Topics in

Undergraduate Mathematics

Ryan Joo

This is (still!) an incomplete draft. For corrections and comments, please send an email to the author at ryanjooruian18@gmail.com, or create a pull request at `https://github.com/Ryanjoo18/undergrad-maths`.

Draft November 28, 2025.

Preface

About This Book

This book is a collection of notes I am currently writing to accompany undergraduate courses at the National University of Singapore (NUS) from 2025 to 2030 (expected). More precisely, it largely follows the content taught in the following courses:

- MA1100T Basic Discrete Mathematics (T): Chapters 1 to 5

As for prerequisites, this book is written such that it is accessible to high school students for self-study. No formal prerequisites are required.

In terms of presentation, this book follows the typical style of "Definition", "Theorem", etc. As far as possible, I will try to make clear what I define, and what results I wish to show. Furthermore, for ease of reference, important terms are **coloured** when first defined, and are included in the glossary for ease of reference; less important terms are **bolded**, and some terms are *emphasised*.

Note on Problem Solving

Mathematics is, at its core, the art of problem solving. In his classic work [Pól45], Pólya outlined a four-step problem-solving cycle:

1. **Understand the problem.**

   Begin by ensuring that the problem is clearly and completely understood. Ask yourself:

   - Do I understand all the terms used in the statement of the problem?
   - Is it possible to satisfy the given conditions? Are they sufficient to determine the unknown, or are they insufficient, redundant, or even contradictory?
   - What exactly am I asked to find or prove? Can I restate the problem in my own words?
   - Can I draw a suitable diagram or introduce helpful notation?
   - Do I have enough information to reach a solution?

2. **Devise a plan.**

   Once the problem is understood, consider possible approaches. Pólya suggested a variety of **heuristics**: rules of thumb that often guide successful problem solving. A non-exhaustive list includes:

   - 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
- Apply a known formula
- Solve an equation
- Be ingenious

3. **Execute the plan.**

   Carrying out the plan is typically easier than devising it – provided one proceeds carefully and patiently. Follow your chosen approach systematically, verifying each step as you go. If the plan fails to yield progress, do not hesitate to revise it and try an alternative route. This process of trial, reflection, and adjustment is an essential part of genuine mathematical work.

   - While executing your plan, check each step critically: is it valid? Can you justify it rigorously?

4. **Check and reflect.**

   Pólya emphasised the importance of reviewing one's work after solving a problem. Reflection deepens understanding and strengthens future problem-solving ability.

   Ask yourself:

   - Can I verify my result or argument in another way?
   - Can I find a more elegant or direct solution?
   - Can this method or result be applied to other problems?

Building upon Pólya's framework, Schoenfeld [Sch92] proposed a more elaborate model of problem solving, consisting of four interrelated components:

1. **Cognitive resources:** the body of facts, techniques, and procedures at one's disposal.
2. **Heuristics:** general strategies or "rules of thumb" for making progress in challenging situations.
3. **Control (metacognition):** the ability to monitor and regulate one's thinking – literally, "thinking about one's own thinking." This includes assessing progress and deciding when to continue, adjust, or abandon a line of reasoning.

   (a) While solving a problem, periodically ask:

   - What am I doing right now? Why am I doing it? How does it fit into the overall plan?
   - How does my current step connect to the broader structure of the solution? What will I do next?

   (b) Stop and reassess your approach if you:

   - cannot answer these questions clearly (perhaps the approach is misguided), or
   - feel stuck (perhaps the approach is correct but presently too difficult).

   (c) Decide whether to:

   - continue with the current plan,
   - abandon it, or
   - temporarily set it aside and pursue another.

4. **Belief system:** one's underlying views about the nature of mathematics and what it means to "do mathematics." Such beliefs profoundly influence motivation, persistence, and the strategies one adopts in problem solving.

Acknowledgements

I am greatly thankful to my course instructors at NUS, as well as the authors listed in the Bibliography.

Contents

I
Preliminaries

We build the necessary mathematical foundation by introducing the basic language, concepts, and methods of contemporary mathematics. The second goal is to develop students' ability to construct rigorous arguments and formal proofs based on logical reasoning.

References: [End77; Lak16]

1
Language, Logic, and Proof

We will begin with mathematical language, the logical connectives and quantifiers, and then we will study the fundamental techniques of proof.

1.1 Propositional Logic

We begin by studying a basic logic known as **propositional logic** (also known as **zeroth order logic**).

Definition 1.1. A **proposition** is a statement which has exactly one truth value, i.e., it is either true or false, but not both and not neither.

Example. The following statement is not a proposition: "This statement is true"; this is because we cannot assign a truth value to it.

Each proposition has a unique truth value: T (for true) or F (for false). If a proposition is true, we say that it **holds**, otherwise we say that it **fails**.

1.1.1 Logical Connectives

We can build more complicated propositions from existing propositions using **logical connectives** (or **logical operators**). The resulting proposition is termed a **propositional formula**.

Definition 1.2. A **propositional formula** is an expression obtained by applying a finite number of logical operators to propositional variables, in some particular order.

Let p and q be propositiosns.

Definition 1.3. The **conjunction** of p and q is the proposition "p and q", denoted by $p \wedge q$. We call p and q the **conjuncts** of $p \wedge q$.

The statement $p \wedge q$ is true when p is true and q is true, and false otherwise. This can be represented by a **truth table**:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 1.1: Truth table for $p \wedge q$.

Remark. When we build a truth table for a compound statement involving two (or more) statement letters (say, p and q), we must consider all the possible truth values for each statement letter. Here there are two possible truth values for p (true, false), and similarly for q, so there are $2 \times 2 = 4$ possible truth values for the statement $p \wedge q$.

Definition 1.4. The **disjunction** of p and q is the statement "p or q", denoted by $p \vee q$. The statements p and q are called the **disjuncts** of the statement $p \vee q$.

In mathematics, the usage of the word "or" is always inclusive (i.e., includes the case where both p and q are true), unless explicitly stated otherwise. Hence $p \vee q$ is true when either p is true, or q is true, or both p and q are true.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 1.2: Truth table for $p \vee q$.

Remark. The notation for disjunction and conjunction is similar to that of union and intersection of sets.

Since there is an *inclusive* or, naturally there is an *exclusive* or:

Definition 1.5. The **exclusive or** of p and q is the statement "either p and not q, or q and not p", denoted by $p \oplus q$.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Table 1.3: Truth table for $p \oplus q$.

Definition 1.6. The **negation** of p is the statement "not p", denoted by $\neg p$.

The truth value of $\neg p$ is the opposite of that of p:

p	$\neg p$
T	F
F	T

Table 1.4: Truth table for $\neg p$.

Definition 1.7. Let F_1 and F_2 be two propositional formulas. We say that F_1 and F_2 are **logically equivalent**, denoted by $F_1 \equiv F_2$, if they have the same truth table.

That is, F_1 and F_2 have the same truth value, for all truth values of the propositional variables in them. To prove that $F_1 \not\equiv F_2$, it suffices to give *one* counterexample where F_1 and F_2 do not have the same truth values.

The next result summarises several useful properties when handling logical statements.

Lemma 1.8.

(i) $p \equiv \neg(\neg p)$ *(double negation law)*

(ii) $p \wedge q \equiv q \wedge p$
$p \vee q \equiv q \vee p$ *(commutative laws)*

(iii) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ *(associative laws)*

(iv) $p \wedge p \equiv p$
$p \vee p \equiv p$ *(idempotent laws)*

(v) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ *(distributive laws)*

(vi) $p \vee (p \wedge q) \equiv p$
$p \wedge (p \vee q) \equiv p$ *(absorption laws)*

(vii) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ *(de Morgan's laws)*

Proof. Use truth tables. □

Remark. Because of the associative laws, we can leave out parentheses in statements of the forms $p \wedge q \wedge r$ and $p \vee q \vee r$ without ambiguity, since the two possible ways of filling in the parentheses are equivalent.

1.1.2 Tautologies and Contradictions

Definition 1.9. A **tautology** is a statement that is always true (regardless of the truth values of the propositional variables in it).
A **contradiction** is a statement that is always false (regardless of the truth values of the propositional variables in it).

Example. $p \vee \neg p$ is a tautology. $p \wedge \neg p$ is a contradiction.

We state a few more useful laws involving tautologies and contradictions.

Lemma 1.10 (Tautology laws)**.** *Let q be a tautology. Then*

(i) $p \wedge q \equiv p$*;*

(ii) $p \vee q$ *is a tautology;*

(iii) $\neg q$ *is a contradiction.*

Lemma 1.11 (Contradiction laws)**.** *Let q is a contradiction. Then*

(i) $p \vee q \equiv p$;

(ii) $p \wedge q$ *is a contradiction;*

(iii) $\neg q$ *is a tautology.*

1.1.3 Implications

Definition 1.12. The **implication** or (**conditional** statement) $p \Rightarrow q$ is the statement "if p then q". We call p the **hypothesis**, q the **conclusion**.

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 1.5: Truth table for $p \Rightarrow q$.

The only case when $p \Rightarrow q$ is false is when the hypothesis p is true and the conclusion q is false. Also note that if p is false, then $p \Rightarrow q$ is true regardless of the truth value of q; we say that $p \Rightarrow q$ is **vacuously true**.

Remark. For any two propositions p and q, we can consider the implication $p \Rightarrow q$, even if p and q are "unrelated"; $p \Rightarrow q$ being true does not suggest a causal relationship between p and q.

Example. The statement "if $2 > 0$, then $4 > 0$" is true; the statement "if $-1 > 0$, then $1 > 0$" is vacuously true; the statement "if 2 is prime, then 3 is not prime" is false.

The following all mean the same thing:

(i) if p then q;

(ii) p implies q;

(iii) q follows from p;

(iv) q unless $\neg p$;

(v) p only if q;

(vi) q if p;

(vii) p is a **sufficient** condition for q;

(viii) q is a **necessary** condition for p;

(ix) p is **stronger** than q. [1]

Lemma 1.13 (Conditional identity)**.** $p \Rightarrow q \equiv q \vee \neg p$.

[1] this is because p implies q, but q may not imply p

Proof. Truth table:

p	q	$p \Rightarrow q$	$\neg p$	$q \vee \neg p$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

□

Definition 1.14. Let p and q be propositions.

- The **converse** of $p \Rightarrow q$ is $q \Rightarrow p$.
- The **inverse** of $p \Rightarrow q$ is $(\neg p) \Rightarrow (\neg q)$.
- The **contrapositive** of $p \Rightarrow q$ is $(\neg q) \Rightarrow (\neg p)$.

Lemma 1.15. *An implication is*

(i) not logically equivalent to its converse.

(ii) not logically equivalent to its inverse.

(iii) logically equivalent to its contrapositive.

Proof.

(i) Example:

p	q	$p \Rightarrow q$	$q \Rightarrow p$
T	F	F	T

(ii) Example:

p	q	$p \Rightarrow q$	$\neg p$	$\neg q$	$(\neg p) \Rightarrow (\neg q)$
T	F	F	F	T	T

(iii) Applying the conditional identity,

$$\begin{aligned} \neg q \Rightarrow \neg p &\equiv \neg p \vee \neg(\neg q) \\ &\equiv \neg p \vee q \\ &\equiv p \Rightarrow q \end{aligned}$$

□

1.1.4 If and only if, iff

Definition 1.16. The **biconditional** statement $p \Leftrightarrow q$ is an abbreviation for $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

$p \Leftrightarrow q$ is true exactly when p and q have the same truth value:

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$p \Leftrightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Table 1.6: Truth table for $p \Leftrightarrow q$.

A biconditional $p \Leftrightarrow q$ is usually best thought of separately as "if" $(q \Rightarrow p)$ and "only if" $(p \Rightarrow q)$ statements.

The following all mean the same thing.

(i) p if and only if q;

(ii) p iff q;

(iii) p is equivalent to q;

(iv) p exactly when q;

(v) p is necessary and sufficient for q.

— Exercises —

Exercise 1.1.1. In this problem we consider binary logical operators in propositional logic.

(i) How many are there? (We regard two binary logical operators as the same if they have the same truth table.)

(ii) Prove that there are **exactly two** binary logical operators $*$ in propositional logic such that $p*(p \vee q)$ is a tautology.

Solution.

(i) Each binary opeartor has two inputs and one output, so there are always four possible cases. Two operators are considered distinct if their truth tables are distinct. Since each output can be either True or False, there are $2^4 = 16$ binary operators.

(ii) We consider the truth table:

p	q	$p \vee q$	$p * (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

This converts to the truth table of $*$ being:

a	b	$a * b$
T	T	T
F	T	T
F	F	T

There are two possible outputs for $a * b$ if a is true and b is false. Hence, we can construct two different truth tables, and we thus have two possibilities for the operator $*$.

□

Exercise 1.1.2. Each card in a pack has a number on one side and a letter on the other. Four cards are placed on the table:

$$\boxed{2} \quad \boxed{3} \quad \boxed{\text{A}} \quad \boxed{\text{B}}$$

You are permitted to turn just two cards over in order to test the following hypothesis: "a card that has an even number on one side has a vowel on the other".

Which two cards should you turn? Or is it impossible?

1.2 Predicate Logic

The statement "$x+1>3$" on its own is not a proposition because it does not have a truth value. Instead, it is a **predicate** because it becomes a proposition when the "free variable" x is replaced by a particular value from the universe in question.

Definition 1.17. A **predicate** is an assignment of truth values to elements of some **domain**.

Given a predicate, a natural question to ask is:

> Is the predicate true for *all*, *some*, or *no* values of elements in the domain?

Let $P(x)$ be a predicate with domain $\mathcal{U}$.

Definition 1.18. The **universal statement** $(\forall x \in \mathcal{U})P(x)$ is defined to mean "$P(x)$ for every $x \in \mathcal{U}$". We call $\forall$ the **universal quantifier**.
The statement $(\forall x \in \mathcal{U})P(x)$ is ture exactly when each individual element x in the universe $\mathcal{U}$ has the property that $P(x)$ is true.

Definition 1.19. The **existential statement** $(\exists x \in \mathcal{U})P(x)$ is defined to mean "there is some $x \in \mathcal{U}$ such that $P(x)$". We call $\exists$ the **existential quantifier**.
The statement $(\exists x \in \mathcal{U})P(x)$ is ture exactly when the universe $\mathcal{U}$ contains at least one element x with $P(x)$ true.

A universal quantification can be interpreted as an implication: if x belongs to the domain of P, then $P(x)$ holds.

Remark. If the domain of P is empty, then $(\forall x)P(x)$ is always (vacuously) true, and $(\exists x)P(x)$ is always false.

Remark. When we specify a predicate, we must specify its domain! The domain affects the truth values of quantifications of the predicate.

A formula of predicate logic is formed by applying finitely many logical operators (existential quantification, universal quantification, $\neg$, $\wedge$, $\vee$, $\oplus$, $\Rightarrow$) to predicates.

Two predicates are **logically equivalent** if they have the same truth values over the domain.

The next result tells us how the quantifiers interact with negation.

Lemma 1.20 (de Morgan's laws)**.**

$$\neg(\forall x \in \mathcal{U})P(x) \equiv (\exists x \in \mathcal{U})(\neg P(x))$$
$$\neg(\exists x \in \mathcal{U})P(x) \equiv (\forall x \in \mathcal{U})(\neg P(x))$$

Example. Negate the statement

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

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

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

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

Statements may contain *multiple* quantifiers and *mixed* quantifiers. Regardless of the number of quantifiers in a quantified statement

$$(Q_1 x_1)(Q_2 x_2) \cdots (Q_n x_n)[\cdots]$$

where $Q_1, \ldots, Q_n$ are quantifiers, we always begin with the outermost quantifier and "work our way in". When we see a string of identical quantifiers, such as in the statements

$$(\forall x)(\forall y)P(x,y) \quad \text{or} \quad (\exists x)(\exists y)(\exists z)Q(x,y,z),$$

then the order of these quantifiers does not matter. For example,

$$(\forall x)(\forall y)P(x,y) \quad \text{and} \quad (\forall y)(\forall x)P(x,y)$$

have the same logical meaning, and both can be thought of as $(\forall x, y)P(x,y)$. Similarly (considering one possible reordering),

$$(\exists x)(\exists y)(\exists z)Q(x,y,z) \quad \text{and} \quad (\exists z)(\exists x)(\exists y)Q(x,y,z)$$

have the same logical meaning, and both can be thought of as $(\exists x, y, z)Q(x,y,z)$.

With mixed quantifiers, the **order of mixed quantifiers matters**. For instance,

$$\begin{aligned} &(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})[x + y = 0] && \text{is true, but} \\ &(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})[x + y = 0] && \text{is false.} \end{aligned}$$

In general, one cannot move quantifiers freely between the premise of an implication and its conclusion. For instance, consider

$$((\forall x)(x \text{ is happy})) \Rightarrow ((\forall y)(y \text{ is happy})).$$

Since the hypothesis and conclusion are the same, this implication is always true; it means "If everyone is happy, then everyone is happy". On the other hand,

$$(\forall x)(x \text{ is happy} \Rightarrow (\forall y)(y \text{ is happy}))$$

means "If one person is happy, then everyone is happy".

— Exercises —

Exercise 1.2.1. Translate the following statements.

(i) Every student sent an email to some other student.

(ii) There is exactly one student.

(iii) There are at least two students. (This can also be phrased as "There are *distinct* students".)

(iv) There are exactly two students.

(v) There are exactly two people that are not students.

Solution. Define $M(x, y)$ to be the predicate "x sent an email to y", with domain being the set of pairs of students.

Define $P(x)$ to be the predicate "x is a student", with domain being the set of all people.

(i)
$$\forall x \exists y((x \neq y) \wedge M(x, y)).$$

(ii)
$$\exists x(P(x) \wedge \forall y(P(y) \Rightarrow y = x)),$$

or equivalently (by contrapositive)

$$\exists x(P(x) \wedge \forall y(y \neq x \Rightarrow \neg P(y))).$$

Yet another equivalent translation is

$$\exists x \forall y(P(x) \wedge (P(y) \Rightarrow y = x)).$$

This is known as *uniqueness*; we write $(\exists! x)P(x)$.

(iii)
$$(\exists x)(\exists y)(P(x) \wedge P(y) \wedge x \neq y).$$

(iv)
$$(\exists x)(\exists y)(\forall z)(P(x) \wedge P(y) \wedge x \neq y \wedge (P(z) \Rightarrow (z = x) \vee (z = y))).$$

(v)
$$(\exists x)(\exists y)(\forall z)(\neg P(x) \wedge \neg P(y) \wedge x \neq y \wedge (\neg P(z) \Rightarrow (z = x) \vee (z = y))).$$

where we replace P with $\neg P$ in (iv).

□

Exercise 1.2.2 (MA1100T AY24/25)**.**

(i) Define predicates $P(x)$ and $Q(x)$ with the same domain such that the formulas

$$(\exists x)(P(x) \to Q(x))$$

and

$$(\exists x)P(x) \to (\exists x)Q(x)$$

have different truth values.

(ii) Define predicates $P(x)$ and $Q(x)$ with the same domain such that the formulas

$$(\forall x)(P(x) \vee Q(x))$$

and

$$(\forall x)P(x) \vee (\forall x)Q(x)$$

have different truth values.

(iii) Define predicates $P(x)$ and $Q(x)$ with the same domain such that the formulas

$$(\forall x)(P(x) \to Q(x))$$

and

$$(\forall x)P(x) \to (\forall x)Q(x)$$

have different truth values.

Solution.

(i) Define $P(x) : x = 0$ and $Q(x) : x < 0$ with domain $\{0, 1\}$.

$P(1)$ is false, so $P(x) \to Q(x)$ is vacuously true. Hence $(\exists x)(P(x) \to Q(x))$ is true.

$P(0)$ is true so $(\exists x)P(x)$ is true, but $(\exists x)Q(x)$ is false. Hence $(\exists x)P(x) \to (\exists x)Q(x)$ is false.

(ii) Define $P(x) : x$ is odd and $Q(x) : x$ is even with domain $\mathbb{Z}$.

Since every integer is either odd or even, $(\forall x)(P(x) \vee Q(x))$ is true.

Not every integer is odd and not every integer is even, so $(\forall x)P(x)$ and $(\forall x)Q(x)$ are false. Hence $(\forall x)P(x) \vee (\forall x)Q(x)$ is false.

(iii) Define $P(x) : x$ is even and $Q(x) : x$ is odd with domain $\mathbb{N}$.

Then $(\forall x)(P(x) \to Q(x))$ is false, because for $x = 2$, $P(2)$ true but $Q(2)$ false.

Not all numbers are even, so $(\forall x)P(x)$ is false. Hence $(\forall x)P(x) \to (\forall x)Q(x)$ is vacuously true.

□

Exercise 1.2.3 (MA1100T AY22/23)**.** Come up with a set D and three predicates $P(x)$, $Q(x)$, and $R(x)$, all with domain D, such that

$$\forall x(P(x) \to Q(x)) \vee \forall x(P(x) \to R(x))$$

and

$$\forall x(P(x) \to (Q(x) \vee R(x)))$$

have opposite truth values. Briefly justify your answer.

Exercise 1.2.4 (CS1231S AY21/22)**.** Which answer in this list is the correct answer to this question?

(A) All of the below.

(B) None of the below.

(C) All of the above.

(D) One of the above.

(E) None of the above.

(F) None of the above.

Exercise 1.2.5 (MA1100T AY25/26)**.** Come up with a set D and predicates $P(x)$, $Q(x)$ and $R(x)$, all with domain D, such that

$$\forall x(P(x) \to R(x)) \vee \forall x(Q(x) \to R(x))$$

and

$$\forall x((P(x) \wedge Q(x)) \to R(x))$$

have opposite truth values.

Solution. Two common types of constructions:

1. $R(x)$ is a condition composed of two conditions $P(x)$ and $Q(x)$, and neither $P(x)$ nor $Q(x)$ impliesthe other (see example 1 below), or

2. $P(x)$ and $Q(x)$ cannot simultaneously hold.

Construction 1: Let $D = \mathbb{Z}$. Define $P(x) : 2 \mid x$, $Q(x) : 3 \mid x$, $R(x) : 6 \mid x$.

Then $\forall x(P(x) \to R(x)) \vee \forall x(Q(x) \to R(x))$ is False ($2 \mid 2$ but $6 \nmid 2$ so LHS of $\vee$ is False, and $3 \mid 3$ but $6 \nmid 3$ so RHS of $\vee$ is False), but $\forall x((P(x) \wedge Q(x)) \to R(x))$ is True (if x has prime factors 2 and 3, then it is divisible by $2 \times 3 = 6$).

Construction 2: Let $D = \mathbb{Z}$. Define $P(x) : x$ is an even integer, $Q(x) : x$ is an odd integer, $R(x) : x$ is a positive integer.

Then $\forall x(P(x) \to R(x)) \vee \forall x(Q(x) \to R(x))$ is False (0 is even but not positive so LHS of $\vee$ is False, and -1 is odd but not positive so RHS of $\vee$ is False), but $\forall x((P(x) \wedge Q(x)) \to R(x))$ is vacuously True (an integer cannot be both even and odd). □

1.3 Methods of Proof

Formally, a **proof** of a proposition p is defined as a sequence of propositions which ends with p, obtained by applying inference rules to premises. Informally, however, we will define a **proof** to be a valid argument which has sufficient detail to convince the reader that the statement being proved is true.

1.3.1 Direct Proof

Many of the statements you will be asked to prove have the form

$$(\forall x \in \mathcal{U})\, P(x) \Rightarrow Q(x).$$

1. Begin by writing "Let $x \in \mathcal{U}$ be such that $P(x)$ holds".
2. Present a sequence of logical steps which shows that $Q(x)$ holds.

To prove a statement of the form $(\exists x \in \mathcal{U})\, P(x)$, there is not such a clear steer about how to continue:

- you can construct such an x with the desired properties (constructive proof);
- you can demonstrate logically that such an x must exist because of some earlier assumption (non-constructive proof);
- you can suppose that such an x does not exist, and consequently arrive at some inconsistency (proof by contradiction).

To prove $P \Leftrightarrow Q$, by definition of a biconditional statement, we need to prove the statement in both directions: $P \Rightarrow Q$ and $Q \Rightarrow P$.

Remark. Remember to make very clear, both to yourself and in your written proof, which direction you are doing.

1.3.2 Proof by Contrapositive

Since a statement is logically equivalent to its contrapositive, to prove the statement, we can prove its contrapositive.

Example. Prove that for all $a \in \mathbb{Z}$, if a^2 is even, then a is even.

Solution. Suppose $a \in \mathbb{Z}$ isodd. Then $a = 2k + 1$ for some $k \in \mathbb{Z}$. We have

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Hence a^2 is odd, so a^2 is not even, as desired. □

Example. Prove that if x is a rational number and xy is an irrational number, then y is irrational.

Proof. This statement has the form

$$\begin{aligned}
&(\forall x)(\forall y)\, (R(x) \wedge Q(x,y)) \Rightarrow \neg R(y) && \\
\equiv&(\forall x)(\forall y)\, R(y) \Rightarrow \neg(R(x) \wedge Q(x,y)) && \text{[contrapositive]} \\
\equiv&(\forall x)(\forall y)\, R(y) \Rightarrow (\neg R(x) \vee \neg Q(x,y)) && \text{[de Morgan's law]}
\end{aligned}$$

which is still a little awkward to prove. (One can do so by cases.) Alternatively, the given statement is also equivalent to

$$(\forall x)(\forall y)\ (R(y) \wedge R(x)) \Rightarrow \neg Q(x, y)$$

which means "If x and y are rational numbers, then xy is rational as well". This is much easier to prove. □

1.3.3 Proof by Contradiction

To prove a statement p is true, sometimes it is difficult to carry out a direct proof, possibly because we do not know how to begin.

One thing to try in such a situation is to assume that $\neg p$ is true. If we can find a contradiction r, then we have a valid proof that $(\neg p) \Rightarrow r$ is true. Since $(\neg p) \Rightarrow r$ is true and r is false, $\neg p$ must be false. Hence p is true, as desired.

To prove a statement p by **contradiction**:

1. Assume p is false, i.e., $\neg p$ is true.
   (E.g. to prove $p \Rightarrow q$ by contradiction, suppose $p \wedge \neg q$.)
2. Show that this leads to a contradiction or inconsistency.

   We may arrive at something that contradicts the hypothesis p, or contradicts the initial supposition that q is not true, or something that we know to be universally false.
3. Conclude that p is true.

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

Proof. Suppose, for a contradiction, that $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some $a, b \in \mathbb{Z}$, $b \neq 0$, where a and b are coprime. Squaring both sides gives

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

Since RHS is even, LHS must also be even. Hence it follows that a is even. Let $a = 2k$ where $k \in \mathbb{Z}$. 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 contradicts the assumption that a and b coprime. □

Example (Euclid)**.** Prove that there are infinitely many prime numbers.

Proof. Suppose, towards a contradiction, that only finitely many prime numbers exist. List them as $p_1, \ldots, p_n$. Consider the number

$$N = p_1 p_2 \cdots p_n + 1.$$

Note that N is divisible by a prime p, yet is coprime to $p_1, \ldots, p_n$. Therefore, p does not belong to our list of all prime numbers, a contradiction. □

Example. Prove that not every positive integer is the sum of the squares of two integers.

Proof. We shall prove that 3 is not the sum of the squares of two integers. Suppose, towards a contradiction, that m and n are integers such that $m^2 + n^2 = 3$.

Case 1: If $|m| \geq 2$, then $m^2 + n^2 \geq m^2 \geq 4 > 3$, contradiction.

Case 2: If $|n| \geq 2$, then $m^2 + n^2 \geq n^2 \geq 4 > 3$, contradiction.

Case 3: Otherwise, m and n can only be -1, 0 or 1. We can try all nine possibilities.

All of these cases lead to a contradiction. □

1.3.4 Proof by Cases

Sometimes one is unable to find a single argument that works in general to prove a statement.

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

Example. Prove that if n is an integer, then $n^2 \geq n$.

Solution. We consider three cases.

Case 1: If $n < 0$, then $n^2 \geq 0 > n$.

Case 2: If $n \geq 1$, multiply both sides of the inequality by the positive number n to obtain $n \cdot n \geq 1 \cdot n$. This yields $n^2 \geq n$.

Case 3: If $n = 0$, we have $0^2 \geq 0$.

Since $n^2 \geq n$ in all three cases, we conclude that $n^2 \geq n$ for every integer n. □

Example. Prove that there are no integers x and y such that $x^2 + 3y^2 = 8$.

Solution. We consider three cases.

Case 1: $x^2 > 8$**.** Then $x^2 + 3y^2 \geq x^2 > 8$.

Case 2: $3y^2 > 8$**.** Then $x^2 + 3y^2 \geq 3y^2 > 8$.

Case 3: $x^2 \leq 8$ **and** $3y^2 \leq 8$**.** Since x and y are integers, this implies that

$$x \in \{-2, -1, 0, 1, 2\} \quad \text{and} \quad y \in \{-1, 0, 1\}\,.$$

But now $x^2 \leq 4$ and $y^2 \leq 1$, so $x^2 + 3y^2 \leq 4 + 3 \cdot 1 < 8$.

Since $x^2 + 3y^2 \neq 8$ in all three cases, we conclude that there are no integers x and y such that $x^2 + 3y^2 = 8$. □

1.3.5 Disproof by Counterexample

To disprove a statement, we show its negation is true.

For instance, to disprove $p \Rightarrow q$, the counterexample should make the hypothesis p true and the conclusion q false. To disprove $(\forall x)\ P(x)$, show its negation $(\exists x)\ \neg P(x)$ holds, i.e., find x such that $P(x)$ does not hold.

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.

Example. Prove or disprove: if n is an integer and n^2 is positive, then n is positive.

Solution. Disproof: We give a counterexample: take $n = -1$. Then n is not positive, yet $n^2 = 1$ is positive. □

1.3.6 Proof of Existence and Uniqueness

To prove existential statements, we can adopt two approaches, the first being a **constructive proof**; this is a form of direct proof. To prove statements of the form $(\exists x \in X)P(x)$, find or construct *a specific example* for x. Similarly, to prove statements of the form $(\forall y \in Y)(\exists x \in X)P(x, y)$, construct example for x in terms of y (since x is dependent on y).

In both cases, you need to justify that your example x belongs to the domain X, and satisfies the condition $P(x)$.

The second approach is a **non-constructive proof**, a form of indirect proof. This approach is used 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.

Sometimes we find that not only do we wish to prove that an object exists, but also we wish to prove that the object that exists is unique, i.e., that there is exactly one such object. We use $\exists!$ to mean "there exists a unique". We can prove $(\exists! x)P(x)$ in the following ways:

- Find x which satisfies property P. Then show if $P(y)$ holds for some arbitrary y, then $x = y$.

  $$(\exists x)[P(x) \land (\forall y)P(y) \Rightarrow x = y].$$

  Equivalently, we first find x such that $P(x)$ holds; then if $P(y)$ and $P(z)$ hold for arbitrary y and z, then $y = z$.

  $$(\exists x)[P(x) \land (\forall y)(\forall z)(y) \land P(z) \Rightarrow y = z].$$

- Alternatively, assume that $\exists x, y$ are distinct such that $P(x) \land P(y)$, then derive a contradiction.

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

Solution. We proceed by constructive proof; we will construct integers $n, n+1, n+2, \dots, n+99$, all of which are composite.

Claim: $n = 101! + 2$.

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

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

Solution. Suppose (x, y, z) is a solution. WLOG assume $z > 0$. By the least integer principle, we may also assume that our solution has z minimal. Taking remainders modulo 3, we see that

$$x^2 + y^2 \equiv 0 \pmod{3}.$$

Since perfect squares can only be congruent to 0 or 1 modulo 3, we must have $x \equiv y \equiv 0 \pmod 3$. Writing $x = 3a$ and $y = 3b$ for $a, b \in \mathbb{Z}$ gives

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

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

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

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

1.3.7 Proof by Mathematical Induction

Theorem 1.21. *The following are equivalent on* $\mathbb{N}$*:*

(i) Principle of induction*: Let* $S \subseteq \mathbb{N}$*. If* $0 \in S$ *and* $n \in S \Rightarrow n + 1 \in S$*, then* $S = \mathbb{N}$*.*

(ii) Principle of strong induction*: Let* $S \subseteq \mathbb{N}$*. If* $1 \in S$ *and* $\{0, \ldots, n\} \subseteq S \Rightarrow n + 1 \in S$*, then* $S = \mathbb{N}$*.*

(iii) Well-ordering principle*: Every non-empty subset of* $\mathbb{N}$ *has a least element.*

(i) is one of *Peano's axioms* for $\mathbb{N}$, known as the *induction axiom.*

Proof.
$\boxed{\text{(i)} \Rightarrow \text{(ii)}}$ Let $S \subseteq \mathbb{N}$ be such that (A) $0 \in S$, and (B) $\{0, \ldots, n\} \subseteq S \Rightarrow n + 1 \in S$. We will show $S = \mathbb{N}$. Define $P(n) : \{0, \ldots, n\} \subseteq S$. Consider the set

$$S' = \left\{n \in \mathbb{N} \mid P(n)\right\}.$$

We shall show that $S' = \mathbb{N}$.

- By (A), $P(0)$ is true, so $1 \in S'$.
- Suppose $P(k)$ is true where $k \geq 0$. So $k \in S'$, and by hypothesis, $\{0, \ldots, k\} \subseteq S$. By (B), $k + 1 \in S$. Thus $\{0, \ldots, k, k + 1\} \subseteq S$. This means $P(k + 1)$ is true, so $k + 1 \in S'$.

Since $0 \in S'$ and $n \in S' \Rightarrow n + 1 \in S'$, by (i), $S' = \mathbb{N}$, so $P(n)$ holds for all $n \in \mathbb{N}$. This means $S = \mathbb{N}$.
$\boxed{\text{(ii)} \Rightarrow \text{(iii)}}$ Let $S \subseteq \mathbb{N}$ be non-empty. We need to show that S has a least element. Suppose, for a contradiction, that S has no minimal element. Let $P(n) : n \notin S$, and

$$S' = \left\{n \in \mathbb{N} \mid P(n)\right\}.$$

- We have $0 \notin S$. (Since 0 is a lower bound for $\mathbb{N}$, 0 is also a lower bound for S. If $0 \in S$, 0 would be the least element of S, a contradiction.) Thus $P(0)$ holds, so $0 \in S'$.
- Suppose $P(j)$ holds for $0 \leq j \leq k$. If $k + 1 \in S$, since $0, \ldots, k \notin S$, it follows that $k + 1$ would then be the minimal element of S. Thus $k + 1 \notin S$, so $k + 1 \in S'$.

By (ii), $S' = \mathbb{N}$. But this means that $S = \emptyset$, a contradiction.
$\boxed{\text{(iii)} \Rightarrow \text{(i)}}$ Let $S \subseteq \mathbb{N}$ be such that (A) $0 \in S$ and (B) $n \in S \Rightarrow n + 1 \in S$. We will show that $S = \mathbb{N}$. Suppose, for a contradiction, that $S \neq \mathbb{N}$.

Consider its complement $\mathbb{N} \setminus S$, which is non-empty. By the well-ordering principle, $\mathbb{N} \setminus S$ has a least element p. Since $0 \in S$, this means $0 \notin \mathbb{N} \setminus S$, so $p \neq 0$. Thus $p > 0$.

Now consider $p - 1$. Since p is the least element of $\mathbb{N} \setminus S$, we have $p - 1 \notin \mathbb{N} \setminus S$, i.e., $p - 1 \in S$. But by (B), $p - 1 \in S$ implies $p \in S$, which contradicts the fact that $p \in \mathbb{N} \setminus S$. □

Since we assume the induction axiom holds for the construction of $\mathbb{N}$, it follows that the well-ordering principle on $\mathbb{N}$ holds.

Corollary 1.22. *Suppose $S \subseteq \mathbb{Z}$ is non-empty and bounded above by some integer m (i.e., $s < m$ for all $s \in S$). Then S has a largest element.*

Proof. Consider the set

$$T = \left\{ m - s \mid s \in S \right\}.$$

Since S is non-empty, T is non-empty. For all $s \in S$, $s < m \Rightarrow m - s > 0 \Rightarrow m - s \geq 1$ since we are dealing with integers; thus $T \subseteq \mathbb{N}$. By the well-ordering principle, T has a least element t_0.

This means for all $s \in S$, $t_0 \leq m - s \Rightarrow s \leq m - t_0$. Hence $m - t_0$ is the largest element of S. □

The principle of induction can be phrased in the following form, which allows us to prove theorems.

Theorem 1.23 (Principle of mathematical induction)**.** *Let $P(n)$ be a family of statements indexed by $\mathbb{N}$. Suppose that*

(i) $P(0)$ is true;

(ii) for all $n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$.

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

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 the **base case** (i) corresponds to knocking over the first one.

To use induction to prove a family of statements, we simply have to demonstrate (i) and (ii).

Proof. Apply the principle of induction to the set $S = \left\{ n \in \mathbb{N} \mid P(n) \text{ is true} \right\}$. □

The general structure of proofs by induction is as follows:

1. Identify the variable x that you want to "do induction over".
2. Define a predicate $P(x)$ and a domain such that the desired conclusion is of the form $(\forall x) P(x)$.
3. Prove the base case.
4. Prove the inductive step.

Example. Prove that for any $n \in \mathbb{N}$, $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Solution. Induct on n. Let $P(n)$ be the predicate $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.
Clearly $P(0)$ holds. Now suppose $P(n)$ holds for some $n \geq 1$:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Adding $n+1$ to both sides,

$$\sum_{i=0}^{n+1} i = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2} = \frac{(n+1)[(n+1)+1]}{2}$$

so $P(n+1)$ is true. □

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

Corollary 1.24. *Let $P(n)$ be a family of statements indexed by integers $n \geq N$ for some $N \in \mathbb{Z}$. Suppose that*

(i) $P(N)$ is true;

(ii) for all $n \geq N$, $P(n) \Rightarrow P(n+1)$.

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

Proof. Apply 1.23 to the statement $Q(n) = P(n+N)$ for $n \in \mathbb{N}$. □

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

Theorem 1.25 (Strong induction)**.** *Let $P(n)$ be a family of statements indexed by $\mathbb{N}$. Suppose that*

(i) $P(0)$ is true;

(ii) for all $n \in \mathbb{N}$, $P(0) \wedge P(1) \wedge \cdots \wedge P(n) \Rightarrow P(n+1)$.

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

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

(i) $Q(0)$ is true;

(ii) for $n \in \mathbb{N}$, $Q(n) \Rightarrow Q(n+1)$.

By 1.23, $Q(n)$ holds for all $n \in \mathbb{N}$, and hence $P(n)$ holds for all $n \in \mathbb{N}$. □

Example. Prove that every natural number greater than 1 may be expressed as a product of one or more prime numbers.

Solution. We proceed by strong induction on n, where $n \geq 2$.
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. Suppose $n \geq 2$, and $P(k)$ holds for all $k < n$. We want to show $P(n)$ holds.

Case 1: If n is prime, then n is trivially the product of the single prime number n.

Case 2: If n is not prime, then $n = rs$ for some integers $r, s > 1$. By inductive hypothesis, each of r and s can be written as a product of primes. Hence $n = rs$ is also a product of primes.

In both cases, $P(n)$ holds. Hence by strong induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

The following is also another variant on induction.

Theorem 1.26 (Cauchy induction)**.** *Let $P(n)$ be a family of statements indexed by $\mathbb{N}_{\geq 2}$. Suppose that*

(i) $P(2)$ is true;

(ii) for all $k \geq 2$, $P(k) \Rightarrow P(2k)$;

(iii) for all $k \geq 3$, $P(k) \Rightarrow P(k-1)$.

Then $P(n)$ is true for all $n \geq 2$.

Proof. Suppose, for a contradiction, that the desired result is not true.
A smallest integer $k \geq 2$ must exist with $\neg P(k)$, and it is easy to prove that $k \geq 4$.
Then also $\neg P(k+1)$ and one of k and $k+1$ is even and can be written as $2m$ where m is an integer such that $2 \leq m < k$.
Then also $\neg P(m)$ but this contradicts the minimality of k. □

Example (AM–GM inequality)**.** Given $n \in \mathbb{N}$, prove that for positive reals $a_1, a_2, \dots, a_n$,

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

Solution. Let $P(n) : \dfrac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}$.

(i) The base case $P(2)$ is true, because

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

(ii) Next we show that $P(n) \Rightarrow P(2n)$. Suppose $P(n)$ holds; that is,

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

We have

$$\begin{aligned}
\frac{a_1 + a_2 + \cdots + a_{2n}}{2n} &= \frac{\frac{a_1+a_2+\cdots+a_n}{n} + \frac{a_{n+1}+a_{n+2}+\cdots+a_{2n}}{n}}{2} \\
&\geq \frac{\sqrt[n]{a_1 a_2 \cdots a_n} + \sqrt[n]{a_{n+1} a_{n+2} \cdots a_{2n}}}{2} && \text{[by induction hypothesis]} \\
&\geq \sqrt{\sqrt[n]{a_1 a_2 \cdots a_n}\,\sqrt[n]{a_{n+1} a_{n+2} \cdots a_{2n}}} && \text{[by 2-variable AM–GM]} \\
&= \sqrt[2n]{a_1 a_2 \cdots a_{2n}}.
\end{aligned}$$

(iii) Finally we show that $P(n) \Rightarrow P(n-1)$. Suppose $P(n)$ holds; that is,

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

Let $a_n := \dfrac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}$. Then

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

Thus

$$\begin{aligned}
&\frac{a_1+a_2+\cdots+a_{n-1}}{n-1} \geq \sqrt[n]{a_1a_2\cdots a_{n-1}\cdot\frac{a_1+a_2+\cdots+a_{n-1}}{n-1}}\\
\implies &\left(\frac{a_1+a_2+\cdots+a_{n-1}}{n-1}\right)^n \geq a_1a_2\cdots a_{n-1}\cdot\frac{a_1+a_2+\cdots+a_{n-1}}{n-1}\\
\implies &\left(\frac{a_1+a_2+\cdots+a_{n-1}}{n-1}\right)^{n-1} \geq a_1a_2\cdots a_{n-1}\\
\implies &\frac{a_1+a_2+\cdots+a_{n-1}}{n-1} \geq \sqrt[n-1]{a_1a_2\cdots a_{n-1}}
\end{aligned}$$

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

1.3.8 Pigeonhole Principle

Theorem 1.27 (Pigeonhole principle). *If k is a positive integer and $k+1$ objects are placed into k boxes, then at least one box contains two ore more objects.*

Proof. Suppose, for a contradiction, that $k+1$ objects are placed into k boxes, and no boxes contain two or more objects.

Then each box has 0 or 1 objects, so the total number of objects is at most k. This is a contradiction. □

In fact, we can generalise the pigeonhole principle further:

Theorem 1.28 (Generalised pigeonhole principle). *If k is a positive integer and n objects are placed into k boxes, then at least one box contains $\left\lceil \frac{n}{k} \right\rceil$ or more objects.*

Example (IMO 1972). Prove that every set of 10 two-digit integer numbers has two disjoint subsets with the same sum of elements.

Proof. Let S be the set of 10 numbers. It has $2^{10}-2=1022$ subsets that differ from both S and the empty set. They are the "pigeons".

If $A \subseteq S$, the sum of elements of A cannot exceed $91+92+\cdots+99=855$. The numbers between 1 and 855, which are all possible sums, are the "holes".

Since the number of "pigeons" exceeds the number of "holes", there will be two "pigeons" in the same "hole". Specifically, there will be two subsets with the same sum of elements. Deleting the common elements, we obtain two disjoint sets with the same sum of elements. □

Example (Putnam 2006). Prove that for every set $X=\{x_1,x_2,\dots,x_n\}$ of n real numbers, there exists a nonempty subset S of X and an integer m such that

$$\left| m + \sum_{x\in S} s \right| \leq \frac{1}{n+1}.$$

Proof. Recall that the fractional part of a real number x is $x-\lfloor x \rfloor$. Consider the fractional parts of the numbers $x_1, x_1+x_2, \dots, x_1+x_2+\cdots+x_n$.

- If any of them is either in the interval $\left[0,\frac{1}{n+1}\right]$ or $\left[\frac{n}{n+1},1\right]$, then we are done.

- If not, consider these n numbers as the "pigeons" and the $n-1$ intervals

$$\left[\frac{1}{n+1}, \frac{2}{n+1}\right], \quad \left[\frac{2}{n+1}, \frac{3}{n+1}\right], \quad \ldots, \quad \left[\frac{n-1}{n+1}, \frac{n}{n+1}\right]$$

as the "holes". By the pigeonhole principle, two of these sums, say $x_1 + x_2 + \cdots + x_k$ and $x_1 + x_2 + \cdots + x_{k+m}$, belong to the same interval. But then their difference $x_{k+1} + \cdots + x_{k+m}$ lies within a distance of $\frac{1}{n+1}$ of an integer, and we are done.

□

— Exercises —

★ **Exercise 1.3.1.** Prove that if an integer is even, then its square is even.

Solution. Let $x \in \mathbb{Z}$ be even. Then $x = 2k$ for some $k \in \mathbb{Z}$. We have $x^2 = (2k)^2 = 2(2k^2)$. Hence x^2 is even. □

★ **Exercise 1.3.2.** Prove that the sum of two rational numbers is rational.

Solution. Let $x_1, x_2 \in \mathbb{Q}$. Then $x_1 = \frac{p_1}{q_1}$ for some $p_1, q_1 \in \mathbb{Z}$, $q_1 \neq 0$; $x_2 = \frac{p_2}{q_2}$ for some $p_2, q_2 \in \mathbb{Z}$, $q_2 \neq 0$. Then

$$x_1 + x_2 = \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2}.$$

Hence $x_1 + x_2 \in \mathbb{Q}$. □

★ **Exercise 1.3.3.** Prove that if $x, y \in \mathbb{R}^+$, then $\frac{x}{y} + \frac{y}{x} \geq 2$.

Solution. We shall work backwards. Note that

$$\begin{aligned} \frac{x}{y} + \frac{y}{x} \geq 2 &\iff x^2 + y^2 \geq 2xy \\ &\iff x^2 - 2xy + y^2 \geq 0 \\ &\iff (x-y)^2 \geq 0 \end{aligned}$$

which is true. □

★ **Exercise 1.3.4.** Prove that if m and n are integers such that mn is even, then either m is even or n is even.

