x_0)}{t - x_0}. \tag{13.1}$$

The function f is differentiable over $[a, b]$ if it is differentiable for each $x \in [a, b]$. It induces the function

$$\frac{\mathrm{d}f}{\mathrm{d}x} = f' : [a, b] \to \mathbb{R},$$

which is called the **derivative** of f.

Theorem 13.1.2

If $f : [a, b] \to \mathbb{R}$ is differentiable at $x_0 \in [a, b]$, then it must be continuous at x_0.

Proof. As $t \to x$,

$$f(t) - f(x) = \frac{f(t) - f(x)}{t - x} \cdot (t - x) \to f'(x) \cdot 0 = 0.$$

□

Remark. The converse of this theorem is not true. It is easy to construct continuous functions which fail to be differentiable at isolated points.

Notation. We use $C_1[a, b]$ to denote the set of differentiable functions over $[a, b]$ whose derivative is continuous. More generally, we use $C_k[a, b]$ to denote the set of functions whose k-th ordered derivative is continuous. In particular, $C_0[a, b]$ is the set of continuous functions over $[a, b]$.

Later on when we talk about properties of differentiation such as the intermediate value theorems, we usually have the following requirement on the function:

f is a continuous function on $[a,b]$ which is differentiable in (a,b).

Theorem 13.1.3 (Differentiation rules)

Suppose $f, g : [a,b] \to \mathbb{R}$ are differentiable at $x_0 \in [a,b]$. Then $f \pm g$, fg and f/g (when $g(x_0) \neq 0$) are differentiable at x_0. Moreover,

(1) $(f \pm g)'(x_0) = f'(x_0) \pm g'(x_0)$;

(2) $(fg)'(x_0) = f'(x_0)g(x_0) + f(x_0)g'(x_0)$;

(3) $\left(\frac{f}{g}\right)'(x_0) = \frac{f'(x_0)g(x_0) - f(x_0)g'(x_0)}{g(x_0)^2}$

Proof. We take (2) as an example.

We calculate

$$\begin{aligned}\frac{f(x)g(x) - f(x_0)g(x_0)}{x - x_0} &= \frac{\big(f(x) - f(x_0)\big)\,g(x) + f(x_0)\,\big(g(x) - g(x_0)\big)}{x - x_0} \\ &= \frac{f(x) - f(x_0)}{x - x_0} \cdot g(x) + f(x_0) \cdot \frac{g(x) - g(x_0)}{x - x_0} \\ &\to f'(x_0)g(x_0) + f(x_0)g'(x_0) \text{ as } x \to x_0\end{aligned}$$

where we use f and g are differentiable at x_0 and Theorem 13.1.2. □

Theorem 13.1.4 (Chain rule)

Let $f : [a,b] \to \mathbb{R}$ be a real-valued function that is differentiable at $x_0 \in [a,b]$. Let g be a real-valued function defined on an interval that contains $f([a,b])$, and g is differentiable at $f(x_0)$. Then the composition

$$h(x) \coloneqq g \circ f(x) \coloneqq g\big(f(x)\big) : [a,b] \to \mathbb{R}$$

is differentiable at x_0 and the derivative at x_0 can be calculated as

$$h'(x_0) = g'\big(f(x_0)\big)\, f'(x_0).$$

Proof. We know that

$$f'(x) = \lim_{t \to x} \frac{f(t) - f(x)}{t - x},$$

so under the assumption that t stays within the domain of f, $\frac{f(t)-f(x)}{t-x}$ should be a good approximation to $f'(x)$.

To actually quantify this, let $u(t) = \frac{f(t)-f(x)}{t-x} - f'(x)$.

Then the differentiability of f tells us that $\lim_{t \to x} u(t) = 0$.

Similarly, let $v(s) = \frac{g(s)-g(y)}{s-y} - g'(y)$, then $\lim_{s\to y} v(s) = 0$, as long as s stays in the domain of g

What's nice here is that we can let $s = f(t)$, then by our assumption s always stays in the domain of g, so nothing fishy will happen

Ah I forgot a small detail here Additionally we also need to define u(x)=0 and v(y)=0

Now let $h(t) = g(f(t))$, then h is defined on $[a, b]$, and we deduce that

$$h(t) - h(x) = (t - x)[f'(x) + u(t)][g'(y) + v(s)]$$

We then check that

$$\lim_{t\to x} \frac{h(t) - h(x)}{t - x} = \lim_{t\to x}[f'(x) + u(t)][g'(y) + v(s)] = f'(x)g'(f(x))$$

and we are done. □

Example 13.1.5. One of the best (worst?) family of pathological examples in calculus are functions of the form

$$f(x) = x^p \sin\frac{1}{x}.$$

- For $p = 1$, the function is continuous and differentiable everywhere other than $x = 0$.
- For $p = 2$, the function is differentiable everywhere, but the derivative is discontinuous.

Other more advanced pathological results (just for fun):

- The graph for $y = \sin\frac{1}{x}$ on $(0, 1]$, together with the interval $[-1, 1]$ on the y-axis, is a connected closed set that is not path-connected.
- For $0 < p < 1$, we obtain functions that are continuous and bounded, but the graphs are of infinite length (ps. I think that this is also true for $p = 1$).

Regarding continuous but not differentiable functions, a more pathological example is the Weierstrass function, which is continuous everywhere over $\mathbb{R}$ but differentiable nowhere.

§13.2 Mean Value Theorems

Definition 13.2.1

Let f be a real valued function defined over a metric space X. We say f has a **local maximum** at $x_0 \in X$ if $\exists \delta > 0$ s.t. $\forall x \in B_\delta(x_0)$,

$$f(x_0) \geq f(x).$$

Similarly, we say f has **local minimum** at $x_0 \in X$ if $\exists \delta > 0$ s.t. $\forall x \in B_\delta(x_0)$,

$$f(x_0) \leq f(x).$$

Definition 13.2.2

For a function $f : (a, b) \to \mathbb{R}$, a point $x_0 \in [a, b]$ is called a **critical point** if f is not differentiable at x_0 or $f'(x_0) = 0$.

Theorem 13.2.3

Assume f is defined over $[a, b]$. If f has a local maximum or local minimum at some $x_0 \in (a, b)$, then x_0 is a critical point of f.

Proof. If f is not differentiable at x_0, we are done. Assume now f is differentiable at x_0 and x_0 is a local maximum.

Then $\exists \delta > 0$ s.t. $\forall x \in B_\delta(x_0)$,

$$f(x_0) \leq f(x).$$

It follows

$$\frac{f(x) - f(x_0)}{x - x_0} \begin{cases} \geq 0 & x_0 - \delta < x < x + \delta \\ \leq 0 & x_0 < x < x_0 + \delta \end{cases}$$

Further since $f'(x_0)$ exists, there is

$$f'(x_0-) \geq 0, \quad f'(x_0+) \leq 0,$$

but $f'(x_0-) = f'(x_0+) = f'(x_0)$. Hence $f'(x_0) = 0$. □

Theorem 13.2.4 (Fermat's Theorem (Interior Extremum Theorem))

If the differential exists, then by comparing the left and right limits it is easy to see that the differential for a local maximum/maximum can only be 0.

To summarize in four words: Local extrema are stationary

There are three mean value theorems, from specific to general:

1. Rolle's Theorem
2. (Lagrange's) Mean Value Theorem
3. Generalised (Cauchy's) Mean Value Theorem

Theorem 13.2.5 (Rolle's Theorem)

If f is continuous on $[a,b]$, differentiable in (a,b) and $f(a) = f(b)$, then there exists $c \in (a,b)$ such that

$$f'(c) = 0.$$

Proof. Let $h(x)$ be a function defined on $[a,b]$ where $h(a) = h(b)$.

The idea is to show that h has a local maximum/minimum, then by Fermat's Theorem this will then be the stationary point that we're trying to find.

First note that h is continuous on $[a,b]$, so h must have a maximum M and a minimum m.

If M and m were both equal to $h(a) = h(b)$, then h is just a constant function and so $h'(x) = 0$ everywhere.

Otherwise, h has a maximum/minimum that is not $h(a) = h(b)$, so this extremal point lies in (a,b).

In particular, this extremal point is also a local extremum. Since h is differentiable on (a,b), by Fermat's theorem this extremum point is stationary, thus Rolle's Theorem is proven. □

Theorem 13.2.6 (Mean Value Theorem)

If f is continuous on $[a,b]$ and differentiable in (a,b), then there exists $c \in (a,b)$ such that

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Exercise 2: Show that the Mean Value Theorem results directly from Rolle's Theorem (the other direction is trivial) : This isn't a very significant exercise because we're going to prove something more general

Theorem 13.2.7 (Generalised Mean Value Theorem)

If f and g are continuous on $[a,b]$ and differentiable in (a,b), then there exists $c \in (a,b)$ such that

$$\frac{f'(c)}{g'(c)} = \frac{f(b) - f(a)}{g(b) - g(a)}.$$

Now we return to the proof of the generalized MVT

We set the function $h(t) = [f(b) - f(a)]g(t) - [g(b) - g(a)]f(t)$, then h is continuous on $[a,b]$ and differentiable on (a,b)

Moreover, $h(a) = f(b)g(a) - f(a)g(b) = h(b)$, thus by Rolle's Theorem, there exists $c \in (a,b)$ such that $h'(c) = 0$, i.e. $[g(b) - g(a)]f'(c) = [f(b) - f(a)]g'(c)$

Corollary: If f and g are continuous on $[a,b]$ and differentiable in (a,b), and $g'(x) \neq 0$ for all $x \in (a,b)$, then there exists

$$c \in (a,b) \text{ s.t. } f'(c)/g'(c) = [f(b) - f(a)]/[g(b) - g(a)]$$

This form of the generalized MVT will be used to prove the most beloved rule of high school students

exercises for the Mean Value Theorem

Exercise 29

Let f and g be continuous on $[a,b]$ and differentiable on (a,b). If $f'(x) = g'(x)$, then $f(x) = g(x) + C$.

Exercise 30

Given that $f(x) = x^\alpha$ where $0 < \alpha < 1$. Prove that f is uniformly continuous on $[0, +\infty)$.

Exercise 31 (Olympiad level)

Let f be a function continuous on $[0,1]$ and differentiable on $(0,1)$ where $f(0) = f(1) = 0$. Prove that there exists $c \in (0,1)$ such that

$$f(x) + f'(x) = 0.$$

§13.3 Darboux's Theorem

Darboux's Theorem implies some sort of a 'intermediate value' property of derivatives that is similar to continuous functions

This is Theorem 5.12 in the book

Now first and foremost, the requirement for this statement is that f must be differentiable on [a,b], not just in (a,b) Otherwise f'(a) and f'(b) may not make sense : One common theme in many of these problems is to construct auxiliary functions Suppose that $f'(a) < \lambda < f'(b)$, then we construct the auxiliary function $g(x) = f(x) - \lambda x$: Then we only need to find a point $x \in (a,b)$ such that g'(x)=0 : This means that we only need to find a local maximum/minimum, which by Fermat's Theorem has to be a stationary point as well : Now we look at the values of g near a and b : Exercise 1: Using the fact that $g'(a) < 0$ and $g'(b) > 0$, show that a and b are local maxima of g

Here we regard g as simply a function on $[a,b]$, so we only need to show that a,b are maximum and corresponding semi-open neighbourhoods $[a, a+\varepsilon)$ and $(b-\varepsilon, b]$: Let m=g'(a)<0 be the slope of the tangent at a : Then lim(h→0+)[g(a+h)-g(a)]/h=m<0 : This means that there should exist $\delta > 0$ such that for $0 < h < \delta$, [g(a+h)-g(a)]/h<m/2<0 : Now we can rewrite the above as g(a+h)<g(a)+mh/2 : Since m<0 and h>0, we obtain $g(a+h) < g(a)$ for $0 < h < \delta$: Thus this proves that x=a is a local maximum of g A similar proof applies for x=b : Now since g is differentiable on [a,b], in particular it has to be continuous on [a,b] : Since [a,b] is compact, g([a,b]) is compact in R and thus g has both maximum and minimum values in [a,b] : Here we'll just focus on the minimum value : As we've shown, x=a is a 'strict' local maxima, in the sense that for any point $x \in (a, a+\varepsilon)$, we actually have the strict inequality $g(x) < g(a)$: This means that x=a

cannot be a local minimum : Similarly, x=b cannot be a local minimum, and therefore g achieves its minimum strictly inside (a,b) : Only then we can say that this local minimum is stationary (This will not work otherwise; note that a and b are both local maxima but are not stationary points of g) : An interesting implication of Darboux's Theorem is that if f is differentiable on [a,b], then f' cannot have simple discontinuities (removable or jump discontinuities), simply because these discontinuities do not allow this 'intermediate value' property : However, we should recall certain pathological examples like $f(x)=x^2 \sin 1/x$ ($f(0)=0$) Here $f'(0)=\lim(h\to 0)[x^2 \sin 1/x-0]/x=0$, but $f'(x)=2x \sin 1/x - \cos 1/x$, so f' is discontinuous at x=0

§13.4 L'Hopital's Rule

Theorem 13.4.1 (L'Hopital's Rule)

Assume f, g are differentiable over (a, b) with $g(x) \neq 0$. If either

(1) $\lim_{x\to a} f(x) = 0$ and $\lim_{x\to a} g(x) = 0$; or

(2) $\lim_{x\to a} |g(x)| = +\infty$,

and

$$\lim_{x\to a} \frac{f'(x)}{g'(x)} = A \in [-\infty, +\infty]$$

assuming $g'(x) \neq 0$ over (a, b), then

$$\lim_{x\to a} \frac{f(x)}{g(x)} = A.$$

Proof. Now the entire proof is quite tedious because there's actually eight main cases to think of 1. $\frac{0}{0}$ or $\frac{\infty}{\infty}$ 2. a is normal or $a = -\infty$ 3. A is normal or $A = \pm\infty$

We'll only prove the most basic one here: 0/0, a and A are normal This is the case which will be required for Taylor series

First we define f(a)=g(a)=0, so that f and g are continuous at $x = a$

Now let $x \in (a, b)$, then f and g are continuous on $[a, x]$ and differentiable in (a, x) : Thus by Cauchy's Mean Value Theorem, there exists $\xi \in (a, x)$ such that

$$\frac{f'(\xi)}{g'(\xi)} = \frac{f(x) - f(a)}{g(x) - g(a)} = \frac{f(x)}{g(x)}$$

For each x, we pick ξ which satisfies the above, so that ξ may be seen as a function of x satisfying $a < \xi(x) < x$

Then by squeezing we have $\lim_{x\to a^+} \xi(x) = a$.

Since $\frac{f'}{g'}$ is continuous near a, the theorem regarding the limit of composite functions give

$$\lim_{x\to a^+} \frac{f(x)}{g(x)} = \lim_{x\to a^+} \frac{f'(\xi)}{g'(\xi)} = \lim_{x\to a^+} \left(\frac{f'}{g'}\right)(\xi(x)) = A$$

Now the same reasoning can be used for b where we will use lim(x→b-) to replace all the $\lim_{x\to a^+}$, and ξ will be a function which maps to (x, b). □

Example 13.4.2.

- $\lim_{x\to 0} \frac{1-\cos x}{x^2} = \frac{1}{2}$.
- $\lim_{x\to+\infty} \frac{x^2}{e^{3x}} = 0$.

§13.5 Taylor Expansion

Consider a function $f : [a, b] \to \mathbb{R}$. We first look at the mean value theorem from the viewpoint of approximations for $f(x)$ near a point $x = a$. We can regard the constant function

$$f_0(x) = f(a)$$

as the *zero order approximation* of $f(x)$. Then we ask if we can understand the remainder

$$R_1(x) \coloneqq f(x) - f(a), \quad x \in [a, b]$$

for this approximation. For this, if we assume $f \in C_0[a, b]$ and f' exists over (a, b), then the mean value theorem tells us that there exists some $a < \xi_x < x$ (here ξ_x emphasises that ξ depends on x) so that we can write R_1 as

$$R_1(x) = f'(\xi_x)(x - a).$$

This is saying that the derivative of f can control the remainder $R_1(x)$ as an order 1 monomial.

The main expression is as follows:

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f'''(a)}{3!}(x-a)^3 + \cdots \tag{13.2}$$

So for example we have the following (we've used the ones for e^x and $\ln x$ for generating functions):

$$\begin{aligned}
e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \\
\sin x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots \\
\cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots \\
\ln(1+x) &= x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots
\end{aligned}$$

There's a lot of things to say about these equations, for example the one for $\ln(1 + x)$ only works for $|x| < 1$

Also, if you want the RHS of the expression to be an infinite power series, $f(x)$ has to be smooth (infinitely differentiable)

Even then, the power series may never converge to $f(x)$ at any interval, no matter how small The most common example given here is $f(x) = e^{\frac{-1}{x^2}}$ (f(0)=0); the Taylor series for $f(x)$ is just 0

Now sometimes we don't actually that nice of a property for f, we're often given that fact that f is only finitely differentiable

Then we will have something along the lines of

$$f(x) \approx f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n$$

where $f^{(n)}$ denotes the n-th differential.

There are two main forms of the statement regarding the error between the original function and the Taylor series estimate

The simpler form is what's known as the Peano form: Given that f is n times differentiable at a, then

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + o((x-a)^n)$$

To show this, we only need to show that we have the following limit:

$$\lim_{x\to a} \frac{f(x) - f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n}{(x-a)^n} = 0$$

The basic idea is to use the L'Hopital Rule n times. The numerator becomes $f^{(n)}(x) - f^{(n)}(a)$ which approaches 0, whereas the denominater is just $n!$, so the limit exists and is equal to 0.

However, we need to verify all the necessary conditions for L'Hopital : Here the main problem is that we don't know if we have the 0/0 indeterminate at each step, so we'll need to check this for the k-th step where k=1,...,n

Fortunately, the k-th derivative of the numerator is $f^{(k)}(x) - f^{(k)}(a) - (x-a)F_k(x)$ where F_k is just a bunch of random stuff, so the numerator approaches 0 as $x \to a$ The k-th derivative of the denominator is $n(n-1)\cdots(n-k+1)(x-a)^{n-k}$ so it also approaches 0, and we're done

The other form is actually a family of similar statements which gives more precise values for the error The Peano form has a fundamental obstacle when used in approximation, we don't have any control on the size of the final term other than its asymptotic behaviour : We'll be talking about the one given in the book, known as the Lagrange form: : Given that f is n times differentiable on (a,b) such that $f^{(n-1)}$ is continuous on $[a,b]$, then

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n-1)}(a)}{(n-1)!}(x-a)^(n-1) + \frac{f^{(n)}(\xi)}{n!}(x-a)^n$$

Just like in L'Hopital, we intuitively think of (a,b) as just a very small interval at the right hand side of x=a : Here we are giving up on the second final term of Peano by

combining it with the infinitesimal (small o) term to give an accurate description of the error

For the proof of this one we'll be using Cauchy's MVT

Fix any $x \in (a, b)$, then we construct the functions

$$F(t) = f(x) - \left(f(t) + \frac{f'(t)}{1!}(x-t) + \frac{f''(t)}{2!}(x-t)^2 + \cdots + \frac{f^{(n-1)}(t)}{(n-1)!}(x-t)^{n-1} \right)$$

$$G(t) = (x-t)^n$$

We calculate $F'(t)$ as follows:

$$-[f'(t) + \frac{f''(t)}{1!} - f'(t) + \frac{f'''(t)}{2!} - \frac{f''(t)}{1!} + \cdots + \frac{f^{(n)}(t)}{(n-1)!}(x-t)^{n-1} - \frac{f^{(n-1)}(t)}{(n-2)!}(x-t)^{n-2}] = -\frac{f^{(n)}(t)}{(n-1)!}(x-t)^{n-1}$$

$G'(t) = -n(x-t)^{n-1}$, so we have

$$\frac{F'(t)}{G'(t)} = \frac{f^{(n)}(t)}{n!}$$

The main reason for why we come up with the strange-looking F and G is that we specifically swap out a for t so that $F(x) = G(x) = 0$, in hopes of getting rid of x:

We apply Cauchy's MVT to F and G on $[a, x]$, so that we obtain $\xi \in (a, x)$ satisfying

$$\frac{F'(\xi)}{G'(\xi)} = \frac{F(x) - F(a)}{G(x) - G(a)} = \frac{F(a)}{G(a)}.$$

Thus the Lagrange form of the remainder is given by

$$F(a) = \frac{f^{(n)}(\xi)}{n!} G(a).$$

Theorem 5.19 is important, so do go through that proof as an exercise

14 Riemann–Stieltjes Integral

§14.1 Definition of Riemann–Stieltjes Integral

Assume $[a,b]$ is a closed interval in $\mathbb{R}$. By a **partition** P, we mean a finite set of points $x_0, x_1, \ldots, x_n$ where

$$a = x_0 \le x_1 \le \cdots \le x_{n-1} \le x_n = b.$$

Assume f is a bounded real-valued function over $[a,b]$ and α is an increasing function over $[a,b]$. Denote by

$$M_i = \sup_{[x_{i-1},x_i]} f(x), \quad m_i = \inf_{[x_{i-1},x_i]} f(x)$$

and by

$$\Delta\alpha_i = \alpha(x_i) - \alpha(x_{i-1}).$$

Define the **upper sum** of f with respect to the partition P and α as

$$U(f,\alpha;P) = \sum_{i=1}^{n} M_i \Delta\alpha_i$$

and the **lower sum** of f with respect to the partition P and α as

$$L(f,\alpha;P) = \sum_{i=1}^{n} m_i \Delta\alpha_i.$$

Define the upper Riemann–Stieltjes integral as

$$\overline{\int_a^b} f(x)\,\mathrm{d}\alpha(x) \coloneqq \inf_P U(f,\alpha;P)$$

and the lower Riemann–Stieltjes integral as

$$\underline{\int_a^b} f(x)\,\mathrm{d}\alpha(x) \coloneqq \sup_P L(f,\alpha;P).$$

It is easy to see from definition that

$$\underline{\int_a^b} f(x)\,\mathrm{d}\alpha(x) \le \overline{\int_a^b} f(x)\,\mathrm{d}\alpha(x)\,.$$

Definition 14.1.1

A function f is **Riemann–Stieltjes integrable** with respect to α over $[a,b]$, if

$$\underline{\int_a^b} f(x)\,\mathrm{d}\alpha(x) = \overline{\int_a^b} f(x)\,\mathrm{d}\alpha(x)\,.$$

Notation. We use $\int_a^b f(x)\,\mathrm{d}\alpha(x)$ to denote the common value, and call it the Riemann–Stieltjes of f with respect to α over $[a,b]$.

Notation. We use the notation $R_\alpha[a,b]$ to denote the set of Riemann–Stieljes integrable functions with respect to α over $[a,b]$.

In particular, when $\alpha(x) = x$, we call the corresponding Riemann–Stieljes integration the **Riemann integration**, and use $R[a,b]$ to denote the set of Riemann integrable functions.

Definition 14.1.2

The partition P' is a **refinement** of P if $P' \supset P$. Given two partitions P_1 and P_2, we say that P' is their **common refinement** if $P' = P_1 \cup P_2$.

Intuitively, a refinement will give a better estimation than the original partition, so the upper and lower sums of a refinement should be more restrictive.

Proposition 14.1.3

If P' is a refinement of P, then

$$L(f,\alpha;P) \le L(f,\alpha;P')$$

and

$$U(f,\alpha;P') \le U(f,\alpha;P).$$

Proof. Suppose that

$$P : a \le x_0 \le x_1 \le \ldots \le x_n = b$$

and

$$P' : a \le y_0 \le y_1 \le \ldots \le y_m = b.$$

Then there exists a strictly increasing sequence of indices $j_0 = 0, j_1, \ldots, j_n = m$ such that $y_{j_k} = x_k$.

Now consider each closed interval $[x_{i-1}, x_i]$

Focusing on the upper sum, we have

$$\sup_{[x_{i-1},x_i]} f \ge \sup_{[y_{k-1},y_k]} f$$

for $k = j_{i-1}+1, \ldots, j_i$. This is because $[y_{k-1}, y_k]$ is contained in $[x_{i-1}, x_i]$

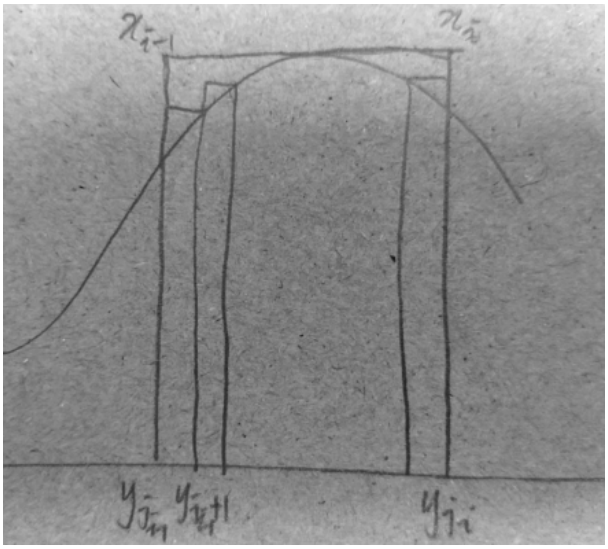

Figure 14.1: Partitions

Continuing from

$$\sup_{[x_{i-1},x_i]} f \geq \sup_{[y_{k-1},y_k]} f,$$

We then multiply by $\alpha(y_k)-\alpha(y_{k-1})$ on both sides and then take the sum from $k = j_{i-1}+1$ to $k = j_i$: The RHS corresponds to the (weighted) sum of the thin rectangles that you see in the above picture : The LHS is actually a telescoping sum, and the sum would be

$$(\sup_{[x_{i-1},x_i]} f)\cdot[\alpha(y_{j_i})-\alpha(y_{j_{i-1}})] = (\sup_{[x_{i-1},x_i]} f)\cdot[\alpha(x_i)-\alpha(x_{i-1})]$$

Finally, we take the sum from $i = 1$ to $i = n$ of the above inequality LHS $\geq$ RHS (sorry I don't know of a better way to put it) We then obtain $U(P, f, \alpha) \geq U(P', f, \alpha)$

(On the LHS we're collecting all the rectangles for the upper sum wrt P, but on the RHS we're collecting up collections of upper rectangles to obtain the entire collective of upper rectangles for the upper sum wrt P') : Lower sum is similar : Now, a lemma used to prove 6.5 Given any two partitions P_1 and P_2, we have

$$L(P_1, f, \alpha) \leq U(P_2, f, \alpha)$$

So a lower sum will always be no larger than any other upper sum : So this includes the cases where we have the most refined of P_1's and P_2's, with no information regarding the partition points whatsoever To be honest, the result seems to be both intuitive and unclear at the same time

The key here is to use common refinements as a link for both sums The idea is stated in the proof of 6.5 and I don't think I need to elaborate further

What's nice here is that now we have two completely independent partitions P_1 and P_2, so by fixing one partition, say P_2, and taking the 'limit' over the other (here we take the supremum over all possible P_1) we then obtain an inequality between a Darboux integral and a Darboux sum (here it's the lower integral and an upper sum)

Since the Darboux integral is just a number, we can then safely take the 'limit' over the other partition to obtain the inequality in 6.5 □

Proposition 14.1.4

$$\underline{\int_a^b} f \, d\alpha = \overline{\int_a^b} f \, d\alpha \, .$$

Proof.

□

Now we move on to integrability conditions for f. The first one looks a lot like the $\varepsilon - N$ or $\varepsilon - \delta$ definition of limits:

Theorem 14.1.5

$f \in R_\alpha[a,b]$ if and only if for each $\varepsilon > 0$, there exists some partition P such that

$$U(f,\alpha;P) - L(f,\alpha;P) < \varepsilon.$$

Proof.

($\implies$) Assume $f \in R_\alpha[a,b]$. By definition,

$$\inf_P U(f,\alpha;P) = \int_a^b f \, d\alpha = \sup_P L(f,\alpha;P).$$

For every $\varepsilon > 0$,

($\impliedby$) □

Example 14.1.6 (Dirichlet function)**.** The Dirichlet function is given by

$$f(x) = \begin{cases} 1 & x \in \mathbb{Q} \\ 0 & x \notin \mathbb{Q} \end{cases}$$

We try to calculate the two on the interval $[0,1]$.

The Dirichlet function is pathological because for each subinterval $[x_{i-1}, x_i]$, the supremum is always 1 and the infimum is always 0.

So no matter what partition we use, $U(f,P)$ is always 1 whereas $L(f,P)$ is always 0. This means that $U(f) = 1$ and $L(f) = 0$, so there are two different values for "the integral of f".

This is like the case where we try to find the limit of the Dirichlet function where x is approaching any given real number r, there exists two sequences approaching r whose image approaches two different values.

Now, a very important and fun case about the more general RS-integral, which we'll discuss next week (do try the exercise yourself first)

Exercise 32

The Heaviside step function H is a real-valued function defined by the following:

$$H(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases}$$

For the purpose of this question we assume the convention $\infty \cdot 0 = 0$.

(a) Let f be a real-valued function over $\mathbb{R}$. Show that $f \in \mathbb{R}_H[a, b]$ if and only if f is continuous at 0, and find the RS-integral $\int_{-\infty}^{\infty} f \, \mathrm{d}H$.