Solution. Contrapositive. □

★ **Exercise 1.3.5** (Bernoulli's inequality)**.** Let $x \in \mathbb{R}$, $x > -1$. Then for all $n \in \mathbb{N}$,

$$(1+x)^n \geq 1 + nx.$$

Solution. Induct on n. Fix $x > -1$. Let $P(n) : (1+x)^n \geq 1 + nx$.
The base case $P(1)$ is clear. Suppose $P(n)$ is true for some $n \geq 1$, i.e., $(1+x)^n \geq 1 + nx$. Then

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &\geq (1+x)(1+nx) && \text{[by induction hypothesis]} \\ &= 1 + (n+1)x + nx^2 \\ &\geq 1 + (n+1)x. \end{aligned}$$

□

★ **Exercise 1.3.6.** Define a sequence (a_n) by the recurrence relation $a_1 = 1$ and $a_{n+1} = 2a_n + 1$ for $n \in \mathbb{N}$. Prove that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$.

Solution. Induct on n. Let $P(n)$ be the predicate $a_n = 2^n - 1$ with domain $\mathbb{N}$.

The base case $P(1)$ holds: $2^1 - 1 = 1 = a_1$.

Suppose $n \in \mathbb{N}$ and $P(n)$ holds. We shall prove that $P(n+1)$ holds:

$$\begin{aligned} a_{n+1} &= 2a_n + 1 \\ &= 2(2^n - 1) + 1 \\ &= 2^{n+1} - 1. \end{aligned}$$

□

★★ **Exercise 1.3.7** (Golomb, 1965)**.** Prove that every $2^n \times 2^n$ board with one square removed can be tiled with L-shaped triominoes.

Solution. Induct on n.

The base case $n = 1$ is clear. Suppose the result holds for n; we wish to prove it for $n + 1$.

A $2^{n+1} \times 2^{n+1}$ board can be partitioned into four $2^n \times 2^n$ boards. Without loss of generality, assume that the square removed is in the top left board. By inductive hypothesis, that board can be tiled with triominoes.

Now place a triomino at the center of the $2^{n+1} \times 2^{n+1}$ board, such that exactly one square of each of the remaining three $2^n \times 2^n$ boards is covered. By inductive hypothesis, the remaining three $2^n \times 2^n$ boards can be tiled with triominoes.

Hence the $2^{n+1} \times 2^{n+1}$ board can be tiled with triominoes. □

★ **Exercise 1.3.8.** Prove that for all $n \in \mathbb{N}$, $F_n < 2^n$.

Solution. Idea: We do strong induction instead of induction because in the recurrence relation defining (F_n), F_{n+1} depends on *multiple* previous values (namely, F_n and F_{n-1}).

We proceed by strong induction on n.

For the base case, $F_1 = 1 < 2 = 2^1$ and $F_2 = 1 < 4 = 2^2$.

Suppose $n \geq 2$ is such that $F_m < 2^m$ for every $m \leq n$. We shall show that $F_{n+1} < 2^{n+1}$:

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ &< 2^n + 2^{n-1} \\ &< 2^n + 2^n = 2^{n+1} \end{aligned}$$

as desired. □

★★ **Exercise 1.3.9.** Prove that the equation $3x + 4y = n$ has some solution in $\mathbb{N}$ for all $n \geq 6$.

Solution. We proceed by strong induction on $n \geq 6$. Let $P(n)$ be the predicate "$3x + 4y = n$ has some solution in $\mathbb{N}$", with domain $\{n \in \mathbb{N} \mid n \geq 6\}$.

Base case: We check $P(6)$: $3x + 4y = 6$ has solution $x = 2, y = 0$; for $P(7)$, $3x + 4y = 7$ has solution $x = 1, y = 1$; for $P(8)$, $3x + 4y = 8$ has solution $x = 0, y = 2$.

Suppose $n \geq 8$ is such that $P(m)$ holds for all $6 \leq m \leq n$. We shall show that $P(n + 1)$ holds. Since $n \geq 8$, we have $n - 2 \geq 6$. Since $6 \leq n - 2 \leq n$, apply inductive hypothesis $P(n - 2)$ to obtain $x, y \in \mathbb{N}$ such that $3x + 4y = n - 2$. Then $x + 1, y \in \mathbb{N}$ and $3(x + 1) + 4y = n + 1$ as desired. □

★★ **Exercise 1.3.10.** Prove that every rational number r can be written in lowest terms, i.e., $r = u/v$ where $u, v \in \mathbb{Z}$ have no common factor other than 1.

Solution. Induct on $n \in \mathbb{N}$. Let $P(n)$ be the predicate "if $r = a/b$ where $a, b \in \mathbb{Z}$ and $|a|, |b| \leq n$, then r can be written in lowest terms".

For the base case, suppose $r = a/b$ where $a, b \in \mathbb{Z}$ and $|a|, |b| \leq 1$. Then $a = 1$, 0 or -1 and $b = 1$ or -1. In all six cases, a and b have no common factor other than 1, as desired.

Suppose $n \in \mathbb{N}$ is such that $P(n)$ holds. We shall show that $P(n+1)$ holds. Suppose $r = a/b$ where $a, b \in \mathbb{Z}$ and $|a|, |b| \leq n + 1$.

Case 1: If a and b have no common factor other than 1, then we are done.

Case 2: Otherwise, let $f > 1$ be a common factor of a and b. Define $c = a/f$ and $d = b/f$. (We have $c, d \in \mathbb{Z}$ since f divides a and b.)

Since $f > 1$, we have $|c| < |a| \leq n + 1$ and $|d| < |b| \leq n + 1$. Then $r = c/d$ and $|c|, |d| \leq n$, so by the inductive hypothesis, r can be written in lowest terms as desired.

□

★★ **Exercise 1.3.11** (Least common multiple)**.**

(i) Prove that for every non-zero integers a and b, there exists a **positive** integer c such that a and b both divide c.

(ii) Hence prove that there is a **smallest** positive integer c such that a and b both divide c.

Solution. Put $c = |ab|$. Then a and b both divide c.

Let S be the set of all positive integers that are common multiples of a and b. Since $|ab| \in S$, S is non-empty. By the well-ordering principle, S has a least element c_0. Hence c_0 is the smallest positive integer that is a common multiple of a and b. □

★ **Exercise 1.3.12.** Use induction to prove that for every $n \in \mathbb{N}$, 3 divides $n^3 - n$.

Solution. Induct on $n \in \mathbb{N}$. Let $P(n)$ be the predicate "3 divides $n^3 - n$".

The base case $P(0)$ holds since $0^3 - 0 = 0$ is divisible by 3.

Suppose $P(n)$ holds for some $n \geq 0$; that is, $3 \mid n^3 - n$. Then

$$\begin{aligned}(n+1)^3 - (n+1) &= (n^3 + 3n^2 + 3n + 1) - (n+1)\\ &= (n^3 - n) + 3(n^2 + n).\end{aligned}$$

Since $n^3 - n$ and $3(n^2 + n)$ are each divisible by 3, it follows that their sum is divisible by 3. Thus $3 \mid (n+1)^3 - (n+1)$. □

★★ **Exercise 1.3.13.** Define a sequence (a_n) of real numbers by $a_0 = 0$ and $a_{n+1} = (a_n)^2 + \frac{1}{4}$ for $n \in \mathbb{N}$. Prove that for all $n \in \mathbb{N}$, we have $0 < a_n < 1$.

Solution. We shall prove a stronger result: for all $n \in \mathbb{N}$, we have $0 < a_n < \frac{1}{2}$.

Induct on $n \in \mathbb{N}$. The base case holds since $a_1 = 0^2 + \frac{1}{4} = \frac{1}{4} < \frac{1}{2}$.

Suppose $0 < a_n < \frac{1}{2}$ holds for some $n \geq 1$. Squaring both sides gives ${a_n}^2 < \frac{1}{4}$. Then add $\frac{1}{4}$ to both sides to get $a_{n+1} = {a_n}^2 + \frac{1}{4} < \frac{1}{2}$ as desired. □

★★★ **Exercise 1.3.14.** Define the predicate $P(n, m)$ to say that there is a finite sequence of positive integers $\{a_i\}_{i=0}^{j}$ such that

$$\frac{n}{m} = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_j}}}}.$$

The domain of $P(n, m)$ is the set $\{(n, m) \mid n, m \in \mathbb{N},\ n < m\}$. The goal of this question is to prove that $P(n, m)$ holds for all m and n (in its domain, of course).

(i) Suppose $n < m$ are positive integers such that n does not divide m. Prove that there is a **largest** positive integer a such that $\frac{n}{m} < \frac{1}{a}$.

(ii) In the context of the previous part, prove that $0 < m - an < n$.

(iii) Suppose $n < m$ are positive integers such that for all positive integers $n' < n$, $P(n', n)$ holds. Prove that $P(n, m)$ holds.

(iv) Convince yourself that we have a proof that $P(n, m)$ holds for all m and n.

Solution.

(i) Consider the set $S = \{a \in \mathbb{N} \mid an < m\}$. Since S is non-empty ($1 \in S$) and bounded above by m, S has a largest element a_0 such that $\frac{n}{m} < \frac{1}{a_0}$.

(ii) Since $\frac{n}{m} < \frac{1}{a}$, multiplying both sides by am and rearranging gives $m - an > 0$.

We prove the other inequality by contradiction. Suppose $m - an \geq n$. Then $\frac{n}{m} \leq \frac{1}{a+1}$. Since n does not divide m, $\frac{n}{m}$ cannot be simplified to a fraction of the form $\frac{1}{k}$ where $k \in \mathbb{Z}$, so equality cannot hold. This implies $\frac{n}{m} < \frac{1}{a+1}$, contradicting the maximality of a.

(iii) We can write

$$\frac{n}{m} = \frac{1}{\frac{m}{n}} = \frac{1}{a + \frac{m-an}{n}}.$$

By (ii), since $0 < m - an < n$, by inductive hypothesis $P(m - an, n)$ holds, i.e., $\frac{m-an}{n}$ can be expressed as a finite continued fraction, say

$$\frac{m - an}{n} = \frac{1}{b_0 + \frac{1}{b_1 + \frac{1}{\ddots + \frac{1}{b_j}}}}$$

for some positive integers $b_1, \ldots, b_j$. Then

$$\frac{n}{m} = \frac{1}{a + \frac{1}{b_0 + \frac{1}{b_1 + \frac{1}{\ddots + \frac{1}{b_j}}}}}$$

so $P(n, m)$ holds.

(iv) Induct on the denominator when a fraction between 0 and 1 is written as $\frac{n}{m}$, where $n, m \in \mathbb{N}$.

Let $Q(m)$ be the predicate that $P(n, m)$ holds for all $n < m$. We induct on m.

The base case $P(1, 2)$ holds since $\frac{1}{2}$ is already in the desired form.

Suppose $Q(k)$ holds for $2 \leq k < m$. We want to show $Q(m)$ holds.

Case 1: If $n \mid m$, then $m = an$, so $\frac{n}{m} = \frac{1}{a}$ is the desired form.

Case 2: If $n \nmid m$, this is (iii), which uses the inductive hypothesis.

Remark. You have to include the case $n \mid m$ somewhere in (iv). Since this is the case that stops the recursion, it turns out to make more sense to include it as a case in the inductive step instead of "Case 1: $n \mid m$, prove Case 1; Case 2: $n \nmid m$, prove Case 2 by induction".

Remark. We don't want to induct on more than one variable simultaneously, so choose one formula whose size gets smaller with each recursive step. In this case, the denominator is a natural choice.

□

★★★ **Exercise 1.3.15.** Let m and n be positive integers. Given a chocolate bar with dimensions m units by n units, your task is to break it down into mn many 1 unit by 1 unit squares. The only operation you can perform is to take a **single** piece and break it vertically or horizontally. (You can't break multiple pieces in one operation!) Use strong induction to prove that one needs **at least** $mn - 1$ operations for this task. (Optional: Is $mn - 1$ operations enough?)

Solution. We proceed by strong induction on the total number of squares N.

The base case where $N = 1$ is trivial.

Suppose that for any chocolate bar with k squares, where $2 \leq k < N$, it requires at least $k - 1$ breaks. Consider a chocolate bar with N squares. Break it into a piece of size N_1 squares and a piece of size N_2 squares, where $N_1 + N_2 = N$ and $N_1, N_2 < N$. The first piece requires at least $N_1 - 1$ breaks, the second piece requires at least $N_2 - 1$ breaks. Hence the total number of breaks is $\geq (N_1 - 1) + (N_2 - 1) + 1 = N_1 + N_2 - 1 = N - 1$.

For an $m \times n$ bar, $mn - 1$ operations is enough. First make $m - 1$ horizontal breaks to get m separate $1 \times n$ pieces. Then for each of the m pieces, make $n - 1$ vertical breaks. Total number of operations is $(m - 1) + m(n - 1) = mn - 1$. □

★ **Exercise 1.3.16.** Given n real numbers $a_1, a_2, \ldots, a_n$, show that there exists a_i $(1 \leq i \leq n)$ such that a_i is greater than or equal to the mean of the n numbers.

Solution. Let $\bar{a}$ denote the mean value of $a_1, \ldots, a_n$. Suppose, for a contradiction, that $a_i < \bar{a}$ for all $i = 1, \ldots, n$. Then

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

a contradiction. □

★★ **Exercise 1.3.17.** Prove of disprove: there is an irrational number a such that for all irrational number b, ab is rational.

Solution. Disprove. For every irrational number a, we shall construct an irrational number b such that ab is irrational (note that we can consider multiple cases and construct more than one b).

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

Case 1: If $\frac{\sqrt{2}}{a}$ is irrational, take $b = \frac{\sqrt{2}}{a}$. Then $ab = \sqrt{2}$ is irrational.

Case 2: If $\frac{\sqrt{2}}{a}$ is rational, then its reciprocal $\frac{a}{\sqrt{2}}$ is also rational.

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

□

★★ **Exercise 1.3.18.** Prove that, for any positive integer n, there exists a perfect square m^2 such that $n \leq m^2 \leq 2n$.

Solution. Suppose, for a contradiction, that $n > m^2$ and $(m + 1)^2 > 2n$ for some positive integer n, so that there is no square between n and $2n$. Then

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

Since we are dealing with integers, we can write

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

which simplifies to

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

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

★ **Exercise 1.3.19.** Prove that $n! > 2^n$ for every positive integer $n \geq 4$.

Solution. Induct on n. Let $P(n) : n! > 2^n$.
The base case $P(4)$ is clear. Suppose $P(n)$ is true for some $n \geq 4$, i.e., $n! > 2^n$. Then

$$(n+1)! = n!(n+1) > 2^n(n+1) > 2^n \cdot 2 = 2^{n+1}.$$

□

★ **Exercise 1.3.20.** Prove that for $n \geq 2$, $\sqrt[n]{n} < 2 - \frac{1}{n}$.

Solution. Induct on n. Let $P(n) : \sqrt[n]{n} < 2 - \frac{1}{n}$ for $n \geq 2$.
The base case $P(2)$ is clear. Suppose $P(n)$ is true for $n \geq 2$, i.e., $\sqrt[n]{n} < 2 - \frac{1}{n}$, or $n < \left(2 - \frac{1}{n}\right)^n$. We want to show that $P(n+1)$ holds: $n + 1 < \left(2 - \frac{1}{n+1}\right)^{n+1}$. Since $n \geq 2$,

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

□

★ **Exercise 1.3.21.** Prove that for all integers $n \geq 3$, $\left(1 + \frac{1}{n}\right)^n < n$.

Solution. The base case $P(3)$ is true, since $\left(1 + \frac{1}{3}\right)^3 = \frac{64}{27} = 2\frac{10}{27} < 3$.
Suppose $P(n)$ is true for some $n \geq 3$, i.e., $\left(1 + \frac{1}{n}\right)^n < n$. Then

$$\begin{aligned}
\left(1 + \frac{1}{n+1}\right)^{n+1} &< \left(1 + \frac{1}{n}\right)^{n+1} \\
&= \left(1 + \frac{1}{n}\right)^{n}\left(1 + \frac{1}{n}\right) \\
&< n\left(1 + \frac{1}{n}\right) = n + 1.
\end{aligned}$$

□

The **Fibonacci sequence** (F_n) is defined recursively by

$$F_1 = 1, \quad F_2 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 3.$$

★ **Exercise 1.3.22.** Let (a_n) be a sequence of integers defined recursively by the 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 $n \in \mathbb{N}$, prove that $a_n \leq 2^{n-1}$.

Solution. Idea: Given the recurrence relation, we may need to use *strong induction*: use $P(k), P(k+1), P(k+2)$ to prove $P(k+3)$, for all $k \in \mathbb{N}$.
Let $P(n) : a_n \leq 2^{n-1}$.

The base cases $P(1)$, $P(2)$ and $P(3)$ are clear. Suppose $P(n)$, $P(n+1)$ and $P(n+2)$ are true for some $n \in \mathbb{N}$. We will show that $P(n+3)$ is true.

By inductive hypothesis, we have

$$a_n \leq 2^n, \qquad a_{n+1} \leq 2^{n+1}, \qquad a_{n+2} \leq 2^{n+2}.$$

Then

$$\begin{aligned} a_{n+3} &= a_n + a_{n+1} + a_{n+2} \\ &\leq 2^n + 2^{n+1} + 2^{n+2} \\ &= 2^n(1 + 2 + 2^2) \\ &< 2^n(2^3) = 2^{n+3}. \end{aligned}$$

□

★★ **Exercise 1.3.23.** For $m, n \in \mathbb{N}$, prove that

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

Solution. Fix m, induct on n. Let $P(n) : F_{n+m+1} = F_n F_m + F_{n+1} F_{m+1}$ for all $m \in \mathbb{N}$ in the cases $k = n$ and $k = n + 1$.

To show that $P(0)$ is true, 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 $F_1 = F_2 = 1$.

Now assume $P(n)$ is true; that is, for all $m \in \mathbb{N}$,

$$\begin{aligned} F_{n+m+1} &= F_n F_m + F_{n+1} F_{m+1}, \\ F_{n+m+2} &= F_{n+1} F_m + F_{n+2} F_{m+1}. \end{aligned}$$

Then

$$\begin{aligned} F_{n+m+3} &= F_{n+m+2} + F_{n+m+1} \\ &= F_n F_m + F_{n+1} F_{m+1} + F_{n+1} F_m + F_{n+2} F_{m+1} \\ &= (F_n + F_{n+1}) F_m + (F_{n+1} + F_{n+2}) F_{m+1} \\ &= F_{n+2} F_m + F_{n+3} F_{m+1} \end{aligned}$$

thus $P(n+1)$ is true, for all $m \in \mathbb{N}$. □

★ **Exercise 1.3.24** (MA1100 AY24/25)**.** Let $a_1 = 11$, $a_2 = 21$ and $a_{n+1} = 3a_n - 2a_{n-1}$ for all integers n with $n \geq 2$. Prove that for all positive integers n,

$$a_n = 5 \cdot 2^n + 1.$$

Solution. We proceed by strong induction.

For the base case, we have $a_1 = 5 \cdot 2^1 + 1 = 11$, so it is true.

Suppose, for all $1 \leq k \leq n$, we have $a_k = 5 \cdot 2^k + 1$. We will prove that $a_{n+1} = 5 \cdot 2^{n+1} + 1$:

$$\begin{aligned} a_{n+1} &= 3a_n - 2_{n-1} \\ &= 3(5 \cdot 2^n + 1) - 2(5 \cdot 2^{n-1} + 1) \\ &= 15 \cdot 2^n + 3 - 5 \cdot 2^n - 2 \\ &= 10 \cdot 2^n + 1 \\ &= 5 \cdot 2^{n+1} + 1 \end{aligned}$$

By strong induction, the result is true for all positive integers n. □

★★★ **Exercise 1.3.25** (MA1100T AY24/25)**.** Recall the Fibonacci numbers:

$$a_1 = 1, \quad a_2 = 2, \quad \text{and} \quad a_{n+2} = a_{n+1} + a_n \qquad \text{for } n \in \mathbb{N}.$$

You may assume without proof that:

$$\text{For all integers } m, n, \quad \text{if } 1 \leq m < n, \quad \text{then } m \leq a_m < a_n. \tag{$*$}$$

(i) For each integer $x \geq 2$, prove there is a largest positive integer n such that $a_n < x$.

(ii) Prove that every positive integer x can be expressed as the sum of a strictly increasing sequence of non-consecutive Fibonacci numbers.

Solution.

(i) Consider the set $S = \{n \in \mathbb{N} : a_n < x\}$.

Since S is non-empty ($1 \in S$) and bounded by x by the given fact $(*)$, then S has a largest element n.

(ii) We proceed by strong induction on x. Base case: $x = 1$.

Inductive step: If x is a Fibonacci number, we are done.

Otherwise, let $n \in \mathbb{N}$ be largest such that $a_n < x$.

By maximality of n, $x \leq a_{n+1}$. Since x is not a Fibonacci number, in fact $x < a_{n+1}$.

Notice n cannot be 1, because $a_1 = 1$ and $a_2 = 2$ have no integer in between. So $n \geq 2$, which means $a_{n+1} = a_n + a_{n-1}$. We may now write

$$x = (x - a_n) + a_n,$$

where $x - a_n$ is a positive integer strictly below a_{n-1}. By applying the inductive hypothesis to $x - a_n$, we may write $x - a_n$ as the sum of distinct non-consecutive Fibonacci numbers.

a_{n-1}, a_n and a_{n+1} do not appear in this sum because they are each larger than $x - a_n$, by the given fact.

So we may add a_n to this sum to express x as a sum of distinct non-consecutive Fibonacci numbers.

□

★ **Exercise 1.3.26** (MA1100T AY24/25)**.** Prove that for every real number x, there is at most one pair of rational numbers p and q such that

$$x = p\sqrt{2} + q.$$

Solution. Suppose, towards a contradiction, that a real number x admits two representations

$$x = p_1\sqrt{2} + q_1 = p_2\sqrt{2} + q_2,$$

where $p_1, p_2, q_1, q_2 \in \mathbb{Q}$ and $p_1 \neq p_2$, $q_1 \neq q_2$. Subtracting gives

$$(p_1 - p_2)\sqrt{2} = q_2 - q_1.$$

Since $p_1 - p_2 \neq 0$, we can solve for

$$\sqrt{2} = \frac{q_2 - q_1}{p_1 - p_2},$$

which would imply that $\sqrt{2}$ is rational, a contradiction.
Hence $p_1 - p_2 = 0$, so $p_1 = p_2$, and consequently $q_1 = q_2$. □

★★★ **Exercise 1.3.27** (MA1100T AY22/23)**.** We aim to prove that every rational number between 0 and 1 can be written as the sum of distinct positive reciprocals. (This is stated precisely in (iv)).

(i) Suppose $n < m$ are positive integers such that n does not divide m. Use well-ordering to prove that there is a **smallest** positive integer a such that

$$a \leq m - 1 \qquad \text{and} \qquad \frac{1}{a} < \frac{n}{m}.$$

(ii) In the context of (i), prove further that $an - m < n$.

(iii) In the context of (i), prove further that $\frac{n}{m} < \frac{2}{a}$.

(iv) Using (i) – (iii) or otherwise, prove that for every rational number r such that $0 < r < 1$, there are distinct positive integers $\{a_i\}_{i=0}^{j}$ such that

$$r = \sum_{i=0}^{j} \frac{1}{a_i}.$$

Solution.

(i)

(ii)

(iii)

(iv)

□

★★ **Exercise 1.3.28** (Binomial theorem)**.** Let x and y be real (or complex numbers), and $n \in \mathbb{N}$. Then

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Solution. Induct on $n \in \mathbb{N}$. Clearly the expression holds for $n = 0$, since LHS is 1, and RHS is also 1 (because $\binom{0}{0} = 1$ and any number raised to the power 0 is 1).
Suppose the expression holds for some $n \in \mathbb{N}$. Then by inductive hypothesis,

$$\begin{aligned}(x + y)^{n+1} &= (x + y)(x + y)^n \\ &= (x + y)\left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}.\end{aligned}$$

Continuing to expand the brackets gives

$$x^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} + y^{n+1},$$

where we have taken out the last term from the first sum and the first term from the second sum. In the first sum we now make a change of indexing variable; we set $k = l - 1$, noting that as k ranges over $0, 1, \ldots, n-1$ then l ranges over $1, 2, \ldots, n$. Thus the above equals

$$\begin{aligned}
&x^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=1}^{n} \binom{n}{k} x^k y^{n+1-k} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k} \right] x^k y^{n+1-k} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n+1-k} + y^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}
\end{aligned}$$

which shows that the expression holds for $n+1$.

Hence by induction, the expression holds for all $n \in \mathbb{N}$. □

★★ **Exercise 1.3.29.** Given n positive numbers $x_1, x_2, \ldots, x_n$ such that $x_1 + x_2 + \cdots + x_n \leq \frac{1}{3}$, prove by induction that

$$(1 - x_1)(1 - x_2) \cdots (1 - x_n) \geq \frac{2}{3}.$$

[*Hint*: For the inductive step, consider $x_1, x_2, \ldots, x_{n-1}, x_n + x_{n+1}$.]

Solution. For the base case $n = 1$, if $x_1 \leq \frac{1}{3}$, then $1 - x_1 \geq 1 - \frac{1}{3} = \frac{2}{3}$.

Suppose the result holds for some $n \in \mathbb{N}^+$. In particular, for positive numbers $x_1, x_2, \ldots, x_{n-1}, x_n + x_{n+1}$, we have $x_1 + \cdots + x_n + x_{n+1} \leq \frac{1}{3}$ and

$$(1 - x_1)(1 - x_2) \cdots (1 - x_{n-1})(1 - (x_n + x_{n+1})) \geq \frac{2}{3}.$$

Note that for non-negative a, b, we have

$$(1 - a)(1 - b) = 1 - (a + b) + ab \geq 1 - (a + b).$$

Thus $(1 - x_n)(1 - x_{n+1}) \geq 1 - (x_n + x_{n+1})$. Hence

$$(1 - x_1)(1 - x_2) \cdots (1 - x_n)(1 - x_{n+1}) \geq \frac{2}{3}$$

as desired. This completes the inductive step. □

★★ **Exercise 1.3.30** (MA1100T AY25/26)**.** Prove that every positive integer n can be written in base 2, i.e., there are distinct natural numbers $\{a_i\}_{i=0}^{j}$ such that $n = \sum_{i=0}^{j} 2^{a_i}$.

Solution. Define a predicate $P(n)$ with domain $\mathbb{N}^+$, which asserts that there are distinct $\{a_i\}_{i=0}^{j}$ in $\mathbb{N}$ such that $n = \sum_{i=0}^{j} 2^{a_i}$. We shall prove $P(n)$ for all $n \in \mathbb{N}^+$ by strong induction.

Base case: $1 = 2^0$, so we can take $a_0 = 1$.

Inductive step: Suppose $n \in \mathbb{N}^+$ is such that $P(m)$ holds for all $m \in \mathbb{N}^+$ less than or equal to n. We shall prove $P(n+1)$. We consider two cases:

Case 1: $n+1$ is even. Say $n+1=2k$ for $k\in\mathbb{Z}$. Note that $k\geq 1$ because $2k=n+1\geq 2$ (here we use $n\geq 1$). Furthermore, $k\leq n$ because $2k=n+1\leq 2n$ (again we use $n\geq 1$).

By inductive hypothesis, there are distinct $\{a_i\}_{i=0}^{j}$ in $\mathbb{N}$ such that $k=\sum_{i=0}^{j}2^{a_i}$. It follows that

$$n+1=2k=2\sum_{i=0}^{j}2^{a_i}=\sum_{i=0}^{j}2\cdot 2^{a_i}=\sum_{i=0}^{j}2^{a_i+1}.$$

Notice that for each i, $a_i+1\in\mathbb{N}$ because $a_i\in\mathbb{N}$. Furthermore, the a_i+1 are distinct because the a_i are distinct.

Case 2: $n+1$ is odd. Say $n+1=2k+1$ for $k\in\mathbb{Z}$. Note that $k\geq 1$ because otherwise $2k$ $(=n)$ would be non-positive, contrary to assumption. Furthermore, $k\leq n$ because $2k=n\leq 2n$.

By inductive hypothesis, there are distinct $\{a_i\}_{i=0}^{j}$ in $\mathbb{N}$ such that $k=\sum_{i=0}^{j}2^{a_i}$. Then

$$n+1=\sum_{i=0}^{j}2^{a_i+1}+1=\sum_{i=0}^{j}2^{a_i+1}+2^0.$$

Notice that for each i, $a_i+1\in\mathbb{N}^+$ because $a_i\in\mathbb{N}$. Furthermore, the numbers 0, a_0+1, $\ldots$, a_j+1 are distinct because the a_i+1 are distinct positive natural numbers.

□

2

Sets

2.1 Naive Set Theory

Definition 2.1. A **set** S is an unordered collection of distinct objects, called **elements** of S. If x is an element of S, we write $x \in S$; otherwise we write $x \notin S$.

There are three ways to describe a set:

1. **Roster notation**: list the elements of the set explicitly.
2. **Set-builder notation**: define a set in terms of some property $P(x)$ that the elements $x \in S$ satisfy:

   $$\{x \in S \mid P(x)\} \quad \text{or} \quad \{x \in S : P(x)\}.$$

   Sometimes it is convenient to use set-builder notation in a different form; for example, the set of even integers can be written as $\{2k \mid k \in \mathbb{Z}\}$ rather than $\{n \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(n = 2k)\}$.
3. By applying **set operations** to other sets, e.g., $S = A \cup B$.

The following sets of numbers are frequently encountered.

- The natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- The integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- The rational numbers $\mathbb{Q} = \left\{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\right\}$.
- The real numbers $\mathbb{R}$ (the construction of $\mathbb{R}$ will be discussed in Chapter 5).
- The complex numbers $\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$.

Definition 2.2. The **empty set** $\emptyset$ is the set with no elements.

Remark. $\{\emptyset\}$ and $\emptyset$ are different sets!

A set which contains some element is said to be **non-empty**.

Definition 2.3. The **universal set** $\mathcal{U}$ is the set containing all objects currently under consideration.

Unlike the empty set, the universal set depends on context.

Definition 2.4. We say A and B are **equal**, denoted by $A = B$, if they contain the same elements:

$$(\forall x)\, x \in A \Leftrightarrow x \in B.$$

Definition 2.5. We say A is a **subset** of B, denoted by $A \subseteq B$, if every element of A is in B:

$$(\forall x)\, x \in A \Rightarrow x \in B.$$

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

Lemma 2.6.

(i) $\emptyset \subseteq A$ *and* $A \subseteq A$.

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

(iii) $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$. *(double inclusion)*

(iii) is useful for proving two sets are equal.

Proof.

(i) Since there are no elements in $\emptyset$, $x \in \emptyset$ is false. Hence $(\forall x)(x \in \emptyset \Rightarrow x \in A)$ is vacuously true.

$(\forall x)(x \in A \Rightarrow x \in A)$ is obviously true.

(ii) Combine the two implications $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in C$.

(iii) $\boxed{\Rightarrow}$ Suppose $A = B$. Then every element in A is an element in B, so certainly $A \subseteq B$, and similarly $B \subseteq A$.

$\boxed{\Leftarrow}$ Suppose $A \subseteq B$ and $B \subseteq A$.

For every x, if $x \in A$, then $A \subseteq B$ implies that $x \in B$. If $x \notin A$, then $B \subseteq A$ means $x \notin B$.

Hence $x \in A$ if and only if $x \in B$, and therefore $A = B$.

□

Some frequently occurring subsets of $\mathbb{R}$ are known as **intervals**, which can be visualised as sections of the real line $\mathbb{R}$. We define **bounded intervals**

$$\begin{aligned}(a,b) &= \{x \in \mathbb{R} \mid a < x < b\},\\ [a,b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\},\\ [a,b) &= \{x \in \mathbb{R} \mid a \leq x < b\},\\ (a,b] &= \{x \in \mathbb{R} \mid a < x \leq b\},\end{aligned}$$

and **unbounded intervals**

$$\begin{aligned}(a,\infty) &= \{x \in \mathbb{R} \mid a < x\},\\ [a,\infty) &= \{x \in \mathbb{R} \mid a \leq x\},\\ (-\infty,a) &= \{x \in \mathbb{R} \mid x < a\},\\ (-\infty,a] &= \{x \in \mathbb{R} \mid x \leq a\}.\end{aligned}$$

An interval of the first type (a,b) is called an **open interval**; an interval of the second type $[a,b]$ is called a **closed interval**.

Note that if $a = b$, then $[a, b] = \{a\}$, while $(a, b) = [a, b) = (a, b] = \emptyset$.

Remark. The notation above uses the ∞ symbol, which you might have seen before to represent the concept of ”infinity”. Please note that $\infty \notin \mathbb{R}$ and it is not meaningful to write things like $x < \infty$. The notation for unbounded intervals is not a subset of the notation for bounded intervals!

Fix a universal set $\mathcal{U}$. Given sets $A, B \subseteq \mathcal{U}$, we define:

Definition 2.7.

(i) The **union** of A and B consists of elements in A or B:

$$A \cup B := \{x \in \mathcal{U} \mid x \in A \vee x \in B\}.$$

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

$$A \cap B := \{x \in \mathcal{U} \mid x \in A \wedge x \in B\}.$$

We say A and B are **disjoint** if $A \cap B = \emptyset$.

(iii) The **complement** of A consists of elements not in A:

$$A^c := \{x \in \mathcal{U} \mid x \notin A\}.$$

(iv) The **difference** of A and B consists of elements in A and not in B:

$$A \setminus B := \{x \in \mathcal{U} \mid x \in A \wedge x \notin B\}.$$

(v) The **symmetric difference** of A and B is

$$\begin{aligned} A \triangle B &:= \{x \in \mathcal{U} \mid x \in A \oplus x \in B\} \\ &= (A \setminus B) \cup (B \setminus A) \\ &= (A \cup B) \setminus (A \cap B). \end{aligned}$$

Venn diagrams are useful for visualising interactions between three or fewer sets. They can help us to discover proofs, but do not themselves constitute proofs.

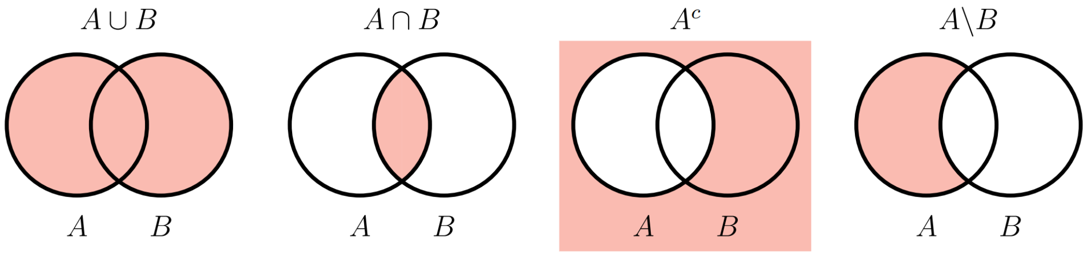


Figure 2.1: Venn diagrams.

One can prove set identities in several ways:

1. Convert the identity to a biconditional/implication in propositional logic and prove that it is a tautology (consider propositions P meaning “$x \in A$” and Q meaning “$x \in B$”.)
2. Element chasing
3. Set identities previously proven

There are many set identities which you can find on Wikipedia: https://en.wikipedia.org/wiki/List_of_set_identities_and_relations. The following result shall summarise the important ones.

Lemma 2.8. *Let $A, B, C \subseteq \mathcal{U}$.*

(i) $A \cup (B \cup C) = (A \cup B) \cup C$. *(associativity)*

(ii) $A \cap (B \cap C) = (A \cap B) \cap C$. *(associativity)*

(iii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. *(distributivity)*

(iv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. *(distributivity)*

(v) $(A \cup B)^c = A^c \cap B^c$. *(de Morgan's laws)*

(vi) $(A \cap B)^c = A^c \cup B^c$. *(de Morgan's laws)*

Proof. Exercise. □

Definition 2.9. An **ordered pair** is denoted by (a, b), where the order of the elements matters.

Equality of ordered pairs is defined as

$$(a_1, b_1) = (a_2, b_2) \iff a_1 = a_2 \text{ and } b_1 = b_2.$$

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*.

Definition 2.10. The **Cartesian product** of sets A and B is the set of all ordered pairs with the first element of the pair coming from A and the second from B:

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

More generally, we define

$$\prod_{i=1}^{n} A_i = A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) \mid a_i \in A_i,\ 1 \leq i \leq n\}.$$

If $A_1 = \cdots = A_n = A$, we denote the product as A^n.

Example. $\mathbb{R}^2$ is the Euclidean plane, $\mathbb{R}^3$ is the Euclidean space, and $\mathbb{R}^n$ is the n-dimensional Euclidean space.

$$\begin{aligned}
\mathbb{R}^2 &= \{(x, y) \mid x, y \in \mathbb{R}\},\\
\mathbb{R}^3 &= \{(x, y, z) \mid x, y, z \in \mathbb{R}\},\\
\mathbb{R}^n &= \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}.
\end{aligned}$$

The Cartesian product is not commutative, i.e., $A \times B \neq B \times A$ for all sets A and B; for example, if $A = \{1\}$, $B = \{2\}$, then $\{(1, 2)\} = A \times B \neq B \times A = \{(2, 1)\}$.
The Cartesian product is not associative (unless one of the involved sets is empty):

$$(A \times B) \times C \neq A \times (B \times C).$$

For example, if $A = \{1\}$, then $(A \times A) \times A = \{((1, 1), 1)\} \neq \{(1, (1, 1))\} = A \times (A \times A)$.

Lemma 2.11. *Let A, B, C, D be sets.*

(i) $A \times \emptyset = \emptyset \times A = \emptyset$.

(ii) $A \times (B \cup C) = (A \times B) \cup (A \times C)$. *(distributivity)*

(iii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$. *(distributivity)*

(iv) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$. *(distributivity)*

(v) $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$. *(intersection)*

(vi) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$. *(union)*

(vii) $(A \cap B) \times (C \cap D) = (A \cap C) \times (B \cap D)$.

(viii) $(A \cup B) \times (C \cup D) \subseteq (A \cup C) \times (B \cup D)$.

Proof.

(i) We shall show $A \times \emptyset = \emptyset$. The proof of $\emptyset \times A = \emptyset$ is similar.

$\boxed{\subseteq}$ Vacuously true.

$\boxed{\supseteq}$ This is equivalent to showing $(\forall x)[x \in A \times \emptyset \implies x \in \emptyset]$. But $x \in \emptyset$ is always false, so we need to show $(\forall x)\neg(x \in A \times \emptyset)$. Note that

$$\begin{aligned} x \in A \times \emptyset &\iff (\exists a \in A)(\exists b \in \emptyset)[x = (a, b)] \\ &\iff (\exists a)(\exists b)[[a \in A] \wedge [b \in \emptyset] \wedge [x = (a, b)]] \end{aligned}$$

is always false, since $b \in \emptyset$ is always false. Hence $(\forall x)\neg(x \in A \times \emptyset)$ is true.

(ii) We have

$$\begin{aligned} x \in A \times (B \cup C) &\iff (\exists a \in A)(\exists b \in B \cup C)x = (a, b) \\ &\iff (\exists a \in A)[(\exists b \in B) \vee (\exists b \in C)]x = (a, b) \\ &\iff [(\exists a \in A)(\exists b \in B)x = (a, b)] \vee [(\exists a \in A)(\exists b \in C)x = (a, b) \\ &\iff (x \in A \times B) \vee (x \in A \times C)] \\ &\iff x \in (A \times B) \cup (A \times C). \end{aligned}$$

(iii) $\boxed{\subseteq}$ Let $x \in A \times (B \cap C)$. Then $x = (a, b)$ for some $a \in A$, $b \in B \cap C \Rightarrow b \in B$ and $b \in C$. Thus $x = (a, b) \in A \times B$ and $x = (a, b) \in A \times C$, so $x \in (A \times B) \cap (A \times C)$.

$\boxed{\supseteq}$ Let $x \in (A \times B) \cap (A \times C)$. Then $x \in A \times B$ and $x \in A \times C$, so $x = (a, b)$ for some $a \in A$, $b \in B$, and $x = (a, b)$ for some $a \in A$, $b \in C$. Thus $x = (a, b)$ for some $a \in A$, $b \in B \cap C$. Hence $x \in A \times (B \cap C)$.

(iv)

(v)

(vi) We have

$$\begin{aligned} x \in (A \times B) \cup (C \times D) &\implies (x \in A \times B) \vee (x \in C \cup D) \\ &\implies [(\exists a \in A)(\exists b \in B)x = (a, b)] \vee [(\exists a \in C)(\exists b \in D)x = (a, b)] \\ &\implies (\exists a \in A \cup C)(\exists b \in B \cup D)x = (a, b) \\ &\implies x \in (A \cup C) \times (B \times D). \end{aligned}$$

Equality need not hold in general. Let $A = \mathbb{Z} = D$ and $B = \emptyset = C$. Then $A \times B = \emptyset = C \times D$, so $(A \times B) \cup (C \times D) = \emptyset$. Thus

$$(A \cup C) \times (B \cup D) = \mathbb{Z} \times \mathbb{Z} \neq \emptyset = (A \times B) \cup (C \times D).$$

(vii)

(viii)

□

Our last operation defines the collection of all subsets of a set.

Definition 2.12. The **power set** $\mathcal{P}(A)$ of A is the set of all subsets of A.

Notation. In other literature, the power set of A is commonly denoted by 2^A. (This notation is suggestive: it hints that if A is finite, then $\left|2^A\right| = 2^{|A|}$.)

For all sets A, we have $\emptyset \in \mathcal{P}(A)$ (since $\emptyset \subseteq A$) and $A \in \mathcal{P}(A)$ (since $A \subseteq A$).

Example.

$$\begin{aligned} \mathcal{P}(\{1,3\}) &= \{\emptyset, \{1\}, \{3\}, \{1,3\}\} \\ \mathcal{P}(\emptyset) &= \{\emptyset\} \\ \mathcal{P}(\{\emptyset\}) &= \{\emptyset, \{\emptyset\}\} \end{aligned}$$

Lemma 2.13. *Let A, B be sets. Then $A \subseteq B \iff \mathcal{P}(A) \subseteq \mathcal{P}(B)$.*

Proof.
$\boxed{\Rightarrow}$ Suppose $A \subseteq B$.
Let $X \in \mathcal{P}(A)$. Then $X \subseteq A$. By assumption, $X \subseteq B$. Thus $X \in \mathcal{P}(B)$.
$\boxed{\Leftarrow}$ Suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
Let $x \in A$. Then $\{x\} \subseteq A$, so $\{x\} \in \mathcal{P}(A)$. By assumption, $\{x\} \in \mathcal{P}(B) \implies \{x\} \subseteq B \implies x \in B$. □

Corollary 2.14. *Let A, B be sets. Then $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.*

Proof.
$\boxed{\subseteq}$ By the preceding lemma, we have $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A)$ and $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(B)$.
$\boxed{\supseteq}$ This follows easily. □

Since unions and intersections are associative, the notation $A \cup B \cup C$ is unambiguous, and we can therefore generalise this notion to arbitrary indexed sets (could be finitely or infinitely many).

Definition 2.15. Let I be a non-empty set, and $\{A_i\}_{i \in I}$ be a family of sets indexed by I. Then

$$\begin{aligned} \bigcup_{i \in I} A_i &:= \{x \in \mathcal{U} \mid (\exists i \in I)\, x \in A_i\}, \\ \bigcap_{i \in I} A_i &:= \{x \in \mathcal{U} \mid (\forall i \in I)\, x \in A_i\}. \end{aligned}$$

If $I = \mathbb{N}$ or $I = \mathbb{Z}$, it is common to denote the union by $\bigcup_{n=0}^{\infty} A_n$ or $\bigcup_{n=-\infty}^{\infty} A_n$ respectively; the intersection is denoted similarly.

Remark. If $I = \emptyset$, then $\bigcup_{i\in I} A_i = \emptyset$ and $\bigcap_{i\in I} A_i = \mathcal{U}$ (since $\forall i \in \emptyset$ is vacuously true).

Lemma 2.16. *Let I be a non-empty set, and let $\{A_i\}_{i\in I}$ be a family of sets indexed by I. Then*

(i) *For each $j \in I$, $\bigcap_{i\in I} A_i \subseteq A_j$.*

(ii) *For each $j \in I$, $A_j \subseteq \bigcup_{i\in I} A_i$.*

(iii) $(\bigcap_{i\in I} A_i) \cup B = \bigcap_{i\in I}(A_i \cup B)$. *(distributivity)*

(iv) $(\bigcup_{i\in I} A_i) \cap B = \bigcup_{i\in I}(A_i \cap B)$. *(distributivity)*

(v) $(\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} {A_i}^c$. *(de Morgan's laws)*

(vi) $(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} {A_i}^c$. *(de Morgan's laws)*

(vii) $(\bigcup_{i\in I} A_i) \cup (\bigcup_{j\in J} B_j) = \bigcup_{(i,j)\in I\times J}(A_i \cup B_j)$.

(viii) $(\bigcap_{i\in I} A_i) \cup (\bigcap_{j\in J} B_j) = \bigcap_{(i,j)\in I\times J}(A_i \cup B_j)$.

Proof.

(i) Let $j \in I$. Let $x \in \bigcap_{i\in I} A_i$. Then for each $i \in I$, $x \in A_i$. In particular, $x \in A_j$.

(ii) Let $j \in I$. Let $x \in A_j$. Then $x \in A_i$ for some $i \in I$, so $x \in \bigcup_{i\in I} A_i$.

(iii) $\boxed{\subseteq}$ Let $x \in (\bigcap_{i\in I} A_i) \cup B$.

Case 1: If $x \in B$, then for every $i \in I$, $x \in A_i \cup B$. Thus $x \in \bigcap_{i\in I}(A_i \cup B)$.

Case 2: If $x \in \bigcap_{i\in I} A_i$, then for every $i \in I$, $x \in A_i$. It follows that for every $i \in I$, $x \in B \cup A_i$. Thus $x \in \bigcap_{i\in I}(A_i \cup B)$ as well.

$\boxed{\supseteq}$ Let $x \in \bigcap_{i\in I}(A_i \cup B)$. Then $x \in A_i \cup B$ for every $i \in I$.

Case 1: If $x \in B$, then $x \in (\bigcap_{i\in I} A_i) \cup B$.

Case 2: If $x \notin B$, then for every $i \in I$, since $x \in A_i \cup B$, we must have $x \in A_i$. This means that $x \in \bigcap_{i\in I} A_i$. Hence $x \in (\bigcap_{i\in I} A_i) \cup B$.

(iv) $\boxed{\subseteq}$ Let $x \in (\bigcup_{i\in I} A_i) \cap B$. Then $x \in (\bigcup_{i\in I} A_i)$ and $x \in B$.

This means there exists $i \in I$ such that $x \in A_i$, and $x \in B$. Corresponding to this $i \in I$, we have $x \in B$.

Hence $x \in \bigcup_{i\in I}(A_i \cap B)$.

$\boxed{\supseteq}$ Let $x \in \bigcup_{i\in I}(A_i \cap B)$. Then there exists $i \in I$ such that $x \in A_i \cap B$, so $x \in A_i$ and $x \in B$.

This means there exists $i \in I$ such that $x \in A_i$, so $x \in \bigcup_{i\in I} A_i$. This also means $x \in B$.

Hence $x \in (\bigcup_{i\in I} A_i) \cap B$.

(v) By de Morgan's laws,

$$\begin{aligned} x \in (\bigcup_{i\in I} A_i)^c &\iff x \notin \bigcup_{i\in I} A_i \\ &\iff \neg[x \in \bigcup_{i\in I} A_i] \\ &\iff \neg[(\exists i \in I)[x \in A_i]] \\ &\iff (\forall i \in I)[x \in {A_i}^c] \\ &\iff x \in \bigcap_{i\in I} {A_i}^c \end{aligned}$$

(vi) Use de Morgan's laws.

(vii)

(viii)

□

When considering families of sets indexed by ℕ, our usual notation will be $\{A_n\}_{n=0}^\infty$.

Definition 2.17. The **limit superior** and **limit inferior** of $\{A_n\}_{n=0}^\infty$ are

$$\limsup A_n := \bigcap_{k=0}^\infty \bigcup_{n=k}^\infty A_n, \qquad \liminf A_n := \bigcup_{k=0}^\infty \bigcap_{n=k}^\infty A_n.$$

A member of $\bigcap_{k=1}^\infty \bigcup_{n=k}^\infty A_n$ is a member of *all* of the sets $\bigcup_{n=k}^\infty A_n$, so it is a member of $A_1 \cup A_2 \cup A_3 \cup \cdots$ and of $A_2 \cup A_3 \cup A_4 \cup \cdots$ and of ... etc. That means no matter how far down the sequence you go, it's a member of at least one of the sets that come later. That means it's a member of infinitely many of them, but there might also be infinitely many that it does not belong to.

A member of $\bigcup_{k=1}^\infty \bigcap_{n=k}^\infty A_n$ is a member of *at least one* of the sets $\bigcup_{n=k}^\infty A_n$, meaning it is a member of either $A_1 \cap A_2 \cap A_3 \cap \cdots$ or $A_2 \cap A_3 \cap A_4 \cap \cdots$ or ... etc. This means that it is a member of all except finitely many of the A_n.

To summarise,

$$\begin{aligned} \limsup A_n &= \{x \mid x \in A_n \text{ for infinitely many } n\}, \\ \liminf A_n &= \{x \mid x \in A_n \text{ for all but finitely many } n\}. \end{aligned}$$

Proposition 2.18. *Let $\{A_n\}_{n=0}^\infty$ be sets. Then*

$$\liminf A_n \subseteq \limsup A_n.$$

Proof. Let $x \in \bigcup_{k=0}^\infty \bigcap_{n=k}^\infty A_n$. Then there exists $k_0 \in \mathbb{N}$ such that $x \in \bigcap_{n=k_0}^\infty A_n$. This means $x \in A_n$ for all $n \geq k_0$:

$$x \in A_{k_0} \quad \text{and} \quad x \in A_{k_0+1} \quad \text{and} \quad \cdots$$

Let $k \in \mathbb{N}$ be arbitrary. We need to show $x \in \bigcup_{n=k}^\infty A_n$, i.e., $x \in A_n$ for some $n \geq k$.

- If $k \leq k_0$, since $x \in A_{k_0}$ and $k_0 \geq k$, it follows that $x \in \bigcup_{n=1}^\infty A_n$.
- If $k \geq k_0$, since $x \in A_n$ for all $n \geq k_0$, in particular we have $x \in A_n$ for all $n \geq k$. Thus $x \in \bigcup_{n=1}^\infty A_n$.

Thus for every $k \in \mathbb{N}$, we have $x \in \bigcup_{n=k}^\infty A_n$. Hence $x \in \bigcap_{k=0}^\infty \bigcup_{n=k}^\infty A_n$. □

— Exercises —

Exercise 2.1.1. Show that for all sets A and B, we have $A \triangle B = A$ if and only if $B = \emptyset$.

Solution.

$\boxed{\Rightarrow}$ Suppose, towards a contradiction, that $A \triangle B = A$ and B is non-empty; fix some $b \in B$. Consider two cases:

Case 1: $b \in A$. Then b lies in both A and B, so $b \notin A \triangle B$. Since $A \triangle B = A$, it follows that $b \notin A$.

Case 2: $b \notin A$. Then $b \notin A$ and $b \in B$, so $b \in A \triangle B$. Since $A \triangle B = A$, it follows that $b \in A$.

Both cases lead to a contradiction. Hence $B = \emptyset$.

$\boxed{\Leftarrow}$ Suppose $B = \emptyset$. Then $A \triangle B = A \triangle \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A$. □

Exercise 2.1.2 ([End77])**.** Show that if $A \subseteq B$, then $C \setminus B \subseteq C \setminus A$.

Solution. Let $x \in C \setminus B$. Then $x \in C$ and $x \notin B$. By assumption, $x \notin A$. Hence $x \in C \setminus A$. □

Exercise 2.1.3. Prove or disprove: If $A \cap B = \emptyset$, then $\mathcal{P}(A) \cap \mathcal{P}(B) = \emptyset$.

Solution. Disprove. $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset\}$. □

Exercise 2.1.4. For all sets A, B and C, show that $A \times B \subseteq A \times C$ if and only if $B \subseteq C$.

Solution. The case where $A = \emptyset$ is trivial. Thus assume A is non-empty.

$\boxed{\Rightarrow}$ Suppose $A \times B \subseteq A \times C$. Let $b \in B$.

Since A is non-empty, fix some $a \in A$. Then $(a, b) \in A \times B$. By assumption, $(a, b) \in A \times C$. Hence $b \in C$.

$\boxed{\Leftarrow}$ Suppose $B \subseteq C$. Let $x \in A \times B$. Then $x = (a, b)$, where $a \in A$, $b \in B$.

By assumption, $b \in C$, so $x = (a, b) \in A \times C$. □

Exercise 2.1.5. Prove that for all sets A, B and C, we have $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

Solution.

$\boxed{\subseteq}$ Let $x \in (A \setminus B) \setminus C$. Then $x \in A \setminus B$ and $x \notin C$. Thus $x \in A$ and $x \notin B$ and $x \notin C$.

- In particular, $x \in A$ and $x \notin C$, so $x \in A \setminus C$, and
- $x \notin B$ implies $x \notin B \setminus C$.

Hence $x \in (A \setminus C) \setminus (B \setminus C)$.

$\boxed{\supseteq}$ Let $x \in (A \setminus C) \setminus (B \setminus C)$. Then $x \in A \setminus C$ and $x \notin B \setminus C$. This means $x \in A$ and $x \notin C$, and $x \notin B$ or $x \in C$. Since $x \notin C$, $x \in C$ is false; thus $x \notin B$.

We have $x \in A$ and $x \notin B$ and $x \notin C$, so $x \in A \setminus B$ and $x \notin C$. Hence $x \in (A \setminus B) \setminus C$. □

Exercise 2.1.6. Prove or disprove: For all sets A, B, C and D, if $A \times B \subseteq C \times D$, then $A \subseteq C$ and $B \subseteq D$.

Solution. Disprove. $\emptyset \times \{1\} = \emptyset \subseteq \emptyset = \{1\} \times \emptyset$.

Remark. Remember to consider empty sets! The above result is true if the sets are non-empty.

□

Exercise 2.1.7. Prove or disprove: For all sets $\{A_i\}_{i \in I}$ and $\{B_i\}_{i \in I}$, we have $(\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i) = \bigcap_{i \in I}(A_i \cup B_i)$.

Solution. Disprove; we show that $\boxed{\supseteq}$ does not hold. The idea is to make $\bigcap_{i\in I} A_i = \bigcap_{i\in I} B_i = \emptyset$, and $\bigcap_{i\in I}(A_i \cup B_i) \neq \emptyset$.
For each $n \in \mathbb{N}^+$, make $A_n \cup B_n$ all the same, equal $[0,1]$:

$$A_n = \left[0, \frac{1}{2^{n-1}}\right), \qquad B_n = \left[\frac{1}{2^{n-1}}, 1\right].$$

□

Exercise 2.1.8 (MA1100T AY22/23)**.**

(a) Prove that for all sets A, B and C, we have $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

(b) Disprove: For all sets A, B and C, we have $A \cup (B \triangle C) = (A \cup B) \triangle (A \cup C)$.

Solution.

(a) $\boxed{\subseteq}$ Let $x \in A \cap (B \triangle C)$. Then $x \in A$ and $x \in B \triangle C$.

- If $x \in B$, then $x \notin C$. Thus $x \in A \cap B$ and $x \notin A \cap C$.
- If $x \in C$, then $x \notin B$. Thus $x \in A \cap C$ and $x \notin B \cap C$.

$\boxed{\supseteq}$ Let $x \in (A \cap B) \triangle (A \cap C)$.

- If $x \in A \cap B$ and $x \notin A \cap C$, then $x \in A$ and $x \in B$, and $x \notin A$ or $x \notin C$. Thus $x \notin A$ cannot hold, so we must have $x \notin C$. Thus $x \in A \cap (B \triangle C)$.
- Similar.

(b)

□

Exercise 2.1.9 (MA1100 AY24/25)**.** For each $n \in \mathbb{N}^+$, let $A_n = \left(1 - \frac{1}{n}, n\right)$. Find

$$\text{(a)} \quad \bigcup_{n=1}^{\infty} A_n \qquad \text{(b)} \quad \bigcap_{n=1}^{\infty} A_n.$$

Solution.

(a) Claim: $\bigcup_{n=1}^{\infty} A_n = (0, \infty)$.

$\boxed{\subseteq}$ Let $x \in \bigcup_{n=1}^{\infty} A_n$. Fix $n \in \mathbb{N}^+$ such that $x \in A_n$, i.e., $1 - \frac{1}{n} < x < n$.

When $n = 1$, we have $0 < x < 1$. As $n \to \infty$, we have $x > 1$. As such, $x > 0$, which follows that $x \in (0, \infty)$.

$\boxed{\supseteq}$ Let $x \in (0, \infty)$. Then for some $n \in \mathbb{N}^+$, we can pick $n > \max\{x, 1/x\}$ such that we have

$$x < n \qquad \text{or} \qquad \frac{1}{n} > x \implies -\frac{1}{n} < -x \implies 1 - \frac{1}{n} < 1 - x < x.$$

Hence $1 - \frac{1}{n} < x < n$, so $x \in \bigcup_{n=1}^{\infty} A_n$.

(b) Claim: $\bigcap_{n=1}^{\infty} A_n = \emptyset$.

Suppose, towards a contradiction, that $\bigcap_{n=1}^{\infty} A_n \neq \emptyset$. Fix $x \in \bigcap_{n=1}^{\infty} A_n$. Then $1 - \frac{1}{n} < x < n$ for all $n \in \mathbb{N}^+$.

Taking $n = 1$, we have $0 < x < 1$; thus $1 - \frac{1}{n} < x < 1$ for all $n \in \mathbb{N}^+$.

By the Archimedian property, since $1 - x > 0$, fix $n_0 \in \mathbb{N}^+$ such that $\frac{1}{n_0} < 1 - x$, i.e., $x < 1 - \frac{1}{n_0}$, a contradiction.

□

Exercise 2.1.10 (MA1100T AY21/22)**.** Prove or disprove: For any sets A and B, there exists a unique set X with the following property:

$$\text{For any set } T\text{, one has } T \subseteq X \text{ if and only if } T \cup B \subseteq A$$

Solution. Disprove by counterexample. Take $A = \{1\}$, $B = \{1, 2\}$, and suppose there exists such a set X. If T is the empty set, then $T \subseteq X$, so we have $T \cup B \subseteq A$. But $T \cup B = \{1, 2\} \nsubseteq A$ which is a contradiction. □

Exercise 2.1.11 (MA1100T AY21/22)**.** Prove or disprove: For any sets A and B, there exists a unique set X with the following property:

$$\text{For any set } T\text{, one has } T \supseteq X \text{ if and only if } T \cup B \supseteq A$$

Solution. True.
$\boxed{\text{Existence}}$ Take $X = A \setminus B$. We will show that X has the desired properties.
$\boxed{\Rightarrow}$ Suppose $T \supseteq A \setminus B$.
Let $x \in A$. We consider two cases:

- If $x \in B$, then $x \in T \cup B$.
- If $x \notin B$, then $x \in A \setminus B \subseteq T \subseteq T \cup B$.

This shows that $T \cup B \supseteq A$.
$\boxed{\Leftarrow}$ Suppose $T \cup B \supseteq A$.
Let $x \in A \setminus B$. Then $x \in A$ and $x \notin B$. By assumption, $x \in T \cup B$, so $x \in T$ or $x \in B$. But $x \notin B$, hence $x \in T$.
This shows that $T \supseteq A \setminus B$.
$\boxed{\text{Uniqueness}}$ Suppose another set Y satisfies the given conditions. Then

$$T \supseteq X \iff T \cup B \supseteq A \iff T \supseteq Y.$$

Then picking $T = X$ and $T = Y$ yields $X \supseteq Y$ and $Y \supseteq X$. Hence we must have $X = Y$. □

Exercise 2.1.12 (MA1100T AY21/22)**.** Let X be any set such that $\emptyset \in X$ and such that for any $x \in X$, one has $\{x\} \in X$. Define a sequence $A_1, A_2, \dots$ of elements of X recursively as follows:

$$A_1 = \emptyset, \qquad A_{n+1} = \{A_n\} \quad (n \in \mathbb{N}).$$

Show thay for any $i, j \in \mathbb{N}$ with $i \neq j$, one has $A_i \neq A_j$.

Solution. Let $P(n)$ be the proposition "for any $i, j \in \mathbb{N}$ with $i, j \leq n$ and $i \neq j$, one has $A_i \neq A_j$". Induct on n.
$\boxed{\text{Base case}}$ If $n = 1$, then $i = j = 1$, so $P(1)$ is vacuously true.
If $n = 2$, WLOG assume $i = 1$ and $j = 2$. Then $A_1 = \emptyset$ and $A_2 = \{\emptyset\}$, so $A_1 \neq A_2$.
$\boxed{\text{Inductive step}}$ Suppose $P(n)$ is true for some positive integer $n \geq 2$. We will prove $P(n+1)$ is true.
Let $i, j \leq n + 1$. If $i, j \leq n$, then by inductive hypothesis, $A_i \neq A_j$. Otherwise, either i or j must be $n + 1$. WLOG assume $i = n + 1$, so $j \leq n$. If $j = 1$ then $A_{n+1} \neq A_1$ since A_1 is empty and A_{n+1} is not. Otherwise, $j > 1$.

Suppose, for a contradiction, that $A_{n+1} = A_j$. Since A_n and A_{j-1} are the only elements of the sets A_{n+1} and A_j respectively, $A_n = A_{j-1}$. But $n, j - 1 \in \mathbb{N}$ and $n, j - 1 \leq n$ with $n \neq j - 1$ therefore by assumption $A_n \neq A_{j-1}$. This is a contradiction; hence $A_{n+1} \neq A_j$. Hence $P(n + 1)$ holds.

Now for any $i, j \in \mathbb{N}$, take $n = \max\{i, j\}$. Since $i, j \leq n$ and $i \neq j$, $P(n)$ witnesses $A_i \neq A_j$ as desired. □

Exercise 2.1.13 (MA1100T AY24/25)**.** Prove or disprove each of the following statements.

(i) For all sets A, B and C, we have $(A \setminus B) \setminus C = A \setminus (B \setminus C)$.

(ii) For all sets A and B, we have $\mathcal{P}(A) \setminus \mathcal{P}(B) \supseteq \mathcal{P}(A \setminus B)$.

Solution.

(i) Disprove: Consider $A = B = C = \{\emptyset\}$.

Then $B \setminus C$ is empty, so $A \setminus (B \setminus C) = A$, which is non-empty.

On the other hand, $A \setminus B$ is empty as well, so $(A \setminus B) \setminus C$ is empty.

(ii) Disprove: Consider $A = B = \emptyset$.

Then $\mathcal{P}(A) \setminus \mathcal{P}(B)$ is empty, but $\mathcal{P}(A \setminus B) = \mathcal{P}(\emptyset)$ is not (because it has an element $\emptyset$).

□

Exercise 2.1.14 (MA1100T AY24/25)**.** Fix a subset $X \subseteq \mathcal{P}(\mathbb{N})$. For each $A \subseteq \mathbb{N}$, define $\mathrm{cl}(A)$ to be the set of all $a \in \mathbb{N}$ such that a lies in every $B \in X$ with $B \supseteq A$:

$$\mathrm{cl}(A) = \left\{a \in \mathbb{N} : (\forall B \in X)\, B \supseteq A \to a \in B\right\}.$$

(i) Prove that for all $A \subseteq \mathbb{N}$, we have $A \subseteq \mathrm{cl}(A)$.

(ii) Prove that for all $A \subseteq \mathbb{N}$, we have $\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A)$.

Solution.

(i) Let $a \in A$. Then if $B \in X$ and $A \subseteq B$, we have $a \in B$, so $a \in \mathrm{cl}_X(A)$.

(ii) $\boxed{\supseteq}$ This follows from (i), by replacing A with $\mathrm{cl}(A)$.

$\boxed{\subseteq}$ Let $x \in \mathrm{cl}(\mathrm{cl}(A))$. To show that $x \in \mathrm{cl}(A)$, suppose $B \in X$ and $A \subseteq B$. Then $\mathrm{cl}(A) \subseteq B$, by definition of cl. So by definition of $\mathrm{cl}(\mathrm{cl}(A))$, we have $x \in B$ as desired.

□

Exercise 2.1.15. For every set F, we define its closure

$$\mathrm{cl}(F) = \bigcup_{X \in F} \mathcal{P}(X).$$

Prove that for every set F,

$$\mathrm{cl}(\mathrm{cl}(F)) = \mathrm{cl}(F).$$

(MA1100T AY22/23)

Solution.

$\boxed{\subseteq}$ Let $x \in \mathrm{cl}(\mathrm{cl}(F))$. Then there exists $X \in \mathrm{cl}(F)$ such that $x \in \mathcal{P}(X)$, i.e., $x \subseteq X$. By definition of cl, there exists $X_0 \in F$ such that $X \in \mathcal{P}(X_0)$, i.e., $X \subseteq X_0$.

Hence $x \subseteq X_0$, so $x \in \mathcal{P}(X_0)$, where $X_0 \in F$. By definition, $x \in \mathrm{cl}(F)$.

$\boxed{\supseteq}$ Let $x \in \mathrm{cl}(F)$. Then there exists $X \in F$ such that $x \subset X$.

Note that $X \in \mathcal{P}(X)$, so $X \in \mathrm{cl}(F)$.

Hence $x \in \mathcal{P}(X)$ with $X \in \mathrm{cl}(F)$, so $x \in \mathrm{cl}(\mathrm{cl}(F))$. □

2.2 Axiomatic Set Theory

Naive set theory has to contend with Russell's paradox[1], which provides a warning as to the looseness of our definition of a set. It goes as follows:

> Suppose H is the collection of sets that are not elements of themselves. The problem arises when we ask the question of whether or not H is itself in H.
>
> **Case 1:** If $H \notin H$, then H meets the precise criterion for being in H, and so $H \in H$, a contradiction.
>
> **Case 2:** If $H \in H$, then by the property required for this to be the case, $H \notin H$, another contradiction.
>
> Thus we have a paradox: H is neither in H, nor not in H.

To avoid contradictions such as Russell's paradox, axiomatic set theory restricts the construction of sets via so-called axioms. The axiom system containing all these axioms is called **Zermelo–Fraenkel Set Theory**.

Before we begin to present the axioms of Set Theory, let us say a few words about Set Theory in general: The language of Set Theory contains only one non-logical symbol, namely the binary membership relation $\in$, and there exists just one type of object, namely sets.

2.2.1 Axiom of Empty Set

Axiom 2.19 (Empty set).

$$\exists x \forall z (z \notin x)$$

This axiom postulates the existence of a set without any elements, i.e., an **empty set**. It also shows that the set-theoretic universe is non-empty, because it contains at least an empty set.

2.2.2 Axiom of Extensionality

Axiom 2.20 (Extensionality).

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

This axiom says that any two sets having the same elements are equal. Hence a set is uniquely determined by its elements.

Remark. If $x = y$, then automatically (i.e., by logic) anything that is true of the object x is also true of the object y (it being the same object). For example, if $x = y$, then it is automatically true that for any object z, $z \in x \leftrightarrow z \in y$. (This is the converse to Extensionality.)

Extensionality also shows that the empty set, postulated by Empty Set, is unique. For assume that there are two empty sets x_0 and x_1, then we have $\forall z (z \notin x_0 \wedge z \notin x_1)$, which implies that $\forall z (z \in x_0 \leftrightarrow z \in x_1)$, and therefore, $x_0 = x_1$.

The empty set is denoted by $\emptyset$.

[1] after the mathematician and philosopher Bertrand Russell (1872–1970)

Definition 2.21. We say that y is a **subset** of x, denoted $y \subseteq x$, if

$$\forall z(z \in y \to z \in x).$$

We say that y is a **proper subset** of x, denoted $y \subset x$, if $y \subseteq x$ and $y \neq x$.

Remark. The empty set is a subset of every set.

2.2.3 Axiom of Pairing

Axiom 2.22 (Pairing)**.**

$$\forall x \forall y \exists u \forall z(z \in u \leftrightarrow (z = x \vee z = y))$$

Informally, we just write

$$\forall x \forall y \exists u(u = \{x, y\}),$$

where $\{x, y\}$ denotes the set which contains just the elements x and y. If $x = y$, then $\{x, x\} = \{x\}$ by Extensionality. Thus if x is a set, then $\{x\}$ is also a set.

Starting with $\emptyset$, an iterated application of Pairing allows us to construct sets with a single element of two elements: $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, $\ldots$, and $\{\emptyset, \{\emptyset\}\}$, $\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, $\ldots$.

For any sets x and y, Extensionality implies that $\{x, y\} = \{y, x\}$. Thus the order in which the elements of a 2-element set are written down does not matter.

Definition 2.23. An **ordered pair** (x, y) is defined as

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

We need to prove that this definition succeeds in capturing the desired property: The ordered pair (x, y) uniquely determines both what x and y are, and the order upon them.

Lemma 2.24. *$(x, y) = (x', y')$ if and only if $x = x'$ and $y = y'$.*

Proof.

$\boxed{\Leftarrow}$ Trivial; if $x = x'$ and $y = y'$, then $(x, y) = \{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} = (x', y')$.

$\boxed{\Rightarrow}$ Suppose $(x, y) = (x', y')$, i.e.,

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}.$$

Then we have

$$\{x\} \in \{\{x'\}, \{x', y'\}\} \quad \text{and} \quad \{x, y\} \in \{\{x'\}, \{x', y'\}\}.$$

From the first of these, we know that either

$$\text{(a) } \{x\} = \{x'\} \quad \text{or} \quad \text{(b) } \{x\} = \{x', y'\},$$

and from the second we know that either

$$\text{(c) } \{x, y\} = \{x'\} \quad \text{or} \quad \text{(d) } \{x, y\} = \{x', y'\}.$$

First suppose (b) holds; then $x = x' = y'$. Then (c) and (d) are equivalent, and tell us that $x = y = x' = y'$. In this case the conclusion of the result holds. Similarly if (c) holds, we have the same situation.

There remains the case in which (a) and (d) hold. From (a) we have $x = x'$. From (d) we get either $x = y'$ or $y = y'$. In the first case (b) holds; that case has already been considered. In the second case we have $y = y'$, as desired. □

Example. If we define $(x, y) := \{x, \{y\}\}$, then this definition is problematic:

$$\begin{aligned}(\{\emptyset\}, \{\emptyset\}) &= (\{\emptyset\}, \{\{\emptyset\}\}) \\ &= (\{\{\emptyset\}\}, \{\emptyset\}) \\ &= (\{\{\emptyset\}\}, \emptyset).\end{aligned}$$

So far, all sets that are guaranteed to exist have at most two elements.

2.2.4 Axiom of Union

Axiom 2.25 (Union).

$$\forall x\, \exists u\, \forall z (z \in u \leftrightarrow (\exists w \in x)\, z \in w)$$

Informally, for each set x, there exists a set whose elements belong to at least one of element of x. We call this set u the **union** of x, denoted $\bigcup x$. For example, if $x = \{\{a, b\}, \{b, c\}\}$, then $\bigcup x = \{a, b, c\}$. For sets x and y, define the (unary) **union** of x and y as

$$x \cup y := \bigcup \{x, y\}.$$

For example. $\{x, y\} \cup \{z\} = \bigcup \{\{x, y\}, \{z\}\} = \{x, y, z\}$. Thus we can construct sets with more than 2 elements.

2.2.5 Axiom Schema of Separation

Axiom 2.26 (Separation). *Let ϕ be a formula with all free variables among $x, z, p_1, \ldots, p_n$ (y is not free in ϕ). Then*

$$\forall x \forall p_1 \cdots \forall p_n \exists y \forall z (z \in y \leftrightarrow (z \in x \wedge \phi(z, p_1, \ldots, p_n)))$$

One can think of the sets $p_1, \ldots, p_n$ as parameters of ϕ, which are usually some fixed sets. Informally, for each set x and every first-order formula $\phi(z)$, there is a set whose elements are exactly those z in x such that $\phi(z)$ holds:

$$\{z \in x \mid \phi(z)\}.$$

Remark. Separation can only construct subsets and does not allow the construction of entities of the more general form

$$\{z \mid \phi(z)\}.$$

This restriction is necessary to avoid Russell's paradox.

Definition 2.27. Define the **intersection** of two sets x_0 and x_1 as

$$x_0 \cap x_1 := \{z \in x_1 \mid z \in x_0\}.$$

Let $\phi(z, x_0)$ be the formula $z \in x_0$ (where x_0 is a parameter), denoted $\phi(z, x_0) := z \in x_0$. By Separation, there exists a set $y = \{z \in x_1 \mid \phi(z, x_0)\}$, i.e.,

$$z \in y \leftrightarrow (z \in x_1 \wedge z \in x_0).$$

In other words, for any sets x_0 and x_1, the collection of all sets which belong to both x_0 and x_1 is a set.

Definition 2.28. For a non-empty set x, the (unary) intersection of x is

$$\bigcap x := \left\{z \in \bigcup x \mid (\forall y \in x)\, z \in y\right\}.$$

This is the intersection of all sets which belong to x. To see that $\bigcap x$ is a set, let $\phi(z, x) := \forall y \in x(z \in y)$ and apply Separation to $\bigcup x$. Notice also that $x \cap y = \bigcap\{x, y\}$.

If $\phi(z, y) := z \notin y$, where y is a parameter, then we make the following definition:

Definition 2.29. The **relative complement** of y in x is

$$x \setminus y := \{z \in x \mid z \notin y\}.$$

Remark. We cannot form (as a set) the "absolute complement" of B, i.e., $\{x \mid x \notin B\}$. This class fails to be a set, for its union with B would be the class of all sets. In any event, the absolute complement is unlikely to be an interesting object of study.

For example, suppose $B \subseteq \mathbb{R}$. Then the relative complement $\mathbb{R} \setminus B$ consists of these real numbers not in B. On the other hand, the absolute complement of B would be a huge class containing all manner of irrelevant things; it would contain any *set* that was not a real number.

The next result states that there does not exist a "set of all sets".

Theorem 2.30. *There is no set to which every set belongs.*

Proof. Let A be a set. We will construct a set not belonging to A. Let $B := \{x \in A \mid x \notin x\}$.

Claim: $B \notin A$.

By the construction of B, $B \in B \iff B \in A$ and $B \notin B$. If $B \in A$, then this reduces to $B \in B \iff B \notin B$, which is impossible. Hence $B \notin A$. □

2.2.6 Axiom of Power Set

Axiom 2.31 (Power set).

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$$

For each set x, there is a set $\mathcal{P}(x)$, called the **power set** of x, which consists of all subsets of x:

$$\mathcal{P}(x) := \left\{z \in y \mid z \subseteq x\right\}.$$

Lemma 2.32. *For all sets A and B, each ordered pair (a, b), where $a \in A$, $b \in B$, is an element of $\mathcal{P}(\mathcal{P}(A \cup B))$.*

Proof. Since a and b are elements of $A \cup B$, $\{a\}$ and $\{a, b\}$ are elements of $\mathcal{P}(A \cup B)$. Hence $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. □

Definition 2.33. The **Cartesian product** of A and B is

$$A \times B := \{p \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid (\exists a \in A)(\exists b \in B)\, p = (a,b)\}.$$

2.2.7 Axiom of Infinity

Axiom 2.34 (Infinity)**.**

$$\exists X(\emptyset \in X \wedge \forall x(x \in X \rightarrow x \cup \{x\} \in X))$$

The set of natural numbers $\mathbb{N}$ is defined to be the intersection of all sets X as described above. Formally, we can define $\mathbb{N}$ by applying separation and infinity as follows. Fix $x \in X$. (The set X is guaranteed to be non-empty by infinity.) Then apply separation to the set X to obtain

$$\big\{x \in X : \forall Y((\emptyset \in Y \wedge \forall y \in Y(y \cup \{y\} \in Y)) \rightarrow x \in Y)\big\}\,.$$

We can now state the principle of induction on $\mathbb{N}$ as follows:

Theorem 2.35. *If $\phi(n)$ is a formula such that*

(i) $\phi(\emptyset)$ holds;

(ii) for all $n \in \mathbb{N}$, $\phi(n) \Rightarrow \phi(n \cup \{n\})$,

then $\phi(n)$ holds for all $n \in \mathbb{N}$.

Remark. $\emptyset$ corresponds to 0, and $n \cup \{n\}$ corresponds to $n+1$.

Proof. Consider the set $\{n \in \mathbb{N} \mid \phi(n)\}$. By the assumptions of induction, we have

(i) $\emptyset \in \{n \in \mathbb{N} \mid \phi(n)\}$, and

(ii) for all $n \in \mathbb{N}$, $n \cup \{n\} \in \{n \in \mathbb{N} \mid \phi(n)\}$.

Thus the set $\{n \in \mathbb{N} \mid \phi(n)\}$ satisfies the conditions for X above. Since $\mathbb{N}$ is the intersection of all sets X, we have $\mathbb{N} \subseteq \{n \in \mathbb{N} \mid \phi(n)\}$, i.e., $\phi(n)$ holds for all $n \in \mathbb{N}$. □

Using Union and Pairing, and by defining the successor x^+ of x by stipulating $x^+ := x \cup \{x\}$, we can construct natural numbers:

$$\begin{aligned}
&0 := \emptyset\\
&1 := 0^+ = 0 \cup \{0\} = \{0\}\\
&2 := 1^+ = 1 \cup \{1\} = \{0,1\}\\
&3 := 2^+ = 2 \cup \{2\} = \{0,1,2\}\\
&\quad\vdots
\end{aligned}$$

Define ordering $<$ on $\mathbb{N}$ as follows: for any $m, n \in \mathbb{N}$,

$$m < n \iff m \in n.$$

For instance, $\emptyset \in \{\emptyset, \{\emptyset\}\}$ means $0 < 2$.

To define $+$ and $\cdot$, we can use recursion. Laws of arithmetic (addition, multiplication, associativity, distributive law, etc) can be proven using the ZFC axioms.

2.2.8 Axiom Schema of Replacement

Axiom 2.36 (Replacement)**.** *For every first-order formula $\phi(x, y, p)$,*

$$\forall A \forall p (\forall x \in A\, \exists! y\, \phi(x, y, p) \to \exists B\, \forall x \in A\, \exists y \in B\, \phi(x, y, p))$$

For each formula $\phi(x, y)$ and each set A, if for every $x \in A$, there is a unique y such that $\phi(x, y)$ holds, then there is a set whose elements are exactly those y for which there is some $x \in A$ with $\phi(x, y)$, i.e.,

$$\{y \mid (\exists x \in A)\phi(x, y)\} \quad \text{exists.}$$

This justifies the alternate set builder notation $\{f(x) \mid x \in A\}$.

2.2.9 Axiom of Foundation

Axiom 2.37 (Foundation)**.**

$$\forall x (x \neq \emptyset \to \exists y \in x\, (y \cap x = \emptyset))$$

Informally, this means that an element cannot be an element of itself.

— Exercises —

Exercise 2.2.1 ([End77])**.** Give an example of sets A and B for which $\bigcup A = \bigcup B$ but $A \neq B$.

Exercise 2.2.2 ([End77])**.** Show that if $A \subseteq B$, then $\bigcup A \subseteq \bigcup B$.

Solution. Let $x \in \bigcup A$. Then there exists $y \in A$ such that $x \in y$.
Since $A \subseteq B$, we have $y \in B$. This implies $x \in y$ where $y \in B$, so $x \in \bigcup B$. □

Exercise 2.2.3 ([End77])**.**

(i) Show that for any set A, $\bigcup \mathcal{P}(A) = A$.

(ii) Show that $A \subseteq \mathcal{P}(\bigcup A)$. Under what conditions does equality hold?

Solution. Let $S \in A$. If $x \in S$, by definition of $\bigcup A$, we have $x \in \bigcup A$. Thus $S \subseteq \bigcup A$. By definition of power set, this means $S \in \mathcal{P}(\bigcup A)$.
Since this holds for every $S \in A$, we obtain $A \subseteq \mathcal{P}(\bigcup A)$.
Claim: $\mathcal{P}(\bigcup A) = A$ if and only if $A = \mathcal{P}(B)$ for some set B.
$\boxed{\Rightarrow}$ Trivial.
$\boxed{\Leftarrow}$ Suppose $A = \mathcal{P}(B)$ for some set B. Then every $X_i \in A$ satisfies $X_i \subseteq B$.
Consider $\bigcup A = \bigcup_{X_i \in A} X_i$. Since $B \in \mathcal{P}(B) = A$, we have $B \in A$, and moreover $X_i \subseteq B$ for all $X_i \in A$. Thus $\bigcup A = B$.
Hence $\mathcal{P}(\bigcup A) = \mathcal{P}(B) = A$. □

Exercise 2.2.4 ([End77])**.**

(i) Show that for any sets A and B, $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

(ii) Show that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. Under what conditions does equality hold?

Exercise 2.2.5. Show that there is no set to which every singleton (that is, every set of the form $\{x\}$) belongs.

[*Hint*: Show that from such a set, we could construct a set to which every set belonged.]

Exercise 2.2.6. Show that if $a \in B$, then $\mathcal{P}(a) \in \mathcal{P}(\mathcal{P}(\bigcup B))$.

3
Relations and Functions

3.1 Relations

3.1.1 Definition and Properties

Definition 3.1. We say $R \subseteq A \times B$ is a **relation** between A and B. If $(a, b) \in R$, we say $a \in A$ and $b \in B$ are **related**, and denote $a \, R \, b$.

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.

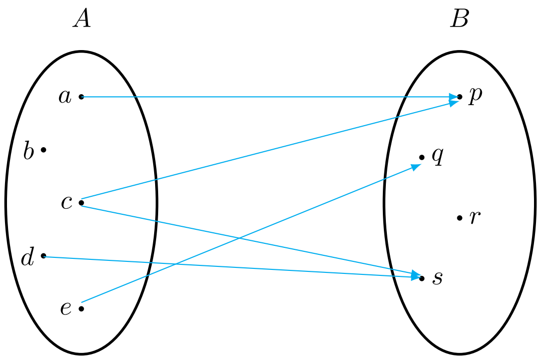


Figure 3.1: A relation $R \subseteq A \times B$ with $R = \{(a, p), (c, p), (c, s), (d, s), (e, q)\}$.

Example. In many cases we do not actually denote the relation by R, because there is some other conventional notation:

- The "less than or equal to" relation $\leq$ on $\mathbb{R}$ is $\big\{(x, y) \in \mathbb{R}^2 \mid x \leq y\big\}$. We write $x \leq y$ if (x, y) is in this set.
- The "divides" relation $\mid$ on $\mathbb{N}$ is $\big\{(m, n) \in \mathbb{N}^2 \mid m \text{ divides } n\big\}$. 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 $\big\{(A, B) \in \mathcal{P}(S)^2 \mid A \subseteq B\big\}$. We write $A \subseteq B$ if (A, B) is in this set.

Definition 3.2. A **binary relation** on A is a relation between A and itself.

Definition 3.3. Let R be a relation on a set A. We say that R is

(i) **reflexive** if $(\forall a \in A)\ a\ R\ a$;

(ii) **symmetric** if $(\forall a, b \in A)\ a\ R\ b \implies b\ R\ a$;

(iii) **anti-symmetric** if $(\forall a, b \in A)\ a\ R\ b$ and $b\ R\ a \implies a = b$;

(iv) **transitive** if $(\forall a, b, c \in A)\ a\ R\ b$ and $b\ R\ c \implies a\ R\ c$.

Example.

- The relation $\leq$ on $\mathbb{R}$ is reflexive, anti-symmetric, and transitive.
- The relation $<$ on $\mathbb{R}$ is not reflexive or symmetric, but it is anti-symmetric and transitive.
- The relation $\neq$ on $\mathbb{R}$ is not reflexive, anti-symmetric or transitive, but it is symmetric.
- The relation $=$ on $\mathbb{R}$ is reflexive, symmetric, and transitive.

Definition 3.4. Suppose $\leq$ is a relation on a non-empty set A. We say that $\leq$ is a **partial order** on A if $\leq$ is

(i) reflexive;

(ii) anti-symmetric;

(iii) transitive.

We also say that A is **partially ordered** by $\leq$. We may refer to the ordered pair $(A, \leq)$ as a **poset**.

Throughout all of these definitions, let $(A, \leq)$ be a partially ordered set.

Definition 3.5. Two elements $a, b \in A$ are called **comparable** if $a \leq b$ or $b \leq a$; otherwise they are called **incomparable**.

Definition 3.6. A subset $C \subseteq A$ is called a **chain** if every pair of elements of A are comparable.

Definition 3.7. A partial order $(A, \leq)$ is called a **total order** if every two elements of A are comparable; that is, for every $a, b \in A$, either $a \leq b$ or $b \leq a$.
We also say that A is **totally ordered** by $\leq$, and $(A, \leq)$ is **totally ordered**.

That is, a partial order is a total order exactly when the whole set is a chain.

3.1.2 Well Orders

Definition 3.8. We say that $\leq$ is a **well order** on A if every non-empty subset of A has a $\leq$-least element:

$$(\forall X \subseteq A)(X = \emptyset \vee (\exists x \in X)(\forall y \in X)\, x \leq y).$$

We also say that A is **well-ordered** by $\leq$, and that the poset $(A, \leq)$ is **well-ordered**.

We will often just say “least” rather than “$\leq$-least”, when the order relation is clear from context. Also, given a subset X of a well-order A, we will denote its least element by $\min(X)$.

To show that $<$ is a well-order, we need to show

1. transitive: if $x < y$ and $y < z$ then $x < z$
2. trichotomy: for every $x, y \in A$, exactly one of $x < y$, $x = y$, $y < x$ holds
3. every non-empty subset of A has a $<$-least element:

$$(\forall X \subseteq A)(X = \emptyset \vee (\exists x \in X)(\forall y \in X)(y \not< x)).$$

Axiom 3.9 (Well-ordering principle)**.** *Every non-empty set has a well-ordering.*

The next result tells us that we can do induction on any well-ordered set.

Theorem 3.10. *Suppose $<$ is a well order on A. Suppose $\phi(x)$ is a formula such that for every $y \in A$, if $\phi(x)$ holds for all $x < y$, then $\phi(y)$ holds. Then $\phi(x)$ holds for all $x \in A$.*

Proof. Suppose, for a contradiction, that $\neg\phi(x)$ holds for some $x \in A$. Consider the set

$$X = \left\{x \in A \mid \neg\phi(x)\right\} \subseteq A.$$

Then X is non-empty. By well-ordering, it has a $<$-least element $y \in A$. Then $\phi(x)$ holds for all $x < y$ but $\phi(y)$ fails, contrary to assumption. □

Consider the special case of the standard ordering $<$ on $\mathbb{N}$. Once we have proved that it is a well-order, we obtain the strong induction on $\mathbb{N}$:

> Suppose for every $n \in \mathbb{N}$, whenever $P(m)$ holds for all $m < n$, then $P(n)$ holds. Then $P(n)$ holds for all $n \in \mathbb{N}$.

It looks like there is no base case, but it is in fact the inductive step for $n = 0$, since “whenever $P(m)$ holds for all $m < n$, then $P(n)$ holds” is vacuously true when $n = 0$.

Also, induction holds even more generally:

Definition 3.11. We say that a relation R on A is **well-founded** if every non-empty subset of A has a minimal element with respect to R:

$$(\forall X \subseteq A)(X = \emptyset \vee (\exists x \in X)(\forall y \in X)\ (y, x) \notin R).$$

Remark. If we assume Choice, then the above is equivalent to saying that there is no infinite descending chain.

Theorem 3.12 (Generalised induction)**.** *Suppose R is a well-founded relation on A is well-founded, and $\phi(x)$ is a formula such that for every $y \in A$, if $\phi(x)$ holds for all x such that $(x, y) \in R$, then $\phi(y)$ holds. Then $\phi(x)$ holds for all $x \in A$.*

The proof is similar to that of the preceding theorem.

Proof. Suppose, for a contradiction, that $\neg\phi(x)$ holds for some $x \in A$. Consider the set

$$X = \left\{x \in A \mid \neg\phi(x)\right\}.$$

Then X is non-empty. By definition of well-foundedness, there exists $x_0 \in X$ such that for all $y \in X$, $(y, x_0) \notin R$. Then $\phi(x)$ holds for all x such that $(x, x_0) \in R$ and $\phi(x_0)$ fails, contradicting the assumption. □

3.2 Functions

3.2.1 Definitions

Formally, a function is defined as follows:

Definition 3.13. Let X and Y be non-empty sets. A **function** f from X to Y is an ordered triple (X, Y, Γ) such that $\Gamma \subseteq X \times Y$ consists of ordered pairs (x, y) such that for each $x \in X$, there exists a unique $y \in Y$ with $(x, y) \in \Gamma$:

$$(\forall x \in X)(\exists! y \in Y) \quad (x, y) \in \Gamma.$$

In this case we denote $f(x) = y$.

However, in practice, we shall use the following intuitive definition instead:

Definition 3.14. Let X and Y be non-empty sets. A **function** $f \colon X \to Y$ is an assignment of every element $x \in X$ to a unique element $y \in Y$, denoted by $f(x)$.

We call X and Y the **domain** and **codomain** of f respectively.

If $x \in X$ and $y \in Y$ are such that $f(x) = y$, we call y the **image** of x under f, and x a **preimage** of y under f. We also say that f **maps** x to y. The action of $f \colon X \to Y$ on an element $x \in X$ is sometimes indicated by a "decorated" arrow, as in

$$x \mapsto f(x).$$

Remark. Definition 3.14 requires that a function f maps every element of domain to a *unique* element of codomain; we say that f is **well-defined**:

- $f(x)$ exists for every $x \in X$, and
- $x = x'$ implies $f(x) = f(x')$.

We say that f is **not well-defined** if f maps some element of domain to zero elements or more than one element of codomain.

To announce that f is a function from a set X to a set Y, one writes $f \colon X \to Y$ or draws the following picture ("diagram"):

$$X \xrightarrow{f} Y$$

The collection of all functions from X to Y is denoted $\mathrm{Maps}(X, Y)$, or Y^X.

Remark. The notation Y^X is derived from the fact that if X and Y are finite sets, then Y^X has $|Y|^{|X|}$ members. (To see this, note that for each of the $|X|$ elements of X, we can choose among $|Y|$ points in Y into which it could be mapped. The number of ways of making all $|X|$ such choices is $\underbrace{|Y| \cdots |Y|}_{|X| \text{ times}}$.)

Example.

- $\{0, 1\}^{\mathbb{N}}$ is the set of all possible functions $f \colon \mathbb{N} \to \{0, 1\}$. Such an f can be thought of as an infinite sequence $f(0), f(1), f(2), \ldots$ of 0's and 1's.
- For a non-empty set A, we have $\emptyset^A = \emptyset$. This is because no function could have a non-empty domain and an empty range.

  On the other hand, $A^\emptyset = \{\emptyset\}$ for any set A, because $\emptyset \colon \emptyset \to A$, but $\emptyset$ is the only function with empty domain.

As a special case, we have $\emptyset^\emptyset = \{\emptyset\}$.

Definition 3.15. Two functions $f\colon X \to Y$ and $g\colon X \to Y$ are **equal**, denoted by $f = g$, if $f(x) = g(x)$ for every $x \in X$.

Definition 3.16. Given a set X, the **identity map** $\mathrm{id}_X\colon X \to X$ is defined by

$$\mathrm{id}_X(x) = x \qquad (x \in X).$$

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

Definition 3.17. Given sets $X \subseteq Y$, the **inclusion function** $\iota\colon X \to Y$ is defined by

$$\iota(x) = x \qquad (x \in X).$$

An inclusion function is often denoted by $\iota\colon X \hookrightarrow Y$. (This notation is also used for embeddings.)

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

Definition 3.18. Let $f\colon X \to Y$. The **restriction** of f to $A \subseteq X$ is the map $f|_A\colon A \to Y$ defined by

$$f|_A(x) = f(x) \quad (a \in A).$$

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

Definition 3.19. Let $f\colon X \to Y$.

- We say that f is **injective** (or **one-to-one**) if no two distinct elements in X are mapped to the same element in Y:

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

  An injective function is termed an **injection**.