(b) Suppose that the definition for H is changed for $x = 0$, say $H(0) = \frac{1}{2}$. Show that the above result still holds.

(c) Examine the RS-integral of f over $\mathbb{R} \setminus \{0\}$ wrt H, where f is a real-valued function over $\mathbb{R} \setminus \{0\}$ such that $\lim_{x \to 0} f(x) = \infty$ or $-\infty$.

(You may read up on more information regarding the Heaviside function, and the (in)famous Dirac delta function)

Now we've been talking a lot about upper and lower sums because they're arguably the simplest way to define integrals, in the sense that there's not a whole lot of things that we could go wrong here By considering only upper and lower bound, we're essentially picking the most conservative route possible

It would be nice if we could just pick like one random point within each interval and consequently calculate the Riemann(-Stieltjes) sums

This method, of course, fails to be well defined for pathological functions like the Dirichlet function On the other hand, by using upper and lower sums, we could give a persuasive explanation as to why the Dirichlet function is not Riemann integrable

However, instead of throwing this idea away, there's actually a way for us to make this into a strict definition

When we were talking about the sequential definition for limits of functions, we noted that there are certain scenarios where the limit cannot exist because there may be two distinct sequences may give different limit Based on this observation, we then gave a reasonable condition as follows: "$\lim_{x \to a} f(x)$ exists and is equal to L if and only if for all sequences x_n converging but not containing a, $f(x_n)$ converges to L"

Well here, it's actually the same kind of scenario Given any partition P, we consider the Riemann sum $\sum f(\xi_i)\Delta x_i$ where ξ_i is any point where $x_{i-1} \leq \xi_i \leq x_i$

For the Dirichlet function over $[0, 1]$, given any partition P (here we may assume that the partition points are distinct), we will always be able to specifically pick $\xi_i, \eta_i \in [x_{i-1}, x_i]$ such that ξ_i is rational but η_i is irrational

Then $\sum f(\xi_i)\Delta x_i = 1$ but $\sum f(\eta_i)\Delta x_i = 0$

Now be very mindful that this alone cannot be evidence that f is non-integrable The key is that this somehow occured for all partitions P, no matter how refined they are; for

every single partition P, there exists two sets of 'representing points' ξ_i, η_i such that the two Riemann sums are constantly far apart (1 and 0 in this case)

Let $\varepsilon_0 = 1$, then this ultimately translates to the following: The Dirichlet function cannot be Riemann integrable because There exists some $\varepsilon_0 > 0$, such that for any given partition P, there exists two sets of representing points ξ_i, η_i such that their corresponding Riemann sums satisfy that

$$|\sum f(\xi_i)\Delta x_i - \sum f(\eta_i)\Delta x_i| \geq \varepsilon_0.$$

Now if we always pick the representatives such that $\xi_i > \eta_i$ then we can neglect the absolute value

So now, let's take the converse A function f is said to be RS-integrable if For every $\varepsilon > 0$, There exists a partition P, such that For any two sets of representing points ξ_i, η_i, Their corresponding Riemann sums satisfy that

$$\sum[f(\xi_i) - f(\eta_i)]\Delta x_i < \varepsilon$$

(The last one should be $\Delta\alpha_i$ for RS-integrals, not Δx_i)

Unfortunately this is still not quite the correct definition according to Apostol, but we're pretty close The problem with this definition is that it is too weak if we're considering general α of bounded variation; if we were only talking about monotonically increasing α then this will actually be an equivalent definition

The official definition for the RS-integral wrt α of bounded variation is as follows:

Definition 14.1.7

For every $\varepsilon > 0$, there exists a partition P, such that [For any refinement P' of P, and] For any two sets of representing points ξ_i, η_i [of P'], their corresponding Riemann sums satisfy that

$$\sum[f(\xi_i) - f(\eta_i)]\Delta x_i < \varepsilon.$$

Now this definition is what mathematicians would refer to as a 'Cauchy' definition, since it defines a notion by comparing a pair of arbitrary values that are similar to one another, and if they agree in some sense then we say that that something satisfies some property.

The integral is then obtained as follows: If f were to satisfy the above Cauchy definition, then we may pick an arbitrary sequence of refinements

$$P_1 \subset P_2 \subset P_3 \subset ...;$$

and for each partition we pick a set of representatives to obtain a sequence RS-sum $I_1, I_2, I_3, ...$: This sequence will be a Cauchy sequence of real numbers, and so will converge to a specific value I which we consider to be RS-integral of f : Now the reason why Apostol needed to strengthen the definition is that, otherwise this value I may not be unique : So if you look at the statement you see in 6.7(b)(c), then they correspond to the Cauchy definition and the 'value-based' definition respectively For monotonically increasing α, it is much easier to discuss them using upper and lower sums So your exercise today will be to read the statements and proofs in Theorem 6.7

Theorem 14.1.8

$f \in R_\alpha[a,b]$, $m \le f \le M$, and ϕ is uniformly continuous on $[m,M]$, then

$$\phi \circ f \in R_\alpha[a,b].$$

Proof. Choose $\varepsilon > 0$. Since ϕ is uniformly continuous on $[m,M]$, there exists $\delta > 0$ such that $\delta < \varepsilon$ and $|\phi(s) - \phi(t)|$ □

§14.2 Properties of the Integral

Theorem 14.2.1

(1) If $f_1, f_2 \in R_\alpha[a,b]$, then

$$f_1 + f_2 \in R_\alpha[a,b];$$

$cf \in R_\alpha[a,b]$ for every $c \in \mathbb{R}$, and

$$\int_a^b (f_1 + f_2)\,\mathrm{d}\alpha = \int_a^b f_1\,\mathrm{d}\alpha + \int_a^b f_2\,\mathrm{d}\alpha\,,$$

$$\int_a^b (cf)\,\mathrm{d}\alpha = c\int_a^b f\,\mathrm{d}\alpha\,.$$

(2) If $f_1, f_2 \in R_\alpha[a,b]$ and $f_1 \le f_2$, then

$$\int_a^b f_1\,\mathrm{d}\alpha \le \int_a^b f_2\,\mathrm{d}\alpha\,.$$

(3) If $f \in R_\alpha[a,b]$ and $c \in [a,b]$, then $f \in R_\alpha[a,c]$ and $f \in R_\alpha[c,b]$, and

$$\int_a^b f\,\mathrm{d}\alpha = \int_a^c \mathrm{d}\alpha + \int_c^b \mathrm{d}\alpha\,.$$

(4) If $f \in R_\alpha[a,b]$ and $|f| \le M$, then

$$\left|\int_a^b f\,\mathrm{d}\alpha\right| \le M\big[\alpha(b) - \alpha(a)\big]\,.$$

(5) If $f \in R_{\alpha_1}[a,b]$ and $f \in R_{\alpha_2}[a,b]$, then $f \in R_{\alpha_1+\alpha_2}[a,b]$ and

$$\int_a^b f\,\mathrm{d}(\alpha_1 + \alpha_2) = \int_a^b f\,\mathrm{d}\alpha_1 + \int_a^b f\,\mathrm{d}\alpha_2\,;$$

if $f \in R_\alpha[a,b]$ and c is a positive constant, then $f \in R_{c\alpha}[a,b]$ and

$$\int_a^b f\,\mathrm{d}(c\alpha) = c\int_a^b f\,\mathrm{d}\alpha\,.$$

(6) If $f \in R_\alpha[a,b]$ and $g \in R_\alpha[a,b]$, then $fg \in R_\alpha[a,b]$.

Proof.

(1) If $f = f_1 + f_2$ and P is any partition of $[a,b]$, we have

$$\begin{aligned} L(f_1,\alpha;P) + L(f_2,\alpha;P) &\le L(f,\alpha;P) \\ &\le U(f,\alpha;P) \\ &\le U(f_1,\alpha;P) + U(f_2,\alpha;P). \end{aligned}$$

If $f_1 \in R_\alpha[a,b]$ and $f_2 \in R_\alpha[a,b]$, let $\varepsilon > 0$ be given. There are partitions P_1 and P_2 such that

(2)

(3)

(4)

(5)

(6)

□

Theorem 14.2.2 (Triangle inequality)
$f \in R_\alpha[a,b]$, then $|f| \in R_\alpha[a,b]$,

$$\left|\int_a^b f \,\mathrm{d}\alpha\right| \leq \int_a^b |f| \,\mathrm{d}\alpha\,.$$

Proof.

□

6.14 6.15 Heaviside step function

6.16 corollary for intinite sum, need $\sum c_n$ to converge (23) comparison test

6.17 integration by substitution

Theorem 14.2.3
α increasing, $\alpha' \in R[a,b]$, f bounded on $[a,b]$, then

$$f \in R_\alpha[a,b] \iff f\alpha' \in R[a,b].$$

6.19 change of variables

§14.3 Fundamental Theorem of Calculus

6.20 6.21

Theorem 14.3.1

6.22 integration by parts

15 Sequence and Series of Functions

§15.1 Uniform Convergence

Definition 15.1.1

Suppose $\{f_n\}$, $n = 1, 2, 3, \ldots$ is a sequence of functions defined on a set E, and suppose that the sequence of numbers $\{f_n(x)\}$ converges for every $x \in E$. We can then define a function f by

$$f(x) = \lim_{n\to\infty} f_n(x).$$

We say that $\{f_n\}$ **converges pointwise** to f on E, denoted by $f_n \to f$.

Similarly, if $\sum f_n(x)$ converges for every $x \in E$, and if we define

$$f(x) = \sum_{n=1}^{\infty} f_n(x)$$

the function f is called the **sum of the series** $\sum f_n$.

pointwise convergence

Definition 15.1.2

Assume $\{f_n\}$ is a sequence of functions defined over a set X and f is also a function defined over X. We say $\{f_n\}$ **uniformly converges** to f over X, if for any $\varepsilon > 0$, there exists $N > 0$ (which is independent of x) so that for any $x \in X$,

$$|f_n(x) - f(x)| < \varepsilon.$$

Notation. We denote this uniform convergence over X by $f_n \rightrightarrows f$.

§15.2 Uniform Convergence and Continuity

§15.3 Uniform Convergence and Integration

Theorem 15.3.1

Assume $\{f_n\}$ is a sequence of functions defined over $[a,b]$ and each $f_n \in R_\alpha[a,b]$. If $f_n \to f$, then $f \in R_\alpha[a,b]$, and

$$\lim_{n\to\infty} \int_a^b f_n \,\mathrm{d}\alpha = \int_a^b f \,\mathrm{d}\alpha\,.$$

Proof. Define □

Corollary 15.3.2

Assume $a_n \in R_\alpha[a,b]$ and

$$f(x) \coloneqq \sum_{n=0}^{\infty} a_n(x)$$

converges uniformly. Then it follows

$$\int_a^b f \,\mathrm{d}\alpha = \sum_{n=0}^{\infty} a_n \,\mathrm{d}\alpha\,.$$

Proof. Consider the sequence of partial sums

$$f_n(x) \coloneqq \sum_{k=0}^{n} a_k(x), \quad n = 0, 1, \ldots$$

It follows $f_n \in R_\alpha[a,b]$ and $f_n \rightrightarrows f$. Apply above theorem to $\{f_n\}$ and the conclusion follows. □

§15.4 Uniform Convergence and Differentiation

Theorem 15.4.1

Assume $\{f_n\}$ is a sequence of functions defined over $[a,b]$ and differentiable. If $\{f_n'\}$ uniformly converges on $[a,b]$ and $\{f_n\}$ converges at some point $x_0 \in [a,b]$, then $\{f_n\}$ uniformly converges on $[a,b]$ to some function f. Moreover, f is differentiable and

$$f'(x) = \lim_{n\to\infty} f_n'(x)$$

for any $x \in [a,b]$.

Proof.

□

§15.5 Stone–Weierstrass Approximation Theorem

16 Some Special Functions

§16.1 Power Series

We derive some properties of functions represented by **power series**, i.e. functions of the form

$$f(x) = \sum_{n=0}^{\infty} c_n x^n$$

or, more generally,

$$f(x) = \sum_{n=0}^{\infty} c_n (x-a)^n.$$

These are called **analytic functions**.

If $f(x)$ converges for $|x-a| < R$, f is said to be expanded in a power series about the point $x = a$. For convenience, we take $a = 0$ without loss of generality. We call R the **radius of convergence**.

Theorem 16.1.1

Suppose the series

$$\sum_{n=0}^{\infty} c_n x^n$$

converges for $x \in (-R, R)$. Then

(1) $\sum_{n=0}^{\infty} c_n x^n$ converges uniformly on the closed interval $[-R, R]$;

(2) $f(x)$ is continuous and differentiable on $(-R, R)$, and

$$f'(x) = \sum_{n=1}^{\infty} n c_n x^{n-1}.$$

Proof.

(i)

(ii)

□

Part V

Complex Analysis

17 Complex Numbers

§17.1 Definition of $\mathbb{C}$

As a set, $\mathbb{C} = \mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$. In other words, elements of $\mathbb{C}$ are pairs of real numbers.

$\mathbb{C}$ can be made into a field, by introducing addition and multiplication as follows:

(1) (addition) $(a, b) + (c, d) = (a + c, b + d)$

(2) (multiplication) $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

$\mathbb{C}$ is an Abelian group under +:

1. (associativity) $((a, b) + (c, d)) + (e, f) = (a, b) + ((c, d) + (e, f))$.
2. (identity) $(0, 0) satisfies (0, 0) + (a, b) = (a, b) + (0, 0) = (a, b)$.
3. (inverse) Given (a, b), $(-a, -b)$ satisfies $(a, b) + (-a, -b) = (-a, -b) + (a, b)$.
4. (commutativity) $(a, b) + (c, d) = (c, d) + (a, b)$.

$\mathbb{C} \setminus \{(0, 0)\}$ is also an Abelian group under multiplication. It is easy to verify the properties above. Note that $(1, 0)$ is the identity and $(a, b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

(Distributivity) If $z_1, z_2, z_3 \in \mathbb{C}$, then $z_1(z_2 + z_3) = (z_1 z_2) + (z_1 z_3)$.

Also, we require that $(1, 0) \neq (0, 0)$, i.e., the additive identity is not the same as the multiplicative identity.

§17.2 Basic properties of $\mathbb{C}$

From now on, we will denote an element of $\mathbb{C}$ by $z = x + iy$ (the standard notation) instead of (x, y). Hence $(a+ib)+(c+id) = (a+c)+i(b+d)$ and $(a+ib)(c+id) = (ac-bd)+i(ad+bc)$.

$\mathbb{C}$ has a subfield $\{(x, 0) \mid x \in \mathbb{R}\}$ which is isomorphic to $\mathbb{R}$. Although the polynomial $x^2 + 1$ has no zeros over $\mathbb{R}$, it does over $\mathbb{C}$: $i^2 = -1$.