- We say that f is **surjective** (or **onto**) if every element of Y is mapped to at least one element of X:

  $$(\forall y \in Y)(\exists x \in X) \quad f(x) = y.$$

  An surjective function is termed an **surjection**.

- We say that f is **bijective** if it is both injective and surjective; a bijective function is termed a **bijection** (or **one-to-one correspondance**).

  We say that X and Y are **isomorphic** sets, and denote $X \cong Y$.

Injections are often drawn $\hookrightarrow$; surjections are often drawn $\twoheadrightarrow$.

Example.

- Define $f\colon \mathbb{N} \to \mathbb{N}$ by $f(n) = n + 1$. Then f is injective but not surjective, since nothing in $\mathbb{N}$ (codomain) is mapped to $0 \in \mathbb{N}$ (domain).

- Define $g\colon \mathbb{R} \to \mathbb{R}$ by $g(x) = x + 1$. Then g is surjective.
- A function $f\colon \emptyset \to B$ can be surjective, when $B = \emptyset$ (such that $(\forall b \in \emptyset) \dots$ is vacuously true).

  The function $f\colon \emptyset \to B$ is vacuously injective.
- A function $f\colon A \to \emptyset$ can be surjective, when $A = \emptyset$; if $A \neq \emptyset$, then $a \in A$ is mapped to nothing, so f is not a function.

  The function $f\colon A \to \emptyset$ is injective if $A = \emptyset$ (otherwise f is not a function).

Example. Negate surjectivity:

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

That is, there exists $y \in Y$ not in the image of X, i.e., $f(x) \neq y$ for all $x \in X$.

3.2.2 Pre-images and Images

Definition 3.20. Let $f\colon X \to Y$.

- The **range** of f is

$$\begin{aligned}
\operatorname{range}(f) &:= \left\{y \in Y \mid (\exists x \in X)\, y = f(x)\right\} \\
&= \left\{f(x) \mid x \in X\right\}.
\end{aligned}$$

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

$$\begin{aligned}
f[A] &:= \left\{y \in Y \mid (\exists x \in A)\, y = f(x)\right\} \\
&= \left\{f(x) \mid x \in A\right\}.
\end{aligned}$$

- The **pre-image** of $B \subseteq Y$ under f is

$$f^{-1}[B] := \left\{x \in X \mid f(x) \in B\right\}.$$

That is, the image of a set consists of the images of its elements; the pre-image of a set consists of pre-images of its elements.

From the definition, a useful identity is

$$x \in f^{-1}[B] \iff f(x) \in B.$$

Remark.

- Notice that $f^{-1}[B]$ is defined even if f^{-1} is not a function.
- If f^{-1} is a function, then the pre-image of B under f agrees with the image of B under f^{-1} , so there is no ambiguity in the notation $f^{-1}[B]$.
- If B is a singleton $\{y\}$, one often abuses notation by writing $f^{-1}(y)$ instead of $f^{-1}[\{y\}]$. The set $f^{-1}(y)$ is called the **fiber** of y.

Notation. Unless mentioned otherwise, we will always assume $A \subseteq X$ and $B \subseteq Y$.

Lemma 3.21. *Let $f\colon X \to Y$.*

(i) $f[f^{-1}[B]] \subseteq B$, where equality holds if and only if f is surjective.

(ii) $A \subseteq f^{-1}[f[A]]$, where equality holds if and only if f is injective.

Proof.

(i) Let $y \in f[f^{-1}[B]]$. Then $y = f(x)$ for some $x \in f^{-1}[B]$. But $x \in f^{-1}[B]$ is equivalent to $f(x) \in B$. Hence $y \in B$.

Equality does not hold in general. For example, consider $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. Take $B = \{-1\}$. Then $f^{-1}[B] = \emptyset$, so

$$f[f^{-1}[B]] = f[\emptyset] = \emptyset \neq C.$$

$\boxed{\Rightarrow}$ Suppose $f[f^{-1}[B]] = B$. Thus $f[f^{-1}[Y]] = Y$. Let $y \in Y$. Then $y \in f[f^{-1}[Y]]$, so $y = f(x)$ for some $x \in f^{-1}[Y] \Rightarrow f(x) \in Y$. This shows surjectivity.

$\boxed{\Leftarrow}$ Suppose f is surjective. Let $y \in B$. By surjectivity there exists $x \in X$ such that $y = f(x)$. Note that $f(x) \in B$, so $x \in f^{-1}[B]$. Thus $y \in f[f^{-1}[B]]$. This shows the reverse inclusion.

(ii) Let $x \in A$. Then $f(x) \in f[A]$ by definition. Hence $x \in f^{-1}[f[A]]$.

Equality does not hold in general. For example, consider $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$. Take $A = \{1\}$. Then

$$f^{-1}[f[A]] = f^{-1}[\{1\}] = \{-1, 1\} \neq \{1\} = A.$$

$\boxed{\Rightarrow}$ Suppose $A = f^{-1}[f[A]]$. Let $x_1, x_2 \in X$ be such that $f(x_1) = f(x_2)$.

$\boxed{\Leftarrow}$ Suppose f is injective. We only need to show the reverse inclusion $f^{-1}[f[A]] \subseteq A$.

Let $x \in f^{-1}[f[A]]$. Then $f(x) \in f[A]$, so $f(x) = f(x')$ for some $x' \in A$. By injectivity, $x = x'$, so $x \in A$.

□

The next result shows that pre-images preserve nice set properties.

Lemma 3.22 (Algebra of pre-images)**.**

(i) If $B_1 \subseteq B_2$, then $f^{-1}[B_1] \subseteq f^{-1}[B_2]$. *(preserve inclusions)*

(ii) $f^{-1}[\bigcup_{i\in I} B_i] = \bigcup_{i\in I} f^{-1}[B_i]$. *(preserve unions)*

(iii) $f^{-1}[\bigcap_{i\in I} B_i] = \bigcap_{i\in I} f^{-1}[B_i]$. *(preserve intersections)*

(iv) $f^{-1}[B_1 \setminus B_2] = f^{-1}[B_1] \setminus f^{-1}[B_2]$. *(preserve set differences)*

In particular, (iv) implies $f^{-1}[B^c] = [f^{-1}[B]]^c$.

Proof.

(i) Let $x \in f^{-1}[B_1]$. Then $f(x) \in B_1$, so $f(x) \in B_2$. Hence $x \in f^{-1}(B_2)$.

(ii)

$$\begin{aligned} x \in f^{-1}\left[\bigcup_{i\in I} B_i\right] &\iff f(x) \in \bigcup_{i\in I} B_i \\ &\iff (\exists i \in I)\, f(x) \in B_i \\ &\iff (\exists i \in I)\, x \in f^{-1}[B_i] \\ &\iff x \in \bigcup_{i\in I} f^{-1}[B_i] \end{aligned}$$

(iii)

$$\begin{aligned} x \in f^{-1}\left[\bigcap_{i\in I} B_i\right] &\iff f(x) \in \bigcap_{i\in I} B_i \\ &\iff (\forall i \in I)\, f(x) \in B_i \\ &\iff (\forall i \in I)\, x \in f^{-1}[B_i] \\ &\iff x \in \bigcap_{i\in I} f^{-1}[B_i] \end{aligned}$$

(iv)

$$\begin{aligned} x \in f^{-1}(B_1 \setminus B_2) &\iff f(x) \in B_1 \setminus B_2 \\ &\iff f(x) \in B_1 \wedge f(x) \notin B_2 \\ &\iff x \in f^{-1}(B_1) \wedge x \notin f^{-1}(B_2) \\ &\iff x \in f^{-1}(B_1) \setminus f^{-1}(B_2) \end{aligned}$$

□

Unfortunately, images do not behave as nicely as pre-images.

Lemma 3.23 (Algebra of images)**.**

(i) If $A_1 \subseteq A_2$, then $f(A_1) \subseteq f(A_2)$. *(preserve inclusions)*

(ii) $f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$. *(preserve unions)*

(iii) $f(\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I} f(A_i)$, where equality holds if f is injective.

(iv) $f(A_1 \setminus A_2) \supseteq f(A_1) \setminus f(A_2)$, where equality holds if f is injective.

In particular, (iv) implies $f(A^c) \supseteq f[A]^c$ by taking $A_1 = \mathcal{U}$, $A_2 = A$.

Proof.

(i) Let $y \in f(A_1)$. Then $y = f(x)$ for some $x \in A_1$. Since $A_1 \subseteq A_2$, we have $x \in A_2$. By definition, $y \in f(A_2)$.

(ii)

$$\begin{aligned} y \in f(\bigcup_{i\in I} A_i) &\iff (\exists x \in \bigcup_{i\in I} A_i)\, y = f(x) \\ &\iff (\exists i \in I)\, x \in A_i \wedge y = f(x) \\ &\iff (\exists i \in I)\, y \in f(A_i) \\ &\iff y \in \bigcup_{i\in I} f(A_i). \end{aligned}$$

(iii) Let $y \in f(\bigcap_{i\in I} A_i)$. Then $y = f(x)$ for some $x \in \bigcap_{i\in I} A_i$. This means $x \in A_i$ for all $i \in I$, so $y = f(x) \in f(A_i)$ for all $i \in I$. Hence $y \in \bigcap_{i\in I} f(A_i)$.

Equality does not hold in general. Counterexample: Let $X = \{1, 2\}$, $Y = \{a\}$, and define $f\colon X \to Y$ by $f(1) = f(2) = a$. Let $A_1 = \{1\}$, $A_2 = \{2\}$. Thus

$$f(A_1 \cap A_2) = \emptyset \subset \{a\} = f(A_1) \cap f(A_2)$$

but the inclusion is strict.

We now prove

$$f(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f(A_i) \iff f \text{ is injective.}$$

$\boxed{\Rightarrow}$ We prove the contrapositive. Suppose f is not injective. Then there exist $x_1, x_2 \in \bigcap_{i\in I} A_i$ with $x_1 \neq x_2$ but $f(x_1) = f(x_2)$. Consider $y = f(x_1) = f(x_2)$. Then $y \in f(\bigcap_{i\in I} A_i)$.

$\boxed{\Leftarrow}$ We only need to show the reverse inclusion $\bigcap_{i\in I} f(A_i) \subseteq f(\bigcap_{i\in I} A_i)$.

Let $y \in \bigcap_{i\in I} f(A_i)$. Then for each $i \in I$, $y \in f(A_i)$, so $y = f(x_i)$ for some $x_i \in A_i$. Since f is injective on $\bigcap_{i\in I} A_i$, all the x_i must be equal; let $x = x_i$. Then $x \in \bigcap_{i\in I} A_i$ and $f(x) = y$, so $y \in f(\bigcap_{i\in I} A_i)$.

(iv) Let $y \in f(A_1) \setminus f(A_2)$. Then $y = f(x)$ for some $x \in A_1$, and $y \notin f(A_2)$ (i.e., $f(x) \neq y$ for all $x \in A_2$).

Suppose, for a contradiction, that $x \in A_2$. Then $f(x) \in f(A_2)$, which contradicts $y \notin f(A_2)$. Thus $x \notin A_2$.

Therefore $x \in A_1 \setminus A_2$, and hence $y = f(x) \in f(A_1 \setminus A_2)$.

Equality does not hold in general. Counterexample: Use the above counterexample for (iii).

□

3.2.3 Composition

Definition 3.24. Let $f\colon X \to Y$, $g\colon Y \to Z$. Define the **composition** $g \circ f\colon X \to Z$ as

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

That is, we use f to go from X to Y, then apply g to reach Z. Graphically we may draw the following picture:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "g\circ f"] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

Such graphical representations of collections of (for example) sets connected by functions are called **diagrams**. We say that the diagram **commutes** if we start from X and travel to Z in either of the two possible ways prescribed by the diagram, the result of applying the functions one encounters is the same.

Example. Let X be a non-empty set. Fix $x_0 \in X$. Define $f, g\colon \mathcal{P}(X) \to \mathcal{P}(X)$ by

$$f(A) = A \setminus \{x_0\}$$
$$g(A) = A \cup \{x_0\}$$

Note that x_0 may or may not belong to A.
Then $g \circ f = g$ (in either case, x_0 is added to A) and $f \circ g = f$ (in either case, x_0 is removed from A).

The composition of functions is not commutative. However, composition is associative:

Lemma 3.25 (Associativity). *Let $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to W$. Then*

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

Proof. Let $x \in X$. By definition of composition,

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

□

The next result states that composition preserves injectivity and surjectivity.

Lemma 3.26. *Let $f\colon X \to Y$, $g\colon Y \to Z$.*

(i) If f and g are injective, then $g \circ f$ is injective.

(ii) If f and g are surjective, then $g \circ f$ is surjective.

Proof.

(i) Suppose $f\colon X \to Y$ and $g\colon Y \to Z$ are injective.

Suppose $(g \circ f)(x) = (g \circ f)(x')$. Then $g(f(x)) = g(f(x'))$. Since g is injective, we have $f(x) = f(x')$; since f is injective, we have $x = x'$.

(ii) Suppose $f\colon X \to Y$ and $g\colon Y \to Z$ are surjective.

Let $z \in Z$. Since g is surjective, there exists $y \in Y$ such that $g(y) = z$. Since f is surjective, there exists $x \in X$ such that $f(x) = y$.

This means that there exists $x \in X$ such that $g(f(x)) = g(y) = z$, as desired.

□

We now provide a partial converse to the previous result.

Lemma 3.27. *Let $f\colon X \to Y$, $g\colon Y \to Z$.*

(i) If $g \circ f$ is injective, then f is injective, but g need not be injective.

(ii) If $g \circ f$ is surjective, then g is surjective, but f need not be surjective.

Proof.

(i) Suppose $f(x) = f(x')$. Then $g(f(x)) = g(f(x')) \implies (g \circ f)(x) = (g \circ f)(x')$. By injectivity of $g \circ f$, this implies $x_1 = x_2$. Hence f is injective.

Let $X = \{1\}$, $Y = \{x, y\}$, $Z = \{z\}$. Define $f\colon X \to Y$ by $f(1) = x$ and $g\colon Y \to Z$ by $g(x) = g(y) = z$. Then f is (trivially) injective, g is not injective, $g \circ f$ is (vacuously) injective.

(ii) Let $z \in Z$. Since $g \circ f$ is surjective, there exists $x \in X$ such that $g(f(x)) = z$. Let $y = f(x) \in Y$. Then $g(y) = z$. Hence g is surjective.

Let $X = \{1\}$, $B = \{x, y\}$, $C = \{z\}$. Define $f\colon X \to Y$ by $f(1) = x$, $g\colon Y \to Z$ by $g(x) = g(y) = z$. Then f is not surjective, g is surjective, $g \circ f$ is surjective.

□

The image and pre-image for composition of functions can be expressed in a very simple way.

Lemma 3.28. *Let $f\colon X \to Y$, $g\colon Y \to Z$. Let $A \subseteq X$, $C \subseteq Z$.*

(i) $(g \circ f)^{-1}[C] = f^{-1}[g^{-1}[C]]$.

(ii) $(g \circ f)[A] = g[f[A]]$.

Proof.

(i) We have

$$\begin{aligned} x \in (g \circ f)^{-1}[C] &\iff (g \circ f)(x) \in C \\ &\iff g(f(x)) \in C \\ &\iff f(x) \in g^{-1}[C] \\ &\iff x \in f^{-1}[g^{-1}[C]]. \end{aligned}$$

(ii) $\boxed{\subseteq}$ Let $z \in g[f[A]]$. Then $z = g(y)$ for some $y \in f[A]$, so $y = f(x)$ for some $x \in A$.

Hence $z = g(f(x)) = (g \circ f)(x)$, so $z \in (g \circ f)[A]$.

$\boxed{\supseteq}$ Let $z \in (g \circ f)[A]$. Then $z = (g \circ f)(x) = g(f(x))$ for some $x \in A$.

Let $y = f(x)$. Then $z = g(y)$ for some $y \in f[A]$. Hence $z \in g[f[A]]$.

□

3.2.4 Monomorphisms and Epimorphisms

Definition 3.29. Let $f\colon X \to Y$.

- We say that f is a **monomorphism** if it is left-cancellative: for all sets Z and all functions $g_1, g_2\colon Z \to X$,
$$f \circ g_1 = f \circ g_2 \implies g_1 = g_2.$$
- We say that f is an **epimorphism** if it is right-cancellative: for all sets Z and all functions $g_1, g_2\colon Z \to X$,
$$g_1 \circ f = g_2 \circ f \implies g_1 = g_2.$$

Proposition 3.30. *A function is injective if and only if it is a monomorphism.*

Proof.
$\boxed{\Rightarrow}$ Suppose f is injective, and suppose $f \circ g_1 = f \circ g_2$. Let $z \in Z$, then

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

Since f is injective, it follows that $g_1(z) = g_2(z)$. Since $z \in Z$ is arbitrary, we conclude $g_1 = g_2$.
$\boxed{\Leftarrow}$ Suppose that for all sets Z and functions $g_1, g_2 \colon Z \to X$,

$$f \circ g_1 = f \circ g_2 \implies g_1 = g_2.$$

Let $x, y \in X$, and consider the one-element set $Z = \{1\}$. Define

$$g_1(1) = x, \quad g_2(1) = y$$

for both $g_1, g_2 \colon Z \to X$. Then

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

which shows that f is injective. □

Proposition 3.31. *A function is surjective if and only if it is an epimorphism.*

Proof.
$\boxed{\Rightarrow}$ Suppose f is surjective, and suppose $g_1 \circ f = g_2 \circ f$ for some functions $g_1, g_2 \colon Y \to Z$.
Let $y \in Y$. Surjectivity of f implies there exists $x \in X$ such that $f(x) = y$. Then

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

Since $y \in Y$ was arbitrary, we conclude that $g_1 = g_2$.
$\boxed{\Leftarrow}$ We prove the contrapositive. Suppose f is not surjective. Then there exists $y_0 \in Y$ not in the image of f, i.e., $f(x) \neq y_0$ for all $x \in X$.
We shall construct a set Z and functions $g_1, g_2 \colon Y \to Z$ such that g_1 and g_2 disagree at y_0 and agree at all other points in Y:

(i) $g_1(y_0) \neq g_2(y_0)$, and

(ii) $g_1(y) = g_2(y)$ for all $y \neq y_0$.

Let $Z = Y \cup \{1, 2\}$ with $1, 2 \notin Y$, and define

$$g_1(y) = \begin{cases} 1 & \text{if } y = y_0 \\ y & \text{if } y \neq y_0 \end{cases} \qquad g_2(y) = \begin{cases} 2 & \text{if } y = y_0 \\ y & \text{if } y \neq y_0 \end{cases}$$

Then for all $x \in X$, since $f(x) \neq y_0$, we have $g_1(f(x)) = g_2(f(x))$, i.e., $g_1 \circ f = g_2 \circ f$, but clearly $g_1 \neq g_2$. □

3.2.5 Invertibility

In this subsection, we answer the question of when it is possible to “reverse” or “undo” the action of a function. As it turns out, the answer is connected to the property of being a bijection.

Definition 3.32. Let $f\colon X \to Y$.

(i) We say that f is **left-invertible** if there exists $g\colon Y \to X$ such that $g \circ f = \mathrm{id}_X$; we call g a **left inverse** of f.

(ii) We say that f is **right-invertible** if there exists $h\colon Y \to X$ such that $f \circ h = \mathrm{id}_Y$; we call h a **right inverse** of f.

(iii) We say that f is **invertible** if there exists $k\colon Y \to X$ which is a left and right inverse of f; we call k an **inverse** of f.

Remark. Notice that if g is a left inverse of f, then f is a right inverse of g (and vice versa). A function can have more than one left inverse, or more than one right inverse.

One easily checks that any invertible function $f\colon X \to Y$ has a unique inverse. Let g_1 and g_2 be two functions for which $g_i \circ f = \mathrm{id}_X$ and $f \circ g_i = \mathrm{id}_Y$ for $i = 1, 2$. Then

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

The inverse of f is denoted by f^{-1}.
The following result provides an important and useful criterion for invertibility.

Lemma 3.33 (Invertibility criterion)**.** *Let $f\colon X \to Y$. Then*

(i) f is left-invertible if and only if f is injective;

(ii) f is right-invertible if and only if f is surjective;

(iii) f is invertible if and only if f is bijective.

Proof.

(i) $\boxed{\Rightarrow}$ Suppose f is left-invertible. Then there exists $g\colon Y \to X$ such that $g \circ f = \mathrm{id}_X$. Suppose $f(x) = f(x')$. Applying g to both sides gives

$$x = g(f(x)) = g(f(x')) = x'.$$

$\boxed{\Leftarrow}$ Suppose f is injective.

Caution: Simply writing "Define $g(f(x)) = x$" is inadequate for the following reasons:

- If $y = f(x)$ for some x, we need to explain why there is only one such x (otherwise $g(f(x))$ would have multiple values).
- If $y \neq f(x)$ for all x, we need to define g for such y as well.

Choose any $x_0 \in X$. Define $g\colon Y \to X$ as follows:

- If y is in the image of f, then $y = f(x)$ for a *unique* $x \in X$. (Uniqueness is due to injectivity of f: if $y = f(x)$ and $y = f(x')$, then $x = x'$.) Define $g(y) = x$.
- If y is not in the image of f, define $g(y) = x_0$.

You should verify that $g \circ f = \mathrm{id}_X$.

(ii) $\boxed{\Rightarrow}$ Suppose f is right-invertible. Then there exists $g\colon Y \to X$ such that $f \circ g = \mathrm{id}_Y$.

Let $y \in Y$. Then $f(g(y)) = \mathrm{id}_Y(y) = y$, which means $g(y) \in X$ is mapped by f to y. Hence f is surjective.

$\boxed{\Leftarrow}$ Suppose f is surjective. Let $y \in Y$. By surjectivity there exists $x \in X$ such that $f(x) = y$.

Note that there may be multiple $x \in X$ such that $f(x) = y$; choose one such x and define $g \colon Y \to X$ by $g(y) = x$ (this requires Choice, since we need to choose *one* preimage for *every* $y \in Y$).

(iii) $\boxed{\Rightarrow}$ Suppose f is invertible. Then f is left-invertible and right-invertible.

By (i) and (ii), f is injective and surjective, so f is bijective.

$\boxed{\Leftarrow}$ Suppose f is bijective. Then f is injective and surjective. By (i) and (ii), f has a left inverse $g \colon Y \to X$ and a right inverse $h \colon Y \to X$.

But "invertible" requires a single function to be *both* a left and right inverse, so we need to show that $g = h$:

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_X \circ h = h.$$

Hence $g = h$ is an inverse of f.

□

Remark. In fact, $\boxed{\Leftarrow}$ of (ii) is equivalent to the Axiom of Choice.

Corollary 3.34. *Let X be a non-empty set. If there is an injection from X to Y, then there exists a surjection from Y to X.*

Proof. Let X be a non-empty set, and $f \colon X \to Y$ is an injection.
Then there exists $g \colon Y \to X$ such that $g \circ f = \mathrm{id}_X$, i.e., g is a left inverse of f.
Then f is a right inverse of g, so g is surjective. □

The next result summarises properties of inverse functions.

Lemma 3.35. *If $f \colon X \to Y$, $g \colon Y \to Z$ are invertible, then*

(i) f^{-1} is invertible, and $(f^{-1})^{-1} = f$.

(ii) $g \circ f$ is invertible, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof.

(i) This follows immediately from definition: since f^{-1} is the inverse of f,

$$\begin{aligned} f^{-1} \circ f = \mathrm{id}_X &\implies f \text{ is a right inverse of } f^{-1} \\ f \circ f^{-1} = \mathrm{id}_Y &\implies f \text{ is a left inverse of } f^{-1} \end{aligned}$$

Hence f is the inverse of f^{-1}, and $(f^{-1})^{-1} = f$.

(ii) Using associativity of function composition, it is easy to show

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

□

As a result, we can describe a rather non-trivial example of a function.

Example. Let X and Y be sets. Let F be the set of all invertible functions from X to Y:

$$F = \{f \in \mathrm{Maps}(X,Y) \mid f \text{ is invertible}\}.$$

Then there is a function $T\colon F \to F$ which sends $f \mapsto f^{-1}$, and this function T is its own inverse, with $T \circ T = \mathrm{id}_F$.

Proposition 3.36. *Let $f\colon X \to Y$. Then there exists $A \subseteq X$ such that $f|_A$ is injective.*

Proof. Take $A = \emptyset$. □

The next result states that we can restrict the domain of a surjection to obtain a bijection.

Proposition 3.37. *Let $f\colon X \to Y$ is surjective. Then there exists $A \subseteq X$ such that $f|_A$ is bijective.*

Proof. The idea is as such: For each $y \in Y$, since f is surjective, there exists (possibly multiple) $x \in X$ such that $f(x) = y$; we want to choose *exactly one* $x \in X$ such that $f(x) = y$.
Since f is surjective, fix a right inverse $g\colon Y \to X$ such that $f \circ g = \mathrm{id}_Y$.
Claim: $A = \mathrm{range}(g)$.
Evidently $\mathrm{range}(g) \subseteq X$. We check that $f|_A$ is bijective:

Injectivity: Suppose $f(a) = f(a')$ where $a, a' \in A$.

By definition of A, there exist $y, y' \in Y$ such that $a = g(y)$ and $a' = g(y')$.

Then $f(g(y)) = f(g(y'))$. Since $f \circ g = \mathrm{id}_Y$, this implies $y = y'$.

Thus $a = g(y) = g(y') = a'$.

Surjectivity: Let $y \in Y$. Then $g(y) \in A$, by definition of A. Since $f \circ g = \mathrm{id}_Y$, we have $f(g(y)) = y$.

Hence $g(y)$ is the pre-image of y, as desired.

□

Alternative: If $f\colon X \to Y$ is surjective, then the set of fibers $\{f^{-1}(y) : y \in Y\}$ forms a partition of X. Now choose for each fiber $f^{-1}(y)$ one representative $x_y \in X$ with $f(x_y) = y$ and you are done.

3.2.6 Infinite Cartesian Products

Earlier we defined the Cartesian product of n sets in terms of ordered n-tuples. However, this definition becomes awkward for infinite families of sets.
Let I be any indexing set. Given a set X, an I-tuple of elements in X is a function

$$x\colon I \to X.$$

Writing $x_i = x(i)$ for its value at $i \in I$, the i-th coordinate of x, we can also denote the I-tuple x by its values $(x_i)_{i \in I}$.

Definition 3.38. Let $\{X_i\}_{i \in I}$ be an indexed family of sets, with union $X = \bigcup_{i \in I} X_i$. Its **Cartesian product** $\prod_{i \in I} X_i$ is the set of all I-tuples $(x_i)_{i \in I}$ of elements in X such that $x_i \in$

A_i for all $i \in I$. In other words, it is the set of functions

$$x\colon I \to \bigcup_{i\in I} X_i$$

such that $x(i) \in X_i$ for all $i \in I$.

Example. If all the sets X_i are all equal to some fixed set X, then $\prod_{i\in I} X = X^I$.

If any X_i is empty, then clearly the product $\prod_{i\in I} X_i$ is empty. Conversely, suppose that $X_i \neq \emptyset$ for every $i \in I$. Does it follow that $\prod_{i\in I} X_i \neq \emptyset$. To obtain a member of the product, we need to select some member from each X_i, and put $f(i)$ equal to that selected member. This requires the axiom of choice, and in fact this is one of the many equivalent ways of stating the axiom.

Axiom 3.39 (Axiom of Choice)**.** *The Cartesian product of any non-empty collection of non-empty sets is non-empty.*

— Exercises —

Exercise 3.2.1. Suppose $f\colon \mathbb{N} \to \mathbb{N}$. Prove that if $A \subseteq \mathbb{N}$ is bounded, then $f[A]$ is bounded.

Solution. Use the fact that bounded subsets of $\mathbb{N}$ are finite. □

Exercise 3.2.2 (MA1100T AY21/22)**.** Prove or disprove the following:

(i) There exists a set B such that for any set A, every map $f\colon A \to B$ is surjective.

(ii) There exists a set B such that for any set A, every map $f\colon A \to B$ is injective.

(iii) There exists a set B such that for any set A, there exists a surjective map $f\colon A \to B$.

(iv) There exists a set B such that for any set A, there exists an injective map $f\colon A \to B$.

Solution.

(i) True. Take $B = \emptyset$. If $f\colon A \to B$ is a function, then this forces $A = \emptyset$. Hence f is vacuously surjective.

(ii) True. Take $B = \emptyset$. If $f\colon A \to B$ is a function, then this forces $A = \emptyset$. Hence f is vacuously injective.

(iii) False. Let B be any set.

- If B is non-empty, take $A = \emptyset$. Then all elements in B will not be reached by f, so f is not surjective.
- If $B = \emptyset$, take $A \neq \emptyset$. Then there exist no function $f\colon A \to B$.

(iv) False. Let B be any set. Then $\mathcal{P}(B)$ does not inject into B, by Cantor's theorem.

□

★ **Exercise 3.2.3** (MA1100T AY25/26)**.** Let S be a set. A *closure operator* on S is a function $\mathrm{cl}\colon \mathcal{P}(S) \to \mathcal{P}(S)$ such that for all $A, B \subseteq S$,

- $A \subseteq \mathrm{cl}(A)$ (cl is extensive)
- $A \subseteq B \implies \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$ (cl is increasing)

- $\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A)$ (cl is idempotent)

Prove that a function $f\colon \mathcal{P}(S) \to \mathcal{P}(S)$ is a closure operator on S if and only if $A \subseteq f(B) \iff f(A) \subseteq f(B)$ for all $A, B \subseteq S$.

Solution. Let $A, B \subseteq S$.

$\boxed{\Rightarrow}$ Suppose that f is a closure operator.

Then $A \subseteq f(B) \implies f(A) \subseteq f(f(B))$ (since f is increasing) $\implies f(A) \subseteq f(B)$ (since f is idempotent). Conversely, $f(A) \subseteq f(B) \implies A \subseteq f(B)$ (since f is extensive).

$\boxed{\Leftarrow}$ Suppose f satisfies the biconditional above.

- Then $f(A) \subseteq f(A) \implies A \subseteq f(A)$, so f is extensive.
- Using extensivity, we obtain $A \subseteq B \implies A \subseteq f(B) \implies f(A) \subseteq f(B)$, so f is increasing.
- Finally, $f(A) \subseteq f(A) \implies f(f(A)) \subseteq f(A)$, where the reverse inclusion holds by extensivity, so f is idempotent.

□

★★ **Exercise 3.2.4** (MA1100T AY23/24)**.** Suppose J is a non-empty indexing set. Let $(A_j)_{j\in J}$ be a family of sets, and define their *disjoint union* as

$$\bigsqcup_{j\in J} A_j = \left\{(j,a) \mid j \in J,\ a \in A_j\right\}.$$

For each $j \in J$, define the function $i_j\colon A_j \to \bigsqcup_{j\in J} A_j$ by $a \mapsto (j,a)$. Define also the family of functions $(f_j\colon A_j \to X)_{j\in J}$. Prove that there exists a unique function $f\colon \bigsqcup_{j\in J} A_j \to X$ such that $f_j = f \circ i_j$ for each $j \in J$.

$$\begin{tikzcd}
A_j \arrow[r, "i_j"] \arrow[rd, "f_j"] & \bigsqcup_{j\in J} A_j \arrow[d, dashed, "\exists! f"] \\
 & X
\end{tikzcd}$$

Solution.

$\boxed{\text{Existence}}$ Define $f\colon \bigsqcup_{j\in J} A_j \to X$ by $f(j,a) = f_j(a)$.

We first show that f is well-defined.

- $f(j,a)$ always exists, because the family of functions has one f_j for every $j \in J$.
- Suppose $(j_1, a_1) = (j_2, a_2)$. Then $j_1 = j_2$, so $f_{j_1} = f_{j_2}$, and $a_1 = a_2$. Since all the f_j's are well-defined functions, and $a_1 = a_2$, we have

$$f(j_1, a_1) = f_{j_1}(a_1) = f_{j_1}(a_2) = f_{j_2}(a_2) = f(j_2, a_2).$$

For each $j \in J$, we have

$$(f \circ i_j)(a) = f(i_j(a)) = f(j,a) = f_j(a)$$

for all $a \in A_j$. Hence $f_j = f \circ i_j$.

$\boxed{\text{Uniqueness}}$ Suppose $g\colon \bigsqcup_{j\in J} A_j \to X$ is such that $f_j = g \circ i_j$ for each $j \in J$.

Note that i_j is surjective, since for each $(j,a) \in \bigsqcup_{j\in J} A_j$, we have $i_j(a) = (j,a)$.

Then for all $(j,a) \in \bigsqcup_{j\in J} A_j$,

$$g(j,a) = g(i_j(a)) = f_j(a) = f(i_j(a)) = f(j,a)$$

so $g = f$ as desired. $\square$

★★★ **Exercise 3.2.5** (MA1100T AY21/22)**.** Let $f\colon X \to Y$ be a function. Prove or disprove: f is injective if and only if for any set T, the "post-composition with f" map

$$\begin{aligned}\Phi_T\colon\ \mathrm{Maps}(T,X) &\to \mathrm{Maps}(T,Y)\\ \phi &\mapsto f\circ\phi\end{aligned}$$

is injective.

Solution. True.

$\boxed{\Rightarrow}$ Suppose f is injective.

Suppose $\Phi_T(\phi_1) = \Phi(\phi_2)$. Then $f\circ\phi_1 = f\circ\phi_2$, i.e., $f(\phi_1(t)) = f(\phi_2(t))$ for all $t\in T$.

Since f is injective, we have $\phi_1(t) = \phi_2(t)$ for all $t\in T$. Thus $\phi_1 = \phi_2$. Hence Φ_T is injective.

$\boxed{\Leftarrow}$ Suppose Φ_T is injective for any set T. In particular, pick a singleton $T = \{0\}$; then Φ_T is injective.

Suppose $f(x) = f(y)$. Choose functions $\phi_x, \phi_y \in \mathrm{Maps}(T,X)$ such that $\phi_x(0) = x$ and $\phi_y(0) = y$.

Then $f(x) = f(y)$ implies $f(\phi_x(t)) = f(\phi_y(t))$ for all $t \in T = \{0\}$, i.e., $f\circ\phi_x = f\circ\phi_y$.

But $\Phi_T(\phi_x) = f\circ\phi_x = f\circ\phi_y = \Phi_T(\phi_y)$. Since Φ_T is injective, we have $\phi_x = \phi_y$. Hence $x = \phi_x(0) = \phi_y(0) = y$. $\square$

★★★ **Exercise 3.2.6** (MA1100T AY21/22)**.** Let $f\colon X \to Y$ be a function. Prove or disprove: f is surjective if and only if for any set T, the "pre-composition with f" map

$$\begin{aligned}\Psi_T\colon\ \mathrm{Maps}(Y,T) &\to \mathrm{Maps}(X,T)\\ \psi &\mapsto \psi\circ f\end{aligned}$$

is surjective.

Solution. False. We shall show $\boxed{\Rightarrow}$ does not hold.

Consider $X = \{1,2\}$, $Y = \{3\}$. Take $T = X$; we will prove that Ψ_T is not surjective.

Define $f\colon X\to Y$ by $f(x) = 3$, which is surjective.

For any $\psi \in \mathrm{Maps}(Y,T)$, note that $\psi(f(1)) = \psi(3) = \psi(f(2))$ but $1 \neq 2$. Hence $\psi\circ f$ is not injective, and is therefore not the identity function id_X. This proves that $\mathrm{id}_X \notin \mathrm{range}(\Psi_T)$. Since $T = X$, $\mathrm{id}_X \in \mathrm{Maps}(X,T)$. Hence Ψ_T is not surjective. $\square$

★★ **Exercise 3.2.7.** Let A be the set of all complex polynomials in n variables. Given a subset $T \subseteq A$, define the *zeros* of T as the set

$$Z(T) := \left\{P \in \mathbb{C}^n \mid f(P) = 0 \text{ for all } f \in T\right\}.$$

We call $Y \subseteq \mathbb{C}^n$ an *algebraic* set if there exists $T\subseteq A$ such that $Y = Z(T)$.

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

Solution. Let X and Y be algebraic sets. Then there exists $S, T \subseteq A$ such that

$$\begin{aligned}X = Z(S) &= \left\{P\in\mathbb{C}^n \mid f(P) = 0 \text{ for all } f\in S\right\}\\ Y = Z(T) &= \left\{P\in\mathbb{C}^n \mid g(P) = 0 \text{ for all } g\in T\right\}\end{aligned}$$

We claim that

$$X\cup Y = Z(U), \qquad \text{where } U = \left\{fg \mid f\in S,\, g\in T\right\}.$$

$\boxed{\subseteq}$ Let $P \in X \cup Y$. Then either $P \in X$ or $P \in Y$.

Case 1: If $P \in X$, then $f(P) = 0$ for all $f \in S$. Hence for any $f \in S$, $g \in T$, we have $(fg)(P) = f(P)g(P) = 0$. Thus $P \in Z(U)$.

Case 2: If $P \in Y$, then $g(P) = 0$ for all $g \in T$, so again $(fg)(P) = 0$ for all $f \in S$, $g \in T$. Thus $P \in Z(U)$.

$\boxed{\supseteq}$ Let $P \in Z(U)$. Suppose, for a contradiction, that $P \notin X \cup Y$. Then $P \notin X$ and $P \notin Y$.

- Since $P \notin X = Z(S)$, there exists $f \in S$ with $f(P) \neq 0$.
- Since $P \notin Y = Z(T)$, there exists $g \in T$ with $g(P) \neq 0$.

Then $(fg)(P) = f(P)g(P) \neq 0$, contradicting $P \in Z(U)$. Hence $P \in X \cup Y$.

Remark. By contrast, intersections are even simpler: if $X = Z(S)$ and $Y = Z(T)$, then

$$X \cap Y = Z(S \cup T).$$

Thus arbitrary intersections of algebraic sets are also algebraic.

□

★★ **Exercise 3.2.8** (MA1100T AY24/25)**.** Let X, Y and Z be sets, and $f\colon X \to Z$ and $g\colon Y \to Z$ be functions. Define

$$E = \left\{(x, y) \in X \times Y : f(x) = g(y)\right\}.$$

(a) Prove that

$$f \circ \pi_1|_E = g \circ \pi_2|_E$$

where $\pi_1\colon X \times Y \to X$ and $\pi_2\colon X \times Y \to Y$ are the usual projections.

(b) Prove that for every set A and every pair of functions $h\colon A \to X$ and $j\colon A \to Y$ such that $f \circ h = g \circ j$, there exists $k\colon A \to E$ such that

$$h = \pi_1 \circ k \qquad \text{and} \qquad j = \pi_2 \circ k.$$

$$\begin{tikzcd}
E \arrow[drr, bend left, "\pi_1"] \arrow[ddr, bend right, "\pi_2"'] & & \\
& A \arrow[ul, dashed, "\exists k"'] \arrow[r, "h"] \arrow[d, "j"] & X \arrow[d, "f"] \\
& Y \arrow[r, "g"] & Z
\end{tikzcd}$$

Solution.

(a) Let $(x, y) \in E$. Then

$$f \circ \pi_1|_E(x, y) = f(x) = g(y) = g \circ \pi_2|_E(x, y).$$

(b) Define $k\colon A \to E$ by

$$k(a) = (h(a), j(a)).$$

We first show that k is well-defined. Note that for every $a \in A$, $k(a) = (h(a), j(a)) \in E$, since $f(h(a)) = g(j(a))$ because $f \circ h = g \circ j$.

Let $a, a' \in A$. Then $k(a) = (h(a), j(a))$ and $k(a') = (h(a'), j(a'))$. But $h(a) = h(a')$ and $j(a) = j(a')$, so $k(a) = k(a')$ as desired.

Then we check that $h = \pi_1 \circ k$ and $j = \pi_2 \circ k$. For every $a \in A$,

$$\pi_1 \circ k(a) = \pi_1(h(a), j(a)) = h(a),$$
$$\pi_2 \circ k(a) = \pi_2(h(a), j(a)) = j(a).$$

□

★ **Exercise 3.2.9** (MA1100T AY22/23)**.** Let A, B and C be sets, with B non-empty.

(i) Prove that for every function $f\colon A \times B \to C$, there is a **unique** function $g\colon A \to \mathrm{Maps}(B, C)$ such that $f(a, b) = g(a)(b)$.

($g(a)(b)$ denotes the output of the function $g(a)$ with input b.)

(ii) Prove that if f is injective, then so is g.

Solution.

(i) $\boxed{\text{Existence}}$ Define $g\colon A \to \mathrm{Maps}(B, C)$ which sends each $a \in A$ to the function $h_a\colon B \to C$:

$$h_a(b) = f(a, b).$$

For each $(a, b) \in A \times B$, we check that

$$g(a)(b) = h_a(b) = f(a, b)$$

as desired.

$\boxed{\text{Uniqueness}}$ Let $j\colon A \to \mathrm{Maps}(B, C)$ be such that $f(a, b) = j(a)(b)$. Then for every $(a, b) \in A \times B$,

$$g(a)(b) = f(a, b) = j(a)(b).$$

Since this holds for arbitrary $b \in B$, we have $g(a) = j(a)$. Since this holds for arbitrary $a \in A$, we have $g = j$, as desired.

(ii) Suppose f is injective. Then

$$g(a) = g(a') \implies g(a)(b) = g(a')(b) \implies f(a, b) = f(a', b).$$

By injectivity of f, we have $(a, b) = (a', b)$, so $a = a'$, as desired.

□

3.3 Number Theory

In this section, we study some properties of the integers.

3.3.1 Infinitude of Primes

Definition 3.40. Let $a, b \in \mathbb{Z}$. We say that a **divides** b, denoted $a \mid b$, if there exists $k \in \mathbb{Z}$ such that $b = ka$. Otherwise, we write $a \nmid b$.

Lemma 3.41. *For all $a, b, c, n, m \in \mathbb{Z}$,*

(i) If $a \mid b$ and $b \neq 0$, then $a \neq 0$.

(ii) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

(iii) If $a \mid b$, then $na \mid nb$.

(iv) If $a \mid b$ and $a \mid c$, then $a \mid nb + mc$.

The next result implies that there are infinitely many primes.

Proposition 3.42. *For every $n \in \mathbb{N}$, there is a prime greater than n.*

Proof. Consider the number $n! + 1$.

- If $n! + 1$ is prime, then we are done, since $n! + 1 > n$.
- Otherwise, $n! + 1$ is divisible by some prime p.

  If $p \leq n$, then $p \mid n!$, so $p \nmid n! + 1$ (because $p \nmid 1$). Hence we must have $p > n$.

□

3.3.2 Bounded Sets

The following notion of bounded refers to subsets of $\mathbb{N}$. Bounded subsets of other sets such as $\mathbb{Q}$ and $\mathbb{R}$ behave differently.

Definition 3.43. Let $S \subseteq \mathbb{N}$. We say S is **bounded** if there exists $M \in \mathbb{N}$ such that $x \leq M$ for all $x \in S$; otherwise, S is **unbounded**.

Remark. We need not define the lower bound, since it is naturally 0.

Remark. The above notion of bounded refers to subsets of $\mathbb{N}$. Bounded subsets of other sets such as $\mathbb{Q}$ and $\mathbb{R}$ behave differently.

We have shown that every non-empty bounded set has a maximum element. This is unique, for if x_1 and x_2 are both maximal, by definition of maximum, since x_1 is a maximum, $x_2 \leq x_1$; similarly $x_1 \leq x_2$. Hence $x_1 = x_2$. Hence we denote the maximum element of S by $\max(S)$.

Lemma 3.44. *The union of two bounded sets is bounded.*

Proof. Consider sets A and B which are bounded by a and b respectively. Let $c = \max(a, b)$. Then for each $x \in A$ or $x \in B$, we have $x \leq c$. Hence $A \cup B$ is bounded by c. □

3.3.3 Greatest Common Divisor

Definition 3.45. Let $a, b \in \mathbb{Z}$ with at least one of a and b non-zero. The **greatest common divisor** (gcd) of a and b is the unique positive integer k such that

(i) $k \mid a$ and $k \mid b$;

(ii) for all $d \in \mathbb{Z}$, if $d \mid a$ and $d \mid b$, then $d \leq k$.

Proposition 3.46. *Given any non-zero integers a and b, their gcd exists. Furthermore, the gcd is unique.*

Proof.
$\boxed{\text{Existence}}$ Consider the set of positive common divisors of a and b:

$$S = \left\{c \in \mathbb{N}^+ : c \mid a \text{ and } c \mid b\right\}.$$

S is non-empty because $1 \in S$, and S is bounded above by $|a|$. Thus let $k = \max(S)$. It follows that $k \mid a$, $k \mid b$, and if $d \mid a$ and $d \mid b$, then $|d| \leq k$.
$\boxed{\text{Uniqueness}}$ The gcd is the maximum of S, which is unique. □

We denote the gcd of a and b by $\gcd(a, b)$.

3.3.4 The Division Theorem

Theorem 3.47 (Division algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = bq + r \tag{3.1}$$

where $0 \leq r < b$.

We call q and r the **quotient** and **remainder** respectively of a when divided by b.

Proof. Let $a, b \in \mathbb{Z}$ with $b > 0$.
$\boxed{\text{Uniqueness}}$ Suppose $a = bq_1 + r_1 = bq_2 + r_2$, where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < b$. We want to show $q_1 = q_2$ and $r_1 = r_2$. Rearranging, we obtain

$$b(q_1 - q_2) = r_2 - r_1.$$

Thus $b \mid r_2 - r_1$. If $r_2 - r_1 \neq 0$, then $b \leq |r_2 - r_1|$. But $0 \leq r_1, r_2 < b$ implies $|r_2 - r_1| < b$. Hence $r_2 - r_1 = 0 \Rightarrow r_1 = r_2$.
Finally, since $b \neq 0$, we can cancel b on both sides: $b(q_1 - q_2) = 0 \Rightarrow q_1 - q_2 = 0 \Rightarrow q_1 = q_2$.
$\boxed{\text{Existence}}$ Consider the set of remainders after subtracting multiples of b from r:

$$S := \left\{r \in \mathbb{Z}_{\geq 0} : (\exists q \in \mathbb{Z})\ a = bq + r\right\}.$$

To show that S is non-empty, consider $q = -|a| \in \mathbb{Z}$. This shows that $a + b|a| \in S$ since it is non-negative:

$$a + b|a| \geq (b - 1)|a| \geq 0.$$

By well-ordering, let r be the least element of S. By construction, $r \geq 0$; it remains to show $r < b$.