Alternate descriptions of $\mathbb{C}$:

1. $\mathbb{R}[x]/(x^2+1)$, the quotient of the ring of polynomials with coefficients in $\mathbb{R}$ by the ideal generated by x^2+1.
2. The set of matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$, where the operations are standard matrix addition and multiplication.

Exercise 33

Prove that the alternate descriptions of $\mathbb{C}$ are actually isomorphic to $\mathbb{C}$.

Theorem 17.2.1 (Fundamental Theorem of Algebra)

$\mathbb{C}$ is algebraically closed, i.e., any polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.

This will be proved later, but at any rate the fact that $\mathbb{C}$ is algebraically closed is one of the most attractive features of working over $\mathbb{C}$.

§17.3 $\mathbb{C}$ as a vector space over $\mathbb{R}$

We will now view $\mathbb{C}$ as a vector space over $\mathbb{R}$. An $\mathbb{R}$-vector space is equipped with addition and scalar multiplication so that it is an Abelian group under addition and satisfies:

(1) $1z = z$,

(2) $a(bz) = (ab)z$,

(3) $(a+b)z = az + bz$,

(4) $a(z+w) = az + aw$.

Here $a, b \in \mathbb{R}$ and $z, w \in \mathbb{C}$. The addition for $\mathbb{C}$ is as before, and the scalar multiplication is inherited from multiplication, namely $a(x+iy) = (ax) + i(ay)$.

$\mathbb{C}$ is geometrically represented by identifying it with $\mathbb{R}^2$. (This is sometimes called the **Argand diagram**.)

§17.4 Complex conjugation and absolute values

Define **complex conjugation** as an $\mathbb{R}$-linear map $\mathbb{C} \to \mathbb{C}$ which sends $z = x + iy$ to $\overline{z} = x - iy$.

Properties of complex conjugation:

(1) $\overline{\overline{z}} = z$.

(2) $\overline{z+w} = \bar{z} + \bar{w}$.

(3) $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$.

Given $z = x + iy \in \mathbb{C}$, x is called the **real part** of C and y the **imaginary part**. We often denote them by $\operatorname{Re} z$ and $\operatorname{Im} z$:

$$\operatorname{Re} z = \frac{z+\bar{z}}{2}, \quad \operatorname{Im} z = \frac{z-\bar{z}}{2i}.$$

Define $|z| = \sqrt{x^2+y^2}$. Observe that, under the identification $z = x + iy \leftrightarrow (x, y)$, $|z|$ is simply the (Euclidean) norm of (x, y).

Properties of absolute values:

(1) $|z|^2 = z\bar{z}$.

(2) $|zw| = |z||w|$.

(3) (triangle inequality) $|z + w| \le |z| + |w|$.

The first two are staightforward. The last follows from computing

$$|z+w|^2 = (z+w)(\bar{z}+\bar{w}) = |z|^2 + |w|^2 + 2\operatorname{Re} z\bar{w} \le |z|^2 + |w|^2 + 2|z\bar{w}| = \big(|z| + |w|\big)^2.$$

18 Complex Functions

§18.1 Basic Topology

$\mathbb{C}$ is a metric space, where

$$d(z,w) = |z-w|.$$

Definition 18.1.1 (Open ball)
An ε-**ball** is defined as

$$B_\varepsilon(a) \coloneqq \{w \in \mathbb{C} \mid |w-a| < \varepsilon\}.$$

Definition 18.1.2 (Open set)
$U \subset \mathbb{C}$ is **open** if $\forall z \in U \exists \varepsilon > 0$ s.t. $B_\varepsilon(z) \subset U$.

The complement of an open set is said to be **closed**.

Proposition 18.1.3
Every ε-ball is open.

Definition 18.1.4 (Limit)
We say that $f(z)$ has **limit** A as $z \to a$, denoted by $\lim_{z\to a} f(z) = A$ if

$$\forall \varepsilon > 0 \exists \delta > 0 \text{ s.t. } 0 < |z-a| < \delta \implies |f(z) - A| < \varepsilon.$$

Definition 18.1.5 (Continuity)
$f : \Omega \to \mathbb{C}$ for $\Omega \subset \mathbb{C}$ open is **continuous** at z_0 if $\lim\limits_{z\to z_0} = f(z_0)$.

Proposition 18.1.6
f is continuous if and only if f is continuous at all $a \in \Omega$.

Proposition 18.1.7

If $f, g : \Omega \to \mathbb{C}$ are continuous, then so are $f+g$, fg and f/g (where the last one is defined over $\Omega \setminus \{x \mid g(x) = 0\}$).

§18.2 Analytic Functions

Definition 18.2.1

$f : \Omega \to \mathbb{C}$ for $\Omega \subset \mathbb{C}$ open is **complex differentiable** at $z_0 \in \Omega$ if the complex derivative

$$f'(z_0) \coloneqq \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

exists. If f is differentiable at all $z_0 \in \Omega$, then f is said to be **analytic** (holomorphic) on Ω.

Proposition 18.2.2

Suppose $f, g : \Omega \to \mathbb{C}$ are analytic. Then so are $f+g$, fg, f/g (where the last one is defined over $\Omega \setminus \{x \mid g(x) = 0\}$).

Example 18.2.3. $f(z) = 1$ and $f(z) = z$ are analytic functions from $\mathbb{C}$ to $\mathbb{C}$, with derivatives $f'(z) = 0$ and $f'(z) = 1$ respectively.

Therefore, all polynomials $f(z) = a_n z^n + \cdots + a_1 z + a_0$ are analytic, with $f'(z) = n a_n z^{n-1} + \cdots + a_1$.

Proposition 18.2.4

An analytic function is continuous.

Proof. Suppose $f : \Omega \to \mathbb{C}$ is analytic with derivative

$$f'(z) = \lim_{h \to 0} \frac{f(z+h) - f(z)}{h}.$$

Then

$$\lim_{h \to 0} \big(f(z+h) - f(z)\big) = f'(z) \lim_{h \to 0} h = 0.$$

□

§18.3 Cauchy–Riemann Equations

Write $f(z) = u(z) + iv(z)$, where $u, v : \Omega \to \mathbb{R}$ are real-valued functions. Suppose f is analytic. We compare two ways of taking the limit $f'(z)$:

First take h to be a real number approaching 0. Then

$$f'(z) = \frac{\partial f}{\partial x} = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x}.$$

Next, take h to be purely imaginary, i.e., let $h = ik$ for some $k \in \mathbb{R}$. Then

$$f'(z) = \lim_{k\to 0} \frac{f(z+ik) - f(z)}{ik} = -i\frac{\partial f}{\partial y} = -i\frac{\partial u}{\partial y} + \frac{\partial v}{\partial y}.$$

Comparing real and imaginary parts, we obtain

$$\frac{\partial f}{\partial x} = -i\frac{\partial f}{\partial y},$$

or, equivalently,

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \quad \text{and} \quad \frac{\partial v}{\partial x} = -\frac{\partial u}{\partial y}.$$

The equations above are called the **Cauchy–Riemann equations**.

Assuming for the time being that u, v have continuous partial derivatives of all orders (and in particular the mixed partials are equal), we can show that

$$\Delta u = \frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0, \quad \Delta v = \frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} = 0.$$

Such an equation $\Delta u = 0$ is called Laplace's equation and its solution is said to be a harmonic function.

§18.3.1 Geometric interpretation

§18.3.2 Harmonic functions

Part VI

Topology

19 Topological Spaces and Continuous Functions

§19.1 Topological Spaces

Definition 19.1.1

A **topological space** $(X, \mathcal{T})$ consists of a non-mepty set X together with a family $\mathcal{T}$ of subsets of X satisfying:

(1) $X, \varnothing \in \mathcal{T}$;

(2) if $U, V \in \mathcal{T}$, then $U \cap V \in \mathcal{T}$;

(3) If $U_i \in \mathcal{T}$ for all $i \in I$, then $\bigcup_{i \in I} U_i \in \mathcal{T}$.

The family $\mathcal{T}$ is called a **topology** for X. The sets in $\mathcal{T}$ are called the **open sets** of X. When $\mathcal{T}$ is understood we talk about the topological space X.

Remark. A consequence of (2) is that if $U_1, \ldots, U_n$ is a collection of open sets, then $U_1 \cap \cdots \cap U_n$ is open. But the intersection of infinitely many open sets need not be open!

On the other hand, in (3), the indexing set I is allowed to be infinite. It may even be uncountable.

Proposition 19.1.2

Let (X, d) be a metric space. Then the open subsets of X form a topology, denoted by $\mathcal{T}_d$.

Proof. Check through the conditions in the definition for a topological space:

(1) Trivial.

(2) Let U and V be open subsets of X. Consider an arbitrary point $x \in U \cap V$.

As U is open, there exists $r_1 > 0$ such that $B_{r_1}(x) \subseteq U$. Likewise, as $x \in V$ and V is open, there exists $r_2 > 0$ such that $B_{r_2}(x) \subseteq V$.

Take $r \coloneqq \min\{r_1, r_2\}$. Then $B_r(x) \subseteq B_{r_1}(x) \subseteq U$ and $B_r(x) \subseteq B_{r_2}(x) \subseteq V$. Hence $B_r(x) \subseteq U \cap V$.

(3) For every $x \in \bigcup_{i\in I} U_i$ there exists $k \in I$ such that $x \in U_k$. Since U_k is open, there exists $r > 0$ such that $B_r(x) \subseteq U_k \subseteq \bigcup_{i\in I} U_i$.

□

Example 19.1.3. The following are some other examples of topological spaces.

- (Discrete spaces) Let X be any non-empty set. The **discrete topology** on X is the set of all subsets of X.
- (Indiscrete spaces) Let X be any non-empty set. The **indiscrete topology** on X is the family of subsets $\{X, \varnothing\}$.
- Let X be any non-empty set. The **co-finite topology** on X consists of the empty set together with every subset U of X such that $X \setminus U$ is finite.

Definition 19.1.4

A topological space $(X, \mathcal{T})$ is **metrisable** if it arises from (at least oe) metric space (X, d), i.e. there is at least one metric d on X such that $\mathcal{T} = \mathcal{T}_d$.

Definition 19.1.5

Two metrics on a set are **topologically equivalent** if they give rise to the same topology.

Example 19.1.6.

- The metrics d_1, d_2, d_∞ on $\mathbb{R}^n$ are all topologically equivalent. (Recall that d_1, d_2, d_∞ are the metrics arising from the norms $\|\cdot\|_1$, $\|\cdot\|_2$, $\|\cdot\|_\infty$, respectively.) We shall call the topology defined by the above metrics the **standard** (or canonical) topology on $\mathbb{R}^n$.
- The discrete topology on a non-empty set X is metrisable, using the metric

$$d(x, y) = \begin{cases} 0 & \text{if } x = y, \\ 1 & \text{if } x \neq y. \end{cases}$$

  It is easy to check that this is a metric. To see that is gives the discrete topology, consider any subset $U \subseteq X$. Then for every $x \in U$, $B_{\frac{1}{2}}(x) \subseteq U$.

Definition 19.1.7

Given two topologies $\mathcal{T}1$ and $\mathcal{T}_2$ on the same set, we say $\mathcal{T}_1$ is **coarser** than $\mathcal{T}_2$ if $\mathcal{T}_1 \subseteq \mathcal{T}2$.

Remark. For any space $(X, \mathcal{T})$, the indiscrete topology on X is coarser than $\mathcal{T}$ which in turn is coarser than the discrete topology on X.

Definition 19.1.8

Let $(X, \mathcal{T})$ be a topological space. A subset V of X is **closed** in X if $X \setminus V$ is open in X (i.e. $X \setminus V \in \mathcal{T}$).

Example 19.1.9.

- In the space $[0, 1)$ with the usual topology coming from the Euclidean metric, $[1/2, 1)$ is closed.
- In a discrete space, all subsets are closed since their complements are open.
- In the co-finite topology on a set X, a subset is closed if and only if it is finite or all of X.

Proposition 19.1.10

Let X be a topological space. Then

(1) X, $\varnothing$ are closed in X;

(2) if V_1, V_2 are closed in X then $V_1 \cup V_2$ is closed in X;

(3) if V_i is closed in X for all $i \in I$ then $\bigcap_{i \in I} Vi$ is closed in X.

Proof. These properties follow from (1), (2), (3) of definition of topological space, and from the De Morgan laws. □

Definition 19.1.11 (Convergent sequence)

A sequence $\{x_n\}_{n \in \mathbb{N}}$ in a topological space X converges to a point $x \in X$ if given any open set U containing x there exists $N \in \mathbb{N}$ such that $x_n \in U$ for all $n > N$.

Example 19.1.12.

- In a metric space this is equivalent to the metric definition of convergence.
- In an indiscrete topological space X any sequence converges to any point $x \in X$.
- In an infinite space X with the co-finite topology any sequence $\{x_n\}$ of pairwise distinct elements (i.e. such that $x_n \neq x_m$ when $n \neq m$) converges to any point $x \in X$.

Part VII

Appendices

A H3 Mathematics

§A.1 A Level past year papers

2023

1. (a) Prove that, for any real numbers $a_1, a_2, \ldots, a_n$,

$$a_1 + a_2 + \cdots + a_n \leq \sqrt{n}\sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.$$

(b) Prove that, for any positive real numbers x, y and z,

$$\sqrt{\frac{x+y}{x+y+z}} + \sqrt{\frac{y+z}{x+y+z}} + \sqrt{\frac{z+x}{x+y+z}} \leq \sqrt{6}.$$

(c) Hence solve the equation

$$2\sqrt{\frac{x+3}{x+6}} + \sqrt{\frac{6}{x+6}} = \sqrt{6}.$$

Solution.

(a) Square both sides, apply Cauchy–Schwarz.

(b) Let

$$a_1 = \sqrt{\frac{x+y}{x+y+z}}, \quad a_2 = \sqrt{\frac{y+z}{x+y+z}}, \quad a_3 = \sqrt{\frac{z+x}{x+y+z}},$$

then apply (a) to the above three real numbers.

(c) Let $y = 3$, $z = 3$, then apply (b).
Equality in the Cauchy–Schwarz inequality holds if and only if

$$\left(\sqrt{\frac{x+3}{x+6}}, \sqrt{\frac{6}{x+6}}, \sqrt{\frac{x+3}{x+6}}\right) = \lambda(1,1,1)$$

for some $\lambda > 0$. This happens exactly when $x = 3$.

2.

3.

4. Let n stones be placed in fixed positions on a line. Each stone is painted using one of four colours (red, white, yellow or blue) in such a way that no two adjacent stones are the same colour. Let r_n be the number of ways of painting the stones such that the first and last stones are both red. Let s_n be the number of ways of painting the stones so that the first stone is red but the last stone is not red.

   (a) Explain why $r_1 = 1$, $r_2 = 0$, $s_1 = 0$ and $s_2 = 3$.

   (b) Find a formula for $r_n + s_n$ and explain why $r_{n+1} = s_n$.

   (c) Using mathematical induction, or otherwise, prove that for all $n \geq 4$,

   $$r_n = \frac{3^{n-1} + 3(-1)^{n-1}}{4}.$$

   (d) Now let n stones, where $n > 1$, be placed on a circle with numbered positions. Find the number of ways of painting these stones, using at most four distinct colours, in such a way that no two adjacent stones are the same colour.

□

Solution.

(a) If $n = 1$, then the first stone is also the las stone, and there is thus only 1 way to paint the stone red. So

$$r_1 = 1.$$

Since the first stone is red and the last stone, which is the first stone, is red, there is no way to paint the stone such that the last (first) stone is not red. So

$$s_1 = 0.$$

If $n = 2$, then the first and last (second) stones must be painted red but in doing so they will become adjacent stones painted red, which violates the condition that no two adjacent stones are the same colour. Hence

$$r_2 = 0.$$

(b) We use the following notation:

$R \coloneqq \{\text{painting arrangements such that first and last stones are red}\}$;
$S \coloneqq \{\text{painting arrangements such that first stone is red and last stone is not red}\}$;
$T \coloneqq \{\text{painting arrangements such that first stone is red}\}$.

By definition of r_n and s_n,

$$|R| = r_n, \quad |S| = s_n.$$

Since R and S are mutually exclusive such that $R \cup S = T$, we have

$$|T| = |R \cup S| = |R| + |S| = r_n + s_n.$$

On the other hand,

$$T = 1 \times \underbrace{3 \times 3 \times \cdots \times 3}_{n-1} = 3^{n-1}.$$

Thus

$$r_n + s_n = 3^{n-1}.$$

Observe that if $n+1$ stones are painted in such a way that the first and last stones are both red, then the n-th stone must necessarily be non-red since no two adjacent stones can share the sae colour. Therefore, the number of ways to paint $n+1$ stones such that the first and last stones are both red is equal to the number of ways to paint n stones such that the first stone is red and the last stone is not red. Thus, $r_{n+1} = s_n$.

(c)

(d)

□

2022

1.

2.

3.

4. (a) Let a and b be positive numbers such that $a + b = 1$. Using a sketch graph of $y = \ln x$, for $x > 0$, show that

$$u^a v^b \leq au + bv$$

for positive u and v.

(b) Let $a_1, a_2, a_3, \ldots$ be a sequence of positive numbers. Define

$$G_n = \sqrt[n]{a_1 a_2 \cdots a_n} \text{ and } A_n = \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

(i) Use the result of part (a) to prove that the sequence $\big(n(G_n - A_n)\big)$ is non-increasing.

(ii) Let the first 3 terms of the sequence (a_n) be 1, 2 and 4. Define a suitable a_n, for $n \geq 4$, so that $\big(n(G_n - A_n)\big)$ is constant for $n \geq 3$.

Solution.

(a) Sketch the graph $y = \ln x$ for $x > 0$, defined on the closed bounded interval $[u, v]$ for two positive real numbers $u < v$.

Since $a + b = 1$, the real number $au + bv$ lies in the interval $[u, v]$; that is,

$$u \leq au + bv \leq v.$$

Note that the equation of the straight line joining $(u, \ln u)$ and $(v, \ln v)$ is given by

$$y - \ln u = \frac{\ln v - \ln u}{v - u} \cdot (x - u).$$

When $x = au + bv$, the y-value on this straight line reads off

$$y = a \ln u + b \ln v.$$

Since $y = \ln x$ is concave, the y-value read off the straight line is at most the y-value read off the curve $y = \ln x$, and thus it follows that

$$a \ln u + b \ln v \leq \ln(au + bv)$$

or equivalently,

$$u^a b^v \leq a + bv.$$

(b)

□

5.

6.

7. (a) The diagram below shows a 3×3 array of circles, five of which are shaded. Of the 20 edges linking pairs of adjacent (including diagonally adjacent) circles, 11 link a shaded and an unshaded circle.

   (i) Describe or draw a 3×3 array of circles for which more than 11 edges link a shaded and an unshaded circle and state the number of such edges.

   The second diagram shows how the edges for a 4×4 array of circles can be grouped into square blocks (consisting of 6 edges) along a diagonal and arrowhead shapes (consisting of 4 edges) elsewhere. For clarity the circles are not shown.

   (ii) For the edges of an $n \times n$ array of circles grouped as in the second diagram, state the number of square blocks and arrowhead shapes that would be required.

   (iii) Explain why at most 3 of the edges in an arrowhead shape can link a shaded and an unshaded circle.

   (b) In the 3×3 grid below, some of the squares are shaded. The number in each unshaded square shows the number of shaded squares with which the unshaded square shares a vertex. The sum of all the numbers, 12, is the score of this arrangement of shaded and unshaded squares.

   (i) Explain, why, for any such arrangement, the score is unaltered by shading each unshaded square and vice versa.

   (ii) Find the maximum possible score for an $n \times n$ grid and prove that it can be attained.

2021

1.

2. Let a, b, c and r be positive real numbers.

   (a) Prove that

   $$a^r(a-b)(a-c) + b^r(b-c)(b-a) + c^r(c-a)(c-b) \geq 0.$$

   (b) Hence, or otherwise, prove that

   (i) $a^3 + b^3 + c^3 + 3abc \geq a^2(b+c) + b^2(c+a) + c^2(a+b)$,

   (ii) $\dfrac{1}{a^5} + \dfrac{1}{b^5} + \dfrac{1}{c^5} + \dfrac{a+b+c}{a^2b^2c^2} \geq \dfrac{b^2+c^2}{a^3b^2c^2} + \dfrac{c^2+a^2}{a^2b^3c^2} + \dfrac{a^2+b^2}{a^2b^2c^3}$.

   Solution.

   (a) WLOG assume $a \geq b \geq c$. Then the given expression can be rewritten as

   $$\underbrace{a^r(a-b)(a-c)}_{(1)} + \underbrace{(b-c)[b^r(b-a) - c^r(c-a)]}_{(2)}.$$

   For (1), since $a \geq b$ and $a \geq c$, we have $a-b \geq 0$ and $a-c \geq 0$. Since $a > 0$, we then have

   $$a^r(a-b)(a-c) \geq 0.$$

   Now for (2), since $b \geq c$ we have

   $$b^r(b-a) - c^r(c-a) \geq c^r(b-a-c+a) = c^r(b-c) \geq 0.$$

   Thus we have proven the given statement.

   (b) Choose $r = 1$, by (a), we have

   $$a(a-b)(a-c) + b(b-c)(b-a) + c(c-a)(c-b) \geq 0.$$

   Expanding LHS gives us the desired statement.

   (c) The term $\dfrac{a+b+c}{a^2b^2c^2}$ can be seen as $\dfrac{1}{ab^2c^2} + \dfrac{1}{bc^2a^2} + \dfrac{1}{ca^2b^2}$. This term can be compared to the term $3abc$ in the first part. From this observation, we consider Schur's inequality exhibited by

   $$\frac{1}{a}\left(\frac{1}{a^2} - \frac{1}{b^2}\right)\left(\frac{1}{a^2} - \frac{1}{c^2}\right) + \frac{1}{b}\left(\frac{1}{b^2} - \frac{1}{c^2}\right)\left(\frac{1}{b^2} - \frac{1}{a^2}\right) + \frac{1}{c}\left(\frac{1}{c^2} - \frac{1}{a^2}\right)\left(\frac{1}{c^2} - \frac{1}{b^2}\right) \geq 0.$$

   Expanding gives us

   $$\begin{aligned} &\frac{1}{a^5} - \frac{1}{a^3c^2} - \frac{1}{a^3b^2} + \frac{1}{ab^2c^2} \\ &+ \frac{1}{b^5} - \frac{1}{b^3a^2} - \frac{1}{b^3c^2} + \frac{1}{bc^2a^2} \\ &+ \frac{1}{c^5} - \frac{1}{c^3b^2} - \frac{1}{c^3a^2} + \frac{1}{ca^2b^2} \geq 0. \end{aligned}$$

Thus

$$\left(\frac{1}{a^5}+\frac{1}{b^5}+\frac{1}{c^5}\right)+\left(\frac{1}{ab^2c^2}+\frac{1}{bc^2a^2}+\frac{1}{ca^2b^2}\right) \geq \left(\frac{1}{a^3c^2}+\frac{1}{a^3b^2}\right)+\left(\frac{1}{b^3a^2}+\frac{1}{b^3c^2}\right)+\left(\frac{1}{c^3b^2}+\frac{1}{c^3a^2}\right).$$

which gives us the desired inequality.

□

3. Let u and v be quadratic functions of x and let

$$y = \frac{u}{v}.$$

(a) Use mathematical induction to prove that

$$v\frac{\mathrm{d}^{n+2}y}{\mathrm{d}x^{n+2}} + (n+2)\frac{\mathrm{d}v}{\mathrm{d}x}\frac{\mathrm{d}^{n+1}y}{\mathrm{d}x^{n+1}} + \binom{n+2}{2}\frac{\mathrm{d}^2v}{\mathrm{d}x^2}\frac{\mathrm{d}^ny}{\mathrm{d}x^n} = 0,$$

for $n \geq 1$.

(b) Now assume that $v = (\alpha - x)^2$ for some real number α and, for all positive integers n, define

$$z_n = \frac{(\alpha-x)^{n+2}}{n!}\frac{\mathrm{d}^ny}{\mathrm{d}x^n}.$$

Use the result of part (a) to prove that $z_1, z_2, z_3, \ldots$ is an arithmetic progression. By writing y as partial fractions, or otherwise, show that the common difference is $u(\alpha)$.

2020

1. (i) For any positive integer n and positive numbers x and y, prove that

$$\big((n-1)x+y\big)^n \geq n^n x^{n-1} y.$$

(ii) Hence, for any positive numbers a, b and c such that $abc = 1$, prove that

$$(1+a)^2(1+b)^3(1+c)^4 > 256.$$

Solution.

(i) Apply AM–GM on $\underbrace{x+\cdots+x}_{n-1}+y$.

(ii) Watching out for the various powers of 2, 3 and 4, we rewrite

$$\begin{aligned}
&(1+a)^2(1+b)^3(1+c)^4 \\
&= \big((2-1)1+a\big)^2 \cdot \left((3-1)\frac{1}{2}+b\right)^3 \cdot \left((4-1)\frac{1}{3}+c\right)^4 \\
&\geq \left(2^2 \cdot 1^{2-1} \cdot a\right) \cdot \left(3^3 \cdot \left(\frac{1}{2}\right)^{3-1} \cdot b\right) \cdot \left(4^4 \cdot \left(\frac{1}{3}\right)^{4-1} \cdot c\right) \\
&= 256abc = 256
\end{aligned}$$

where equality (for AM–GM) holds if and only if $a = \frac{1}{2}$, $b = \frac{1}{3}$ and $c = \frac{1}{4}$, which is impossible as it contradicts the given condition of $abc = 1$. Thus equality never holds, and so the inequality is a strict one.

□

2.

3. For any non-negative integer n, the function P_n is defined by

$$P_n(t) = \sum_{i=0}^{n} \frac{t^i}{i!}.$$

(i) Use mathematical induction to prove that

$$\int_0^t x^n e^{-x}\,\mathrm{d}x = n!\left(1 - e^{-t}P_n(t)\right).$$

(ii) State the value of

$$\int_0^\infty x^n e^{-x}\,\mathrm{d}x,$$

and briefly justify your answer.

(iii) For $n > t > 0$, prove that

$$\left(1+\frac{t}{n}\right)^n \leq P_n(t) < \left(1-\frac{t}{n}\right)^{-n}.$$

Solution.

(i) Formalise by stating the statement we want to prove:

$$P(n): \int_0^t x^n e^{-x}\,\mathrm{d}x = n!\left(1 - e^{-t}P_n(t)\right), \quad n = 0, 1, \ldots$$

When $n = 0$, we must prove that

$$\int_0^t x^0 e^{-x}\,\mathrm{d}x = 0!\left(1 - e^{-t}P_0(t)\right).$$

The working is direct:

$$\begin{aligned}\int_0^t x^0 e^{-x}\,\mathrm{d}x &= \int_0^t e^{-x}\,\mathrm{d}x \\ &= \left[-e^{-x}\right]_0^t \\ &= -e^{-t} + 1 \\ &= \underbrace{0!}_{=1}(1 - e^{-1}\ \underbrace{P_0(t)}_{=1})\end{aligned}$$

Assume that $P(n)$ holds, we want to prove that

$$P(n+1): \int_0^t x^{n+1} e^{-x}\,\mathrm{d}x = (n+1)!\left(1 - e^{-t}P_{n+1}(t)\right)$$

holds.

Integrating by parts, let

$$u = x^{n+1}, \quad \frac{\mathrm{d}v}{\mathrm{d}x} = e^{-x},$$

we have

$$\begin{aligned}&\int_0^t x^{n+1} e^{-x}\,\mathrm{d}x \\ &= \left[-x^{n+1}e^{-x}\right]_0^t - \int_0^t (n+1)x^n\left(-e^{-x}\right)\mathrm{d}x \\ &= \left(-t^{n+1}e^{-t}\right) + (n+1)\int_0^t x^n e^{-x}\,\mathrm{d}x \\ &= (n+1)!\left(1 - e^{-t}\left(P_n(t) + \frac{t^{n+1}}{(n+1)!}\right)\right) \\ &= (n+1)!\left(1 - e^{-t}P_{n+1}(t)\right)\end{aligned}$$

(ii)

$$\int_0^\infty x^n e^{-x}\,\mathrm{d}x = \lim_{t\to\infty} n!\left(1 - e^{-t}P_n(t)\right) = n!$$

since $\lim\limits_{t\to\infty} \dfrac{P_n(t)}{e^t} = 0$.