Suppose, for a contradiction, that $r \geq b$. Then $r - b \in S$; this is because if $r = a - bq$, then

$$a = b(q+1) + (r-b).$$

Since $r - b < r$, this contradicts the minimality of r. □

Remark. For $b = 2$, existence means "every integer is either even or odd", while uniqueness of r means "no integer is both even and odd".

Remark. The existence part of the division theorem allows us to prove statements of the form $(\forall a \in \mathbb{Z})\, P(a)$ by cases (fix $b \in \mathbb{N}$ and consider the remainder of a when divided by b).

3.3.5 Bezout's Identity

Definition 3.48. A non-empty subset $I \subseteq \mathbb{Z}$ is an **ideal** if

(i) $a - b \in I$ for all $a, b \in I$; (closed under addition)

(ii) $na \in I$ for all $n \in \mathbb{Z}$, $a \in I$. (closed under left multiplication)

It follows that 0 is an element of every ideal, since $0 = a - a \in I$.

Ideals in $\mathbb{Z}$ are **principal**, i.e., generated by a single integer.

Proposition 3.49. *For each ideal $I \subseteq \mathbb{Z}$, there exists $k \in I \cap \mathbb{N}$ such that*

$$I = \{nk : n \in \mathbb{Z}\}.$$

Proof. If $I = \{0\}$, then we take $k = 0$. Otherwise, consider $S := I \cap \mathbb{N}$.

We claim S is non-empty. If not, I must contain some negative integer k. But then $-k \in S$. By well-ordering, let $k \in \mathbb{N}$ be the least element of S.

Claim: $I = \{nk : n \in \mathbb{Z}\}$.

$\boxed{\supseteq}$ Since $k \in I$, we have $nk \in I$ for all $n \in \mathbb{Z}$, by (ii) in Definition 3.48.

$\boxed{\subseteq}$ Let $a \in I$. By the division theorem, there exist integers n and r such that $a = nk + r$ and $0 \leq r < k$.

Claim: $r = 0$.

Since $a, k \in I$, we have $r = a - nk \in I$. Suppose, for a contradiction, that $r \neq 0$. Then $r \in S$. Since $r < k$, this contradicts the minimality of k.

Hence $r = 0$, so $a = nk$ as desired. □

We shall prove **Bezout's identity**, which expresses the gcd of two integers as a linear combination of the two integers. We first prove a lemma, which express common divisors of a and b as linear combinations of a and b.

Lemma 3.50. *For every non-zero $a, b \in \mathbb{Z}$, there exists $k \in \mathbb{N}$ such that $k \mid a$, $k \mid b$, and*

$$k = na + mb$$

for some $n, m \in \mathbb{Z}$.

Proof. Consider the set of linear combinations of a and b:

$$I = \{na + mb : n, m \in \mathbb{Z}\}.$$

We check that I is an ideal. (Clearly I is non-empty, since $a, b \in I$.)

- Let $n_1a + m_1b, n_2a + m_2b \in I$. Then $(n_1a + m_1b) - (n_2a + m_2b) = (n_1 - n_2)a + (m_1 - m_2)b \in I$.
- Let $n \in \mathbb{Z}$, $n_1a + m_1b \in I$. Then $n(n_1a + m_1b) = (nn_1)a + (nm_1)b \in I$.

Since ideals in $\mathbb{Z}$ are principal, there exists $k \in I \cap \mathbb{N}$ such that $I = \{nk : n \in \mathbb{Z}\}$. Note that $k \neq 0$ because I contains a non-zero number, so $k \in \mathbb{N}$.
Since $a, b \in I = \{nk : n \in \mathbb{Z}\}$, we have $k \mid a$ and $k \mid b$.
Since $k \in I = \{na + mb : n, m \in \mathbb{Z}\}$, there exist $n, m \in \mathbb{Z}$ such that $k = na + mb$. □

Theorem 3.51 (Bezout's identity)**.** *For every non-zero $a, b \in \mathbb{Z}$,*

$$\gcd(a, b) = na + mb \tag{3.2}$$

for some $n, m \in \mathbb{Z}$. Furthermore, if $d \mid a$ and $d \mid b$, then $d \mid \gcd(a, b)$.

This also shows that any common divisor divides the gcd.

Proof. By 3.50, there exist $k \in \mathbb{N}$ and $n, m \in \mathbb{Z}$ such that $k \mid a$, $k \mid b$, and $k = na + mb$. We shall prove $k = \gcd(a, b)$.

- Since $k \mid a$ and $k \mid b$, by definition $k \leq \gcd(a, b)$.
- By definition $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$, so we have $\gcd(a, b) \mid na + mb = k$. Thus $\gcd(a, b) \leq k$.

Hence $\gcd(a, b) = k = na + mb$.
Furthermore, if $d \mid a$ and $d \mid b$, then $d \mid na + mb = \gcd(a, b)$ as desired. □

Theorem 3.52 (Euclid's lemma)**.** *Suppose $a, b \in \mathbb{N}$ and p is prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Consider

$$I = \left\{n \in \mathbb{Z} : p \mid na\right\}.$$

We claim that I is an ideal. (Clearly I is non-empty since $0 \in I$.)

- Let $n_1, n_2 \in I$. Then $p \mid n_1a$ and $p \mid n_2a$, so $p \mid (n_1 - n_2)a$. Thus $n_1 - n_2 \in I$.
- Let $n \in \mathbb{Z}$, $n_1 \in I$. Then $p \mid n_1a$, so $p \mid (nn_1)a$. Thus $nn_1 \in I$.

Since every ideal in $\mathbb{Z}$ is principal, fix $k \in I \cap \mathbb{N}$ such that $I = \{nk : n \in \mathbb{Z}\}$.
We now have $p \in \left\{n \in \mathbb{Z} : p \mid na\right\} = \{nk : n \in \mathbb{Z}\}$. Then $p = nk$ for some $n \in \mathbb{Z}$, so k divides p. Since p is prime, either $k = 1$ or $k = p$.

Case 1: If $k = 1$, then $p \mid a$ because $p \mid ka$.

Case 2: If $k = p$, since $b \in I$, k divides b, i.e., $p \mid b$.

□

Corollary 3.53. *Suppose $a_1, \ldots, a_n \in \mathbb{N}$ and p is prime. If $p \mid a_1 \cdots a_n$, then $p \mid a_i$ for some i.*

Proof. Induct on n. □

Let us summarise our discussion of ideals. Since $\mathbb{Z}$ is an integral domain, 3.49 implies that $\mathbb{Z}$ is a principal ideal domain. By 3.52, a positive integer n is a prime number if and only if $n\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

3.3.6 Fundamental Theorem of Arithmetic

Let $P \subseteq \mathbb{N}$ denote the set of primes. A function $e\colon P \to \mathbb{N}$ takes a prime number $p \in P$ and assigns it to a non-negative integer $e(p)$.

Think of $e(p)$ as the exponent of the prime p in some factorisation.

Example. Suppose $e\colon P \to \mathbb{N}$ is defined by $e(2) = 3$, $e(3) = 1$, and $e(p) = 0$ for all other primes p. Then e “encodes” the number $2^3 \cdot 3^1 = 24$.

Thus e is a way of representing numbers by their prime factorisation, with $e(p)$ being the power of p.

Definition 3.54. The **support** of $f\colon X \to \mathbb{R}$ is the set of points in X where f is non-zero:

$$\operatorname{supp}(f) := \left\{x \in X \mid f(x) \neq 0\right\}.$$

If $\operatorname{supp}(f)$ is finite (i.e., $f(x) = 0$ for all but finitely many $x \in X$), then f is said to have **finite support**.

Definition 3.55. Let $\mathcal{F}$ denote the set of all functions $e\colon P \to \mathbb{N}$ with finite support, i.e., $\left\{p \in P \mid e(p) \neq 0\right\}$ is bounded.

Finite support just says almost all primes are raised to the 0-th power, i.e., they do not appear in the factorisation.

Theorem 3.56 (Fundamental theorem of arithmetic)**.** *For each $a \in \mathbb{N}$, there exists a unique $e_a \in \mathcal{F}$ such that*

$$a = \prod_{e_a(p) \neq 0} p^{e_a(p)}.$$

That is, every natural number has a unique factorisation, where finitely many primes have non-zero exponents.

Proof. Let $a \in \mathbb{N}$.

$\boxed{\text{Existence}}$ Proceed by strong induction on $a \in \mathbb{N}$.

When $a = 1$, define $e_1(p) = 0$ for all $p \in P$. Thus $\left\{p \in P \mid e_1(p) \neq 0\right\} = \emptyset$ is bounded, so $e_1 \in \mathcal{F}$. we have

$$\prod_{e_1(p) \neq 0} p^{e_1(p)} = \prod \emptyset = 1.$$

Suppose for all $a' < a$, there exist $e_{a'} \in \mathcal{F}$ such that $a' = \prod_{e_{a'}(p) \neq 0} p^{e_{a'}(p)}$. We consider cases:

Case 1: If $a \in P$, define $e_a\colon P \to \mathbb{N}$ by

$$e_a(p) = \begin{cases} 1 & (p = a) \\ 0 & (p \neq a) \end{cases}$$

One easily checks that $e_a \in \mathcal{F}$, and $a = a^{e_a(a)}$.

Case 2: If $a \notin P$, then $a = kq$ for some $q \in P$, $k \geq 2$. Notice that $k < a$. By induction hypothesis, there exists $e_k \in \mathcal{F}$ such that $k = \prod_{e_k(p)\neq 0} p^{e_k(p)}$. Define $e_a \colon P \to \mathbb{N}$ by

$$e_a(p) = \begin{cases} e_k(p) + 1 & (p = q) \\ e_k(p) & (p \neq q) \end{cases}$$

Claim: $e_a \in \mathcal{F}$.

Since $\operatorname{supp}(e_k) = \{p \in P \mid e_k(p) \neq 0\}$ is bounded, suppose it has a bound b. Clearly $q \in \{p \in P \mid e_a(p) \neq 0\}$. If $q \leq b$, then $\{p \in P \mid e_a(p) \neq 0\}$ is bounded by b. Otherwise it is bounded by q. Therefore $e_a \in \mathcal{F}$.

Notice that $e_a(p) \neq 0$ whenever $e_k(p) \neq 0$, so one easily verifies that

$$a = qk = \prod_{e_a(p)\neq 0} p^{e_a(p)-e_k(p)} \prod_{e_a(p)\neq 0} p^{e_k(p)} = \prod_{e_a(p)\neq 0} p^{e_a(p)}.$$

$\boxed{\text{Uniqueness}}$ Suppose, for a contradiction, that for some $a \in \mathbb{N}$, there exist distinct functions $e, e' \in \mathcal{F}$ such that

$$a = \prod_{e(p)\neq 0} p^{e(p)} = \prod_{e'(p)\neq 0} p^{e'(p)}.$$

Since $e \neq e'$, fix $q \in P$ such that $e(q) \neq e'(q)$. WLOG assume $e(q) < e'(q)$. Divide both sides by $q^{e(q)}$:

$$\prod_{\substack{e(p)\neq 0 \\ p\neq q}} p^{e(p)} = q^{e'(q)-e(q)} \prod_{\substack{e'(p)\neq 0 \\ p\neq q}} p^{e'(p)}.$$

Since q divides RHS, q must divide LHS. By Euclid's lemma, q must divide some prime $p \neq q$, which is absurd. This yields the desired contradiction. □

We present several consequences of the fundamental theorem of arithmetic.

Corollary 3.57. *The function $a \mapsto e_a$ is a bijection from $\mathbb{N}$ to $\mathcal{F}$.*

Proof. By 3.56, the function $a \mapsto e_a$ is well-defined.

Injectivity: Consider $a, a' \in \mathbb{N}$. Suppose $e_a = e_{a'}$. Then we have

$$a = \prod_{e_a(p)\neq 0} p^{e_a(p)} = \prod_{e_{a'}(p)\neq 0} p^{e_{a'}(p)} = a'.$$

Surjectivity: Let $e \in \mathcal{F}$. Define $a = \prod_{e(p)\neq 0} p^{e(p)}$. This product is well-defined because $e \in \mathcal{F}$. Also, by 3.56, since $a \in \mathbb{N}$, $a = \prod_{e_a(p)\neq 0} p^{e_a(p)}$ and e_a is unique. Hence we have $e = e_a$.

□

Remark. The proof for surjectivity uses the uniqueness of e_a. If e_a is characterised by a certain property and we want to show $e = e_a$, it suffices to prove that e has the same property as e_a.

Remark. The FTA does not give us constructive definition of e_a. It only asserts that there is unique e_a with certain properties. So in this proof what matters is the property of e in the set $\mathcal{F}$.

When we multiply two numbers, the prime factorisation of the product is obtained by summing the corresponding exponents.

Corollary 3.58. *For every $a, b \in \mathbb{N}$, we have*

$$e_{ab}(p) = e_a(p) + e_b(p)$$

for all $p \in P$.

Proof. By the definition of e_a and e_b,

$$a = \prod_{e_a(p)\neq 0} p^{e_a(p)} \qquad \text{and} \qquad b = \prod_{e_b(p)\neq 0} p^{e_b(p)}.$$

Multiplying them together, we have

$$ab = \prod_{e_a(p)\neq 0 \vee e_b(p)\neq 0} p^{e_a(p)+e_b(p)} = \prod_{e_a(p)+e_b(p)\neq 0} p^{e_a(p)+e_b(p)}.$$

Let $e = e_a + e_b$, where addition is defined pointwise, i.e., $e(p) = e_a(p) + e_b(p)$ for each $p \in P$. Then

$$ab = \prod_{e(p)\neq 0} p^{e(p)}.$$

We check that $e \in \mathcal{F}$. Note that

$$\begin{aligned}
\operatorname{supp}(e) &= \{p \in P \mid e(p) \neq 0\} \\
&= \{p \in P \mid e_a(p) + e_b(p) \neq 0\} \\
&= \{p \in P \mid e_a(p) \neq 0 \vee e_b(p) \neq 0\} \\
&= \{p \in P \mid e_a(p) \neq 0\} \cup \{p \in P \mid e_b(p) \neq 0\} \\
&= \operatorname{supp}(e_a) \cup \operatorname{supp}(e_b).
\end{aligned}$$

Since $\operatorname{supp}(e_a)$ and $\operatorname{supp}(e_b)$ are bounded, and the union of two bounded sets is bounded, we conclude that $\operatorname{supp}(e)$ is bounded and thus finite. Hence $e \in \mathcal{F}$.

By the uniqueness of e_{ab}, we have $e_{ab} = e = e_a + e_b$. □

Remark. The subtlety in this proof is that in order to apply the unique property of e_{ab}, one must prove that $e = e_a + e_b$ is actually in $\mathcal{F}$, because the uniqueness property only applies to elements in $\mathcal{F}$.

divisibility - a divides b if and only if in the prime factorisation, exponents of a are less than or equal to corresponding ones in b.

Corollary 3.59. *For every $a, b \in \mathbb{N}$,*

$$a \mid b \iff e_a(p) \leq e_b(p) \quad \textit{for every } p \in P.$$

Proof.

$\boxed{\Rightarrow}$ Suppose $a \mid b$. Then $b = ka$ for some $k \in \mathbb{N}$. By 3.58, we have

$$e_b(p) = e_{ak}(p) = e_a(p) + e_k(p)$$

for all $p \in P$. Since $e_k(p) \geq 0$ for all $p \in P$, we have $e_a(p) \leq e_b(p)$ for all $p \in P$.

$\boxed{\Leftarrow}$ Suppose $e_a(p) \leq e_b(p)$ for all $p \in P$. Define

$$k = \prod_{e_b(p)\neq 0} p^{e_b(p)-e_a(p)}.$$

Since $0 \leq e_a(p) \leq e_b(p)$, whenever $e_a(p) \neq 0$, we have $e_b(p) \neq 0$; whenever $e_a(p) = 0$, we have $p^{e_a(p)} = 1$. Thus

$$a = \prod_{e_a(p)\neq 0} p^{e_a(p)} = \prod_{e_a(p)\neq 0} p^{e_b(p)}.$$

It follows that

$$\begin{aligned} ka &= \prod_{e_b(p)\neq 0} p^{e_b(p)-e_a(p)} \prod_{e_a(p)\neq 0} p^{e_b(p)} \\ &= \prod_{e_b(p)\neq 0} p^{e_b(p)} \\ &= b. \end{aligned}$$

□

Remark. Two subtleties in this proof:

- When defining k, we only restrict $e_b(p)$ to be non-zero. Noting that $e_a(p) \neq 0$ is stronger than $e_b(p) \neq 0$, we must allow $e_a(p) = 0$. Otherwise, we may completely neglect those prime factors which divide b but do not divide a. We also do not restrict $e_b(p) - e_a(p) \neq 0$ because we need the all terms with $e_b(p) \neq 0$ for later use.
- We changed $a = \prod_{e_a(p)\neq 0} p^{e_a(p)}$ to $a = \prod_{e_a(p)\neq 0} p^{e_b(p)}$ to make the condition in the set builder notation match with that of b. We can do this precisely because $e_a(p) \neq 0$ is stronger than $e_b(p) \neq 0$ and, in cases where $e_a(p) = 0$ and $e_b(p) \neq 0$, changing the condition has no effect on the product as $p^{e_a(p)} = 1$.

Proposition 3.60 (Existence of gcd)**.** *For every $a, b \in \mathbb{N}$, there exists $k \in \mathbb{N}$ such that*

(i) $k \mid a$ and $k \mid b$;

(ii) if $d \mid a$ and $d \mid b$, then $d \mid k$.

Notice that $k = \gcd(a, b)$.

Proof. Define $f\colon P \to \mathbb{N}$ by

$$f(p) = \min\left\{e_a(p), e_b(p)\right\} \qquad (p \in P).$$

That is, the exponents of gcd is the smaller of a and b.

Claim: $f \in \mathcal{F}$.

By definition, $f(p) \leq e_a(p)$ and $f(p) \leq e_b(p)$ for all $p \in P$. Hence $f(p) \neq 0$ is stronger than $e_a(p) \neq 0$, so $\left\{p \in P \mid f(p) \neq 0\right\} \subseteq \left\{p \in P \mid e_a(p) \neq 0\right\}$. It follows that $\left\{p \in P \mid f(p) \neq 0\right\}$ is bounded. Hence $f \in \mathcal{F}$.

Since $a \mapsto e_a$ is a surjection from $\mathbb{N}$ to $\mathcal{F}$, we can fix some $k \in \mathbb{N}$ such that $f = e_k$. Then $e_k(p) \leq e_a(p)$ and $e_k(p) \leq e_b(p)$ for all $p \in P$. By 3.59, $k \mid a$ and $k \mid b$.

If $d \mid a$ and $d \mid b$, then $e_d(p) \leq e_a(p)$ and $e_d(p) \leq e_b(p)$ for all $p \in P$. Hence

$$e_d(p) \leq \min\left\{e_a(p), e_b(p)\right\} = f(p) = e_k(p)$$

for all $p \in P$. By 3.59, $d \mid k$. □

Remark. We need to prove f has finite support before applying the properties of the functions with finite support.

3.3.7 Modular Arithmetic

Fix $b \in \mathbb{N}$. Denote $[b] = \{0, 1, \ldots, b-1\}$.

Definition 3.61. The **remainder function**

$$R_b \colon \mathbb{Z} \to [b]$$

maps every integer to its remainder when divided by b. That is, $R_b(a)$ is the remainder of a when divided by b.

Remark. By the division theorem, $R_b \colon \mathbb{Z} \to [b]$ is well-defined.

Lemma 3.62. *R_b is surjective but not injective.*

Proof. Surjectivity: Let $c \in [b]$. Then $R_b(c) = c$.
Non-injectivity: $R_b(c) = R_b(c + b) = 0$ but $c \neq c + b$. □

Lemma 3.63. $R_b(a) = R_b(a') \iff b \mid (a - a')$.

Proof.
$\boxed{\Rightarrow}$ Suppose $R_b(a) = R_b(a') = r$. Then $a = qb + r$ and $a' = q'b + r$ for some $q, q' \in \mathbb{Z}$. Rearranging,

$$a - a' = (q - q')b$$

so $b \mid (a - a')$.
$\boxed{\Leftarrow}$ We prove the contrapositive. Suppose $R_b(a) \neq R_b(a')$. Then $a - bq = r$ and $a' - bq' = r'$, where $r \neq r'$. WLOG assume $r > r'$. Then

$$(a - a') = b(q - q') + (r - r').$$

Since $0 < r' < r < b$, we have $0 < r - r' < b$. Thus, b does not divide $a - a'$. □

Define addition and multiplication on $[b]$ as

$$R_b(a) +_b R_b(a') = R_b(a + a')$$
$$R_b(a) \cdot_b R_b(a') = R_b(a \cdot a').$$

We need to check that these operations are well-defined:

Addition: Suppose $R_b(a_1) = R_b(a_2) = c$ and $R_b(a_1') = R_b(a_2') = d$. We need to show that $R_b(a_1 + a_1') = R_b(a_2 + a_2')$.

Write $a_1 = bq_1 + c$, $a_2 = bq_2 + c$, $a_1' = bq_1' + d$, $a_2' = bq_2' + d$ for some $q_1, q_2, q_1', q_2' \in \mathbb{Z}$. Then

$$a_1 + a_1' = b(q_1 + q_1') + (c + d)$$
$$a_2 + a_2' = b(q_2 + q_2') + (c + d).$$

Since $b \mid (a_1 + a_1') - (a_2 + a_2')$, it follows that $R_b(a_1 + a_1') = R_b(a_2 + a_2')$.

Multiplication:

3.3.8 Congruence Classes

Definition 3.64. Fix $b \in \mathbb{N}$. We say that a and a' are **congruent (mod b)** if $b \mid (a - a')$.

That is, a and a' have the same remainder divided by b.

Definition 3.65. Define $C_b\colon \mathbb{Z} \to \mathcal{P}(\mathbb{Z})$ by

$$\begin{aligned} C_b(a) &= \left\{a' \in \mathbb{Z} : b \mid (a - a')\right\} \\ &= \left\{a' \in \mathbb{Z} : R_b(a) = R_b(a')\right\}. \end{aligned}$$

We call $C_b(a)$ the **congruence class** of a modulo b.

Hence C_b is the function that sends every integer to its congruence class modulo b. We call C_b the **congruence class function**.

Example. Fix $b = 6$. Then $C_6(2) = \{\dots, -4, 2, 8, \dots\}$.

Lemma 3.66. *If $b \mid (a - a')$, then $C_b(a) = C_b(a')$.*

Proof. Note that $b \mid (a - a')$ is equivalent to $R_b(a) = R_b(a')$.

$\boxed{\subseteq}$ Let $c \in C_b(a)$. Then $R_b(a) = R_b(c)$. Since $R_b(a) = R_b(a')$, we have $R_b(c) = R_b(a')$. Thus $c \in C_b(a')$.

$\boxed{\supseteq}$ Similar to above. □

Let $Q_b \subseteq \mathcal{P}(\mathbb{Z})$ denote the range of C_b. We restrict the codomain of C_b to be Q_b. (This makes C_b surjective.)

Theorem 3.67 (Universal property)**.** *Suppose $f\colon \mathbb{Z} \to X$ is such that if $b \mid (a - a')$ then $f(a) = f(a')$. Then there exists a unique $g\colon Q_b \to X$ such that*

$$f = g \circ C_b.$$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "C_b"] \arrow[dr, "f"] & Q_b \arrow[d, dashed, "\exists! g"] \\ & X \end{tikzcd}$$

Proof.

$\boxed{\text{Existence}}$ Define $g\colon Q_b \to X$ by $g(C) = f(a)$ for any $a \in C$.

We first show that g is well-defined. Let $C \in Q_b$. Then $C = C_b(a)$ for some $a \in \mathbb{Z}$. If $a_1, a_2 \in C_b(a)$, then $b \mid (a - a_1)$ and $b \mid (a - a_2)$, so $b \mid (a_1 - a_2)$. By assumption, $f(a_1) = f(a_2)$ as desired.

To show that $f = g \circ C_b$, note that $a \in C_b(a)$, so $g(C_b(a)) = f(a)$.

$\boxed{\text{Uniqueness}}$ Suppose $h\colon Q_b \to X$ is such that $f = h \circ C_b$. Then for every $C_b(a) \in Q_b$, we have $h(C_b(a)) = f(a) = g(C_b(a))$, so $g = h$ as desired. □

Example. Let us consider some special f and find out their corresponding g.

- If $f\colon \mathbb{Z} \to X$ is a constant function that maps all integers to some $x \in X$, then $g\colon Q_b \to X$ is also a constant function which maps all $C \in Q_b$ to $x \in X$.
- If f is $C_b\colon \mathbb{Z} \to Q_b$, then $g\colon Q_b \to Q_b$ is the identity function.
- If f is $R_b\colon \mathbb{Z} \to [b]$, then $g\colon Q_b \to [b]$ is such that $g(C_b(a)) = R_b(a)$.

From the earlier example, $C_b \colon \mathbb{Z} \to Q_b$ is an example of such an f (with $X = Q_b$). Hence we can read the universal property as saying that all functions f with a certain property "come from" a single function with said property (namely C_b).

Corollary 3.68. *For each set X, denote*

$$\begin{aligned} \mathcal{G} &= \{g \colon Q_b \to X\} \\ \mathcal{F} &= \{f \colon \mathbb{Z} \to X \mid (\forall a, a' \in \mathbb{Z})\, b \mid (a - a') \Rightarrow f(a) = f(a')\} \end{aligned}$$

Then $\mathcal{G} \cong \mathcal{F}$.

Proof. Define $\Phi \colon \mathcal{G} \to \mathcal{F}$ by

$$g \mapsto g \circ C_b.$$

First, we prove that Φ is well defined. Whenever $b \mid (a - a')$, we have $g(C_b(a)) = g(C_b(a'))$ (because $C_b(a) = C_b(a')$). Thus $g \circ C_b \in \mathcal{F}$. So $g \mapsto g \circ C_b$ is well-defined.

Injectivity: Let $g_1, g_2 \in \mathcal{G}$. Suppose $f = g_1 \circ C_b = g_2 \circ C_b$. By 3.67 there exists a unique $g \in \mathcal{G}$ such that $f = g \circ C_b$. Thus we have $g_1 = g = g_2$.

Surjectivity: Let $f \in \mathcal{F}$. By 3.67, there exists a unique $g \in \mathcal{G}$ such that $f = g \circ C_b$.

□

— Exercises —

Exercise 3.3.1. Prove Lemma 3.41.

Solution.

(i) Let $b = ka$ for some $k \in \mathbb{Z}$. Since $b \neq 0$, it follows that $a \neq 0$ and $k \neq 0$. In particular, $a \neq 0$.

(ii) Let $b = ka$ for some $k \in \mathbb{Z}$. Thus $|b| = |k||a|$. Since $|k| \geq 1$, it follows that $|a| \leq |b|$.

(iii) Let $b = ka$ for some $k \in \mathbb{Z}$. Then $nb = n(ka) = k(na)$, so $na \mid nb$.

(iv) Let $b = ka$ for some $k \in \mathbb{Z}$, $c = la$ for some $l \in \mathbb{Z}$. Then $nb + mc = n(ka) + m(la) = a(nk + ml)$, so $a \mid nb + mc$.

□

Exercise 3.3.2. We say an integer is 1 mod 4 if it equals $4k + 1$ for some integer k.

(a) Prove that if integers a and b are 1 mod 4, then ab is 1 mod 4.

(b) Prove by strong induction on x that if all primes which divide $x \in \mathbb{N}$ are 1 mod 4, then x is itself 1 mod 4.

(c) Prove that the set of primes which are not 1 mod 4 is unbounded.

Solution.

(a) Suppose integers a and b are 1 mod 4. Then $a = 4m + 1$, $b = 4n + 1$ for some $m, n \in \mathbb{Z}$. Thus

$$ab = (4m + 1)(4n + 1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1$$

so ab is 1 mod 4.

(b) The base case is true for $x = 1$.

Suppose the desired result is true for all k, where $1 \leq k \leq x$. We wish to prove it true for $x + 1$.

Suppose all primes which divide $x + 1$ are 1 mod 4. We consider two cases:

Case 1: If $x + 1$ is prime, then by assumption $x + 1$ is 1 mod 4.

Case 2: If $x + 1$ is not prime, then $x + 1 = ab$ for some $a, b \in \mathbb{Z}$, where $a, b < x + 1$. Then apply inductive hypothesis and (a).

(c) Suppose, for a contradiction, that the set of primes which are not 1 mod 4 is bounded. Then there are finitely many primes which are not 1 mod 4.

Since 2 is one such prime and all other primes not 1 mod 4 are 3 mod 4, it follows that there are finitely many primes which are 3 mod 4, say $p_1, \dots, p_n$. Consider

$$N = 4p_1 \cdots p_n - 1,$$

which is 3 mod 4. N is divisible by some prime q, but none of the primes p_i divides N, so $q \notin \{p_1, \dots, p_n\}$. By contrapositive of (b), q is 3 mod 4. This yields the desired contradiction.

□

Exercise 3.3.3. Prove that if I is an ideal, then there is at most one positive integer $k \in I$ such that $I = \{nk : n \in \mathbb{Z}\}$.

Solution. Let I be an ideal of $\mathbb{Z}$. Suppose $k, k' \in I \cap \mathbb{N}$ are such that

$$I = \{nk : n \in \mathbb{Z}\} = k\mathbb{Z} \qquad \text{and} \qquad I = \big\{nk' : n \in \mathbb{Z}\big\} = k'\mathbb{Z}.$$

Since $k' \in I = k\mathbb{Z}$, we have $k \mid k'$. Similarly $k' \mid k$. Hence $k = k'$. □

Exercise 3.3.4. Prove that if I is an ideal and $a, b \in I$, then $na + mb \in I$ for every $n, m \in \mathbb{Z}$. Conclude that if $a, b \in I$ are non-zero, then $\gcd(a, b) \in I$.

Solution. Let $I \subseteq \mathbb{Z}$ be an ideal, and let $a, b \in I$. For every $n, m \in \mathbb{Z}$, then by property (ii) of ideals we have $na \in I$ and $mb \in I$. Since I is closed under subtraction (hence under addition) by property (i), it follows that

$$na + mb = (na) - (-mb) \in I.$$

By Bezout's identity, $\gcd(a, b) = na + mb$ for some $n, m \in \mathbb{Z}$, so $\gcd(a, b) \in I$. □

Exercise 3.3.5. Prove that if a, b and k are positive integers, then $\gcd(ka, kb) = k \cdot \gcd(a, b)$.

Solution. We will show

$$\gcd(ka, kb) \leq k \cdot \gcd(a, b) \qquad \text{and} \qquad k \cdot \gcd(a, b) \leq \gcd(ka, kb).$$

By Bezout's identity, there exist integers $s, t \in \mathbb{Z}$ such that

$$sa + tb = \gcd(a, b).$$

Multiplying through by k gives

$$s(ka) + t(kb) = k \cdot \gcd(a, b).$$

This shows that $k \cdot \gcd(a, b)$ is a linear combination of ka and kb. Thus every common divisor of ka and kb divides $k \cdot \gcd(a, b)$. In particular,

$$\gcd(ka, kb) \mid k \cdot \gcd(a, b).$$

Hence $\gcd(ka, kb) \leq k \cdot \gcd(a, b)$.

Since $\gcd(a, b)$ divides both a and b, it follows that $k \cdot \gcd(a, b)$ divides both ka and kb. Thus $k \cdot \gcd(a, b)$ is a common divisor of ka and kb. By definition of gcd,

$$k \cdot \gcd(a, b) \mid \gcd(ka, kb).$$

Hence $k \cdot \gcd(a, b) \leq \gcd(ka, kb)$. □

Exercise 3.3.6. Suppose a, b, c are non-zero integers such that $c \mid ab$.

(i) Define $I = \{n \in \mathbb{Z} : c \mid an\}$. Prove that I is an ideal.

(ii) Use (i) to prove that $c \mid a \cdot \gcd(b, c)$.

Solution.

(i) I is non-empty, since $0 \in I$.

Let $n, m \in I$. Then $c \mid an$ and $c \mid am$. Thus $c \mid a(n - m)$, so $n - m \in I$.

Let $n \in I$, $s \in \mathbb{Z}$. Then $c \mid an$, so $c \mid a(sn) = s(an)$; thus $tn \in I$.

(ii) By assumption $c \mid ab$, so $b \in I$. Since $c \mid ac$, we have $c \in I$.

By Bezout's identity, there exist integers s, t such that

$$\gcd(b, c) = sb + tc.$$

By the previous question, every ideal of $\mathbb{Z}$ is closed under linear combinations. Hence $\gcd(b, c) \in I$.

□

Exercise 3.3.7. A positive integer a is said to be **square-free** if there is no integer $k \geq 2$ such that $k^2 \mid a$. Prove that a is square-free if and only if $e_a(p) \leq 1$ for all primes p.

Solution.

$\boxed{\Rightarrow}$ Suppose a is square-free.

Suppose, for a contradiction, that there exists a prime q with $e_a(q) \geq 2$. Since

$$\begin{aligned} e_{q^2}(q) &= 2 \leq e_a(q) \\ e_{q^2}(p) &= 0 \leq e_a(p) \quad \text{for } p \neq q \end{aligned}$$

we have $e_{q^2}(p) \leq e_a(p)$ for all $p \in P$. By 3.59, it follows that $q^2 \mid a$.

This contradicts the assumption that no square k^2 with $k \geq 2$ divides a.

$\boxed{\Leftarrow}$ Suppose $e_a(p) \leq 1$ for every prime p.

Suppose, for a contradiction, that there exists an integer $k \geq 2$ such that $k^2 \mid a$. By 3.59, for every prime p, we have

$$2e_k(p) = e_{k^2}(p) \leq e_a(p) \leq 1.$$

Thus $2e_k(p) \leq 1$ for all p. This forces $e_k(p) = 0$ for every prime p. Hence $k = 1$, which contradicts $k \geq 2$. □

★ **Exercise 3.3.8** (MA1100T AY22/23)**.**

(a) Prove that for all $x, y, n \in \mathbb{N}$, we have $\min\{nx, ny\} = n \min\{x, y\}$.

(b) Prove that for all positive integers a, b and n, we have $\gcd(a^n, b^n) = (\gcd(a, b))^n$.

Solution.

(a) WLOG assume $x \leq y$, so $\min\{x, y\} = x$. Then $nx \leq ny$, so $\min\{nx, ny\} = nx$.

(b) Let $a = \prod\{p^{e_a(p)} : e_a(p) \neq 0\}$ and $b = \prod\{p^{e_b(p)} : e_b(p) \neq 0\}$.

Then $a^n = \prod\{p^{n \cdot e_a(p)} : e_a(p) \neq 0\}$ and $b^n = \prod\{p^{n \cdot e_b(p)} : e_b(p) \neq 0\}$. Hence we have

$$\begin{aligned} \gcd(a^n, b^n) &= \prod p^{\min\{n \cdot e_a(p), n \cdot e_b(p)\}} \\ &= \prod p^{n \cdot \min\{e_a(p), e_b(p)\}} \\ &= \left(\prod p^{\min\{e_a(p), e_b(p)\}}\right)^n \\ &= (\gcd(a, b))^n. \end{aligned}$$

□

Exercise 3.3.9. Given $b \in \mathbb{N}$, prove that the function $\cdot_b \colon [b] \times [b] \to [b]$ defined by

$$R_b(a) \cdot_b R_b(a') = R_b(a \cdot a')$$

is well-defined.

Solution. Since R_b is surjective, $R_b(a)$ exists for all $a \in \mathbb{Z}$. Thus $R_b(a \cdot a')$ exists for all $a, a' \in \mathbb{Z}$. Suppose $R_b(a_1) = R_b(a_2)$ and $R_b(a_1') = R_b(a_2')$. We want to show that $R_b(a_1 \cdot a_1') = R_b(a_2 \cdot a_2')$. Recall that $R_b(a) = R_b(a') \iff b \mid (a - a')$, so

$$b \mid (a_1 - a_2) \qquad \text{and} \qquad b \mid (a_1' - a_2').$$

Write $a_1 = mb + a_2$, $a_1' = m'b + a_2'$ for some $m, m' \in \mathbb{Z}$. Thus

$$\begin{aligned} a_1 \cdot a_1' - a_2 \cdot a_2' &= (mb + a_2)(m'b + a_2') - a_2 \cdot a_2' \\ &= b(mm'b + ma_2' + a_2 m'). \end{aligned}$$

Hence $b \mid (a_1 \cdot a_1' - a_2 \cdot a_2')$, so $R_b(a_1 \cdot a_1') = R_b(a_2 \cdot a_2')$. □

★ **Exercise 3.3.10.** Given $b \in \mathbb{N}$:

(a) Prove that the "function" $\oplus \colon [b] \times \mathbb{Z} \to [b]$ defined by $R_b(a) \oplus a' = a + a'$ is not well-defined.

(b) Prove that the "function" $\boxplus \colon [b] \times \mathbb{Z} \to \mathbb{Z}$ defined by $R_b(a) \boxplus a' = a + a'$ is not well-defined.

Solution. Different representatives for the same remainder results in different outputs.

(a) Fix $b = 5$. Then $R_5(2) = R_5(7)$, but

$$\begin{aligned} &R_5(2) \boxplus 0 = 2 + 0 = 2 \\ &R_5(7) \boxplus 0 = 7 + 0 = 7 \quad \text{is not in the codomain} \end{aligned}$$

(b) Fix $b = 5$. Then $R_5(2) = R_5(7)$, but

$$\begin{aligned} R_5(2) \boxplus 0 = 2 + 0 = 2 \\ R_5(7) \boxplus 0 = 7 + 0 = 7 \end{aligned}$$

□

★ **Exercise 3.3.11** (MA1100T AY23/24)**.** Suppose $m, n \in \mathbb{N}^+$. We attempt to define a function $f\colon [mn] \to [m] \times [n]$ by

$$f(R_{mn}(a)) = (R_m(a), R_n(a)).$$

Prove that f is well-defined.

Solution.

- Let $c \in [mn]$. Since $R_{mn}\colon \mathbb{Z} \to [mn]$ is surjective, there exists $a \in \mathbb{Z}$ such that $c = R_{mn}(a)$. Hence $R_m(a)$ and $R_n(a)$ exist, so $f(c)$ exists.
- Suppose $R_{mn}(a_1) = R_{mn}(a_2) = c$. Then there exist $q_1, q_2 \in \mathbb{Z}$ such that

$$a_1 = q_1(mn) + c \quad \text{and} \quad a_2 = q_2(mn) + c.$$

We have

$$\begin{aligned} a_1 - a_2 = (q_1 - q_2)mn &\implies m \mid a_1 - a_2 \implies R_m(a_1) = R_m(a_2) \\ &\implies n \mid a_1 - a_2 \implies R_n(a_1) = R_n(a_2). \end{aligned}$$

Hence $(R_m(a_1), R_n(a_1)) = (R_m(a_2), R_n(a_2))$, so $f(R_{mn}(a_1)) = f(R_{mn}(a_2))$. Thus $f(c)$ has a unique value.

□

★ **Exercise 3.3.12** (MA1100T AY24/25)**.** Let $A = \{a_0, a_1, \dots, a_m\}$ be a non-empty finite set of integers. Define

$$I = \left\{ \sum_{i=0}^{m} c_i a_i \in \mathbb{Z} : c_1, c_1, \dots, c_m \in \mathbb{Z} \right\}.$$

(a) Prove that I is an ideal.

(b) Using (a) or otherwise, prove that there exists $k \in \mathbb{N}^+$ such that

  (i) k divides every $a \in A$, and

  (ii) if $d \in \mathbb{Z}$ divides every $a \in A$, then d divides k.

Solution.

(a) Obvious; check closure under addition and multiplication.

(b) Since I is an ideal, there exists $k \in \mathbb{N}^+$ such that $I = \{nk \mid n \in \mathbb{Z}\}$. We check that (i) and (ii) hold:

  (i) Let $a \in A$. Then $a \in I$, so $a = nk$ for some $n \in \mathbb{Z}$. Thus k divides a.

  (ii) Let $d \in \mathbb{Z}$ be such that d divides every $a \in A$. Then d divides every element of I. Since $k \in I$, it follows that d divides k.

□

★ **Exercise 3.3.13** (MA1100T AY22/23)**.** Prove that for all positive integers a, b, and c, we have

$$\gcd(a, b) \text{ divides } c$$

if and only if there is some integer x such that b divides $ax - c$.

Solution.

$\boxed{\Rightarrow}$ Suppose $\gcd(a,b) \mid c$. By Bezout's identity, write $\gcd(a,b) = ma + nb$ for some $m, n \in \mathbb{Z}$. Then $p(ma + nb) = c$ for some $p \in \mathbb{Z}$. Rearranging gives $(pm)a - c = (pn)b$.

$\boxed{\Leftarrow}$ Suppose there is some integer x such that $b \mid ax - c$. Then $ax - c = nb$ for some $n \in \mathbb{Z}$. Rearranging gives $ax - nb = c$.

Let $d = \gcd(a,b)$. By definition $d \mid a$ and $d \mid b$, so $d \mid (ax - nb) = c$, i.e., $d \mid c$. □

★★ **Exercise 3.3.14** (MA1100T AY23/24)**.** Suppose a, b and n are positive integers. Suppose $\gcd(a,b)$ is a prime, say q, and that $ab = n^2$. Prove that there exists **integers** c and d such that

$$\frac{a}{q} = c^2 \quad \text{and} \quad \frac{b}{q} = d^2.$$

Solution. Since q is a prime, $e_q(p) = 0$ for all primes $p \neq q$, and $e_q(q) = 1$.

Since $ab = n^2$, we have $e_a(p) + e_b(p) = 2e_n(p)$ for all primes p.

We construct c and d by

$$e_c(p) = \begin{cases} \frac{1}{2}e_a(p) & \text{if } p \neq q \\ \frac{1}{2}(e_a(p) - 1) & \text{if } p = q \end{cases} \qquad e_d(p) = \begin{cases} \frac{1}{2}e_b(p) & \text{if } p \neq q \\ \frac{1}{2}(e_b(p) - 1) & \text{if } p = q \end{cases}$$

The idea is as such: Informally we consider the "positive square root" $c = \sqrt{\frac{a}{q}}$, so the exponents of c are half of the exponents of $\frac{a}{q}$; the exponents of $\frac{a}{q}$ are $e_a(p)$ if $p \neq q$, and $e_a(p) - 1$ if $p = q$.

We now check that $\frac{a}{q} = c^2$ and $\frac{b}{q} = d^2$:

$$\begin{aligned} e_{c^2 q} &= 2e_c + e_q = e_a \\ e_{d^2 q} &= 2e_d + e_q = e_b. \end{aligned}$$

It remains to show that e_c and e_d are well defined. Consider cases:

Case 1: $p = q$. Since $\gcd(a,b) = q$, either $1 = e_a(q) \le e_b(q)$ or $1 = e_b(q) \le e_a(q)$.

In either case, since $e_a(p) + e_b(p) = 2e_n(p)$ is even, both $e_a(q)$ and $e_b(q)$ are positive odd integers.

Case 2: $p \neq q$. Since $\gcd(a,b) = q$, at least one of $e_a(p)$ and $e_b(p)$ is 0.

- If $e_a(p) = 0$, then $e_b(p) = 2e_n(p)$, so $e_c(p) = 0$ and $e_d(p) = e_n(p)$.
- If $e_b(p) = 0$, then $e_a(p) = 2e_n(p)$, so $e_c(p) = e_n(p)$ and $e_c(p) = 0$.

Hence for all primes p, $e_c(p), e_d(p) \in \mathbb{N}$.

Furthermore, $e_c(p) \le e_a(p)$ and $e_d(p) \le e_a(p)$ for all primes p. Since e_a and e_b have finite support, so do e_c and e_d. □

★★ **Exercise 3.3.15** (MA1100T AY23/24)**.** Suppose $a, b \in \mathbb{N}^+$. Prove that $\gcd(a,b) = 1$ if and only if $\gcd(ab, a + b) = 1$.

Solution. We first prove a lemma:

Lemma. *Suppose $x, y \in \mathbb{N}^+$. If there exists $m, n \in \mathbb{Z}$ such that $mx + ny = 1$, then* $\gcd(x,y) = 1$.

Proof. Let $d = \gcd(x,y)$. Then $d \mid x$ and $d \mid y$, so $d \mid mx + ny = 1$. Thus $d = 1$. □

$\boxed{\Rightarrow}$ Suppose $\gcd(a,b) = 1$. By Bezout's identity, $ha + kb = 1$ for some $h, k \in \mathbb{Z}$.

The idea is to square $ha + kb$ in order to get terms of the form ab:

$$\begin{aligned}
1 &= ha + kb \\
&= (ha + kb)^2 \\
&= h^2a^2 + 2hkab + k^2b^2 \\
&= (h^2a^2 + h^2ab + k^2ab + k^2b^2) + (2hkab - h^2ab - k^2ab) \\
&= (h^2a + k^2b)(a + b) + (2hk - h^2 - k^2)ab.
\end{aligned}$$

By the lemma, $\gcd(ab, a + b) = 1$.

$\boxed{\Leftarrow}$ Suppose $\gcd(ab, a + b) = 1$. By Bezout's identity, $p(ab) + q(a + b) = 1$ for some $p, q \in \mathbb{Z}$. Then

$$\begin{aligned}
1 &= pab + q(a + b) \\
&= (pb + q)a + qb.
\end{aligned}$$

By the lemma, $\gcd(a, b) = 1$. □

3.4 Equivalence Relations

3.4.1 Equivalence Relation and Quotient Map

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 3.69. A relation $\sim$ on a set A is an **equivalence relation** if it is

(i) reflexive,

(ii) symmetric,

(iii) transitive.

Example. The following are all examples of equivalence relations:

- On $\mathbb{C}$, define $z \sim w \iff |z| = |w|$.
- On $\mathbb{R} \times \mathbb{R}$, define $(a, b) \sim (c, d) \iff a^2 + b^2 = c^2 + d^2$. Geometrically, the two points lie on the same circle centered at the origin.
- On the set of polygons in $\mathbb{R}^2$, define $\sim$ as congruence.
- On the set of differentiable functions on $\mathbb{R}$, define $f \sim g \iff f'(x) = g'(x)$.
- On $\mathbb{Z}$, define $a \sim b \iff n \mid (a - b)$. In this case $\sim$ represents congruence modulo n. It is the basis for modular arithmetic, and $a \sim b$ is usually denoted as $a \equiv b \pmod{n}$.