(iii) We start by proving the LHS:

$$\left(1 + \frac{t}{n}\right)^n \le P_n(t).$$

Using binomial expansion,

$$\left(1+\frac{t}{n}\right)^n = \sum_{k=0}^{n}\binom{n}{k}\frac{t^k}{n^k}.$$

We want to show that

$$\sum_{k=0}^{n}\binom{n}{k}\frac{t^k}{n^k} \le \sum_{k=0}^{n}\frac{t^k}{k!}.$$

This can be achieved if we are able to prove that

$$\frac{\binom{n}{k}}{n^k} \le \frac{1}{k!}$$

for $k = 0, 1, 2, \ldots, n$. And this is best approached by working backwards: since for all $j = 0, 1, 2, \ldots, n$, it holds that

$$\frac{n-(j-1)}{n} \le 1,$$

we must have that

$$\frac{n\times(n-1)\times\cdots\times(n-(k-1))}{n\times n\times\cdots\times n} \le 1.$$

Thus,

$$\frac{n!}{(n-k)!k!}\frac{1}{n^k} \le \frac{1}{k!}$$

and we have proved that

$$\frac{\binom{n}{k}}{n^k} \le \frac{1}{k!}$$

for $k = 0, 1, 2, \ldots, n$, as planned. This then implies that

$$\left(1+\frac{t}{n}\right)^n = \sum_{k=0}^{n}\binom{n}{k}\frac{t^k}{n^k} \le \sum_{k=0}^{n}\frac{t^k}{k!}.$$

We now prove the RHS:

$$P_n(t) < \left(1-\frac{t}{n}\right)^{-n}.$$

Note that $n > t > 0$, which implies that $-n$ is a negative integer and $\left|-\frac{t}{n}\right| < 1$, flagging out the warrant for us to apply Newton's binomial expansion:

$$\begin{aligned}
\left(1-\frac{t}{n}\right)^{-n} &= 1+(-n)\left(-\frac{t}{n}\right)+\frac{(-n)(-n-1)}{2!}\left(-\frac{t}{n}\right)^2+\frac{(-n)(-n-1)(-n-2)}{3!}\left(-\frac{t}{n}\right)^3+\cdots\\
&\quad+\frac{(-n)(-n-1)(-n-2)\cdots(-n-(k-1))}{k!}\left(-\frac{t}{n}\right)^k+\cdots\\
&= 1+t+\frac{n(n+1)}{2!}\left(\frac{t}{n}\right)^2+\frac{n(n+1)(n+2)}{3!}\left(\frac{t}{n}\right)^3+\cdots\\
&\quad+\frac{n(n+1)(n+2)\cdots(n+(k-1))}{k!}\left(\frac{t}{n}\right)^k+\cdots\\
&= 1+t+\frac{1\left(1+\frac{1}{n}\right)}{2!}t^2+\frac{1\left(1+\frac{1}{n}\right)\left(1+\frac{2}{n}\right)}{3!}t^3+\cdots+\frac{1\left(1+\frac{1}{n}\right)\left(1+\frac{2}{n}\right)\cdots\left(1+\frac{k-1}{n}\right)}{k!}t^k+\cdots\\
&> 1+t+\frac{t^2}{2!}+\frac{t^3}{3!}+\cdots+\frac{t^n}{n!}\\
&= P_n(t)
\end{aligned}$$

□

2019

1.

2.

3. A sequence is defined by

$$x_1 = 1 \text{ and } x_{i+1} = \left(\frac{i+a}{i+1}\right)x_i,\ i \geq 1.$$

(i) Assume that $a \geq 0$.

(a) Prove that $x_i \geq \frac{1}{i}$, for all positive integers i.

(b) Prove that

$$\sum_{i=n+1}^{2n} x_i \geq \frac{1}{2},$$

for all positive integers n.

(c) Hence prove that $\sum_{i=1}^{\infty} x_i$ is unbounded.

(ii) Assume that $a < 0$.

(a) Prove that

$$a\sum_{i=m}^{n} x_i = (n+1)x_{n+1} - mx_m$$

for all positive integers m and n such that $n > m$.

(b) For any sufficiently large integers m and n, prove that $x_m x_n \geq 0$.

Solution.

(i) (a) We proceed to prove the statement

$$P(n) : x_n \geq \frac{1}{n}, \quad n = 1, 2, 3, \ldots$$

$P(1)$ is true since $x_1 = 1 \geq \frac{1}{1}$.
Assume that $P(k)$ holds for some $k \in \mathbb{Z}^+$; that is,

$$x_k \geq \frac{1}{k}.$$

We want to prove $P(k+1)$ holds; that is,

$$x_{k+1} \geq \frac{1}{k+1}.$$

Since $x_{k+1} = \left(\frac{k+a}{k+1}\right)x_k$, by the inductive hypothesis $P(k)$ we deduce that

$$x_{k+1} = \left(\frac{k+a}{k+1}\right)x_k \geq \left(\frac{k+a}{k+1}\right)\cdot\frac{1}{k} = \underbrace{\left(1+\frac{a}{k}\right)}_{\geq 1}\cdot\frac{1}{k+1} \geq \frac{1}{k+1}.$$

Since $P(1)$ holds and $P(k) \implies P(k+1)$ for all $k \in \mathbb{Z}^+$, by mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}^+$.

(b)

$$\begin{aligned}\sum_{i=n+1}^{2n} x_i &= x_{n+1} + x_{n+2} + \cdots + x_{2n} \\ &\geq \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \\ &\geq \frac{1}{2n} + \frac{1}{2n} + \cdots + \frac{1}{2n} \\ &= \frac{1}{2n} \times n = \frac{1}{2}\end{aligned}$$

(c) Informally, we see that

$$\begin{aligned}\sum_{i=1}^{\infty} &= x_1 + x_2 + (x_3 + x_4) + (x_5 + x_6 + x_7 + x_8) + \cdots \\ &\geq 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots\end{aligned}$$

which provides compelling evidence that $\sum_{i=1}^{\infty} x_i$ is unbounded.
We not write this argument in a rigorous manner. To show that $\sum_{i=1}^{\infty} x_i$ is unbounded, one must show that for any $M > 0$, there exists $N \in \mathbb{Z}^+$ such that

$$\sum_{i=1}^{N} x_i > M.$$

Indeed, given any $M > 0$, there exists $k \in \mathbb{Z}^+$ so large that

$$k > 2(M-1) \iff 1 + k \cdot \frac{1}{2} > M.$$

Thus it follows that

$$\begin{aligned}\sum_{i=1}^{2^k} x_i &= x_1 + x_2 + (x_3 + x_4) + (x_5 + x_6 + x_7 + x_8) + \cdots + (x_{2^{k-1}+1} + \cdots + x_{2^k}) \\ &> 1 + \underbrace{\frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2}}_{k \text{ terms}} \\ &= 1 + k \cdot \frac{1}{2} > M.\end{aligned}$$

(ii) (a) By definition,

$$x_{i+1} = \left(\frac{i+a}{i+1}\right) x_i, \quad i \geq 1.$$

So

$$(i+1)x_{i+1} = (i_1)x_i \iff (i_1)x_{i+1} - ix_i = ax_i.$$

Thus, if $n > m$ we have

$$\begin{aligned}\sum_{i=m}^{n} ax_i &= \sum_{i=m}^{n}[(i+1)x_{i+1} - ix_i] \\ &= (m+1)x_{m+1} - mx_m \\ &+ (m+2)x_{m+2} - (m+1)x_{m+1} \\ &+ \vdots \\ &+ (n+1)x_{n+1} - nx_n \\ &= (n+1)x_{n+1} - mx_m\end{aligned}$$

by the method of difference.

(b) For We want to prove that there exists a large enough $N \in \mathbb{N}$ such that if $m, n \geq N$ then $x_m x_n \geq 0$. Notice that in the situation when neither of x_m or x_n is zero these two numbers will have the same sign, i.e. either they are both negative or both positive.
By the recursive definition of x_i's, if $n > m$ then

$$x_n = \frac{n-1+a}{n} \cdot \frac{n-2+a}{n-1} \cdots \frac{m+a}{m+1} x_m.$$

Since $a < 0$ is fixed, there exists a sufficiently large positive integer N such that $N - a > 0$. Consequently, if $n > m \geq N$, we have

$$x_n = \underbrace{\frac{n-1+a}{n}}_{>0} \cdot \underbrace{\frac{n-2+a}{n-1}}_{>0} \cdots \underbrace{\frac{m+a}{m+1}}_{>0} x_m.$$

Hence x_n and x_m are of the same sign.

□

Remark. The question whether one can make use of (a) to solve (b) remains open.

4. An n-digit number uses no digits other than 1, 2 and 3. It does not have any 2s adjacent to each other, and it does not have any 3s adjacent to each other. Let there be T_n such numbers, with X_n of these having first digit 1 and Y_n having first digit 2.

   (a) Prove that, for any $n \geq 2$,
   (i) $Y_n = X_{n-1} + Y_{n-1}$,
   (ii) $X_n = X_{n-1} + 2Y_{n-1}$,
   (iii) $X_{n+1} = 2X_n + X_{n-1}$.

   (b) Use mathematical induction to prove that, for $n \geq 1$,

$$X_n \equiv n^2 - n + 1 \pmod 4.$$

   (c) Find and simplify an expression for $T_n \pmod 4$.

5. (i) Use the substitution $t = \frac{du}{dx}$ to find the general solution of the equation

$$\frac{d^2u}{dx^2} = \frac{du}{dx}.$$

(ii) Show that the differential equation can be transformed into the equation

$$f(x)\frac{d^2u}{dx^2} - \left(f'(x) + f(x)g(x)\right)\frac{du}{dx} = 0$$

by the substitution

$$u = e^{-\int f(x)y\,dx}.$$

(iii) A solution curve of the differential equation

$$\frac{dy}{dx} = e^{-2x}y^2 + 3y$$

passes through the point $\left(0, -\frac{1}{4}\right)$. Find the equation of the curve.

2018

1. A triangle has sides of lengths a, b and c units. In each of the following cases, prove that there is a triangle having sides of the given lengths.

   (i) $\dfrac{a}{1+a}$, $\dfrac{b}{1+b}$ and $\dfrac{c}{1+c}$ units.

   (ii) $\sqrt{a}$, $\sqrt{b}$ and $\sqrt{c}$ units.

   (iii) $\sqrt{a(b+c-a)}$, $\sqrt{b(c+a-b)}$ and $\sqrt{c(a+b-c)}$ units.

2.

3.

4. A clothes shop sells a particular make of T-shirt in four different colours. The shopkeeper has a large number of T-shirts of each colour.

   (i) A customer wishes to buy seven T-shirts.

   (a) In how many ways can he do this?

   (b) In how many ways can he do this if he buys at least one of each colour.

   (ii) The shopkeeper places seven T-shirts in a line.

   (a) In how many ways can she do this?

   (b) In how many ways can she do this if no two T-shirts of the same colour are to be next to each other?

   (c) Use the principle of inclusion and exclusion to find the number of ways in which she can do this if she has to use at least one T-shirt of each colour but with no other restrictions.

5. A $p \times q$ chessboard can be tessellated with $a \times b$ tiles.

   A unit square (x, y) is shaded if and only if $x \equiv y \pmod{a}$.

   (i) Explain why the following are necessary conditions for such a tessellation

   (a) ab is a factor of pq.

   (b) p and q can be written in the form $ma+nb$ where m and n are non-negative integers.

   (c) The $p \times q$ chessboard has $\dfrac{pq}{a}$ shaded squares.

   (ii) Let t be the smaller of r and s such that

   $$\begin{aligned} p &\equiv r \pmod{a} \quad 0 \le r < a \\ q &\equiv s \pmod{a} \quad 0 \le s < a \end{aligned}$$

   (a) Explain why the number of shaded squares in the $p \times q$ chessboard is $\dfrac{pq - rs}{a} + t$.

   (b) Hence prove that for a tessellation, either $a \mid p$ or $a \mid q$.

   Solution.

(i) (a) A $p \times q$ chessboard has pq squares, a $a \times b$ tile has ab squares.
Suppose k tiles are used to tessellate the board. Then $pq = kab$. Hence $ab \mid pq$.

(b) p and q are the height and base of the $p \times q$ chessboard respectively, a and b are the height and base of each $a \times b$ tile respectively. Each tile can be places horizontally or vertically in the tessellation.
If we tessellate the board at the bottom from left to right with m vertical and n horizontal tiles, there will be $ma + nb$ squares at the bottom row of the board. Each row of the board is made up of q squares. So we get $q = ma + nb$.
Similarly, if we tessellate the board on the left from bottom to top, we will get $p = sa + tb$ (with s horizontal and t vertical tiles).

(ii) (a)

□

6. (Dirichlet's approximation theorem) Let x be any positive real numbers and n be any positive integer. Prove that there are integers a and b with $1 \le b \le n$, such that

$$\left| x - \frac{a}{b} \right| < \frac{1}{bn}.$$

Solution. For any real number y, we write $y = \lfloor y \rfloor + \{y\}$, where $\lfloor y \rfloor$ denotes the integer part of y and $\{y\}$ denotes the fractional part of y, $0 \le \{y\} < 1$.

We divide the interval $[0, 1)$ into n smaller intervals of measure $\frac{1}{n}$. Consider $\{x\}, \{2x\}, \ldots, \{nx\}$. Let I_i denote the interval $\left[\frac{i-1}{n}, \frac{i}{n}\right]$, where $1 \le i \le n$.

We now consider two cases:

Case 1: Some $\{kx\}$ falls in I_1

Then $kx - \lfloor kx \rfloor = \{kx\} < \frac{1}{n}$.

Dividing both sides by k,

$$\left| x - \frac{\lfloor kx \rfloor}{k} \right| < \frac{1}{kn}.$$

By taking $a = \lfloor kx \rfloor$ and $b = k$, we have the inequality.

Case 2: None of $\{kx\}$ falls in I_1

This means all $\{kx\}$ fall into $I_2, I_3, \ldots, I_n$. By Pigeonhole Principle, at least two $\{kx\}$ fall in the same I_i.

Let $\frac{i-1}{n} \le \{px\} < \frac{i}{n}$ and $\frac{i-1}{n} \le \{qx\} < \frac{i}{n}$. Then

$$\begin{aligned}
\big|\{px\} - \{qx\}\big| &< \frac{1}{n} \\
\big|(px - \lfloor px \rfloor) - (qx - \lfloor qx \rfloor)\big| &< \frac{1}{n} \\
\big|(px - qx) - (\lfloor px \rfloor - \lfloor qx \rfloor)\big| &< \frac{1}{n} \\
\big|(p - q)x - (\lfloor px \rfloor - \lfloor qx \rfloor)\big| &< \frac{1}{n}
\end{aligned}$$

Dividing both sides by $p-q$,

$$\left| x - \frac{(\lfloor px \rfloor - \lfloor qx \rfloor)}{p-q} \right| < \frac{1}{(p-q)n}.$$

WLOG assume $p > q$. Then $1 \leq p-q < n$. By taking $a = \lfloor px \rfloor - \lfloor qx \rfloor$ and $b = p-q$, we have the inequality. □

7. The differential equation

$$y\frac{\mathrm{d}y}{\mathrm{d}x} = x\left(\frac{\mathrm{d}y}{\mathrm{d}x}\right)^2 + 1, \quad \text{for } x > 0 \tag{1}$$

has a solution curve S such that $\frac{\mathrm{d}^2y}{\mathrm{d}x^2}$ is non-zero for all points of S.