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

Definition 3.70. Suppose $\sim$ is an equivalence relation on a non-empty set A. For each $a \in A$, the **equivalence class** of a is

$$[a] := \left\{a' \in A : a' \sim a\right\}.$$

The set of all equivalence classes is called the **quotient set**:

$$A/{\sim} := \left\{[a] : a \in A\right\}.$$

We read $A/{\sim}$ as "A mod $\sim$". Note that $A/{\sim} \subseteq \mathcal{P}(A)$.

If $\sim$ is an equivalence relation on a set A, there is a (clearly surjective) *canonical* projection

$$\begin{tikzcd} A \arrow[r, two heads] & A/{\sim} \end{tikzcd}$$

obtained by sending every $a \in A$ to its equivalence class $[a]$.

Definition 3.71. The **quotient map** $\pi \colon A \to A/{\sim}$ is defined by $\pi(a) = [a]$.

Lemma 3.72. *Quotient maps are surjective.*

Proof. By construction, every equivalence class $[a] \in A/{\sim}$ is the image of some $a \in A$, namely $\pi(a) = [a]$. □

Let $f\colon A \to C$ be a map. We say that f **factors** through a set B if there exist $g\colon A \to B$ and $h\colon B \to C$ such that $f = h \circ g$.

Theorem 3.73 (Universal property)**.** *For every set X and every function $f\colon A \to X$ such that if $a \sim b$, then $f(a) = f(b)$, there exists a unique $g\colon A/{\sim} \to X$ such that*

$$f = g \circ \pi.$$

In this case, f **factors uniquely** through the quotient set $A/{\sim}$ via π. In the language of category theory, the quotient set is called a **universal object**, and every other set factors through it.

$$\begin{tikzcd}
A \arrow[r, "\pi"] \arrow[d, "f"] & A/{\sim} \arrow[dl, dashed, red, "\exists ! g"] \\
X &
\end{tikzcd}$$

By the universal property, all functions f which treat $\sim$ as equality "come from" π, i.e., f equals some function composed with π.

Proof.
$\boxed{\text{Existence}}$ Define $g\colon A/{\sim} \to X$ by $g([a]) = f(a)$, for all $a \in [a]$.
We first prove g is well defined. Fix $[a] \in A/{\sim}$, let $a_1, a_2 \in [a]$. Then $a_1 \sim a$ and $a_2 \sim a$, so $a_1 \sim a_2$. By assumption, $f(a_1) = f(a_2)$.
We check that $f = g \circ \pi$:

$$(g \circ \pi)(a) = g(\pi(a)) = g([a]) = f(a).$$

$\boxed{\text{Uniqueness}}$ Suppose $g'\colon A/{\sim} \to X$ is such that $f = g' \circ \pi$. For every $[a] \in A/{\sim}$, we have

$$g'([a]) = f(a) = g([a]).$$

Hence $g = g'$, as desired. □

One can interpret the universal property as a recipe for defining functions on $A/{\sim}$: In order to define a function on $A/{\sim}$ to X, it suffices to define a function $f\colon A \to X$ such that if $a \sim a'$, then $f(a) = f(b)$, and then apply the universal property to find g.
In fact, by the preceding result, every function $g\colon A/{\sim} \to X$ can be obtained in this way, because the function $g \circ \pi\colon A \to X$ satisfies the following condition: if $a \sim b$, then $g(\pi(a)) = g(\pi(b))$.

Corollary 3.74.

$$\mathrm{Maps}(A/{\sim}, X) \cong \left\{ f \in \mathrm{Maps}(A, X) : (\forall a, b \in A)\; a \sim b \Rightarrow f(a) = f(b) \right\}.$$

Proof. Denote $\mathcal{F} := \left\{ f \in \mathrm{Maps}(A, X) : (\forall a, b \in A)\; a \sim b \Rightarrow f(a) = f(b) \right\}$. Define

$$\begin{aligned} \Phi\colon \mathrm{Maps}(A/{\sim}, X) &\to \mathcal{F} \\ g &\mapsto g \circ \pi \end{aligned}$$

We show Φ is a bijection.

Well-definedness: If $g \in \mathrm{Maps}(A/{\sim}, X)$, then $\Phi(g) = g \circ \pi$ is a map from A to X.

If $a \sim b$, then $g \circ \pi(a) = g([a]) = g([b]) = g \circ \pi(b)$. Hence $g \circ \pi \in \mathcal{F}$.

Injectivity: Suppose $\Phi(g) = \Phi(g')$. Then $g \circ \pi = g' \circ \pi$; that is, $g \circ \pi(a) = g' \circ \pi(a)$ for all $a \in A$. Then $g([a]) = g'([a])$ for each $a \in A$. Thus $g([a]) = g'([a])$ for each $[a] \in A/\!\sim$. Hence $g = g'$.

Surjectivity: Let $f \in \mathcal{F}$. By the universal property (3.73), there exists a unique function $g \in \text{Maps}(A/\sim, X)$ such that $f = g \circ \pi$, i.e., $f = \Phi(g)$.

□

3.4.2 Equivalence Relations and Partitions

The next result shows that distinct equivalence classes are disjoint.

Lemma 3.75. *Let $\sim$ be an equivalence relation on a non-empty A. For every $a, a' \in A$, the following are equivalent:*

$$a \sim a' \iff [a] = [a'] \iff (\exists b \in A)\, a, a' \in [b] \iff [a] \cap [a'] \neq \emptyset.$$

Proof.

$\boxed{\text{(i)} \Rightarrow \text{(ii)}}$ Suppose $a \sim b$. Since $a \in [a]$ and $a \in [b]$, we have $[a] \subseteq [b]$. The reverse inclusion follows similarly.

$\boxed{\text{(ii)} \Rightarrow \text{(iii)}}$ Suppose $[a] = [a']$. By reflexivity, we have $a \in [a]$ and $a' \in [a'] = [a]$.

$\boxed{\text{(iii)} \Rightarrow \text{(iv)}}$ Suppose $a, a' \in [b]$. Then $a \sim b$ and $a' \sim b$. By symmetry, we have $b \sim a$ and $b \sim a'$. Thus $b \in [a] \cap [a']$.

$\boxed{\text{(iv)} \Rightarrow \text{(i)}}$ Suppose $[a] \cap [a'] \neq \emptyset$. Fix $b \in [a] \cap [a']$. Then $b \sim a$ and $b \sim a'$, so $a \sim a'$. □

Grouping the elements of a set into equivalence classes provides a **partition** of the set. As you would expect, a partition of a set A is a family of disjoint non-empty subsets of A, whose union is A.

Definition 3.76. A set $P \subseteq \mathcal{P}(A)$ is a **partition** of A if

(i) $\emptyset \notin P$; (all subsets are non-empty)

(ii) $\bigcup P = A$; (every element belongs to one of the subsets)

(iii) for every $C, D \in P$, either $C = D$ or $C \cap D = \emptyset$. (subsets are equal or disjoint)

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

The next result shows that the equivalence classes for any equivalence relation form a partition.

Proposition 3.77. *Suppose $\sim$ is an equivalence relation on a non-empty set A. Then the quotient set is a partition of A.*

Proof.

(i) By reflexivity, $a \sim a$. Thus $a \in [a]$, so $[a] \neq \emptyset$. Hence $\emptyset \notin A/\!\sim$.

(ii) We need to show that $\bigcup(A/\!\sim) = A$.

$\boxed{\subseteq}$ Let $x \in \bigcup(A/\!\sim)$. Then $x \in [a]$ for some $a \in A$. By definition of $[a]$, we have $x \in A$.

$\boxed{\supseteq}$ Let $a \in A$. By reflexivity, $a \in [a]$. Thus $a \in \bigcup(A/\!\sim)$.

(iii) By 3.75, distinct elements of $A/\!\sim$ are disjoint.

□

Conversely, we can use any given partition to define an equivalence relation, by saying that $a \sim b$ if and only if a and b are elements of the same part of the partition.

Proposition 3.78. *Given a partition P of a set A, there exists an equivalence relation $\sim$ on A such that $P = A/{\sim}$.*

Proof. For $a, b \in A$, define

$$a \sim b \iff (\exists C \in P)\, a, b \in C.$$

That is, two elements are related if and only they belong to the same part of the partition.

We check that $\sim$ is an equivalence relation:

(i) Reflexivity: Fix $a \in A$. Since P is a partition of A, by definition, there exists $C \in P$ such that $a \in C$. Hence $a \sim a$ as desired.

(ii) Symmetry: Suppose $a \sim b$. Then there exists $C \in P$ such that $a, b \in C$. Then it is trival that $b \sim a$.

(iii) Transitivity: Suppose $a \sim b$ and $b \sim c$. Then there exist $C_1, C_2 \in P$ such that $a, b \in C_1$ and $b, c \in C_2$. Since $C_1 \cap C_2 \neq \emptyset$ (because they have a common element b), we have $C_1 = C_2 = C$. Thus $a, c \in C$, so $a \sim c$ as desired.

Next, we shall prove that $P = A/{\sim}$.

$\boxed{\subseteq}$ Fix $C \in P$, and suppose $a \in C$. By definition, for all $a' \in A$, if $a' \in C$, then $a' \sim a$. This means that C is an equivalence class. Hence we have $C \in A/{\sim}$.

$\boxed{\supseteq}$ Fix $[a] \in A/{\sim}$. Then $a' \sim a$ for all $a' \in [a]$. So there exists $C \in P$ such that $a \in C$ and for all $a' \in [a]$, $a' \in C$. Furthermore, for all $x \in C$, $x \sim a$. Thus $x \in [a]$. It follows that $C = [a]$. Hence $[a] \in P$. $\square$

Thus, there is a *natural correspondence* between equivalence relations and partitions of a set.

Corollary 3.79.

$$\{\textit{equivalence relations on } A\} \cong \{\textit{partitions of } A\}$$

Proof. Define

$$\begin{aligned} \mathcal{G}\colon \{\text{equivalence relations on } A\} &\to \{\text{partitions of } A\} \\ \sim &\mapsto A/{\sim} \end{aligned}$$

We show $\mathcal{G}$ is a bijection.

Well-definedness: For each equivalence relation $\sim$, the quotient set $A/{\sim}$ is a partition of A, so $\mathcal{G}$ is well-defined.

Injectivity: Define the map in the opposite direction

$$\mathcal{H}\colon \{\text{partitions of } A\} \to \{\text{equivalence relations on } A\}$$

by the rule: if P is a partition of A, then for $a, b \in A$, set

$$a\mathcal{H}(P)b \iff \text{there exists } C \in P \text{ such that } a, b \in C.$$

By the preceding result, $\mathcal{H}(P)$ is an equivalence relation, so $\mathcal{H}$ is well-defined. Furthermore, we have

$$(\mathcal{H} \circ \mathcal{G})(\sim) = \mathcal{H}(\mathcal{G}(\sim)) = \mathcal{H}(A/{\sim}) = \sim.$$

Hence

$$\mathcal{H} \circ \mathcal{G} = \mathrm{id}_{\{\text{equivalence relations on } A\}} .$$

Since $\mathcal{G}$ is left-invertible, it follows that $\mathcal{G}$ is injective.

Surjectivity: Let P be a partition of A. By the preceding result, we can define an equivalence relation on A such that $P = A/\sim$.

□

Since an equivalence relation on A is equivalent to a partition of A, it follows that the number of equivalence relations on A is equal to the number of partitions of A.

Example. How many different equivalence relations can be defined on the set $\{1, 2, 3\}$?

Solution. Since $\{1, 2, 3\}$ is small, we can determine this by hand:

$$\begin{aligned}
P_1 &= \{\{1, 2, 3\}\} \\
P_2 &= \{\{1\}, \{2\}, \{3\}\} \\
P_3 &= \{\{1, 2\}, \{3\}\} \\
P_4 &= \{\{1\}, \{2, 3\}\} \\
P_5 &= \{\{1, 3\}, \{2\}\}
\end{aligned}$$

Hence there can be only 5 equivalence relations defined on $\{1, 2, 3\}$. □

3.4.3 Range isomorphic to quotient by some equivalence relation

Fix a set B and a surjection $\sigma \colon A \to B$. Define a relation $\sim$ on A by

$$a \sim a' \iff \sigma(a) = \sigma(a').$$

One can easily check that $\sim$ is an equivalence relation on A:

(i) Reflexivity: For any $a \in A$, we have $\sigma(a) = \sigma(a)$, so $a \sim a$.

(ii) Symmetry: Suppose $a \sim a'$. Then $\sigma(a) = \sigma(a')$, so $\sigma(a') = \sigma(a)$. Thus $a' \sim a$.

(iii) Transitivity: Suppose $a \sim a'$ and $a' \sim a''$. Then $\sigma(a) = \sigma(a') = \sigma(a'')$, so $a \sim a''$.

Theorem 3.80. *For every set X and every function $f \colon A \to X$ such that if $a \sim b$ then $f(a) = f(b)$, there exists a unique $h \colon B \to X$ such that*

$$f = h \circ \sigma.$$

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\sigma"] & X \\
B \arrow[ur, dashed, "\exists! h"'] &
\end{tikzcd}$$

Proof.

$\boxed{\text{Existence}}$ Define $h \colon B \to X$ by

$$h(b) = f(a) \qquad (b \in B)$$

where $a \in A$ is such that $\sigma(a) = b$. Surjectivity of σ guarantees the existence of such a, for every $b \in B$.
We first show that h is well defined. Let $b \in B$. Consider $a, a' \in A$ such that $\sigma(a) = \sigma(a') = b$. By definition, $a \sim a'$, so by assumption, $f(a) = f(a')$.
It is easy to check that $(h \circ \sigma)(a) = h(b) = f(a)$ for every $a \in A$. Hence $f = h \circ \sigma$.
$\boxed{\text{Uniqueness}}$ Suppose $h' \colon B \to X$ is such that $f = h' \circ \sigma$. Then for each $b \in B$,

$$h'(b) = h'(\sigma(a)) = f(a) = h(b).$$

Hence $h = h'$, as desired. □

In particular, if we replace $f \colon A \to X$ with $\pi \colon A \to A/\sim$, we obtain the following result.

Corollary 3.81. *For every set X and every function $\pi \colon A \to A/\sim$ such that if $a \sim b$ then $\pi(a) = \pi(b)$, there exists a unique $h \colon B \to A/\sim$ such that*

$$\pi = h \circ \sigma.$$

$$\begin{tikzcd}
A \arrow[r, "\pi"] \arrow[d, "\sigma"'] & A/\sim \\
B \arrow[ur, dashed, "\exists! h"'] &
\end{tikzcd}$$

In the universal property (3.73), if we replace $f \colon A \to X$ with $\sigma \colon A \to B$, then we have the following:

> There exists a unique function $g \colon A/\sim \to B$ such that $\sigma = g \circ \pi$.

$$\begin{tikzcd}
A \arrow[r, "\pi"] \arrow[d, "\sigma"'] & A/\sim \arrow[dl, dashed, "\exists! g"'] \\
B &
\end{tikzcd}$$

Combining the two diagrams, we obtain the following diagram:

$$\begin{tikzcd}
A \arrow[r, "\pi"] \arrow[d, "\sigma"'] & A/\sim \arrow[dl, dashed, shift right, "\exists! g"'] \\
B \arrow[ur, dashed, shift right, "\exists! h"'] &
\end{tikzcd}$$

We construct the following diagram:

$$\begin{tikzcd}
& A \arrow[dl, "f"] \arrow[d] \arrow[dr, "f"'] \arrow[drr] & & \\
B \arrow[r, dashed, "\exists! h"'] & A/\sim \arrow[r, dashed, "\exists! g"'] & B \arrow[r, dashed, "\exists! h"'] & A/\sim
\end{tikzcd}$$

From the diagram, it follows that $g \circ h = \mathrm{id}_B$ and $h \circ g = \mathrm{id}_{A/\sim}$. Hence $h \colon B \to A/\sim$ and $g \colon A/\sim \to B$ are bijections which are inverses of each other. Therefore there is a (unique) bijection between B and $A/\sim$, i.e., $B \cong A/\sim$.

Remark. This reasoning (two objects satisfying the same universal property can be proved to be isomorphic) can be applied in other contexts.

Example. Let G be a group and $N \triangleleft G$ a normal subgroup. The quotient group G/N comes equipped with a canonical projection

$$\pi \colon G \to G/N, \qquad \pi(g) = gN.$$

It satisfies the following universal property:

> For every group H and group homomorphism $f \colon G \to H$ such that $N \subseteq \ker f$, there exists a unique group homomorphism $\bar{f} \colon G/N \to H$ such that $f = \bar{f} \circ \pi$.

$$\begin{tikzcd}
G \arrow[r, "\pi"] \arrow[d, "f"] & G/N \arrow[dl, dashed, "\bar{f}"] \\
H &
\end{tikzcd}$$

In particular, take $N = \ker f$ and $H = \operatorname{im} f$ (so that f is surjective). Then $G/N \cong \operatorname{im} f$. This is the first isomorphism theorem for groups.

— Exercises —

Exercise 3.4.1 (Lexicographic order on $\mathbb{N} \times \mathbb{N}$)**.** Define a relation $\prec$ on the Cartesian product $\mathbb{N} \times \mathbb{N}$ as follows: $(a, b) \prec (c, d)$ if and only if either $a < c$, or ($a = c$ and $b < d$). Our aim is to prove that $\prec$ is a well-order on $\mathbb{N} \times \mathbb{N}$, which would imply a corresponding induction principle.

(i) Prove that $\prec$ is transitive.

(ii) Prove that $\prec$ satisfies trichotomy.

(iii) Prove that every non-empty subset of $\mathbb{N} \times \mathbb{N}$ has a least element with respect to the ordering $\prec$.

Solution.

(i) Suppose $(a, b) \prec (c, d)$ and $(c, d) \prec (e, f)$. We want to show that $(a, b) \prec (e, f)$.

Since $(a, b) \prec (c, d)$, we have two cases:

- If $a < c$, then $(c, d) \prec (e, f)$ implies $c < e$ or ($c = e$ and $d < f$). In both cases, $a < e$. Thus $(a, b) \prec (e, f)$.
- Otherwise, $a = c$ and $b < d$. Then $(c, d) \prec (e, f)$ implies $c < e$ or ($c = e$ and $d < f$).
  - If $c < e$, then $a < e$.
  - Else if $c = e$ and $d < f$, then $a = e$ and $b < f$, so $(a, b) \prec (e, f)$.

(ii) Let $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. We want to show that exactly one of $(a, b) \prec (c, d)$ or $(a, b) = (c, d)$ or $(c, d) \prec (a, b)$ holds. We consider all possible cases:

- If $a < c$, then $(a, b) \prec (c, d)$.
- If $a > c$, then $(c, d) \prec (a, b)$.
- If $a = c$,
  - If $b < d$, then $(a, b) \prec (c, d)$.

- If $b > d$, then $(c, d) \prec (a, b)$.
- If $b = d$, then $(a, b) = (c, d)$.

(iii) Let $S \subseteq \mathbb{N} \times \mathbb{N}$ be non-empty. Consider the set of first components:

$$A = \left\{a \in \mathbb{N} \mid (a, b) \in S \text{ for some b}\right\}.$$

SInce $\mathbb{N}$ is well-ordered, A has a least element, say a_0.

Consider the set

$$S_{a_0} = \left\{b \in \mathbb{N} \mid (a_0, b) \in S\right\}.$$

Since S_{a_0} is non-empty, it has a least element b_0.

Claim: (a_0, b_0) is the least element of S under $\prec$.

To see this, for any $(a, b) \in S$, either

- $a > 0 \Rightarrow (a_0, b_0) \prec (a, b)$, or
- $a = 0$ and $b \geq b_0 \Rightarrow (a_0, b_0) \prec (a, b)$ or $(a_0, b_0) = (a, b)$.

□

Exercise 3.4.2. For each of the following properties, either give an example of a relation (on a set of your choice) with said property, or prove that for every set A, no relation on A can have said property.

(i) reflexive but neither symmetric nor transitive,

(ii) symmetric and transitive, but not reflexive,

(iii) symmetric but neither reflexive nor transitive.

Solution.

(i) On the set $A = \{1, 2, 3\}$, define the relation

$$R = \left\{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)\right\}.$$

Then R is symmetric, but not symmetric (we have $(1, 2) \in R$ but $(2, 1) \notin R$) and not transitive (we have $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$).

Alternatively, on $\mathbb{R}$, define aRb if $b - a \leq 1$.

(ii) On the set $A = \{1, 2, 3\}$, define the relation

$$\begin{aligned} R &= \{1, 2\} \times \{1, 2\} \\ &= \left\{(1, 1), (1, 2), (2, 1), (2, 2)\right\}. \end{aligned}$$

Then R is symmetric and transitive, but not reflexive because $(3, 3) \notin R$.

More generally, let A be any set and $S \subset A$ be a proper non-empty subset. Define

$$R = S \times S = \left\{(x, y) \mid x \in S,\ y \in S\right\}.$$

Then R is symmetric and transitive, but not reflexive on A (because points of $A \setminus S$ do not relate to themselves).

(iii) $\neq$ relation on $\mathbb{R}$.

Alternatively, on $\mathbb{R}$, define aRb if $|a - b| = 1$.

□

Exercise 3.4.3 (Conjugacy)**.** Fix a set X. Let S_X denote the set of all bijections from X to X. Define a relation $\sim$ on S_X as follows:

$$f \sim g \iff (\exists h \in S_x)\, g = h^{-1} \circ f \circ h.$$

Prove that $\sim$ is an equivalence relation.

Solution.

(i) Reflexivity: We have $f = \mathrm{id}_X{}^{-1} \circ f \circ \mathrm{id}_X$, so $f \sim f$.

(ii) Symmetry: Suppose $f \sim g$. Then there exists $h \in S_X$ such that $g = h^{-1} \circ f \circ h$, so $f = h \circ g \circ h^{-1}$. Since h is a bijection, h^{-1} is a bijection, so $h^{-1} \in S_X$. Thus $g \sim f$.

(iii) Transitivity: Suppose $e \sim f$ and $f \sim g$. Then there exists $h_1 \in S_X$ such that $f = h_1^{-1} \circ e \circ h_1$, and there exists $h_2 \in S_X$ such that $g = h_2^{-1} \circ f \circ h_2$. We have

$$\begin{aligned} g &= h_2^{-1} \circ f \circ h_2 \\ &= h_2^{-1} \circ (h_1^{-1} \circ e \circ h_1) \circ h_2 \\ &= (h_2^{-1} \circ h_1^{-1}) \circ e \circ (h_1 \circ h_2) \\ &= (h_1 \circ h_2)^{-1} \circ e \circ (h_1 \circ h_2). \end{aligned}$$

Thus $e \sim g$.

□

Exercise 3.4.4. For each Cartesian product $A_1 \times A_2$, define the *projection* $\pi_1 \colon A_1 \times A_2 \to A_1$ by $\pi_1(a_1, a_2) = a_1$. Similarly, define $\pi_2 \colon A_1 \times A_2 \to A_2$ by $\pi_2(a_1, a_2) = a_2$.

Prove that for any set B and any functions $p_1 \colon B \to A_1$ and $p_2 \colon B \to A_2$, there is a unique function $f \colon B \to A_1 \times A_2$ such that $p_1 = \pi_1 \circ f$ and $p_2 = \pi_2 \circ f$.

$$\begin{tikzcd}
B \arrow[dr, dashed, "\exists ! f"] \arrow[drr, bend left, "p_1"] \arrow[ddr, bend right, "p_2"'] & & \\
& A_1 \times A_2 \arrow[r, "\pi_1"] \arrow[d, "\pi_2"] & A_1 \\
& A_2 &
\end{tikzcd}$$

This exercise shows that the Cartesian product is $A_1 \times A_2$ is a universal object, since B factors through $A_1 \times A_2$.

Solution. Fix a set B and functions $p_1 \colon B \to A_1$ and $p_2 \colon B \to A_2$.

$\boxed{\text{Existence}}$ Define $f \colon B \to A_1 \times A_2$ by

$$f(b) = (p_1(b), p_2(b)).$$

We first show f is well-defined. Suppose $b = b'$. Then $f(b) = (p_1(b), p_2(b))$ and $f(b') = (p_1(b'), p_2(b'))$. Since p_1 and p_2 are well-defined, we have $p_1(b) = p_1(b')$ and $p_2(b) = p_2(b')$. Thus $(p_1(b), p_2(b)) = (p_1(b'), p_2(b'))$, so $f(b) = f(b')$.

We check that $p_1 = \pi_1 \circ f$ and $p_2 = \pi_2 \circ f$. For every $b \in B$,

$$\begin{aligned} (\pi_1 \circ f)(b) &= \pi_1(f(b)) = \pi_1(p_1(b), p_2(b)) = p_1(b) \\ (\pi_2 \circ f)(b) &= \pi_2(f(b)) = \pi_2(p_1(b), p_2(b)) = p_2(b). \end{aligned}$$

$\boxed{\text{Uniqueness}}$ Suppose $g\colon B \to A_1 \times A_2$ satisfying $p_1 = \pi_1 \circ g$ and $p_2 = \pi_2 \circ g$. For each $b \in B$, write $g(b) = (a_1', a_2')$. Then

$$\begin{aligned} a_1' &= \pi_1(g(b)) = p_1(b), \\ a_2' &= \pi_2(g(b)) = p_2(b), \end{aligned}$$

so $g(b) = (p_1(b), p_2(b)) = f(b)$. Hence $g = f$. □

Exercise 3.4.5. Suppose A is a set.

(i) Prove that for every relation R on A, there is an equivalence relation S on A such that $R \subseteq S$.

(ii) For every relation R on A, consider the relation

$$E = \bigcap \{S \subseteq A \times A : S \supseteq R \text{ and } S \text{ is an equivalence relation on } A\}.$$

Prove that E is an equivalence relation.

In fact E is the smallest equivalence relation on A that contains R; we call E the equivalence relation **generated** by R, and also say that E is the **equivalence closure** of R.

Solution.

(i) Take $S = A \times A$, which is the universal relation on A. It is easy to check that S is an equivalence relation on A.

(ii) By (i), the set

$$\mathcal{F} := \{S \subseteq A \times A : S \supseteq R \text{ and } S \text{ is an equivalence relation on } A\}$$

is non-empty, since $A \times A \in \mathcal{F}$. Then define

$$E := \bigcap_{S \in \mathcal{F}} S$$

which is well-defined, since the intersection is non-empty.

  (i) Reflexivity: For every $S \in \mathcal{F}$, S is reflexive, so $(a, a) \in S$ for every $a \in A$. Hence $(a, a) \in E$ for every $a \in A$.

  (ii) Symmetry: Suppose $(a, b) \in E$. Then $(a, b) \in S$ for every $S \in \mathcal{F}$. Since each S is symmetric, we have $(b, a) \in S$ for every $S \in \mathcal{F}$. Hence $(b, a) \in E$.

  (iii) Transitivity: Suppose $(a, b), (b, c) \in E$. Then for every $S \in \mathcal{F}$, we have $(a, b), (b, c) \in S$. Since each S is transitive, we have $(a, c) \in S$ for every $S \in \mathcal{F}$. Hence $(a, c) \in E$.

□

Exercise 3.4.6. Suppose $\sim$ is an equivalence relation on a set A. Prove that there is some set X and some function $f\colon A \to X$ such that for all $a, a' \in A$, we have $a \sim a' \iff f(a) = f(a')$.

Solution. Choose $X = A/{\sim}$ and $f\colon A \to A/{\sim}$ defined by $f(a) = [a]$.

$\boxed{\Rightarrow}$ If $a \sim a'$, then $[a] = [a']$. Hence $f(a) = f(a')$.

$\boxed{\Leftarrow}$ If $f(a) = f(a')$, then $[a] = [a']$. Hence $a \sim a'$. □

Exercise 3.4.7. Define a relation on $\mathbb{R} \times \mathbb{R} \setminus \big\{(0, 0)\big\}$ by

$$(a, b) \sim (c, d) \iff \text{there exists some nonzero } \lambda \in \mathbb{R} \text{ such that } \lambda a = c \text{ and } \lambda b = d.$$

(i) Prove that $\sim$ is an equivalence relation.

(ii) Describe the equivalence class of $(-1, 2)$. In general, what do the sets in the partition corresponding to $\sim$ look like, when interpreted as a subset of the plane $\mathbb{R}^2$?

(That is, interpret each (a, b) as the point with x-coordinate a and y-coordinate b.)

Solution.

(i) Reflexivity: $1a = a$ and $1b = b$, so $(a, b) \sim (a, b)$.

Symmetry: Suppose $(a, b) \sim (c, d)$. Then there exists $\lambda \in \mathbb{R} \setminus \{0\}$ such that $\lambda a = c$ and $\lambda b = d$. Since $\lambda \neq 0$, we have $c = \frac{1}{\lambda}a$ and $d = \frac{1}{\lambda}b$. Thus $(c, d) \sim (a, b)$.

Transitivity: Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then there exists $\lambda_1 \in \mathbb{R} \setminus \{0\}$ such that $\lambda_1 a = c$ and $\lambda_1 b = d$, and there exists $\lambda_2 \in \mathbb{R} \setminus \{0\}$ such that $\lambda_2 c = e$ and $\lambda_2 d = f$. Thus

$$(\lambda_1\lambda_2)a = e \qquad \text{and} \qquad (\lambda_1\lambda_2)b = f$$

so $(a, b) \sim (e, f)$.

(ii) We have

$$\begin{aligned}[(1,2)]_\sim &= \big\{(a,b) \mid (1,2) \sim (a,b)\big\} \\ &= \big\{(a,b) \mid (\exists\lambda \in \mathbb{R}\setminus\{0\})\ a = \lambda,\ b = 2\lambda\big\} \\ &= \big\{(\lambda, 2\lambda) \mid \lambda \in \mathbb{R}\setminus\{0\}\big\}.\end{aligned}$$

In general, every set in the partition corresponds to all points except the origin that lies on the same line that passes through the origin.

□

Exercise 3.4.8 (MA1100T AY24/25)**.** Define a relation $\sim$ on $\mathbb{N}^+$ by $a \sim b$ if and only if their product ab is a square. You may use the following fact without proof: $a \in \mathbb{N}^+$ is a square if and only if for every prime p, the exponent $e_a(p)$ of p in the prime factorisation of a is even.

(a) Prove that $\sim$ is an equivalence relation.

(b) Prove that each $\sim$-class has a unique square-free element.

Solution.

(a) Reflexivity: For every $a \in \mathbb{N}^+$, evidently a^2 is a square.

Symmetry: Suppose $a \sim b$. Then ab is a square. Since multiplication is commutative, ba is a square. Thus $b \sim a$.

Reflexivity: Suppose $a \sim b$ and $b \sim c$. Then ab and bc are squares. Thus for every prime p, $e_{ab}(p) = e_a(p) + e_b(p)$ and $e_{bc}(p) = e_b(p) + e_c(p)$ are even.

For each prime p, consider the parity of $e_b(p)$:

Case 1: If $e_b(p)$ is even, then $e_a(p)$ and $e_c(p)$ are even, so $e_{ac}(p) = e_a(p) + e_c(p)$ is even.

Case 2: If $e_b(p)$ is odd, then $e_a(p)$ and $e_c(p)$ are odd, so $e_{ac}(p) = e_a(p) + e_c(p)$ is even.

Hence ac is a square.

(b) Suppose, towards a contradiction, that some $\sim$-class $[a]_\sim$ has two distinct square-free elements b and c. Then for all primes p, we have $e_b(p), e_c(p) \leq 1$, so $e_b(p), e_c(p) \in \{0, 1\}$.

Since $b \neq c$, there exists p_0 such that $e_b(p_0) \neq e_c(p_0)$. WLOG assume $e_b(p_0) = 1$ and $e_c(p_0) = 0$.

Since $b \sim c$, bc is a square. Then $e_{bc}(p_0) = e_b(p_0) + e_c(p_0)$ is even, a contradiction.

□

Exercise 3.4.9 (MA1100T AY22/23)**.** Fix an integer $b \geq 2$. Let $\sim$ denote congruence modulo b, i.e., $a \sim a'$ if and only if b divides $a - a'$. Construct a function $f_b \colon \mathbb{Z} \to \mathbb{Z}$ satisfying all of the following:

- $\pi \circ f_b = \pi$, where $\pi \colon \mathbb{Z} \to \mathbb{Z}/\sim$ denotes the projection map
- $f_b \neq \mathrm{id}_Z$
- f_b is injective.

Solution. Define $f_b(n) = n + b$.

- To show that $\pi \circ f_b = \pi$, see that $n \sim f_b(n)$ for all $n \in \mathbb{Z}$. Thus $\pi(n) = \pi \circ f_b(n)$.
- It is clear that $f_b \neq \mathrm{id}_Z$.
- To show that f_b is injective, suppose $f_b(n) = f_b(m)$. Then $n + b = m + b$, so $n = m$ as desired.

□

Exercise 3.4.10 (MA1100 AY24/25)**.** Let $\sim$ be the relation on $\mathbb{R}^2$ defined by, for all $(a, b), (c, d) \in \mathbb{R}^2$,

$$(a, b) \sim (c, d) \iff |a| + |b| = |c| + |d|.$$

(i) Prove that $\sim$ is an equivalence relation.

(ii) Give a geometrical description of the equivalence class $[(1, 0)]$ as a subset of $\mathbb{R}^2$.

(iii) Find a bijection $g \colon \mathbb{R}^2/\sim \to [0, \infty)$.

Solution.

(i) Trivial.

(ii) We have
$$[(1, 0)] = \left\{(x, y) \in \mathbb{R}^2 : |x| + |y| = 1\right\}.$$
This is the set of all points in $\mathbb{R}^2$ whose Manhattan norm (magnitude) is 1. This describes a diamond centered at the origin with vertices at $(1, 0)$, $(0, 1)$, $(-1, 0)$, $(0, -1)$.

(iii) Since we have
$$[(a, b)] = \left\{(x, y) \in \mathbb{R}^2 : |a| + |b| = 1\right\},$$
we can define $g \colon \mathbb{R}^2/\sim \to [0, \infty)$ by
$$g([a, b]) = |a| + |b|.$$
It remains to check that g is a bijection.

□

3.5 Constructing the Familiar Numbers

3.5.1 Integers

First we want to extend our set $\mathbb{N}$ of natural numbers to a set $\mathbb{Z}$ of integers (both positive and negative). Here "extend" is to be loosely interpreted, since $\mathbb{N}$ will not actually be a subset of $\mathbb{Z}$. But $\mathbb{Z}$ will include an *isomorphic copy* of $\mathbb{N}$.

Definition 3.82. Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by

$$(m, n) \sim (p, q) \iff m + q = p + n.$$

Informally, we think about a pair (m, n) as the "difference $m - n$".

Remark. Formally, we cannot define $\sim$ using subtraction, since subtraction is not defined on $\mathbb{N}$.

Lemma 3.83. *The relation $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Proof.

(i) Reflexivity: Since $m + n = m + n$, we have $(m, n) \sim (m, n)$.

(ii) Symmetry: Suppose $(m, n) \sim (p, q)$. Then $m + q = p + n$, so $p + n = m + q$. Thus $(p, q) \sim (m, n)$.

(iii) Transitivity: Suppose $(m, n) \sim (p, q)$ and $(p, q) \sim (r, s)$. Then $m + q = p + n$ and $p + s = r + q$, so $m + q + s = p + n + s = r + n + q$ implies $m + s = r + n$. Thus $(m, n) \sim (r, s)$.

□

Definition 3.84. The set of **integers** $\mathbb{Z}$ is defined as

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim .$$

Example. The integer $2_{\mathbb{Z}}$ is the equivalence class

$$[(2, 0)] = \{(2, 0), (3, 1), (4, 2), \dots\}$$

and the integer $-3_{\mathbb{Z}}$ is the equivalence class

$$[(0, 3)] = \{(0, 3), (1, 4), (2, 5), \dots\}.$$

These equivalence classes can be pictured as 45° straight lines in the Cartesian product $\mathbb{N} \times \mathbb{N}$.

Next we want to endow $\mathbb{Z}$ with a suitable addition operation. Informally, we can add differences:

$$(m - n) + (p - q) = (m + p) - (n + q).$$

This indicates that the correct addition function $+_{\mathbb{Z}}$ for integers will satisfy the equation

$$[(m, n)] +_{\mathbb{Z}} [(p, q)] = [(m + p, n + q)].$$

In other words, for integers a and b, our addition formula is

$$a +_{\mathbb{Z}} b = [(m + p, n + q)]$$

where (m,n) is chosen from a, and (p,q) is chosen from b. We check that addition is well-defined, i.e., the equivalence class on the RHS is independent of how these choices are made.

Proof. Suppose $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$. Then

$$m + n' = m' + n \quad \text{and} \quad p + q' = p' + q.$$

Adding the two equations gives

$$m + p + n' + q' = m' + p' + n + q.$$

Hence $(m+p, n+q) \sim (m'+p', n'+q')$, as desired. □

Example. We can calculate $2_{\mathbb{Z}} +_{\mathbb{Z}} (-3_{\mathbb{Z}})$. Since $2_{\mathbb{Z}} = [(2,0)]$ and $-3_{\mathbb{Z}} = [(0,3)]$, we have

$$\begin{aligned} 2_{\mathbb{Z}} +_{\mathbb{Z}} (-3_{\mathbb{Z}}) &= [(2,0)] +_{\mathbb{Z}} [(0,3)] \\ &= [(2+0, 0+3)] \\ &= [(2,3)] \\ &= -1_{\mathbb{Z}}. \end{aligned}$$

Lemma 3.85. *Addition on $\mathbb{Z}$ is commutative and associative.*

Proof. Let $a = [(m,n)]$, $b = [(p,q)]$, $c = [(r,s)]$.

(i) This follows from commutativity of addition on $\mathbb{N}$:

$$\begin{aligned} a +_{\mathbb{Z}} b &= [(m,n)] + [(p,q)] \\ &= [(m+p, n+q)] \\ &= [(p+m, q+n)] \\ &= [(p,q)] +_{\mathbb{Z}} [(m,n)] \\ &= b +_{\mathbb{Z}} a. \end{aligned}$$

(ii) This follows from associativity of addition on $\mathbb{N}$:

$$\begin{aligned} a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c) &= [(m,n)] +_{\mathbb{Z}} ([(p,q)] +_{\mathbb{Z}} [(r,s)]) \\ &= [(m,n)] +_{\mathbb{Z}} [(p+r, q+s)] \\ &= [(m+p+r, n+q+s)] \\ &= [(m+p, n+q)] +_{\mathbb{Z}} [(r,s)] \\ &= ([(m,n)] +_{\mathbb{Z}} [(p,q)]) +_{\mathbb{Z}} [(r,s)] \\ &= (a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c \end{aligned}$$

□

Lemma 3.86. *Define $0_{\mathbb{Z}} = [(0,0)]$.*

(i) $0_{\mathbb{Z}}$ is an additive identity: $a +_{\mathbb{Z}} 0_{\mathbb{Z}} = a$ for every $a \in \mathbb{Z}$.

(ii) Additive inverses exist: for every $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$.

Proof. Let $a = [(m,n)]$.

(i) $a +_{\mathbb{Z}} = [(m,n)] + [(0,0)] = [(m+0, n+0)] = [(m,n)] = a$.

(ii) Take $b = [(n,m)]$. Then $a +_{\mathbb{Z}} b = [(m,n)] + [(n,m)] = [(m+n, n+m)] = [(0,0)] = 0_{\mathbb{Z}}$.

Moreover, inverses are unique. Suppose $a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$ and $a +_{\mathbb{Z}} b' = 0_{\mathbb{Z}}$. Then

$$b = b +_{\mathbb{Z}} (a +_{\mathbb{Z}} b') = (b +_{\mathbb{Z}} a) +_{\mathbb{Z}} b' = b'.$$

□

The inverse of a is denoted as $-a$. Then the proof above shows that $-[(m,n)] = [(n,m)]$. Inverses provide us with a **subtraction** operation, which we define by $b - a = b +_{\mathbb{Z}} (-a)$.

We can also endow $\mathbb{Z}$ with a **multiplication** operation, which we obtain in much the same way as we obtained the addition operation. First we look at the informal calculation with differences

$$(m-n)\cdot(p-q) = (mp+nq) - (mq+np),$$

which tells us that the desired operation $\cdot_{\mathbb{Z}}$ will satisfy the equation

$$[(m,n)] \cdot_{\mathbb{Z}} [(p,q)] = [(mp+nq, mq+np)].$$

We check that multiplication is well-defined.

Proof. Suppose $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$. Then

$$m + n' = m' + n \tag{1}$$

$$p + q' = p' + q \tag{2}$$

and we want to obtain the equation

$$mp + nq + m'q' + n'p' = m'p' + n'q' + mq + np.$$

The idea is take multiples of (1) and (2) that contain the terms we need.

First multiply (1) by p; this gives us mp on LHS and np on RHS. Second, multiply the reverse of (1) by q; this gives us nq on LHS and mq on RHS. Third, multiply (2) by m'. Fourth, multiply the reverse of (2) by n'.

Now add the four equations we have obtained from (1) and (2). All the unwanted terms cancel, and we are left with the desired equation. □

Lemma 3.87. *Multiplication on $\mathbb{Z}$ is commutative, associative, and distributive over addition.*

Proof. Let $a = [(m,n)]$, $b = [(p,q)]$, $c = [(r,s)]$.

(i) We have

$$\begin{aligned} a \cdot_{\mathbb{Z}} b &= [(mp+nq, mq+np)], \\ b \cdot_{\mathbb{Z}} a &= [(pm+qn, pn+qm)]. \end{aligned}$$

The equality of these two follows from the commutativity of addition and multiplication on $\mathbb{N}$.

(ii) We have

$$\begin{aligned} (a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c &= [((mp+nq)r + (mq+np)s, (mp+nq)s + (mq+np)r)], \\ a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c) &= [(m(pr+qs) + n(ps+qr), m(ps+qr) + n(pr+qs))]. \end{aligned}$$

The equality of these follows laws of arithmetic on $\mathbb{N}$.

(iii) Expanding gives

$$\begin{aligned} a \cdot_{\mathbb{Z}} (b +_{\mathbb{Z}} c) &= [(m(p+r)+n(q+s), m(q+s)+n(p+r))], \\ a \cdot_{\mathbb{Z}} b +_{\mathbb{Z}} a \cdot_{\mathbb{Z}} c &= [(mp+nq+mr+ns, mq+np+ms+nr)]. \end{aligned}$$

Again equality is clear from laws of arithmetic on $\mathbb{N}$.

□

Lemma 3.88. *Define* $1_{\mathbb{Z}} = [(1,0)]$.

(i) $1_{\mathbb{Z}}$ *is a multiplicative identity:* $a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = a$ *for every* $a \in \mathbb{Z}$.

(ii) $0_{\mathbb{Z}} \neq 1_{\mathbb{Z}}$.

(iii) There are no zero divisors in $\mathbb{Z}$*: if* $a \cdot_{\mathbb{Z}} b = 0_{\mathbb{Z}}$*, then either* $a = 0_{\mathbb{Z}}$ *or* $b = 0_{\mathbb{Z}}$.

Proof.

(i) Trivial calculation.

(ii) It is necessary to check that $(0,0) \not\sim (1,0)$. This reduces to checking that $0 \neq 1$ in $\mathbb{N}$, which is true.

(iii) We prove the contrapositive. Suppose $a \neq 0_{\mathbb{Z}}$ and $b \neq 0_{\mathbb{Z}}$. Write $a = [(m,n)]$, $b = [(p,q)]$. Then

$$a \cdot_{\mathbb{Z}} b = [(mp+nq, mq+np)].$$

Since $a \neq [(0,0)]$, we have $m \neq n$, so either $m < n$ or $n < m$. Similarly, either $p < q$ or $q < p$. This leads to a total of four cases, but in each case we have

$$mp + nq \neq mq + np.$$

Hence $a \cdot_{\mathbb{Z}} b \neq [(0,0)]$.

□

In algebraic terminology, we can say that $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, 0_{\mathbb{Z}}, 1_{\mathbb{Z}})$ forms an **integral domain**. This means that:

1. $\mathbb{Z}$ with $+_{\mathbb{Z}}$ and $0_{\mathbb{Z}}$ forms an Abelian group.
2. Multiplication is commutative, associative, and distributive over addition.
3. $1_{\mathbb{Z}}$ is a multiplicative identity (different from $0_{\mathbb{Z}}$), and no zero divisors exist.

Next we develop an ordering relation $<_{\mathbb{Z}}$ on the integers. The informal calculation

$$m - n < p - q \iff m + q < p + n$$

indicates that ordering $<_{\mathbb{Z}}$ on $\mathbb{Z}$ should be defined by

$$[(m,n)] <_{\mathbb{Z}} [(p,q)] \iff m + q < p + n.$$

As usual, it is necessary to check that this condition yields a well-defined relation on the integers.

Proof. Suppose $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$. Then

$$m + n' = m' + n \quad \text{and} \quad p + q' = p' + q.$$

Adding n' and q' to each side of the inequality gives

$$\begin{aligned} m + q < p + n &\iff m + q + n' + q' < p + n + n' + q' \\ &\iff m' + n + q + q' < p' + q + n + n' \\ &\iff m' + q' < p' + n' \end{aligned}$$

where the middle step uses the given equations. □

Lemma 3.89. *$<_{\mathbb{Z}}$ is an order on $\mathbb{Z}$.*

Proof. Let $a = [(m, n)]$, $b = [(p, q)]$, $c = [(r, s)]$.

Transitivity: We have

$$\begin{aligned} a <_{\mathbb{Z}} b \quad \text{and} \quad b <_{\mathbb{Z}} c &\implies m + q < p + n \quad \text{and} \quad p + s < r + q \\ &\implies m + q + s < p + n + s \quad \text{and} \quad p + s + n < r + q + n \\ &\implies m + q + s < r + q + n \\ &\implies m + s < r + n \\ &\implies a <_{\mathbb{Z}} c. \end{aligned}$$

Trichotomy: To say that exactly one of

$$a <_{\mathbb{Z}} b, \quad a = b, \quad b <_{\mathbb{Z}} a$$

holds is to say that exactly one of

$$m + q < p + n, \quad m + q = p + n, \quad p + n < m + q$$

holds. Thus the result follows from trichotomy in $\mathbb{N}$.

□

An integer b is called **positive** if $0_{\mathbb{Z}} <_{\mathbb{Z}} b$. It is easy to check that $b <_{\mathbb{Z}} 0_{\mathbb{Z}} \iff 0_{\mathbb{Z}} <_{\mathbb{Z}} -b$. Thus a consequence of trichotomy is the fact that for an integer b, exactly one of

$$b \text{ is positive}, \quad b \text{ is zero}, \quad -b \text{ is positive}$$

holds.

Lemma 3.90. *Addition preserves order, as does multiplication by a positive integer:*

(i) $a <_{\mathbb{Z}} b \iff a +_{\mathbb{Z}} c <_{\mathbb{Z}} b +_{\mathbb{Z}} c$.

(ii) If c is positive, then $a <_{\mathbb{Z}} b \iff a \cdot_{\mathbb{Z}} c <_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c$.

Proof. Let $a = [(m, n)]$, $b = [(p, q)]$, $c = [(r, s)]$.

(i) The result to be proved translates to

$$m + q < p + n \iff m + r + q + s < p + r + n + s.$$

This is an immediate consequence of the fact that addition on $\mathbb{N}$ preserves order.

(ii) It suffices to prove $\boxed{\Rightarrow}$. This translates to

$$s < r \text{ and } m + q < p + n \implies mr + ns + ps + qr < pr + qs + ms + nr.$$

Let $k = m + q$ and $l = p + n$. Then the above becomes

$$s < r \text{ and } k < l \implies kr + ls < ks + lr.$$

□

Corollary 3.91. *For any integers a, b, c, the cancellation laws hold:*

(i) If $a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c$, then $a = b$.

(ii) If $c \neq 0_{\mathbb{Z}}$, $a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c$, then $a = b$.

Although $\mathbb{N}$ is not actually a subset of $\mathbb{Z}$, nonetheless $\mathbb{Z}$ has a subset that is "just like" $\mathbb{N}$. To make this precise, define the function $E \colon \mathbb{N} \to \mathbb{Z}$ by

$$E(n) = [(n, 0)].$$

The following result, in algebraic terminology, says that E is an **isomorphic embedding** of $\mathbb{N}$ into $\mathbb{Z}$; that is, E is an injection that preserves addition, multiplication, and order.

Lemma 3.92. *E is injective, and for every $m, n \in \mathbb{N}$,*

(i) $E(m + n) = E(m) +_{\mathbb{Z}} E(n)$.

(ii) $E(mn) = E(m) \cdot_{\mathbb{Z}} E(n)$.

(iii) $m < n \iff E(m) <_{\mathbb{Z}} E(n)$.

Proof. To show that E is injective, we calculate

$$\begin{aligned} E(m) = E(n) &\implies [(m, 0)] = [(n, 0)] \\ &\implies (m, 0) \sim (n, 0) \\ &\implies m = n. \end{aligned}$$

Parts (i), (ii), and (iii) are proved by routine calculations. □

Notation. Henceforth we will streamline our notation by omitting the subscript "$\mathbb{Z}$" on $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$, $<_{\mathbb{Z}}$, $0_{\mathbb{Z}}$, $1_{\mathbb{Z}}$ etc. Furthermore $a \cdot b$ will usually be written as just ab.

3.5.2 Rational Numbers

The extension from $\mathbb{Z}$ to $\mathbb{Q}$ is to multiplication what the extension from $\mathbb{N}$ to $\mathbb{Z}$ is to addition. In the integers we get additive inverses; in the rationals we will get multiplicative inverses.

By a **fraction** we mean an ordered pair of integers, the second component of which (called the denominator) is non-zero. For example, $(1, 2)$ and $(6, 12)$ are fractions.

We want a suitable equivalence relation $\sim$ for which $(1, 2) \sim (6, 12)$. Since $a/b = c/d$ iff $ad = bc$, we choose to define $\sim$ as follows.

Definition 3.93. Define a relation on $\mathbb{Z} \times \mathbb{Z}^*$, where $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$:

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

Lemma 3.94. *The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$.*

Proof.

(i) Reflexivity: Obvious.

(ii) Symmetry: Obvious.

(iii) Transitivity: Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. Multiply the first equation by f and the second by b to get

$$adf = cbf = edb.$$

Thus $adf = edb$. By cancelling the non-zero d, we get $af = be$. Hence $(a, b) \sim (e, f)$.

□

Definition 3.95. The set of **rational numbers** $\mathbb{Q}$ is the set of all equivalence classes of fractions:

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^* / \sim .$$

We arrive at addition and multiplication operations for $\mathbb{Q}$ by the same methods used for $\mathbb{Z}$. For addition, the informal calculation

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

indicates that addition should be defined as

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

Note that $bd \neq 0$ since $b \neq 0$ and $d \neq 0$. Hence $(ad + bc, bd)$ is a fraction. As usual, we must check that addition is well-defined.

Proof. Suppose $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Then $ab' = a'b$ and $cd' = c'd$.
We want the equation

$$(ad + cb)b'd' = (a'd' + c'b')bd,$$

which, when expanded, becomes

$$ab'dd' + bb'cd' = a'bdd' + bb'c'd.$$

□

Example. Let $2_{\mathbb{Q}} = [(2, 1)]$ and $4_{\mathbb{Q}} = [(4, 1)]$. Then

$$\begin{aligned} 2_{\mathbb{Q}} +_{\mathbb{Q}} 2_{\mathbb{Q}} &= [(2, 1)] +_{\mathbb{Q}} [(2, 1)] \\ &= [(2 + 2, 1)] \\ &= [(4, 1)] = 4_{\mathbb{Q}} \end{aligned}$$

where we use the fact that $2 + 2 = 4$ in $\mathbb{Z}$.

Lemma 3.96. *$\mathbb{Q}$ is an Abelian group under addition.*

(i) Addition is associative and commutative.

(ii) $0_{\mathbb{Q}}$ is an identity element: $r +_{\mathbb{Q}} 0_{\mathbb{Q}} = r$ for all $r \in \mathbb{Q}$.

(iii) Additive inverses exist: for every $r \in \mathbb{Q}$, there exists $s \in \mathbb{Q}$ such that $r +_{\mathbb{Q}} s = 0_{\mathbb{Q}}$.

Proof.

(i)

(ii)

(iii)

□

Proposition 3.97. *$\mathbb{Q}$ is a field, with addition and multiplication defined on $\mathbb{Q}$ as*

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

Define ordering on $\mathbb{Q}$ as

$$\frac{a}{b} < \frac{c}{d} \iff \begin{cases} ad < bc & (b, d > 0 \text{ or } b, d < 0) \\ ad > bc & (b > 0 \text{ and } d < 0, \text{ or } b < 0 \text{ and } d > 0) \end{cases}$$

Finally, we want to show that, although $\mathbb{Z}$ is not a subset of $\mathbb{Q}$, nevertheless $\mathbb{Q}$ has a subset that is "just like" $\mathbb{Z}$. Define the embedding $E \colon \mathbb{Z} \to \mathbb{Q}$ by

$$E(a) = [(a, 1)].$$

This function gives us an isomorphic embedding in the sense that the following theorem holds.

Lemma 3.98. *E is an injection satisfying the following conditions:*

(i) $E(a + b) = E(a) +_{\mathbb{Q}} E(b)$.

(ii) $E(ab) = E(a) \cdot_{\mathbb{Q}} E(b)$.

(iii) $E(0) = 0_{\mathbb{Q}}$ and $E(1) = 1_{\mathbb{Q}}$.

(iv) $a < b \iff E(a) <_{\mathbb{Q}} E(b)$.

Proof. We first check that E is injective:

$$\begin{aligned} E(a) = E(b) &\implies [(a,1)] = [(b,1)] \\ &\implies (a,1) \sim (b,1) \\ &\implies a = b. \end{aligned}$$

(i) $E(a) +_{\mathbb{Q}} E(b) = [(a, 1)] +_{\mathbb{Q}} [(b, 1)] = [(a + b, 1)] = E(a, b)$.

(ii) $E(a) \cdot_{\mathbb{Q}} E(b) = [(a, 1)] \cdot_{\mathbb{Q}} [(b, 1)] = [(ab, 1)] = E(ab)$.

(iii) This is a restatement of the definitions of $0_{\mathbb{Q}}$ and $1_{\mathbb{Q}}$.

(iv) $E(a) <_{\mathbb{Q}} E(b) \iff [(a,1)] <_{\mathbb{Q}} [(b,1)] \iff a \cdot 1 < b \cdot 1 \iff a < b$.

□

Notation. Henceforth we will simplify the notation by omitting the subscript $\mathbb{Q}$ on $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$, $0_{\mathbb{Q}}$, and so forth. Also the product $r \cdot s$ will usually be written as just rs.

— Exercises —

Exercise 3.5.1. Define an equivalence relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by

$$(m,n) \sim (p,q) \iff m+q = p+n.$$

(This is the equivalence relation used to define $\mathbb{Z}$ from $\mathbb{N}$ in set theory, but the context of this question is different. In particular, we freely assume basic properties of $\mathbb{Z}$, subtraction, absolute value, etc.)

(i) We attempt to define a function $f\colon (\mathbb{N} \times \mathbb{N})/\sim \to \mathbb{N}$ by $f([(m,n)]_\sim) = m+n$. Prove that f is **not** well-defined.

(ii) We attempt to define a function $g\colon (\mathbb{N} \times \mathbb{N})/\sim \to \mathbb{N}$ by $g([(m,n)]_\sim) = |m-n|$. Prove that g is well-defined.

Solution.

(i) We have $(m,n), (m+1,n+1) \in [(m,n)]$. But $f([m,n]) = m+n$ and $f([m+1,n+1]) = m+n+2$.

(ii) Suppose $(m_1,n_1), (m_2,n_2) \in [(m,n)]$. Then $(m_1,n_1) \sim (m,n)$, so $m_1 - n_1 = m - n$. Similarly, $(m_2,n_2) \sim (m,n)$, so $m_2 - n_2 = m - n$. Thus

$$g([m_1,n_1]) = |m_1 - n_1| = |m-n| = |m_2 - n_2| = g([m_2,n_2]).$$

□

Exercise 3.5.2 (Complex numbers)**.** On the set of real polynomials $\mathbb{R}[x]$, define

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

The set of complex numbers is defined as

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

Thus 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.

Solution.

(a) For two equivalence classes $[f(x)]$ and $[g(x)]$ in $\mathbb{C}$, define

$$[f(x)] + [g(x)] := [f(x) + g(x)]$$
$$[f(x)] \cdot [g(x)] := [f(x)g(x)]$$

We first show addition is well-defined. Suppose $f_1(x) \sim f_2(x)$ and $g_1(x) \sim g_2(x)$. Then $x^2+1 \mid f_1(x) - f_2(x)$ and $x^2+1 \mid g_1(x) - g_2(x)$. Thus

$$(f_1 + g_1) - (f_2 + g_2) = (f_1 - f_2) + (g_1 - g_2),$$

which is divisible by x^2+1 since both terms are. Hence $f_1 + g_1 \sim f_2 + g_2$.

Next we show multiplication is well-defined. We compute

$$f_1 g_1 - f_2 g_2 = (f_1 - f_2) g_1 + f_2 (g_1 - g_2).$$

Since x^2+1 divides both $f_1 - f_2$ and $g_1 - g_2$, and the ring $\mathbb{R}[x]$ is closed under multiplication, it follows that x^2+1 divides RHS. Hence $f_1 g_1 \sim f_2 g_2$.

By the division theorem, every polynomial $f(x) \in \mathbb{R}[x]$ can be divided by x^2+1 to obtain

$$f(x) = q(x)(x^2+1) + (a + bx)$$

for some unique $a, b \in \mathbb{R}$. Hence each equivalence class $[f(x)]$ has a unique representative of the form $[a + bx]$. We therefore identify $a + bi$ with the class $[a + bx]$, where i denotes the class of $[x]$. Then under this identification,

$$(a+bi)(c+di) = (a+c) + (b+d)i$$
$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

since $i^2 = [x] \cdot [x] = [-1] = -1$.

(b) Let $z = a + bi = [a + bx]$, where not both a and b are zero. We wish to find z^{-1}.

We seek another element $[c + dx]$ such that

$$[a + bx][c + dx] = [1].$$

Computing in $\mathbb{R}[x]/(x^2+1)$:

$$(a + bx)(c + dx) = (ac - bd) + (ad + bc)x.$$

Then

$$\begin{cases} ac - bd = 1 \\ ad + bc = 0 \end{cases}$$

Solving for c and d gives $c = \dfrac{a}{a^2+b^2}$, $d = \dfrac{-b}{a^2+b^2}$. Hence $z^{-1} = [c + dx] = \left[\dfrac{a - bx}{a^2+b^2}\right]$. Equivalently,

$$(a+bi)^{-1} = \frac{a - bi}{a^2+b^2}.$$

□

4
Cardinality and Choice

4.1 Equinumerous Sets

Definition 4.1. Two sets X and Y are **equinumerous**, denoted $X \approx Y$, if there exists a bijection from X to Y.

Proposition 4.2. $\approx$ *is reflexive, symmetric and transitive.*

Proof.

(i) Reflexivity: The identity map gives a bijection from a set to itself.

(ii) Symmetry: Suppose $f\colon X \to Y$ is a bijection. Then f is invertible, with inverse $f^{-1}\colon Y \to X$. Since f^{-1} is invertible (with inverse f), it is bijective.

(iii) Transitivity: Suppose $f\colon X \to Y$ and $g\colon Y \to Z$ are bijections, and thus they are invertible. Then $g \circ f$ is invertible and thus bijective.

□

Remark. $\approx$ is not an (equivalence) relation. If $\approx$ were a relation, then it is defined on the "set" of all sets, which is not a set.

Example. The following are some examples of bijections (presented without proof).

- The tangent function restricted to the interval $\big(-\pi/2, \pi/2\big)$ is a bijection from $(-\pi/2, \pi/2)$ to $\mathbb{R}$.
- The exponential function is a bijection from $\mathbb{R}$ to $\mathbb{R}^+$.
- The function $x \mapsto 2x$ defines a bijection from $\mathbb{Z}$ to the set of even integers $2\mathbb{Z}$.
- The function $x \mapsto x + 1$ defines a bijection from $\mathbb{N}$ to $\mathbb{N}^+$.
- We can define a bijection from $\mathbb{N}^+$ to $\mathbb{Z}$:

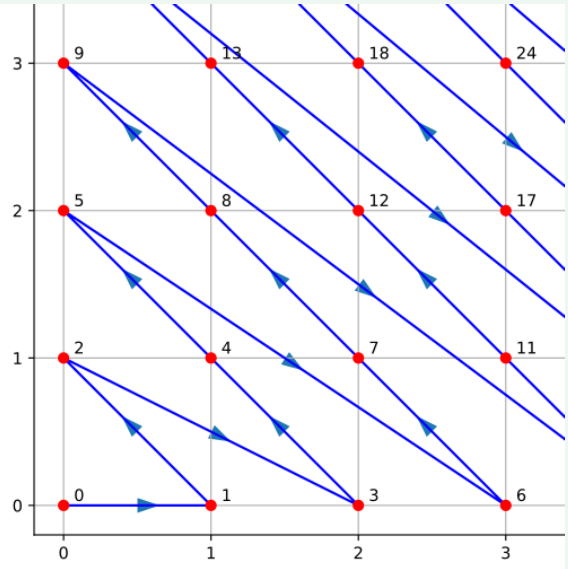
$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even,} \\[2ex] \dfrac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

$$\begin{array}{cccccccccc} \mathbb{N}^+ & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \mathbb{Z} & 0 & 1 & -1 & 2 & -2 & 3 & -3 & \cdots \end{array}$$

- We can define a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$:

$$f(a,b) = \frac{1}{2}(a+b)(a+b+1) + b.$$

This is known as *Cantor's paring function.*



Hence we have

$$\mathbb{R} \approx \mathbb{R}^+ \approx (-\pi/2, \pi/2)$$
$$2\mathbb{Z} \approx \mathbb{Z} \approx \mathbb{N} \approx \mathbb{N}^+ \approx \mathbb{N} \times \mathbb{N}.$$

Notice many of the above sets are equinumerous with some proper subset of themselves. (Later we will show that such sets are infinite sets.)

In light of the examples presented up to now, you might well ask whether any two infinite sets are equinumerous. Such is not the case; some infinite sets are much larger than others.

Cantor's theorem states that no set is equinumerous with its power set:

Theorem 4.3 (Cantor's theorem)**.** *For every set X, we have $X \not\approx \mathcal{P}(X)$.*

Proof. Let $f\colon X \to \mathcal{P}(X)$ be an arbitrary function. We will construct a subset of X that is not in the range of f. Specifically, let

$$A := \{x \in X \mid x \notin f(x)\} \in \mathcal{P}(X).$$

Suppose, towards a contradiction, that f is surjective. Then there exists $x \in X$ such that $f(x) = A$. We consider if $x \in A$ or not:

Case 1: If there exists $x \in A$ such that $f(x) = A$, then $x \in f(x)$, so by construction $x \notin A$.

Case 2: If there exists $x \notin A$ such that $f(x) = A$, then $x \notin f(x)$, so by construction $x \in A$.

Hence we have $x \in A \iff x \notin A$, a contradiction. □

However there exists an injection from X to $\mathcal{P}(X)$, which is the map $x \mapsto \{x\}$.

— Exercises —

Exercise 4.1.1 ([End77])**.** Find a one-to-one correspondence between the open unit interval $(0,1)$ and $\mathbb{R}$ that takes rationals to rationals and irrationals to irrationals.

Solution. The idea is to modify the function $x \mapsto \frac{1}{x}$.
Define $f\colon (0,1) \to \mathbb{R}$ by

$$f(x) = \begin{cases} \frac{1}{x} - 2 & \text{if } x \in \left(0, \frac{1}{2}\right], \\ 2 - \frac{1}{1-x} & \text{if } x \in \left(\frac{1}{2}, 1\right). \end{cases}$$

□

Exercise 4.1.2 ([End77])**.** Prove that $[0,1] \approx (0,1)$.

Solution. Define $f\colon [0,1] \to (0,1)$ by

$$f(x) = \begin{cases} \frac{1}{2} & \text{if } x = 0 \\ \frac{1}{4}x & \text{if } x = \frac{1}{2^n} \text{ for some } n \in \mathbb{N}^+ \\ x & \text{otherwise} \end{cases}$$

That is, f shifts $0 \mapsto 1/2$, $1 \mapsto 1/4$, and $1/2 \mapsto 1/8$, $1/4 \mapsto 1/16$, $\ldots$; all other points are unchanged. It then remains to check that f is a bijection. (Since f is a piecewise function, consider cases.) □

Exercise 4.1.3. Let A be an infinite set. Prove that for every finite $X \subseteq A$, there is some finite $Y \subseteq A$ such that $X \subsetneq Y$.

Solution. Let A be infinite and let $X \subseteq A$ be finite. Note that $X \neq A$, so $X \subsetneq A$, i.e., $A \setminus X$ is non-empty. Fix $a \in A \setminus X$. Define

$$Y = X \cup \{a\}.$$

Since X is finite and $\{a\}$ is finite, their union Y is finite. Since $a \in Y$ but $a \notin X$, we have $X \subsetneq Y$. □

Exercise 4.1.4. Fix a set C. A function $F\colon \mathcal{P}(C) \to \mathcal{P}(C)$ is said to be *monotone* if $X \subseteq Y \subseteq C$ implies $F(X) \subseteq F(Y)$.
(For example, if c is a fixed element of C, then the function $X \mapsto X \setminus \{c\}$ is monotone. Note that in the definition of monotone, we do not require that $F(X) \subseteq F(Y)$ implies $X \subseteq Y$. We do not require that $X \subseteq F(X)$ either.)
If F is monotone, define

$$S = \bigcap \{X \subseteq C : F(X) \subseteq X\}.$$

(i) Prove that the above intersection is well-defined.

(ii) Prove that $F(S) = S$.

(iii) Suppose $A \subseteq B \subseteq C$ and that $f\colon C \to A$ is a bijection. Prove that the function $F\colon \mathcal{P}(C) \to \mathcal{P}(C)$ defined by $F(X) = (C \setminus B) \cup f[X]$ is monotone.

(iv) By the previous parts, we know there is some set $S \subseteq C$ such that $S = (C \setminus B) \cup f[S]$. Use S to construct a bijection $g\colon C \to B$.

(Hint: Given $x \in C$, consider cases depending on whether $x \in S$.)

Solution. Let $\mathcal{A} = \{X \subseteq C : F(X) \subseteq X\}$. Then $S = \bigcap \mathcal{A}$.

(i) Since F maps into $\mathcal{P}(C)$, we have $F(C) \subseteq C$, so $C \in \mathcal{A}$. Hence $\mathcal{A}$ is non-empty.

(ii) $\boxed{\subseteq}$ Let $X \in \mathcal{A}$. Then $F(X) \subseteq X$.

Since $S \subseteq X$, by monotonicity, we obtain $F(S) \subseteq F(X)$. Thus $F(S) \subseteq F(X) \subseteq X$.

Since this holds for every $X \in \mathcal{A}$, taking the intersection over all $X \in \mathcal{A}$ yields $F(S) \subseteq \bigcap \mathcal{A} = S$. Hence $F(S) \subseteq S$.

$\boxed{\supseteq}$ Since $F(S) \subseteq S$ (as shown above), monotonicity implies that $F(F(S)) \subseteq F(S)$. Hence $F(S) \in \mathcal{A}$.

But S is the intersection of all members of $\mathcal{A}$, so we must have $S \subseteq F(S)$.

(iii) If $X \subseteq Y \subseteq C$, then $f[X] \subseteq f[Y]$, so

$$F(X) = (C \setminus B) \cup f[X] \subseteq (C \setminus B) \cup f[Y] = F(Y).$$

Hence F is monotone.

(iv) Define $g\colon C \to B$ by

$$g(x) = \begin{cases} f(x) & \text{if } x \in S, \\ x & \text{if } x \notin S. \end{cases}$$

(Elements of S are sent into A, while elements not in S are left fixed.)

We check that g is a bijection from C to B:

Injectivity: Suppose $g(x) = g(y)$.

- If $x \notin S$, then $g(x) = x$. So $g(y) = x$. If $y \in S$ then $g(y) = f(y) \in f[S]$, but $x \notin S$ implies $x \notin f[S]$ (since $C \setminus S \subseteq B \setminus f[S]$), a contradiction. Hence $y \notin S$ and then $g(y) = y = x$.
- If $x \in S$ and $y \in S$, then $g(x) = f(x) = f(y) = g(y)$. Since f is injective, $x = y$.
  If $x \in S$ and $y \notin S$, then $g(x) = f(x) \in f[S]$ while $g(y) = y \in C \setminus S \subseteq B \setminus f[S]$, so equality is impossible.

Surjectivity: Let $b \in B$.

- If $b \notin S$, then $b \in C \setminus S$ and by definition $g(b) = b$.
- If $b \in S$, then $b \notin C \setminus B$ (since $b \in B$), so from $S = (C \setminus B) \cup f[S]$ we conclude $b \in f[S]$; thus there exists $s \in S$ with $f(s) = b$ and then $g(s) = f(s) = b$.

□

4.2 Finite Sets

Recall that $[n] = \{0, 1, \dots, n-1\}$.

Definition 4.4. A set X is **finite** if $X \approx [n]$ for some $n \in \mathbb{N}$. Otherwise, X is **infinite**.

Remark. Notice that whenever we list a finite set $X = \{x_0, x_1, \dots, x_{n-1}\}$ without repetition, we are in fact choosing a bijection between X and $[n]$, defined by $x_i \mapsto i$ for $i = 0, 1, \dots, n-1$.

Proposition 4.5. *Let A be a non-empty set. Then the following are equivalent:*

(i) A is finite.

(ii) There is a surjection from a section of $\mathbb{N}$ onto A.

(iii) There is an injection from A into a section of $\mathbb{N}$.

Proof.
$\boxed{\text{(i)} \Rightarrow \text{(ii)}}$ Let A be finite. Fix a bijection $f\colon [n] \to A$ for some $n \in \mathbb{N}$, which is surjective.

$\boxed{\text{(ii)} \Rightarrow \text{(iii)}}$ Suppose $f\colon [n] \to A$ is surjective. Define $g\colon A \to [n]$ by

$$g(a) = \min f^{-1}(a) \qquad (a \in A).$$

Since f is surjective, the set $f^{-1}(a)$ is non-empty; by the well-ordering principle, $g(a)$ exists and is uniquely defined.

Suppose $a \neq a'$. Then $f^{-1}(a)$ and $f^{-1}(a')$ are disjoint, so their smallest elements must be different. Hence g is injective.

$\boxed{\text{(iii)} \Rightarrow \text{(i)}}$ Suppose $g\colon B \to \mathbb{N}_n$ is injective. Then changing the range of g gives a bijection of B with a subset of $\mathbb{N}_n$. It follows from the preceding corollary that B is finite. □

Proposition 4.6. *If X is finite and $f\colon X \to X$ is surjective, then f is injective.*

Proof. Let X be a finite set, and $f\colon X \to X$ is surjective.

Suppose, towards a contradiction, that f is not injective. Then there exist distinct $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Consider the function $g\colon X \setminus \{x_1\} \to X$ defined by

$$g = f|_{X \setminus \{x_1\}}.$$

Then g is surjective.

But g is a surjective function from a set of size $|X| - 1$ onto a set of size $|X|$. This is impossible for finite sets, since a surjection cannot map a smaller finite set onto a larger one. □

4.2.1 Pigeonhole Principle

Theorem 4.7 (Pigeonhole principle)**.** *Every injection $f\colon [n] \to [n]$ must be surjective.*

Here the domain $[n]$ represents the **pigeons**, the codomain $[n]$ represents the **pigeonholes**, and the function f assigns each pigeon to a hole. If f is injective, no two pigeons occupy the same hole. Since there are exactly n pigeons and n holes, each hole must contain one pigeon; thus f is surjective.

Proof. Induct on $n \in \mathbb{N}$.

$\boxed{\text{Base case}}$ Every function from $[0] = \emptyset$ to $[0] = \emptyset$ is (vacuously) surjective.

$\boxed{\text{Inductive step}}$ Suppose $n \in \mathbb{N}$ is such that every injection $f\colon [n] \to [n]$ is surjective. Consider an injection $f\colon [n+1] \to [n+1]$.

We consider which element is mapped to n:

Case 1: For all $m \in [n]$, $f(m) \neq n$. Then the restriction $f|_{[n]}$ is an injection from $[n]$ to $[n]$. By inductive hypothesis, $f|_{[n]}$ is surjective.

Since f is injective, $f(n)$ must be in $[n+1] \setminus [n] = \{n\}$, so $f(n) = n$. Hence f is surjective.

Case 2: Otherwise, there exists $m \in [n]$ such that $f(m) = n$. By injectivity of f, we have $f(n) \neq n$, so $f(n) \in [n]$. Define $g\colon [n] \to [n]$ by

$$g(k) = \begin{cases} f(n) & \text{if } f(k) = n \\ f(k) & \text{otherwise} \end{cases}$$

One can check that g is injective. By inductive hypothesis, g is surjective. Hence f is surjective.

□

Therefore, to check if a function from a *finite* set to itself is bijective, it suffices to check either injectivity or surjectivity.

Corollary 4.8. *No finite set is equinumerous to a proper subset of itself.*

Proof. Let B be a finite set, and $A \subsetneq B$. Let $f\colon B \to A$ is an arbitrary function; we will show that f is not injective.

Suppose, towards a contradiction, that f is injective. Suppose $|B| = n$; fix a bijection $g\colon B \to [n]$. Since g and g^{-1} are bijective, and f is injective, it follows that the composition

$$g \circ f \circ g^{-1}\colon [n] \to [n]$$

is injective. By the pigeonhole principle, $g \circ f \circ g^{-1}$ is surjective.

Since $A \subsetneq B$, fix $b \in B \setminus A$. Since $g(b) \in [n]$, and $g \circ f \circ g^{-1}$ is surjective, there exists $m \in [n]$ such that $g(f(g^{-1}(m))) = g(b)$. Since g is injective, we get $f(g^{-1}(m)) = b$.

But $\operatorname{range}(f) \subseteq A$, so $b \notin \operatorname{range}(f)$, yielding a contradiction.

Since there does not exist injections from B to A, there does not exist bijections from B to A. □

Corollary 4.9. *If a set is equinumerous to a proper subset of itself, then it is infinite.*

Hence $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{R}$ are infinite, since $\mathbb{N} \approx \mathbb{N}^+$, $\mathbb{Z} \approx 2\mathbb{Z}$, and $\mathbb{R} \approx \mathbb{R}^+$.

4.2.2 Cardinality

Corollary 4.10. *Every finite set is equinumerous to a unique* $[n]$.

Proof. Suppose, towards a contradiction, that $|A| = m$ and $|A| = n$ for some distinct $m, n \in \mathbb{N}$. Fix bijections $f\colon A \to [n]$ and $g\colon A \to [m]$.

WLOG assume $m < n$. Then $g \circ f^{-1}\colon [n] \to [m]$ is a bijection of the finite set $[n]$ with a proper subset of itself, a contradiction. □

The preceding result allows us to make the following definition:

Definition 4.11. Let A be a finite set. If $A \approx [n]$, we say that the **cardinality** of A is $|A| = n$.

We first show that subsets of $[n]$ are finite.

Lemma 4.12. *If $A \subsetneq [n]$, then A is finite and $|A| < n$.*

Proof. Induct on $n \in \mathbb{N}$.

$\boxed{\text{Base case}}$ $[0] = \emptyset$ has no proper subsets, so the desired result is vacuously true.

$\boxed{\text{Inductive step}}$ Suppose every proper subset of $[n]$ is equinumerous to $[m]$ for some $m < n$. Consider $A \subsetneq [n+1]$.

Since $[n+1] = \{0, 1, \dots, n-1, n\}$, we ask the question of whether $n \in A$ or $n \notin A$.

Case 1: If $n \notin A$, then either

- $A = [n]$, so $|A| = n < n+1$,
- or $A \subsetneq [n]$; by inductive hypothesis, $|A| < n < n+1$.

Case 2: Otherwise, $n \in A$ so $A \setminus \{n\} \subsetneq [n]$.

By inductive hypothesis, $A \setminus \{n\} \approx [m]$ for some $m < n$. Fix a bijection $f \colon A \setminus \{n\} \to [m]$. Define $g \colon A \to [m+1]$ by

$$g(k) = \begin{cases} f(k) & \text{if } k \neq n \\ m & \text{if } k = n \end{cases}$$

(That is, we extend f by mapping $n \mapsto m$.)

Then $A \approx [m+1]$, so $|A| = m + 1 < n + 1$.

□

As a consequence, subsets of finite sets are finite.

Corollary 4.13. *If B is finite and $A \subsetneq B$, then A is finite and $|A| < |B|$.*

Proof. Suppose B is finite. Then $|B| = n$ for some $n \in \mathbb{N}$. Fix a bijection $g \colon B \to [n]$.

Then $g[A] \subsetneq [n]$ (to prove properness, take any $b \in B \setminus A$, then $g(b) \notin g[A]$ due to injectivity of g). By the preceding lemma, $g[A]$ is finite and $|g[A]| < n$.

Since $A \approx g[A]$ (via g), it follows that A is finite and $|A| = |g[A]| < n$. □

The next few results say that we can compare cardinality of finite sets with injections and surjections.

Proposition 4.14. *Let A and B be finite sets. Then $|A| \leq |B|$ if and only if there exists an injection from A to B.*

Proof. Suppose A and B are finite.

$\boxed{\Leftarrow}$ Fix an injection $f \colon A \to B$. Then $f[A] \subseteq B$. We consider two cases:

Case 1: If $f[A] = B$, f is surjective and thus bijective. Since $f \colon A \to B$ is a bijection, it follows that A is finite and $|A| = |B|$.

Case 2: Otherwise, $f[A] \subsetneq B$. By the previous result, $f[A]$ is finite and $|f[A]| < |B|$.

Note that the restriction $f|_A\colon A \to f[A]$ is surjective and thus bijective. Thus A is finite and $|A| = |f[A]| < |B|$.

$\boxed{\Rightarrow}$ Since A and B are finite, we have $A \approx [m]$ and $B \approx [n]$ for some $m, n \in \mathbb{N}$. Since $|A| \leq |B|$, we have $m \leq n$.

Construct an injection from A to B by composition:

$$\begin{tikzcd} A \arrow[r, "f"] & {[m]} \arrow[r, "\iota"] & {[n]} \arrow[r, "g^{-1}"] & B \end{tikzcd}$$

□

We first need a lemma, which states that every surjection from a subset of $\mathbb{N}$ has a right-inverse.

Lemma 4.15. *Let A be a set, $B \subseteq \mathbb{N}$. For every surjection $g\colon B \to A$, there exists an injection $f\colon A \to B$ such that $g \circ f = \mathrm{id}_A$.*

Proof. Define $f\colon A \to B$ by

$$f(a) = \min g^{-1}(a).$$

- Each fiber $g^{-1}(a)$ is non-empty because g is surjective. By well-ordering, $\min g^{-1}(a)$ exists and is unique. Hence f is well-defined.
- We now check that f is injective. Suppose $f(a) = f(a')$. Then $f(a) \in g^{-1}(a)$ and $f(a') \in g^{-1}(a')$, so
$$a = g(f(a)) = g(f(a')) = a'.$$
- Finally, for each $a \in A$, we have $g(f(a)) = a$ since $f(a) \in g^{-1}(a)$. Hence $g \circ f = \mathrm{id}_A$.

□

Proposition 4.16. *Let A and B be non-empty finite sets. Then $|B| \geq |A|$ if and only if there exists a surjection from B to A.*

Proof. Let A and B be non-empty finite sets.

$\boxed{\Rightarrow}$ Suppose $|A| \leq |B|$. Then there exists an injection from A to B, so there exists a surjection from B to A.

$\boxed{\Leftarrow}$ Fix a surjection $f\colon B \to A$. Suppose $|B| = n$; fix a bijection $g\colon [n] \to B$. Then the composition $f \circ g\colon [n] \to A$ is surjective.

Since $[n] \subseteq \mathbb{N}$, there exists an injection from A to $[n]$. Hence $|A| \leq n = |B|$, as desired. □

Remark. If A is empty but B is not, then $|A| \leq |B|$ but there is no surjection from B to $A = \emptyset$.

4.2.3 Set Operations

Proposition 4.17. *Finite unions of finite sets are finite.*

Proof. We first prove the case for two sets.

Lemma. *If A and B are finite, then $A \cup B$ is finite.*

Proof. The result is trivial if A or B is empty. Thus assume both A and B are non-empty. Fix bijections $f\colon [m] \to A$ and $g\colon [n] \to B$ for some $m, n \in \mathbb{N}$.

Define $h\colon [n+m] \to A \cup B$ by

$$h(i) = \begin{cases} f(i) & (i = 0, \dots, m-1) \\ g(i-m) & (i = m, \dots, m+n-1) \end{cases}$$

It is easy to check that h is surjective, from which it follows that $A \cup B$ is finite. □

Now we show by induction that finiteness of the sets $A_1, \dots, A_n$ implies finiteness of their union. This result is trivial for $n = 1$. Assuming it true for $n-1$, we note that

$$A_1 \cup \dots \cup A_n = (A_1 \cup \dots \cup A_{n-1}) \cup A_n,$$

each of which are finite, so the lemma applies. □

Proposition 4.18. *Finite Cartesian products of finite sets are finite.*

Proof. We first prove the case for two sets.

Lemma. *If A and B are finite, then $A \times B$ is finite.*

Proof. For each $a \in A$, the set $\{a\} \times B$ is finite, since $\{a\} \times B \approx B$. Then

$$A \times B = \bigcup_{a \in A} \{a\} \times B$$

which is a finite union of finite sets (since there are finitely many $a \in A$). Hence $A \times B$ is finite. □

To prove that the product $A_1 \times \dots \times A_n$ is finite if each A_i is finite, one proceeds by induction. □

Lemma 4.19. *Let A and B be finite. If A and B are disjoint, then*

$$|A \sqcup B| = |A| + |B|.$$

Proof. Fix bijections $f\colon [n] \to A$ and $g\colon [m] \to B$ for some $n, m \in \mathbb{N}$. Define $h\colon [n+m] \to A \cup B$ by

$$h(i) = \begin{cases} f(i) & \text{if } i = 0, \dots, n-1, \\ g(i-n) & \text{if } i = n, \dots, n+m-1. \end{cases}$$

One can check that h is a bijection. □

Proposition 4.20 (Principle of inclusion and exclusion)**.** *Let A and B be finite. Then*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. Note that we have the disjoint union

$$A \cup B = (A \setminus B) \sqcup (A \cap B) \sqcup (B \setminus A)$$

as well as $A = (A \setminus B) \sqcup (A \cap B)$ and $B = (B \setminus A) \sqcup (A \cap B)$. By the preceding lemma,

$$\begin{aligned} |A \cup B| &= |(A \setminus B) \sqcup (A \cap B) \sqcup (B \setminus A)| \\ &= |A \setminus B| + |A \cap B| + |B \setminus A| \\ &= (|A \setminus B| + |A \cap B|) + (|B \setminus A| + |A \cap B|) - |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

□

Proposition 4.21. *Let A be finite. Then $\mathcal{P}(A)$ is finite, and*

$$|\mathcal{P}(A)| = 2^{|A|}.$$

Proof. Induct on $n = |A|$.
If $n = 0$, then $A = \emptyset$, so $\mathcal{P}(A) = \{\emptyset\}$. Hence $|\mathcal{P}(A)| = 1 = 2^0$.
Suppose $|P(S)| = 2^n$ for any set S with $|S| = n,$. Let A be any set with $|A| = n + 1$.
Fix $a \in A$. Consider the set $A' = A \setminus \{a\}$. Then $|A'| = n$. Any subset of A must either contain the element a or not, so we can partition

$$\begin{aligned} \mathcal{P}(A) &= \{S \subset A : a \in A\} \sqcup \{S \subset A : a \notin A\} \\ &= \{S \cup \{a\} : S \in \mathcal{P}(A')\} \sqcup \mathcal{P}(A'). \end{aligned}$$

By inductive hypothesis, each of the above two sets has cardinality 2^n. Hence $|\mathcal{P}(A)| = 2^n + 2^n = 2^{n+1}$. □

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.

4.2.4 Boundedness

Definition 4.22. We say that $A \subseteq \mathbb{R}$ is **bounded** in $\mathbb{R}$ if there are $u, l \in \mathbb{R}$ such that $l \leq a \leq u$ for all $a \in A$.
The **maximum** $\max(A)$ is defined to be the number $m \in A$ such that $a \leq m$ for all $a \in A$.

Remark. Analogously, we can define "bounded", "max" and "min" in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, provided that we have total ordering.

Proposition 4.23. *Let A be a non-empty finite subset of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Then* $\max(A)$ *and* $\min(A)$ *exist. In particular, A is bounded.*
(Contrapositive: Every set which is unbounded in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ is infinite.)

Proposition 4.24. *A subset of $\mathbb{N}$ is finite if and only if it is bounded in $\mathbb{N}$.*

Proof. Let $X \subseteq \mathbb{N}$.
$\boxed{\Rightarrow}$ Obvious.
$\boxed{\Leftarrow}$ Suppose X is bounded in $\mathbb{N}$. Then there exists $b \in \mathbb{N}$ such that $x \leq b$ for all $x \in X$. Then $X \subseteq [b + 1]$. Since $[b + 1]$ is finite, X is finite as well. □

Remark. In other orders (such as the standard ordering on $\mathbb{R}$), bounded sets may not be finite. For example, $[0,1]$ is bounded but not finite, since it is equinumerous to a proper subset of itself (witnessed by the bijection $x \mapsto x/2$ from $[0,1]$ to $[0,1/2]$).

Proposition 4.25. *The following are sufficient conditions for A to be infinite.*

(i) A is unbounded in $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

(ii) There is an injection from an infinite set to A.

(iii) A is equinumerous with a proper subset of itself.

Proof.

(i) Done.

Remark. (i) is not a necessary condition for A to be infinite, since A can be infinite but bounded.

(ii) Let X be infinite, and $f\colon X \to A$ an injection. Suppose, towards a contradiction, that A is finite. Then $f[X] \subseteq A$, so $f[X]$ is finite. Thus X is finite.

Remark. (ii) is necessary because every infinite set is equinumerous to itself (in particular, $\mathrm{id}\colon A \to A$ is an injection).

(iii) Done.

□

— Exercises —

★★ **Exercise 4.2.1** (MA1100T AY23/24)**.** Define a relation $\sim$ on $\mathbb{R}$ such that

$$x \sim y \iff x - y \in \mathbb{Q}.$$

(i) Prove that $\sim$ is an equivalence relation on $\mathbb{R}$.

(ii) Prove that the quotient set $\mathbb{R}/\sim$ is infinite.

Solution.

(i) Reflexivity: For all $x \in \mathbb{R}$, $x - x = 0 \in \mathbb{Q}$, so $x \sim x$.

Symmetry: Suppose $x \sim y$. Then $x - y \in \mathbb{Q}$, so $y - x = -(x-y) \in \mathbb{Q}$. Thus $y \sim x$.

Transitivity: Suppose $x \sim y$ and $y \sim z$. Then $x - y, y - z \in \mathbb{Q}$, so $x - z = (x-y) + (y-z) \in \mathbb{Q}$. Thus $x \sim z$.

(ii) To show a set is infinite, it suffices to show that it has an infinite subset.

Consider the set $S = \left\{[\sqrt{2}k] : k \in \mathbb{Z}\right\}$.

Claim: S is infinite. (Since $S \subseteq \mathbb{R}/\sim$, this will imply that $\mathbb{R}/\sim$ is infinite.)

Define the map $f\colon \mathbb{Z} \to S$ by $k \mapsto [\sqrt{2}k]$. We shall show that f is injective.

Suppose $[\sqrt{2}k] = [\sqrt{2}k']$. Then $\sqrt{2}k \sim \sqrt{2}k'$. Thus $\sqrt{2}k - \sqrt{2}k' = (k-k')\sqrt{2} \in \mathbb{Q}$.

Since $k - k' \in \mathbb{Z}$ and $\sqrt{2}$ is irrational, we must have $k - k' = 0$, so $k = k'$.

□

4.3 Countability

Definition 4.26. Let X be a set. We say that

- X is **countably infinite** if $X \approx \mathbb{N}$;
- X is **countable** if X is finite or countably infinite;
- X is **uncountable** if X is not countable.

Informally, a set X is countably infinite if X can be listed without repetition: if $f\colon \mathbb{N} \to X$ is a bijection, then we can list the elements of X as

$$f(1), f(2), f(3), \dots .$$

If we define $x_i = f(i)$ for all $i \in \mathbb{N}$, then we can write X as

$$X = \{x_1, x_2, x_3, \dots\}.$$

This technique is particularly useful when it is difficult or not possible to deduce an explicit formula for a bijection.

Remark. The use of the word "countable" to describe the sets that are either finite or countably infinite is deliberate. Informally, a countable set is one whose elements can be "counted", or listed, although the list may or may not "end".

Since $\mathbb{N}$ is infinite, any countably infinite set is infinite.

Example. $\mathbb{N}$, $n\mathbb{N}$, $\mathbb{Z}$ are countable.

Example. $\mathcal{P}(\mathbb{N})$ is uncountable. We show that $\mathcal{P}(\mathbb{N})$ is (i) not equinumerous to $\mathbb{N}$, and (ii) not finite.

(i) Cantor's theorem shows that $\mathbb{N} \not\approx \mathcal{P}(\mathbb{N})$.

(ii) There exists an injection from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$ defined by $n \mapsto \{n\}$. Since $\mathbb{N}$ is infinite, so is $\mathcal{P}(\mathbb{N})$.

The following result is a very useful criteron for showing that a set is countable.

Proposition 4.27. *Let A be a non-empty set. Then the following are equivalent:*

(i) A is countable.

(ii) There exists a surjection $f\colon \mathbb{N} \to A$.

(iii) There exists an injection $g\colon A \to \mathbb{N}$.

Proof.

$\boxed{\text{(i)} \Rightarrow \text{(ii)}}$ If A is countably infinite, there exists a bijection from $\mathbb{N}$ to A, which is surjective.

If A is finite, suppose $|A| = n$ for some $n \geq 1$. Fix a bijection $h\colon [n] \to A$. Extend h to a surjection $f\colon \mathbb{N} \to A$ by defining

$$f(k) = \begin{cases} h(k) & \text{if } 0 \leq k \leq n-1, \\ h(k) & \text{if } k \geq n. \end{cases}$$

$\boxed{\text{(ii)} \Rightarrow \text{(iii)}}$ Let $f\colon \mathbb{N} \to A$ be a surjection. Then for each $a \in A$, the fiber $f^{-1}(a)$ is non-empty.

Define $g\colon A \to \mathbb{N}$ by
$$g(a) = \min f^{-1}(a).$$
If $a \neq a'$, then the sets $f^{-1}(a)$ and $f^{-1}(a')$ are disjoint, so their smallest elements are different. Thus $g(a) \neq g(a')$. Hence g is injective.

$\boxed{\text{(iii)} \Rightarrow \text{(i)}}$ Let $g\colon A \to \mathbb{N}$ be an injection. Then $g[A] \subseteq \mathbb{N}$ is either finite or countably infinite.

Case 1: If $g[A]$ is finite, then A is finite (being in bijection with $g[A]$).

Case 2: If $g[A]$ is infinite, then g exhibits a bijection between A and the infinite subset $g[A] \subseteq \mathbb{N}$, so A is countably infinite.

In either case, A is countable. □

Corollary 4.28. *Every subset of a countable set is countable.*

Proof. Let $A \subseteq B$, where B is countable. Fix an injection $f\colon B \to \mathbb{N}$. Then the composition $f \circ \iota\colon A \to \mathbb{N}$ is an injection, so A is countable.

$$\begin{tikzcd} A \arrow[r, "\iota"] & B \arrow[r, "f"] & \mathbb{N} \end{tikzcd}$$

□

to prove

Corollary 4.29. *If $X \subseteq \mathbb{N}$ is infinite, then $X \approx \mathbb{N}$.*

Proposition 4.30. *The union of two countable sets is countable.*

Proof. Let A_0 and A_1 be countable. If either are empty, then their union is clearly countable. Thus suppose both A_0 and A_1 are non-empty.