(i) By substituting $t = \frac{\mathrm{d}y}{\mathrm{d}x}$ into equation (1) and differentiating with respect to x, show that S has equation $y^2 = 4x$.

(ii) Show that a straight line is tangent to the curve S if and only if it is itself a solution of the equation.

8. For any positive real number x, $\mathrm{n}(x)$ is defined as the nearest integer to x, with halves rounded up.

For example, $\mathrm{n}(3.5) = 4$, and $\mathrm{n}(\pi) = 3$.

(a) Show that $\sum_{r=1}^{3} \mathrm{n}\left(\frac{11}{7}r\right) = 10$.

The diagram shows the line $y = \frac{7}{11}x + \frac{1}{2}$ and the integer (x, y) such that $1 \leq x \leq 5$, $1 \leq y \leq 3$.

(b) Find $\sum_{r=1}^{5} \mathrm{n}\left(\frac{7}{11}r\right)$ and explain the connection between your answer and the points underneath the line $y = \frac{7}{11}x + \frac{1}{2}$.

(c) The line $y = \frac{7}{11}x + \frac{1}{2}$ is rotated through 180° about $(3, 2)$. Find the equation of the new line in the form $x = my + c$ and hence comment on the connection between

$$\sum_{r=1}^{3} \mathrm{n}\left(\frac{11}{7}r\right) = \sum_{r=1}^{5} \mathrm{n}\left(\frac{7}{11}r\right).$$

(d) Let p and q be odd integers greater than 1 and consider the integer points (x, y) such that $1 \leq x \leq \frac{p-1}{2}$, $1 \leq y \leq \frac{q-1}{2}$. Let N be the number of points which lie in between the lines $y = \frac{q}{p}x + \frac{1}{2}$ and $x = \frac{p}{q}y + \frac{1}{2}$.

Explain why $N + \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) \equiv 0 \pmod 2$.

2017

1.

2. (i) Let y be a differentiable function of x. For any positive integer n, prove that

$$\frac{\mathrm{d}^n}{\mathrm{d}x^n}(xy) = x\frac{\mathrm{d}^n y}{\mathrm{d}x^n} + n\frac{\mathrm{d}^{n-1}y}{\mathrm{d}x^{n-1}}.$$

(ii) For any non-negative integer n, define

$$y_n = e^{x^2}\frac{\mathrm{d}^n}{\mathrm{d}x^n}\left(e^{-x^2}\right).$$

(a) Find y_0, y_1 and y_2.
(b) Prove that $y_{n+2} + 2xy_{n+1} + 2(n+1)y_n = 0$, for $n \geq 0$.
(c) Hence prove that $\frac{\mathrm{d}}{\mathrm{d}x}(y_{n+1}) = -2(n+1)y_n$, for $n \geq 0$.

3. (a) Consider integer solutions of the equation

$$1591x + 3913y = 9331.$$

Show that there is no solution with x prime.

(b) Let a, b, r and s be integers such that

$$ra + sb = 1.$$

(i) Prove that, if a and b are both factors of an integer n, then ab is a factor of n.
(ii) Given that any integers u and v, prove by construction that there is an integer x such that both

$$x \equiv u \pmod{a} \quad \text{and} \quad x \equiv v \pmod{b}.$$

Solution.

(a) First we find $\gcd(1591, 3913)$ using the Euclidean Algorithm.

$$\begin{aligned} 3913 &= 2 \times 1591 + 731 \\ 1591 &= 2 \times 731 + 129 \\ 731 &= 5 \times 129 + 86 \\ 129 &= 1 \times 86 + 43 \\ 86 &= 2 \times 43 + 0 \end{aligned}$$

Thus $\gcd(1591, 3913) = 43$. By Bezout's Lemma, there are integer solutions for $1591x + 3913y = 43$. Since $43 \mid 9331$, multiplying both sides by some constant, there are also integer solutions for $1591x + 3913y = 9331$.

To prove by contradiction, we assume that x is prime, and there exists some integer y such that $1591x + 3913y = 9331$. Dividing both sides by 43,

$$37x + 91y = 217. \qquad (\star)$$

Observe that $7 \mid 91y$ and $7 \mid 217$, so $7 \mid 37x$.
Since $\gcd(7, 37) = 1$ so $7 \mid x$. By our assumption, x is a prime so $x = 7$.
Substituting $x = 7$ into $(\star)$, we get $y = -\dfrac{6}{13}$, which contradicts y being an integer.
Hence we conclude that x cannot be a prime.

(b) (i) If a and b are both factors of n, then we have $n = pa$ and $n = qb$ for some integers p and q.
Given $ra + sb = 1$, we have

$$\begin{aligned} rna + snb &= n \\ r(qb)a + s(pa)b &= n \\ (rq + sp)ab &= n \end{aligned}$$

and hence ab is a factor of n.

(ii) Prove by construction.
Given that $ra + sb = 1$. Multiplying both sides by $v - u$ gives

$$\begin{aligned} ra(v-u) + sb(v-u) &= v - u \\ ra(v-u) + u &= sb(u-v) + v \end{aligned}$$

We define $x = ra(v-u) + u = sb(u-v) + v$. Then $x \equiv u \pmod{a}$ and $x \equiv v \pmod{b}$. **Remark.** The above proof shows the *existence* of solution by a construction.

□

4. Let $I_n = \displaystyle\int_0^{\frac{\pi}{4}} \tan^n x \, \mathrm{d}x$.

(i) For $n > 1$, prove that $I_n + I_{n+2} = \dfrac{1}{n-1}$.

(ii) Justify the statement that $\tan x \le \dfrac{4}{\pi}x$ on $\left[0, \dfrac{\pi}{4}\right]$.

(iii) Hence, prove that I_n tends to zero as n tends to infinity.

(iv) Find the sum of the infinite series

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

Solution.

(i)

$$\begin{aligned} I_n + I_{n-2} &= \int_0^{\frac{\pi}{4}} \left(\tan^n x + \tan^{n-2} x\right) \mathrm{d}x \\ &= \int_0^{\frac{\pi}{4}} \tan^{n-2} x \left(\tan^2 x + 1\right) \mathrm{d}x \\ &= \int_0^{\frac{\pi}{4}} \tan^{n-2} x \cdot \sec^2 x \, \mathrm{d}x \\ &= \left[\frac{\tan^{n-1} x}{n-1}\right]_0^{\frac{\pi}{4}} = \frac{1}{n-1}. \end{aligned}$$

(ii) Sketch the graphs of $y = \tan x$ and $y = \frac{4}{\pi}x$ over the interval $\left[0, \frac{\pi}{4}\right]$.
Since $y = \tan x$ is convex over $\left[0, \frac{\pi}{4}\right]$, it follows that

$$\tan x \leq \frac{4}{\pi}x$$

for all $x \in \left[0, \frac{\pi}{4}\right]$.

(iii)

(iv)

□

5. (i) Explain why the number of ways to distribute r distinct objects, where $r \geq 2$, into 2 distinct boxes such that neither is empty is $2^r - 2$.

(ii) Let $S(r, n)$ denote the number of ways to distribute r objects into n identical boxes such that no box is empty.

(a) Explain why, for $r \geq 3$,

$$S(r, 3) = 2^{r-2} - 1 + 3S(r-1, 3).$$

(b) Prove that, for $r \geq 3$,

$$S(r, 3) = \begin{cases} 0 \pmod 6 & \text{if } r \text{ is even,} \\ 1 \pmod 6 & \text{if } r \text{ is odd.} \end{cases}$$

6.

7.

8. The Fibonacci sequence is defined recursively by $F_{n+1} = F_n + F_{n-1}$ and $F_1 = 1, F_2 = 1$.

(i) Find the periods of Fibonacci sequences modulo 3 and 4.

(ii) For any positive integer m, show that we can find two pairs (F_j, F_{j+1}) and (F_k, F_{k+1}) which are the same modulo m with $1 \leq j < k \leq m^2 + 1$.

(iii) For m, j and k as in (ii), explain why the Fibonacci sequence modulo m is periodic with period dividing $k - j$.

(iv) For any positive integer m, prove that there is a Fibonacci number which is a multiple of m.

0

Solution.

(i) Modulo 3: $1, 1, 2, 0, 2, 2, 1, 0, 1, 1, \ldots$ has period 8.
Modulo 4: $1, 1, 2, 3, 1, 0, 1, 1, \ldots$ has period 6.

(ii) Modulo m, there are m possible values $0, 1, 2, \ldots, m-1$. So there are exactly m^2 possible distinct pairs (a, b).
If we consider $m^2 + 1$ pairs of (F_i, F_{i+1}) modulo m where $1 \leq i \leq m^2 + 1$, we can find two pairs (F_j, F_{j+1}) and (F_k, F_{k+1}) which are the same modulo m, by Pigeonhole Principle.

(iii) This is the same as showing $F_{j+n} \equiv F_{k+n} \pmod{m}$ for all non negative integer n.

We prove using mathematical induction.

Basis step: $P(0)$ and $P(1)$

$$F_j \equiv F_k \pmod{m} \quad F_{j+1} \equiv F_{k+1} \pmod{m}$$

Inductive step: $P(q-1) \wedge P(q) \implies P(q+1)$ for all $q \geq 1$

Given $F_{j+q-1} \equiv F_{k+q-1} \pmod{m}$ and $F_{j+q} \equiv F_{k+q} \pmod{m}$. Then $F_{j+q-1} + F_{j+q} \equiv F_{k+q-1} + F_{k+q} \pmod{m}$ so $F_{j+q+1} \equiv F_{k+q+1} \pmod{m}$.

By mathematical induction, the sequence repeats itself after $k-j$ terms. This implies the period of the sequence divides $k-j$.

(iv) For any positive m, by part (iii), the Fibonacci sequence modulo m is periodic. That is, (F_1, F_2) is congruent to (F_i, F_{i+1}) modulo m for some $i > 2$:

$$F_i \equiv F_1 \equiv 1 \pmod{m} \quad F_{i+1} \equiv F_2 \equiv 1 \pmod{m}$$

Then $F_{i-1} = F_{i+1} - F_i \equiv 1 - 1 \equiv 0 \pmod{m}$, which means $m \mid F_{i-1}$.

We have proven that there is a Fibonacci number which is a multiple of m.

□

Specimen

1.

2.

3. (Fermat's Little Theorem)

   (i) Let p be an odd prime and let a be an integer not divisible by p.

      (a) Let T be the set of remainders for $a, 2a, \ldots, (p-1)a$, when divided by p. Show that $T = \{1, 2, \ldots, p-1\}$.

      (b) Hence prove that $a^{p-1} \equiv 1 \pmod{p}$.

   (ii) Let x and y be two integers such that $x^5 + y^5$ is divisible by 5. Prove that $x^5 + y^5$ is divisible by 25.

   Solution.

   (i) (a) Let $S = \{1, 2, 3, \ldots, p-1\}$, the set of all non-zero positive remainders obtained when integers are divided by p.
   Known fact: $p \nmid k$ for all $k \in S = \{1, 2, 3, \ldots, p-1\}$.
   Given that T is the set of remainders when $a, 2a, 3a, \ldots, (p-1)a$ are divided by p.
   Clearly, $T \subseteq S \cup \{0\}$.
   Claim 1: $0 \notin T$. **Proof.** Prove by contradiction.
   Suppose $0 \in T$. Then $p \mid ka$ for some $k \in S = \{1, 2, 3, \ldots, p-1\}$. Since p is prime and $p \nmid a$, we apply Euclid's Lemma to conclude that $p \mid k$, which contracts Fact 1.]
   Thus $T \subseteq S$. □
   Claim 2: $T = S$ itself. **Proof.** Prove by contradiction.
   Suppose, on the contrary, that $T \neq S$.
   Then, $T \subset S$ (i.e. T is a proper subset of S).
   Since the sets are finite sets, $n(T) < n(S) = p - 1$. By the Pigeonhole Principle, there are (at least) two distinct ia and ja (from the list of $p-1$ terms: $a, 2a, 3a, \ldots, (p-1)a$ – the "pigeons"), where $1 \leq i \neq j \leq p-1$ that share the same remainder when divided p. The "holes" are the elements in T; here we get less holes: $n(T) < p - 1$ based on our (wrong) assumption.

$$\begin{aligned} ia &\equiv ja \pmod{p} \\ ia - ja &\equiv 0 \pmod{p} \\ (i-j)a &\equiv 0 \pmod{p} \end{aligned}$$

   We can cancel a on both sides due to Euclid's lemma. Hence $i \equiv j \pmod{p}$. Since both i and j belong to S, having them share the same remainder when divided by p means that they are actually the same. Thus $i = j$. This contradicts our initial choice of distinct ia and ja.
   Hence $T = S = \{1, 2, 3, \ldots, p-1\}$. □

(b) Let

$$\begin{aligned} a \cdot 1 &\equiv r_1 \pmod{p} \\ a \cdot 2 &\equiv r_2 \pmod{p} \\ a \cdot 3 &\equiv r_3 \pmod{p} \\ &\vdots \\ a \cdot (p-1) &\equiv r_{p-1} \pmod{p} \end{aligned}$$

where $r_1, r_2, r_3, \ldots, r_{p-1}$ are distinct elements of $T = S = \{1, 2, 3, \ldots, p-1\}$. So multiplying the LHS and RHS respectively of these congruence equations,

$$a^{p-1}(p-1)! \equiv r_1 r_2 r_3 \cdots r_{p-1} \pmod{p}$$

Since $r_1, r_2, r_3, \ldots, r_{p-1}$ is just a rearrangement of $1, 2, 3, \ldots, p-1$,

$$a^{p-1}(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

or

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

But $p \nmid (p-1)!$ so by Euclid's lemma,

$$a^{p-1} \equiv 1 \pmod{p}$$

as desired.

(ii) Prove by cases

Given 5 divides $x^5 + y^5$.

Case 1: either x or y is divisible by 5

WLOG, assume $5 \mid x$. Then $x = 5k$ for some integer k.

Then $x^5 = (5k)^5 = 5^2(5^3k^5) = 25t$ so $25 \mid x^5$.

Since we can write $y^5 = (x^5 + y^5) - x^5$, $5 \mid y^5$ so $5 \mid y$. We can then similarly show that $25 \mid y^5$.

Hence $25 \mid x^5 + y^5$.

Case 2: both x and y are not divisible by 5

Since 5 is a prime, by Fermat's Little Theorem, $x^5 \equiv x \pmod 5$ and $y^5 \equiv y \pmod 5$, so $x^5 + y^5 \equiv x + y \pmod 5$.

Since $5 \mid x^5 + y^5$, we have also $5 \mid x + y$, i.e. $x + y = 5k$ for some integer k. We rewrite $y = 5k - x$.

Then by binomial expansion,

$$y^5 = (5k - x)^5 = \sum_{i=0}^{5} \binom{5}{i} (5k)^{5-i}(-x)^i$$

which gives $y^5 \equiv (-x)^5 \pmod{25}$ as all the other terms are divisible by 25.

Hence $x^5 + y^5 \equiv 0 \pmod{25}$.

□

4.

5.

6.

7. The figures below show, respectively, a square board of 4 unit squares with one unit square covered, and a triomino consisting of 3 unit squares.

   Irrespective of which unit square is covered, a triomino can cover the remaining 3 unit squares of the square board as shown.

   Consider a square board made up of 4^n squares, where $n \geq 1$, with one of the unit squares covered. An example of such a square, with $n = 3$, is shown below.

   (i) Explain how, irrespective of unit square is covered, a triomino can be placed on the board in such a way that each quarter of the board now has one unit square covered.

   (ii) Use mathematical induction to prove that, irrespective of which unit square is initially covered, the remaining squares can be covered by triominoes. State the number of triominoes required.

Problem 30 (H3M 2021)**.** Let $Q = \{1, 2, \ldots, p-1\}$ for some prime p, and let there be N integers in Q whose cubes are congruent to 1 modulo p.

(a) Use the pigeonhole principle to prove that for each integer $x \in Q$ there is precisely one integer $y \in Q$ such that $xy \equiv 1 \pmod{p}$.

(b) Explain why the number of choices of integers $x, y, z \in Q$ such that $xyz \equiv 1 \pmod{p}$ is $(p-1)^2$.

(c) Use the principle of inclusion and exclusion to prove that the number of choices of three different integers $x, y, z \in Q$ such that $xyz \equiv 1 \pmod{p}$ is $(p-1)(p-4) + 2N$.

(d) Hence prove that $N \equiv (p-1)^2 \pmod{3}$.

(e) Given that $p \equiv 1 \pmod{3}$, prove that there is an integer $x \in Q$ such that $x^2+x+1 \equiv 0 \pmod{p}$.

Solution.

(a) Note that, by Quotient Remainder Theorem, every integer not divisible by p is congruent to an integer in Q modulo p, and no two integers in Q are congruent to each other modulo p.

We have two parts to prove: existence and uniqueness of inverse modulo p

Existence: prove by contradiction

Suppose there is an $x \in Q$ such that for all $y \in Q$, $xy \not\equiv 1 \pmod{p}$.

There are $p-1$ possible $y \in Q$, but there are less than $p-1$ possible $xy \in Q$ (since $xy \equiv 1 \pmod{p}$ is excluded).

By Pigeonhole Principle, there are two different $y_1, y_2 \in Q$ such that $xy_1 \equiv xy_2 (\not\equiv 1) \pmod{p}$. Then

$$p \mid xy_1 - xy_2 \implies p \mid x(y_1 - y_2) \implies p \mid y_1 - y_2 \implies y_1 \equiv y_2 \pmod{p} \implies y_1 = y_2$$

which is a contradiction. Hence every $x \in Q$ has a $y \in Q$ such that $xy \equiv 1 \pmod{p}$.

Uniqueness: prove by contradiction

Suppose there are two different $y_1, y_2 \in Q$ such that $xy_1 \equiv xy_2 (\equiv 1) \pmod{p}$.

The rest is similar to the above, and thus left as an exercise to the reader.

(b) Use combinatorics.

There are $p-1$ ways each to choose x and y.

By (a), there is only 1 way to choose $z \in Q$, the modular inverse of xy mod p, such that $(xy)z \equiv 1 \pmod{p}$.

Hence there is a total number of $(p-1)^2$ choices of x, y, z such that $xyz \equiv 1 \pmod{p}$.

(c) Let U contain all (x, y, z) such that $xyz \equiv 1 \pmod{p}$, A is a subset of U such that $x \equiv y \pmod{p}$, B is a subset of U such that $x \equiv z \pmod{p}$, C is a subset of U such that $y \equiv z \pmod{p}$.

Note that $A \cap B = A \cap C = B \cap C = A \cap B \cap C$ are all subsets of U such that $x \equiv y \equiv z \pmod{p}$, i.e. this subset of U contains all (x, x, x) such that $x^3 \equiv 1 \pmod{p}$.

We have $|U| = (p-1)^2$ from (b), $|A| = |B| = |C| = p-1$, and $|A \cap B \cap C| = N$.

By principle of inclusion and exclusion,

$$|A \cup B \cup C| = 3(p-1) - 2N.$$

To find the complement of $A \cup B \cup C$,

$$|U - (A \cup B \cup C)| = (p-1)^2 - \big(3(p-1) - 2N\big) = (p-1)(p-4) + 2N.$$

(d) From (c), the number of choices of three different $x, y, z \in Q$ such that $xyz \equiv 1 \pmod{p}$ is $(p-1)(p-4) + 2N$.

Since the number of combinations of such x, y, z are symmetrical, this number is divisible by 3. That is,

$$\begin{aligned} (p-1)(p-4) + 2N &\equiv 0 \pmod{3} \\ (p-1)(p-1) - N &\equiv 0 \pmod{3} \\ (p-1)^2 &\equiv N \pmod{3} \end{aligned}$$

(e) From (d), $N \equiv (p-1)^2 \equiv 0 \pmod{3} \implies 3 \mid N \implies N \geq 3$.

There are at least 3 different x such that $x^3 \equiv 1 \pmod{p}$. Choose such an $x \in Q$ such that $x \neq 1$.

$$x^3 - 1 \equiv 0 \pmod{p}$$

Factorising this gives

$$(x-1)(x^2 + x + 1) \equiv 0 \pmod{p}$$

Hence

$$p \mid (x-1)(x^2 + x + 1)$$

Since $\nmid x - 1$ as $x \in \{1, 2, \ldots, p-1\}$,

$$p \mid x^2 + x + 1$$

thus $x^2 + x + 1 \equiv 0 \pmod{p}$

□

Problem 31 (H3M Specimen)**.** For any positive integer n, if one square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be completely covered by triominoes (an L-shaped domino consisting of three squares).

Solution. Prove by induction.

Base case: $P(1)$ is clearly true.

Inductive step: $P(k) \implies P(k+1)$ is true for all k, i.e. if a $2^k \times 2^k$ checkerboard with a square removed can be completely covered by triominoes, then a $2^{k+1} \times 2^{k+1}$ checkerboard with a square removed can be completely covered by triominoes.

(i) Divide the $2^{k+1} \times 2^{k+1}$ checkerboard into four $2^k \times 2^k$ sub-boards.

(ii) One of the sub-boards include the removed square.

(iii) WLOG, assume the top left sub-board has the removed square.

(iv) By induction hypothesis, this sub-board can be covered by triominoes.

(v) For the top right sub-board, we cover it with trominoes with a remaining square at the bottom left corner.

(vi) For the bottom right sub-board, we cover it with trominoes with a remaining square at the top left corner.

(vii) For the bottom left sub-board, we cover it with trominoes with a remaining square at the top right corner.

(viii) The remaining three squares from (v) to (vii) are connected and can be covered by one triomino.

□

Remark. Although it is easy to visualise this by drawing it out, always produce a written proof.

Problem 32 (H3M Specimen N03)**.** Functions f and g are defined for $x \in \mathbb{R}$ by

$$f(x) = ax + b, \quad g(x) = cx + d$$

where a, b, c, d are constants with $a =\neq 0$. Given that $gf = f^{-1}g$, show that

- either g is a constant function, i.e. $g(x)$ is constant for all $x \in \mathbb{R}$,
- or f^2 is the identity function, i.e. $ff(x) = x$ for all $x \in \mathbb{R}$,
- or g^2 is the identity function.

[9]

Solution. Given that $gf = f^{-1}g$,

$$\begin{aligned} cf(x) + d &= f^{-1}(cx + d) \\ c(ax + b) + d &= \frac{(cx + d) - b}{a} \\ a^2cx + abc + ad &= cx + d - b \end{aligned}$$

Comparing coefficients,

$$\begin{cases} a^2c = c \\ c(a - 1)(a + 1) = 0 \\ abc + ad = d - b \end{cases}$$

and we have three cases to work with. □

§A.2 Selected problems from school papers

§A.2.1 Number Theory

§A.2.2 Analysis

1. (2024 DHS Timed Practice Q1) Prove that for any positive real numbers x, y, z satisfying $xy + yz + zx = x + y + z$,

   (a) $x^2 + y^2 + z^2 \le xy + yz + zx \ge 3$, and [3]

   (b) $\dfrac{1}{x^2+y+1} + \dfrac{1}{y^2+z+1} + \dfrac{1}{z^2+x+1} \le 1$ using the Cauchy–Schwarz inequality. [4]

   Solution.

   (a) By AM–GM, we have $x^2 + y^2 \ge 2xy$. Similarly, $y^2 + z^2 \ge 2yz$ and $z^2 + x^2 \ge 2zx$. Summing up these three equation gives

   $$x^2 + y^2 + z^2 \ge xy + yz + zx.$$

   For the second part, from the given condition,

   $$\begin{aligned}(xy + yz + zx)^2 &= (x + y + z)^2 \\ &= x^2 + y^2 + z^2 + 2(xy + yz + zx) \\ &\ge 3(xy + yz + zx) \quad \text{from the above part}\end{aligned}$$

   and cancelling on both sides gives us the desired inequality.

   (b) Considering the denominator,

   $$(x + y + z)^2 \le (1 + y + z^2)(x^2 + y + 1)$$

   by Cauchy–Schwarz inequality. Thus

   $$\frac{1}{x^2+y+1} \le \frac{1+y+z^2}{(x+y+z)^2}.$$

   Similarly,

   $$\frac{1}{y^2+z+1} \le \frac{1+z+x^2}{(x+y+z)^2}$$

   and

   $$\frac{1}{z^2+x+1} \le \frac{1+x+y^2}{(x+y+z)^2}.$$

   Summing up the three equations gives

   $$\frac{1}{x^2+y+1} + \frac{1}{y^2+z+1} + \frac{1}{z^2+x+1} \le \frac{3+x+y+z+x^2+y^2+z^2}{(x+y+z)^2}.$$

   From part (a), we have $xy + yz + zx = x + y + z \ge 3$. Thus

   $$\begin{aligned}\frac{3+x+y+z+x^2+y^2+z^2}{(x+y+z)^2} &\le \frac{2(x+y+z)+x^2+y^2+z^2}{(x+y+z)^2} \\ &= \frac{2(xy+yz+zx)+x^2+y^2+z^2}{(x+y+z)^2} = 1.\end{aligned}$$

   □

§A.2.3 Counting

1. (2019 DHS–EJC Prelim Q6) You have an unlimited supply of 1×1, 1×2 and 2×2 tiles. Tiles of the same size are indistinguishable.

   (i) Let T_n is the number of ways of tiling a $1 \times n$ path.
   State the value of T_1 and T_2. Write down an appropriate recurrence relation between T_{n+2}, T_{n+1} and T_n. [1]

   Consider the tilings of a $2 \times n$ path. (The 1×2 tiles can be rotated in the tilings.)

   Let P_n be the number of tilings of

   Let Q_n be the number of tilings of

   (ii) Show that $P_{n+1} = P_n + Q_n$ for $n \geq 1$. Explain your reasoning clearly. [2]

   (iii) Show that $Q_{n+1} = 2P_{n+1} + 2Q_{n+1}$ for $n \geq 2$. Explain your reasoning clearly. [4]

   (iv) Use (ii) and (iii) to show that $P_{n+2} + 2P_{n-1} = 3P_{n+1} + 2P_n$ for $n \geq 2$. [2]

   It is given that the solution to the above recurrence relation is

   $$P_n = -\frac{(-1)^n}{7} + \frac{1+2\sqrt{2}}{14}(2+\sqrt{2})^n + \frac{1-2\sqrt{2}}{14}(2-\sqrt{2})^n.$$

   (v) Find the number of distinct ways of tiling a $2 \times n$ path. [2]

   Solution.

   (i) $T_1 = 1$, $T_2 = 2$.
   $T_{n+2} = T_{n+1} + T_n$ for $n \geq 1$.

   (ii) Consider the "odd" tile / last tile in a tiling of P_{n+1}. It can only be covered by a 1×1 or a 1×2 tile.
   Consider cases:

   - If it is covered by a 1×1 tile, the rest for a tiling of Q_n.
   - If it is covered by a 1×2 tile, the rest form a tiling of P_n.

   Thus $P_{n+1} = P_n + Q_n$.

   (iii) Consider the last column of 2 tiles in a tiling of Q_{n+1}. The following cases are possible:

   - 2×2 tile: The rest form a tiling of Q_{n-1}.
   - 1×2 tile (vertical): The rest form a tiling of Q_n.
   - Two 1×1 tiles: The rest form a tiling of Q_n.
   - Two 1×2 tiles (horizontal): The rest form a tiling of Q_{n-1}.
   - One 1×1 tile and one 1×2 tile (horizontal): The rest form a tiling of P_n. Note that this case counts twice (depending on which tile covers the top line and which tile covers the bottom line).

   Thus $Q_{n+1} = 2Q_n + 2Q_{n-1} + 2P_n = 2P_{n+1} + 2Q_{n-1}$ using the result from (ii).

(iv) Add $P_{n+1} + 2P_{n-1}$ to both sides of (iii):

$$P_{n+1} + 2P_{n-1} + Q_{n+1} = P_{n+1} + 2P_{n-1} + 2P_{n+1} + 2Q_{n-1}$$

and thus

$$P_{n+2} + 2P_{n-1} = 3P_{n+1} + 2P_n$$

using result from (ii).

(v) Number of tilings of $2 \times n$ path is Q_n. Thus

$$\begin{aligned} Q_n &= P_{n+1} - P_n \\ &= \frac{2}{7}(-1)^n + \frac{1+2\sqrt{2}}{14}(2+\sqrt{2})^n(2+\sqrt{2}-1) + \frac{1-2\sqrt{2}}{14}(2-\sqrt{2})^n(2-\sqrt{2}-1) \\ &= \frac{2}{7}(-1)^n + \frac{5+3\sqrt{2}}{14}(2+\sqrt{2})^n + \frac{5-3\sqrt{2}}{14}(2-\sqrt{2})^n \end{aligned}$$

□

2.

Bibliography

[Ahl79] L. V. Ahlfors. *Complex Analysis*. McGraw-Hill, 1979.

[Apo57] T. M. Apostol. *Mathematical Analysis*. Addison-Wesley, 1957.

[DF04] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley & Sons, 2004.

[HKll] K. Hoffman and R. Kunze. *Linear Algebra*. 1971, Prentice-Hall.

[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.