By 4.27, fix surjections $f_0\colon \mathbb{N} \to A_0$ and $f_1\colon \mathbb{N} \to A_1$. Define $g\colon \mathbb{N} \to A_0 \cup A_1$ by
$$g(n) = \begin{cases} f_0\left(\dfrac{n}{2}\right) & \text{if } n \text{ is even,} \\ f_1\left(\dfrac{n-1}{2}\right) & \text{if } n \text{ is odd.} \end{cases}$$
We check that g is surjective. Let $x \in A \cup B$. We consider two cases:

Case 1: If $x \in A$, since f_1 is surjective, there exists $n_1 \in \mathbb{N}$ such that $f_1(n_1) = x$. Since $2n_1$ is even, we have
$$g(2n_1) = f_1(n_1) = x.$$

Case 2: If $x \in B$, since f_2 is surjective, there exists $n_2 \in \mathbb{N}$ such that $f_2(n_2) = x$. Since $2n_2 + 1$ is odd, we have
$$g(2n_2 + 1) = f_2(n_2) = x.$$

By 4.27, we conclude that $A_0 \cup A_1$ is countable. □

Corollary 4.31. *A finite union of countable sets is countable.*

Corollary 4.32. *An uncountable set cannot be expressed as the union of two countable sets.*

A countable union of countable sets is countable, but this requires the Axiom of choice.

Lemma 4.33. *If $A \approx X$ and $B \approx Y$, then $A \times B \approx X \times Y$.*

Proof. Fix bijections $f\colon A \to X$ and $g\colon B \to Y$. Define $\Phi\colon A \times B \to X \times Y$ by

$$(a, b) \mapsto (f(a), g(b)).$$

It remains to check that Φ is a bijection. □

Proposition 4.34. *If X and Y are countably infinite, then $X \times Y$ is countably infinite.*

Proof. Since $X \approx \mathbb{N}$ and $Y \approx \mathbb{N}$, we have $\mathbb{N} \approx \mathbb{N} \times \mathbb{N} \approx X \times Y$. □

Corollary 4.35. *A finite product of countable sets is countable.*

— Exercises —

Exercise 4.3.1 (MA1100T AY21/22)**.** Prove or disprove: For any countable set A, the power set $\mathcal{P}(A)$ is countable.

Solution. False. Cantor's Theorem. □

Exercise 4.3.2 (MA1100 AY24/25)**.** Let X and Y be non-empty sets, and $f\colon X \to Y$ be a surjection. Define a relation $\sim$ on X by

$$x \sim y \iff f(x) = f(y).$$

(i) Prove that $\sim$ is an equivalence relation.

(ii) Prove that $X/\sim$ is equinumerous with Y.

Solution.

(i) Reflexivity: For all $x \in X$, since f is well-defined $f(x) = f(x)$. Thus $x \sim x$.

Symmetry: Suppose $x \sim y$. Then $f(x) = f(y)$, so $f(y) = f(x)$. Thus $y \sim x$.

Transitivity: Suppose $x \sim y$ and $y \sim z$. Then $f(x) = f(y)$ and $f(y) = f(z)$, so $f(x) = f(z)$. Thus $x \sim z$.

(ii) **Claim:** The map $\phi\colon X/{\sim} \to Y$ defined by $\phi([x]) = f(x)$ is a bijection.

Well-definedness: Suppose $[x] = [x']$. Then $x \sim x' \iff f(x) = f(x') \implies \phi([x]) = \phi([x'])$. This shows ϕ is well-defined.

Injectivity: Suppose $\phi([x]) = \phi([x'])$. Then $f(x) = f(x') \implies x \sim x' \implies [x] = [x']$. This shows ϕ is injective.

Surjectivity: Since f is surjective, for every $y \in Y$, there exist $x \in X$ such that $f(x) = y$. Then $\phi([x]) = f(x) = y$, so ϕ is surjective.

□

Exercise 4.3.3 ([Rud76] 2.2)**.** We say $z \in \mathbb{C}$ is *algebraic* if there exist integers $a_0, \dots, a_n$, not all zero, such that

$$a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0.$$

Prove that the set of all algebraic numbers is countable. *Hint*: For every positive integer N there are only finitely many equations with

$$n + |a_0| + |a_1| + \cdots + |a_n| = N.$$

Solution. Following the hint, let A_N be the set of numbers z that satisfy $a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0$, for some coefficients $a_0, \dots, a_n$ which satisfy

$$n + |a_0| + |a_1| + \cdots + |a_n| = N.$$

By the fundamental theorem of algebra, $a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0$ has at most n solutions, so each A_N is finite. Hence the set of algebraic numbers, which is the union

$$\bigcup_{N=2}^{\infty} A_N$$

is at most countable. Since all rational numbers are algebraic, it follows that the set of algebraic numbers is exactly countable. □

Exercise 4.3.4 ([Rud76] 2.3)**.** Prove that there exist real numbers which are not algebraic.

Solution. By the previous exercise, the set of real algebraic numbers is countable. If every real number were algebraic, the entire set of real numbers would be countable, a contradiction. □

★ **Exercise 4.3.5** ([Rud76] 2.4)**.** Is the set of irrational real numbers countable?

Solution. No. Suppose, towards a contradiction, that $\mathbb{R} \setminus \mathbb{Q}$ is countable. Then $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ would be countable, which is clearly false. □

Exercise 4.3.6 (MA1100T AY21/22)**.** For any infinite set A, show that the power set $\mathcal{P}(A)$ is uncountable.

Solution. Since A is infinite, by Choice, we have $\mathbb{N} \preceq A$. Then $\mathcal{P}(\mathbb{N}) \preceq \mathcal{P}(A)$. Since $\mathcal{P}(\mathbb{N})$ is uncountable, it follows that $\mathcal{P}(A)$ is also uncountable. □

Exercise 4.3.7 (MA1100T AY21/22)**.** Prove or disprove the following:

(a) Let I be an uncountable indexing set, and suppose for each $i \in I$, the set X_i is an uncountable set. Then $\bigcup_{i \in I} X_i$ is uncountable.

(b) Let I be a countable indexing set, and suppose for each $i \in I$, the set X_i is a countable set. Then $\bigcup_{i \in I} X_i$ is countable.

(c) Let I be a finite indexing set, and suppose for each $i \in I$, the set X_i is a finite set. Then $\bigcup_{i \in I} X_i$ is finite.

(d) Let I be an uncountable indexing set, and suppose for each $i \in I$, the set X_i is a countable set. Then $\bigcup_{i \in I} X_i$ is uncountable.

(e) Let I be an infinite indexing set, and suppose for each $i \in I$, the set X_i is an infinite set. Then $\bigcup_{i \in I} X_i$ is infinite.

(f) Let I be a finite indexing set, and suppose for each $i \in I$, the set X_i is an infinite set. Then $\bigcup_{i \in I} X_i$ is infinite.

(g) Let I be an infinite indexing set, and suppose for each $i \in I$, the set X_i is a finite set. Then $\bigcup_{i \in I} X_i$ is infinite.

(h) Let I be a countable indexing set, and suppose for each $i \in I$, the set X_i is an uncountable set. Then $\bigcup_{i \in I} X_i$ is uncountable.

Solution.

(a) True. If $\bigcup_{i \in I} X_i$ were countable, then it contains uncountable sets X_i, a contradiction.

(b) True. Axiom of Choice needed.

(c) True.

(d) False. All the X_i could be equal to each other, and the union would be countable.

(e) True.

(f) False. If I is empty, then $\bigcup_{i \in I} X_i$ is empty.

(g) False. Take $X_i = \emptyset$ for all $i \in I$. Then $\bigcup_{i \in I} X_i$ is finite.

(h) False. This will not hold when the indexing set I is empty.

□

4.4 Size of $\mathrm{Maps}([n], X)$

Every $f \in \mathrm{Maps}([n], X)$ is in bijection with a sequence of length n with values in X as follows:

$$f \mapsto (f(0), f(1), \ldots, f(n-1)).$$

For each set X and each $n \in \mathbb{N}$, how many sequences of length n are there with values in X? Equivalently, what is the size of $\mathrm{Maps}([n], X)$?

Example.

- $\mathrm{Maps}([1], X) \approx X$. To see this, consider the bijection $f(0) = x \leftrightarrow x$.
- $\mathrm{Maps}([2], X) \approx X \times X$. To see this, the map $f \mapsto (f(0), f(1))$ is a bijection.

Lemma 4.36. *For all sets X and for all $n \in \mathbb{N}$,*

$$\mathrm{Maps}([n+1], X) \approx \mathrm{Maps}([n], X) \times X.$$

Proof. Define $\Phi\colon \mathrm{Maps}([n+1], X) \to \mathrm{Maps}([n], X) \times X$ as

$$f \mapsto (f|_{[n]}, f(n)).$$

It remains to be shown that that Φ is a bijection. □

Proposition 4.37. *If X is countably infinite, then for each $n \in \mathbb{N}^+$, $\mathrm{Maps}([n], X)$ is countably infinite.*

Proof. Induct on $n \in \mathbb{N}^+$.
$\boxed{\text{Base case}}$ When $n = 1$, $[1] = \{0\}$. Each $f \in \mathrm{Maps}([1], X)$ is determined by its value $f(0)$, so the map

$$\mathrm{Maps}([1], X) \to X, \qquad f \mapsto f(0)$$

is a bijection. Since X is countably infinite, so is $\mathrm{Maps}([1], X)$.
$\boxed{\text{Inductive step}}$ Assume $\mathrm{Maps}([n], X)$ is countably infinite for some $n \geq 1$. By the lemma,

$$\mathrm{Maps}([n+1], X) \approx \mathrm{Maps}([n], X) \times X.$$

Since the product of two countably infinite sets is countably infinite, it follows that $\mathrm{Maps}([n+1], X)$ is countably infinite. □

Remark. We exclude $n = 0$, since $[0] = \emptyset$, so $\mathrm{Maps}([0], X)$ contains only the empty function to X.

We can transfer the previous result to arbitrary finite sets A in place of $[n]$.

Lemma 4.38. *If $A \approx B$, then $\mathrm{Maps}(A, X) \approx \mathrm{Maps}(B, X)$.*

Proof. Fix a bijection $f\colon B \to A$. Define $\Phi\colon \mathrm{Maps}(A, X) \to \mathrm{Maps}(B, X)$ by

$$g \mapsto g \circ f.$$

It remains to be shown that Φ is a bijection. □

Proposition 4.39. *If A is non-empty finite, and X is countably infinite, then* $\operatorname{Maps}(A, X)$ *is countably infinite.*

Proof. Since A is finite and non-empty, fix $n \in \mathbb{N}^+$ such that $A \approx [n]$. By the preceding lemma, $\operatorname{Maps}([n], X) \approx \operatorname{Maps}(A, X)$.

But $\operatorname{Maps}([n], X)$ is countably infinite, so $\operatorname{Maps}(A, X)$ is countably infinite as well. □

Proposition 4.40. *If X is countably infinite, then* $\operatorname{Maps}(X, [2])$ *is uncountable.*

It follows that if X and Y are countably infinite, then $\operatorname{Maps}(X, Y)$ is uncountable.

Proof. We will construct a bijection from $\mathcal{P}(X)$ to $\operatorname{Maps}(X, [2])$ as follows. Define $F \colon \mathcal{P}(X) \to \operatorname{Maps}(X, [2])$ which sends each subset of X to its characteristic function:

$$F(S) = \chi_S \qquad (S \subseteq X).$$

Recall that for $x \in X$,

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

Injectivity: Suppose $F(S_1) = F(S_2)$. Then $\chi_{S_1} = \chi_{S_2}$, so $\chi_{S_1}(x) = \chi_{S_2}(x)$ for every $x \in X$. Since

$$x \in S_1 \iff \chi_{S_1}(x) = 1 \iff \chi_{S_2}(x) = 1 \iff x \in S_2$$

we have $S_1 = S_2$, so F is injective.

Surjectivity: Let $f \colon X \to [2]$. Define $S_f := \{x \in X \mid f(x) = 1\} \subseteq X$. By construction, $F(S_f) = \chi_{S_f} = f$.

Hence $\operatorname{Maps}(X, [2]) \approx \mathcal{P}(X)$. □

Let X be a non-empty countable set. Let $X^{<\mathbb{N}}$ denote the set of **all finite sequences** with values in X:

$$X^{<\mathbb{N}} := \bigcup_{n \in \mathbb{N}} \operatorname{Maps}([n], X).$$

Lemma 4.41. $\mathbb{N}^{<\mathbb{N}}$ *is countably infinite.*

Proof. Since the set of primes P is an unbounded subset of $\mathbb{N}$, by 4.24, P is an infinite subset of $\mathbb{N}$. Thus $P \approx \mathbb{N}$. Fix a bijection $f \colon \mathbb{N} \to P$. Define $F \colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}$ by

$$F(a_0, a_1, \ldots, a_n) = f(0)^{a_0+1} f(1)^{a_1+1} \cdots f(n)^{a_n+1}.$$

F is injective because by FTA, the exponent on each prime number in the prime factorisation is unique. Hence $\mathbb{N}^{<\mathbb{N}}$ is countable.

To prove $\mathbb{N}^{<\mathbb{N}}$ is infinite, note that there is an injection from $\mathbb{N}$ to $\mathbb{N}^{<\mathbb{N}}$, which maps $n \mapsto (n)$. By 4.25, $\mathbb{N}^{<\mathbb{N}}$ is infinite. □

Remark. We added 1 to each exponent to ensure that the function is injective. For example, if we do not add 1, then (1) and $(1, 0)$ are both mapped to 2.

Remark. F is not surjective (e.g. 10 is not in the range).

Proposition 4.42. *$X^{<\mathbb{N}}$ is countably infinite.*

Proof. Since X is countably infinite and non-empty, fix a surjection $g\colon \mathbb{N} \to X$. Define $\Phi\colon \mathbb{N}^{<\mathbb{N}} \to X^{<\mathbb{N}}$ by

$$(a_0, a_1, \ldots, a_n) \mapsto (g(a_0), g(a_1), \ldots, g(a_n)).$$

Φ is well-defined and surjective because g is well-defined and surjective.

Since $\mathbb{N}^{<\mathbb{N}}$ is countably infinite, fix a bijection $f\colon \mathbb{N} \to \mathbb{N}^{<\mathbb{N}}$. Then $\Phi \circ f$ is a surjection from $\mathbb{N}$ to $X^{<\mathbb{N}}$. Hence $X^{\mathbb{N}}$ is countable.

To prove $X^{\mathbb{N}}$ is infinite, notice that there is an injection from $\mathbb{N}$ to $X^{<\mathbb{N}}$. (Fix $x_0 \in X$. Map each $n \in \mathbb{N}$ to the constant sequence x_0 with length n.) □

— Exercises —

★ **Exercise 4.4.1.** Disprove: For all sets A, B, X, Y, if $A \approx X$ and $B \approx Y$, then $A \cup B \approx X \cup Y$.

Solution. A counterexample is $A = \{0, 1\}$, $X = \{2, 3\}$, $B = \{0\}$, $Y = \{4\}$.
Then $A \cup B = \{0, 1, 2, 3\}$ and $X \cup Y = \{2, 3, 4\}$. □

★★ **Exercise 4.4.2** (MA1100T AY23/24)**.** Let C be the set of functions from $\mathbb{N}$ to $\{0, 1\}$ that are *eventually constant*, that is, for each $f \in C$, there exists $n \in \mathbb{N}$ such that for all $m > n$, $f(m) = f(n)$. For each $f \in C$, define the set

$$S_f := \{n \in \mathbb{N} : (\forall m > n)\, f(m) = f(n)\}.$$

Define the function $F\colon C \to \{0, 1\}^{<\mathbb{N}}$ by

$$F(f) = (f(0), f(1), \ldots, f(\min(S_f))).$$

(i) Prove that F is injective.

(ii) Prove that C is countable.

Solution.

(i) Suppose $F(f_1) = F(f_2)$. By definition of F, we have

$$(f_1(0), f_1(1), \ldots, f_1(\min(S_{f_1}))) = (f_2(0), f_2(1), \ldots, f_2(\min(S_{f_2}))).$$

For the two sequences to be equal, they must have equal length. Hence $\min(S_{f_1}) = \min(S_{f_2})$; let $\min(S_{f_1}) = \min(S_{f_2}) = k$.

For the two sequences to be equal, they are also termwise equal. Hence $f_1(m) = f_2(m)$ for all $m \leq k$.

By definition of S_f, we have $f(m) = f(k)$ for all $m > k$. Thus $f_1(m) = f_1(k) = f_2(k) = f_2(m)$.

Hence $f_1(m) = f_2(m)$ for all $m \in \mathbb{N}$, so $f_1 = f_2$ as desired.

(ii) Since $\{0, 1\}^{<\mathbb{N}}$ is countably infinite, fix a bijection $g\colon \{0, 1\}^{<\mathbb{N}} \to \mathbb{N}$.

By (i), $g \circ F$ is an injection from C to $\mathbb{N}$. Hence C is countable.

□

Exercise 4.4.3 (MA1100T AY22/23)**.** For each set A, let $\mathcal{P}_{\text{fin}}(A)$ denote the set of finite subsets of A.

(a) Define a function $G\colon \bigcup_{n\in\mathbb{N}} \text{Maps}([n], \mathbb{N}) \to \mathcal{P}_{\text{fin}}(\mathbb{N})$ by $G(f) = \text{range}(f) \subseteq \mathbb{N}$. Prove that G is well-defined and surjective.

(b) Prove that $\mathcal{P}_{\text{fin}}(\mathbb{N})$ is countably infinite.

(c) Prove that if A is countably infinite, then $\mathcal{P}_{\text{fin}}(A)$ is countably infinite.

Solution.

(a) Let $f \in \bigcup_{n\in\mathbb{N}} \text{Maps}([n], \mathbb{N})$. Fix $n \in \mathbb{N}$ such that $f \in \text{Maps}([n], \mathbb{N})$, i.e., $f\colon [n] \to \mathbb{N}$. Thus $\text{range}(f) \subseteq \mathbb{N}$ and is finite. Hence $G(f) \in \mathcal{P}_{\text{fin}}(\mathbb{N})$, so G is well-defined.

To prove surjectivity, let $S \in \mathcal{P}_{\text{fin}}(\mathbb{N})$. Since S is finite, fix $n \in \mathbb{N}$ such that $S \approx [n]$. Fix a bijection $f\colon [n] \to S$; note that $f \in \text{Maps}([n], \mathbb{N})$, so $f \in \bigcup_{n\in\mathbb{N}} \text{Maps}([n], \mathbb{N})$. Then $\text{range}(f) = S$, so $G(f) = S$.

(b) Since $\bigcup_{n\in\mathbb{N}} \text{Maps}([n], \mathbb{N})$ is countably infinite, fix a bijection $F\colon \mathbb{N} \to \bigcup_{n\in\mathbb{N}} \text{Maps}([n], \mathbb{N})$.

By (a), $G\colon \bigcup_{n\in\mathbb{N}} \text{Maps}([n], \mathbb{N}) \to \mathcal{P}_{\text{fin}}(\mathbb{N})$ is a surjection. Hence $G \circ F\colon \mathbb{N} \to \mathcal{P}_{\text{fin}}(\mathbb{N})$ is surjective, so $\mathcal{P}_{\text{fin}}(\mathbb{N})$ is countably infinite.

(c) Since $A \approx \mathbb{N}$, fix a bijection $h\colon A \to \mathbb{N}$. Define $\Phi\colon \mathcal{P}_{\text{fin}}(A) \to \mathcal{P}_{\text{fin}}(\mathbb{N})$ by

$$S \mapsto h[S]$$

which is a bijection. Thus $\mathcal{P}_{\text{fin}}(A) \approx \mathcal{P}_{\text{fin}}(\mathbb{N})$. By (b), $\mathcal{P}_{\text{fin}}(\mathbb{N}) \approx \mathbb{N}$. Hence $\mathcal{P}_{\text{fin}}(A) \approx \mathbb{N}$.

□

4.5 Axiom of Choice

Let X be a non-empty set of non-empty sets. A function $F\colon X \to \bigcup X$ is called a **choice function** for X if $F(S) \in S$ for all $S \in X$.

Intuitively, F is looking into every element S of X and then choose an element of S for us.

Example.

- Let X be the set of countries on Earth, thinking of each country as a collection of cities. Then $\bigcup X$ is the set of all cities on Earth, and the function F that assigns to each country its capital city is an example of a choice function for X.
- (The classic example.) Let X be the collection of all pairs of shoes in the world. Then the function that picks the left shoe out of each pair is a choice function for X.
- Let $X = \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$. The function $f(S) = \min(S)$ is a choice function for X.
- In fact, we can generalise the above to any well-order! Let $(W, \leq)$ be a well-order, and let $X = \mathcal{P}(W) \setminus \{\emptyset\}$. Again, the function $f(S) = \min(S)$ is a choice function on X.

  (This is the essence of the proof that the Well-Ordering Theorem implies the Axiom of Choice. More on that later.)

Axiom 4.43 (Axiom of Choice)**.** *Let X be a non-empty set of non-empty sets. There exists a choice function for X.*

The ZF axioms together with Choice are known as ZFC.

Remark.

- For a finite set X, Choice is provable in ZF. (Induct on n. Base case: $X = \{S\}$; since S is non-empty, there exists $x \in S$, so define $f(S) = x$.)
- For X such that every $S \in X$ is a singleton, Choice is provable in ZF, by defining $F(S)$ to be the unique element in S. (If S is finite, then Choice is not provable in ZF.)
- For $X \subseteq \mathcal{P}(\mathbb{N})$, Choice is provable in ZF. (Since each $S \in X$ is a non-empty subset of $\mathbb{N}$, we can use well-ordering to choose the minimum element of each S.)
- Neither Choice or its negation is provable in ZF (assuming ZF is consistent), by Cohen (1963) and G odel (1938) respectively.

Proposition 4.44. *A countable union of countable sets is countable.*

Proof. Suppose $\{A_i\}_{i\in\mathbb{N}}$ is a sequence of countable sets. WLOG assume each A_i is non-empty. Consider the set

$$X := \{\{g \in \operatorname{Maps}(\mathbb{N}, A_i) : g \text{ is surjective}\} : i \in \mathbb{N}\}.$$

Since each A_i is non-empty and countable, there is a surjection from $\mathbb{N}$ to A_i, so $\{g \in \operatorname{Maps}(\mathbb{N}, A_i) : g \text{ is surjective}\} \neq \emptyset$. Thus $\emptyset \notin X$. Assuming Choice, there exists a choice function $F\colon X \to \bigcup X$ such that for each $i \in \mathbb{N}$, we have

$$F(\{g \in \operatorname{Maps}(\mathbb{N}, A_i) : g \text{ is surjective}\}) \in \{g \in \operatorname{Maps}(\mathbb{N}, A_i) : g \text{ is surjective}\}.$$

Let $F(\{g \in \operatorname{Maps}(\mathbb{N}, A_i) : g \text{ is surjective}\}) = g_i$. Define $G\colon \mathbb{N} \times \mathbb{N} \to \bigcup_{i\in\mathbb{N}} A_i$ by

$$G(i, n) = g_i(n).$$

G is well-defined because each g_i is well-defined.

To prove G is surjective, fix any $a \in \bigcup_{i\in\mathbb{N}} A_i$. Then there exists $i \in \mathbb{N}$ such that $a \in A_i$. Since g_i is surjective, there exists $n \in \mathbb{N}$ such that $g_i(n) = a$. Thus there exists $(i, n) \in \mathbb{N} \times \mathbb{N}$ such that $G(i, n) = a$.

By composing a bijection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$ with G, we obtain a surjection from $\mathbb{N}$ to $\bigcup_{i\in\mathbb{N}} A_i$, proving that $\bigcup_{i\in\mathbb{N}} A_i$ is countable. □

4.6 Cantor–Schröder–Bernstein

Definition 4.45. A set A is **dominated** by a set B, denoted $A \preceq B$, if there exists an injection from A to B.

If $A \preceq B$ and $A \not\approx B$, we say that A is **strictly dominated** by B, and write $A \prec B$.

Evidently $\preceq$ is transitive, since the composition of injections is an injection.

Since $\preceq$ resembles $\leq$, we can think of $A \preceq B$ as comparing the cardinalities of A and B: "$|A| \leq |B|$"; in fact, this is true when A and B are finite.

Example. Let A be a set. By Cantor's theorem, $A \not\approx \mathcal{P}(A)$. We have an injection from A to $\mathcal{P}(A)$ defined by $a \mapsto \{a\}$, so $A \preceq \mathcal{P}(A)$. Hence $A \prec \mathcal{P}(A)$.

Remark. The above tells us that there is no largest size of infinite set, since

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \cdots$$

A natural question to ask, then, is whether there exists a set X such that $\mathbb{N} \prec X \prec \mathcal{P}(\mathbb{N})$. Assuming that $\mathbb{R} \approx \mathcal{P}(\mathbb{N})$ (we will show this later), we can restate the negation of the above question as follows:

Is every uncountable subset of $\mathbb{R}$ equinumerous to $\mathbb{R}$?

By work of Gödel (1940) and Cohen (1963), the answers to the above questions are not decided by ZFC (assuming ZFC is consistent). This is known as the **Continuum Hypothesis** (CH).

Lemma 4.46. *If $A \approx B$, then $A \preceq B$ and $B \preceq A$.*

Proof. Since $A \approx B$, fix a bijection $f\colon A \to B$. Then $f\colon A \to B$ and $f^{-1}\colon B \to A$ are injections. □

How about the converse?

Theorem 4.47 (Cantor–Schröder–Bernstein)**.** *Let A and B be sets. If $A \preceq B$ and $B \preceq A$, then $A \approx B$.*

Proof. It is done with mirrors. Fix injections $f\colon A \to B$ and $g\colon B \to A$. Define C_n recursively as follows:

$$C_0 = A \setminus \operatorname{range}(g), \qquad C_{n+1} = g[f[C_n]] \quad (n \in \mathbb{N}^+).$$

Thus C_0 is the troublesome part that keeps g from being a bijection between B and A. We bounce it back and forth, obtaining $C_1, C_2, \ldots$. The function showing that $A \approx B$ is the function $h\colon A \to B$ defined by

$$h(x) = \begin{cases} f(x) & \text{if } x \in C_n \text{ for some } n, \\ g^{-1}(x) & \text{otherwise.} \end{cases}$$

Note that in the second case ($x \in A$ but $x \notin C_n$ for any n), it follows that $x \notin C_0$ and hence $x \in \operatorname{range}(g)$. Thus $g^{-1}(x)$ makes sense in this case.

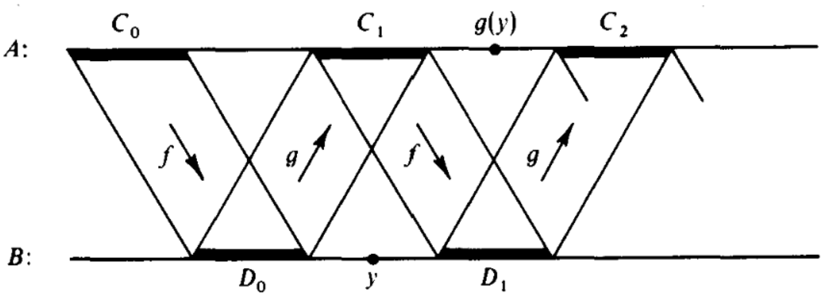


Figure 4.1: The Cantor–Schröder–Bernstein theorem. [End77]

We check that h is a bijection. Define $D_n = f[C_n]$, so that $C_{n+1} = g[D_n]$.

Injectivity: Consider distinct $x, x' \in A$. Since both f and g^{-1} are injective, the only possible problem arises when, say, $x \in C_m$ and $x' \in \bigcup_{n\in\mathbb{N}} C_n$. In this case,

$$h(x) = f(x) \in D_m,$$

whereas

$$h(x') = g^{-1}(x') \notin D_m,$$

lest $x' \in C_{m+1}$. Thus $h(x) \neq h(x')$.

Surjectivity: Finally we must check that range(h) exhausts B. Certainly each $D_n \subseteq \text{range}(h)$, because $D_n = h[C_n]$. Consider then a point y in $B \setminus \bigcup_{n\in\mathbb{N}} D_n$.

Where is $g(y)$? Certainly $g(y) \notin C_0$. Also $g(y) \notin C_{n+1}$, because $C_{n+1} = g[D_n]$, $y \notin D_n$, and g is injective. Thus $g(y) \notin C_n$ for any n. Hence $h(g(y)) = g^{-1}(g(y)) = y$. This shows that $y \in \text{range}(h)$.

□

Recall **Hilbert's Hotel**: Consider points in A as guests, and points in B as rooms of a hotel. The function f tells us which room each guest currently occupies, and g tells us which guest currently occupies each room.

To estalish a bijection from A to B, we need to find a way to accomodate all the guests into the rooms. In particular, we need that each guest is mapped to a distinct room (injectivity), and all of the rooms are occupied (surjectivity).

1. If g is not surjective, then there are some guests that do not have rooms; let $C_0 = A \setminus \text{range}(g)$ be the set of unaccomodated guests.

   We are going to try to find rooms to accomodate the guests in C_0.

2. We use f to indicate the rooms to which we would like to map these guests. Of course, we can't just shove them in those rooms, because we already have guests occupying those rooms.

   We can see which guests those are by applying g to that image set, i.e., $C_1 = g[f[C_0]]$; this is the set of guests currently occupying the rooms where we would like to put the guests in C_0.

3. To accomodate the guests in C_0, we displace the guests in C_1 from their rooms, and put the guests in C_0 into those rooms.

4. Now we have a new set of guests C_1 that don't have rooms; we can repeat the same process to find rooms for them.

As a consequence, for any sets A and B,

$$A \approx B \iff A \preceq B \text{ and } B \preceq A.$$

In order to show $A \approx B$, instead of explicitly constructing a bijection from A to B (which may be difficult), it suffices to show that $A \preceq B$ and $B \preceq A$.

Example. To show that the intervals $(0, 1)$ and $[0, 1]$ are equinumerous, it suffices to construct injections

$$(0, 1) \hookrightarrow [0, 1] \hookrightarrow (0, 1).$$

For the former, consider the inclusion map. For the latter, consider $x \mapsto (x + 2)/4$; this maps $[0, 1]$ to $[1/2, 3/4]$.

If a set is "sandwiched" between two equinumerous sets, we would expect the set to be equinumerous with those two sets too.

Corollary 4.48. *If $A \approx C$ and $A \subseteq B \subseteq C$, then $A \approx B \approx C$.*

Proof. Since $A \subseteq B$, we have $A \preceq B$ (as witnessed by the inclusion function).

Since $A \approx C$ and $B \subseteq C$, fix a bijection $f : A \to C$ and (injective) inclusion $\iota : B \to C$. Then $f^{-1} \circ \iota : B \to A$ is an injection. Hence $B \preceq A$.

By Cantor–Schröder–Bernstein, we conclude $A \approx B$. □

— Exercises —

Exercise 4.6.1. Suppose $A \preceq B$. Prove that for each set C, we have $\mathrm{Maps}(C, A) \preceq \mathrm{Maps}(C, B)$.

Solution. Fix an injection $f : A \to B$. Define $\Phi : \mathrm{Maps}(C, A) \to \mathrm{Maps}(C, B)$ by

$$g \mapsto f \circ g.$$

Suppose $\Phi(g) = \Phi(g')$. Then $f \circ g = f \circ g'$. Since f is injective, f is left-cancellative, so $g = g'$. Hence Φ is injective. □

4.7 Comparability

Given any sets A and B, is it true that either $A \preceq B$ or $B \preceq A$ (can "compare" any two arbitrary sets using the preceding relation)? This result turns out to be true, and proving it will be the main goal of this section.

4.7.1 Zorn's Lemma

Let $(P, \leq)$ be a partially ordered set.

Definition 4.49. Let $A \subseteq P$. We say that $u \in P$ is an **upper bound** for A if $x \leq u$ for all $x \in A$.

Definition 4.50. We say that $m \in P$ is **maximal** if there is no $x \in P$ such that $m < x$.

Remark. A maximal element does not have to be bigger than everything else: it just mustn't be smaller than anything else.

Axiom 4.51 (Zorn's lemma)**.** *Let P be a partially ordered set. If every chain in P has an upper bound, then P has a maximal element.*

This terminology of partially ordered sets will often be applied to an arbitrary family of sets. When this is done, it should be understood that the family is being regarded as a partially ordered set under the subset relation $\subseteq$.

Thus a maximal member of $\mathcal{S}$ is a set $M \in \mathcal{S}$ such that M is a subset of no other member of $\mathcal{S}$; a chain of sets is a family $\mathcal{C}$ of sets such that $X \subseteq Y$ or $Y \subseteq X$ for all $X, Y \in \mathcal{C}$.

Zorn's lemma is as follows:

> Let $\mathcal{S}$ be a set such that for every chain $\mathcal{C} \subseteq \mathcal{S}$, we have $\bigcup \mathcal{C} \in \mathcal{S}$. Then there exists $M \in S$ which is maximal, i.e., for every $X \in \mathcal{S}$, M is not a proper subset of X.

Remark.

- It is false that for finite $\mathcal{S}$, if M is maximal, then M has the largest cardinality.

  One counterexample is $\mathcal{S} = \{\emptyset, \{1\}, \{0\}, \{1, 2\}\}$. Note that $\{0\}$ and $\{1, 2\}$ are both maximal, but $\{0\}$ does not have the largest cardinality.

- It is also false that if M has maximal cardinality, then it is maximal.

  For example, consider $\mathcal{S} = P(\mathbb{N})$. $\mathbb{N} \setminus \{0\} \in \mathcal{P}(\mathbb{N})$ has the largest cardinality, but $\mathbb{N} \setminus \{0\}$ is not maximal.

- In general, it is false that the maximal element is the unary union of some $\mathcal{C} \subseteq \mathcal{S}$.

We are now in a very typical situation where Zorn's lemma can be applied. We would like to build a maximal object, and we feel as though we ought to be able to, because any non-maximal object can easily be extended.

Example.

- Fix a set X. Then $\mathcal{S} = \mathcal{P}(X)$ satisfies the assumptions of ZL. We can take $M := X$.

- Fix sets A and B. Let $\mathcal{S}$ be the set of graphs of injections f such that $\mathrm{dom}(f) \subseteq A$ and $\mathrm{range}(f) \subseteq B$. Then $\mathcal{S}$ satisfies the assumptions of ZL. Intuitively, the maximal element of $\mathcal{S}$ is our best attempt to construct an injection from A to B. In this case, the maximal element is not unique.

- Let $\mathcal{S}$ is the set of all finite subsets of $\mathbb{N}$. Then $\mathcal{S}$ does not satisfy the assumptions of ZL; consider the chain $C = \{[n] \mid n \in \mathbb{N}\} \subseteq \mathcal{S}$. Then $\bigcup \mathcal{C} = \mathbb{N} \notin \mathcal{S}$.

Theorem 4.52. *The following are equivalent:*

(i) Axiom of choice

(ii) Zorn's lemma

(iii) Well-ordering principle

Proof. We direct the reader to Section 3 of [HS65] for the complete proof. □

> The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?
>
> — Jerry L. Bona

This is a joke: although the three are all mathematically equivalent, many mathematicians find the axiom of choice to be intuitive, the well-ordering principle to be counterintuitive, and Zorn's lemma to be too complex for any intuition.

4.7.2 Applications of Zorn's Lemma

Since we are applying Zorn's lemma, we shall assume that the Axiom of Choice holds for this subsection.

Definition 4.53. Let R be a ring. A non-empty subset $I \subseteq R$ is an **ideal** if

(i) if $a, b \in I$, then $a + b \in I$; (closed under addition)

(ii) if $r \in R$ and $a \in I$, then $ra \in I$. (closed under left multiplication)

Trivially, R is an ideal itself. Other ideals are said to be **proper**.

A proper ideal M is a **maximal ideal** of R if M is not contained within any larger proper ideal of R. In other words, there is no proper ideal I such that $M \subsetneq I$.

Theorem 4.54. *Every (non-trivial, unital) ring contains a maximal ideal.*

Proof. Let $\mathcal{S} = \{\text{all proper ideals in } R\}$. By ZL, it suffices to prove that $\mathcal{S}$ satisfies the assumptions of ZL.

Let $\mathcal{C} \subseteq \mathcal{S}$ be a chain. We claim that $\bigcup \mathcal{C} \in \mathcal{S}$, i.e., $\bigcup \mathcal{C}$ is a proper ideal.

To prove $\bigcup \mathcal{C}$ is proper ($\bigcup \mathcal{C} \neq R$), it suffices to show that $1 \notin \bigcup \mathcal{C}$. Suppose, towards a contradiction, that $1 \in \bigcup C$. Fix $I \in \mathcal{C}$ such that $1 \in I$. By definition of ideal, for each $r \in R$, we have $1 \cdot r = r \in I$. Thus $I = R$, contradicting the fact that I is a proper ideal.

To prove that $\bigcup \mathcal{C}$ is an ideal:

(i) Let $a, b \in \bigcup \mathcal{C}$. Fix $I, J \in \mathcal{C}$ such that $a \in I$ and $b \in J$.

Since $\mathcal{C}$ is a chain, we have $I \subseteq J$ or $J \subseteq I$; WLOG assume $J \subseteq I$. Then $a, b \in I$, so $a + b \in I$. Thus $a + b \in \bigcup \mathcal{C}$.

(ii) Let $a \in \bigcup \mathcal{C}$. Fix $I \in \mathcal{C}$ such that $a \in I$.

For each $r \in R$, we have $ra \in I$, so $ra \in \bigcup \mathcal{C}$.

By ZL, there exists $M \in \mathcal{S}$ which is maximal in $\mathcal{S}$, as desired. □

Remark. In fact, this result is equivalent to the Axiom of Choice.

Example. In $\mathbb{Z}$, a proper ideal is maximal if and only if it is the set of multiples of some prime.

- $6\mathbb{Z}$ is not maximal, since $6\mathbb{Z} \subsetneq 2\mathbb{Z}$.
- $2\mathbb{Z}$ is maximal, since the other ideal that contains it is $\mathbb{Z}$.

Theorem 4.55. *Every vector space has a basis.*

Proof. If $V = \{\mathbf{0}\}$, then the empty set is a basis for V. Thus assume $V \neq \{\mathbf{0}\}$.

Let $\mathcal{S} = \{\text{linearly independent subsets of } V\}$. We shall prove that $\mathcal{S}$ satisfies the assumptions of ZL. Let $\mathcal{C} \subseteq \mathcal{S}$ be a non-empty chain.

Claim: $\bigcup \mathcal{C}$ is an upper bound for $\mathcal{C}$ in $\mathcal{S}$. (It suffices to show that $\bigcup \mathcal{C} \in \mathcal{S}$, i.e., $\bigcup \mathcal{C}$ is a linearly independent subset of V.)

Suppose, towards a contradiction, that $\bigcup \mathcal{C}$ is linearly dependent. Then there exists vectors $v_1, \ldots, v_n \in \bigcup \mathcal{C}$ and scalars $a_1, \ldots, a_n$, not all zero, such that

$$a_1 v_1 + \cdots + a_n v_n = \mathbf{0}.$$

Since $\bigcup \mathcal{C}$ is the union of all the sets in $\mathcal{C}$, fix $S_1, \ldots, S_n \in \mathcal{C}$ such that $v_i \in S_i$ for $i = 1, \ldots, n$.

Since $\mathcal{C}$ is totally ordered, one of the sets $S_1, \ldots, S_n$ must contain the others, so there is some set S_i that contains all of $v_1, \ldots, v_n$. This tells us there is a linearly dependent set of vectors in S_i, contradicting that S_i is linearly independent (because it is a member of $\mathcal{S}$).

By Zorn's lemma, $\mathcal{S}$ has a maximal element, i.e., a maximal linearly independent $B \subseteq V$.

Finally, we show that B is a basis of V. It suffices to show that B is a spanning set of V. Suppose, towards a contradiction, that B is not spanning. Fix $v \in V \setminus \operatorname{span}(B)$. Then $B' = B \cup \{v\}$ is a linearly independent subset of V that is larger than B, contradicting the maximality of B.

Therefore, B is a spanning set of V, and thus, a basis of V. □

4.7.3 Back to Comparability

Theorem 4.56 (Comparability)**.** *For all sets A and B, either $A \preceq B$ or $B \preceq A$.*

(Assuming Choice)

Proof. If $A \preceq B$, then we are done. Thus assume $A \npreceq B$, i.e., there are no injections from A to B.

Let $\mathcal{S}$ be the set of graphs of injections f with $\operatorname{dom}(f) \subseteq A$ and $\operatorname{range}(f) \subseteq B$.

Let $\mathcal{C} \subseteq \mathcal{S}$ be a chain. We claim $\bigcup \mathcal{C} \in \mathcal{S}$; let g denote $\bigcup \mathcal{C}$.

- First note that $g \subseteq A \times B$, since every element of $\mathcal{C}$ is a subset of $A \times B$.
- We check that g is a function. It suffices to show that if $(a, b), (a, b') \in g$, then $b = b'$.

  Let $(a, b), (a, b') \in g = \bigcup \mathcal{C}$. Fix $f, f' \in \mathcal{C}$ such that $(a, b) \in f$ and $(a, b') \in f'$.

  Since $\mathcal{C}$ is a chain, either $f \subseteq f'$ or $f' \subseteq f$. WLOG assume $f \subseteq f'$. Then $(a, b), (a, b') \in f'$. Since f' is a function, we have $b = b'$, as desired.

- Next we show that g is injective.

Hence $\mathcal{S}$ satisfies the assumptions of ZL. By ZL, fix $g \in \mathcal{S}$ which is maximal in $\mathcal{S}$.
Since $A \preceq B$ by assumption, the domain of g cannot be all of A (otherwise g would be an injection from A to B); thus $\operatorname{dom}(g) \subsetneq A$.
Claim: $\operatorname{range}(g) = B$.
If not, pick any $b \in B \setminus \operatorname{range}(g)$ and any $a \in A \setminus \operatorname{dom}(g)$. Then we can extend g to an injection by mapping a to b, which has a larger graph than g, contradicting the maximality of g (because $g \subsetneq g \cup \{(a, b)\}$).
Hence g is a bijection from $\operatorname{dom}(g)$ to B, so its inverse $g^{-1} \colon B \to \operatorname{dom}(g)$ is an injection from B to A. Therefore $B \preceq A$. □

Remark. The proof uses the maximality of g in a crucial way. Intuitively, imagine we are constructing an injection from A to B, but get stuck somewhere because we have used up all elements of B. Now, this g we get is maximal, and by taking its inverse, we have a injection from B to A.

Corollary 4.57. *A set A is infinite if and only if $\mathbb{N} \preceq A$.*
(Assuming Choice for $\boxed{\Rightarrow}$ *)*

Proof.
$\boxed{\Rightarrow}$ Assuming Choice, by Comparability, we have $\mathbb{N} \preceq A$ or $A \preceq \mathbb{N}$. If $\mathbb{N} \preceq A$, then we are done; thus assume $A \preceq \mathbb{N}$. Fix an injection $f \colon A \to \mathbb{N}$.
Since $\operatorname{range}(f) \subseteq \mathbb{N}$ and $\operatorname{range}(f)$ is infinite, by 4.29, $\operatorname{range}(f) \approx \mathbb{N}$. Since f is injective, $A \approx \operatorname{range}(f)$. Thus $A \approx \mathbb{N}$, and in particular, $\mathbb{N} \preceq A$.
$\boxed{\Leftarrow}$ This holds by 4.25. □

Remark. An interpretation of this result is that $\mathbb{N}$ is the smallest infinite set.

Definition 4.58. A set is **Dedekind infinite** if it is equinumerous to a proper subset of itself.

Proposition 4.59. *A set is Dedekind infinite if and only if it is infinite.*
(Assuming Choice for $\boxed{\Leftarrow}$ *)*

Proof. Let A be a set.
$\boxed{\Rightarrow}$ This holds by 4.9.
$\boxed{\Leftarrow}$ Suppose A is infinite. Assuming Choice, by 4.57, $\mathbb{N} \preceq A$; fix an injection $f \colon \mathbb{N} \to A$.
Define a function $g \colon A \to A \setminus \{f(0)\}$ by

$$g(a) = \begin{cases} a & \text{if } a \notin \operatorname{range}(f), \\ f(n+1) & \text{if } a = f(n). \end{cases}$$

(shifting to empty out one slot)
We check that g is a bijection:

Well-definedness: Since f is well-defined and injective, it follows that g is well-defined.

Injectivity: Suppose $g(a) = g(a')$.

- If $a, a' \notin \operatorname{range}(f) \setminus \{f(0)\}$, then we have $a = a'$.
- If $a, a' \in \operatorname{range}(f) \setminus \{f(0)\}$, fix n, n' such that $a = f(n)$ and $a' = f(n')$. Then $g(a) = g(a')$ implies $f(n+1) = f(n'+1)$. Since f is injective, we have $n = n'$. Thus $a = f(n) = f(n') = a'$.

- If $a \in \text{range}(f)$ and $a' \notin \text{range}(f) \setminus \{f(0)\}$, then $g(a) \in \text{range}(f) \setminus \{f(0)\}$ and $g(a') \notin \text{range}(f) \setminus \{f(0)\}$. Thus we cannot have $g(a) = g(a')$.

Surjectivity: Let $a \in A \setminus \{f(0)\}$.

- If $a \notin \text{range}(f)$, then $g(a) = a$.
- If $a \in \text{range}(f) \setminus \{f(0)\}$, there is a unique $n \in \mathbb{N}^+$ such that $f(n) = a$ (since f is injective). Let $a' = f(n-1)$. By definition, $g(a') = f(n) = a$.

Since $A \approx A \setminus \{f_0\}$, we conclude that A is Dedekind infinite. □

— Exercises —

Exercise 4.7.1. In this problem, we take $\mathbb{Q}$ to be a quotient of $\mathbb{Z} \times (\mathbb{Z} - \{0_{\mathbb{Z}}\})$, as defined in lecture.

(i) Prove that $\mathbb{Q}$ is countable.

(ii) Prove that the set of single-variable polynomials with rational coefficients is countable.

(iii) A real number is *algebraic* if it is a root of some single-variable polynomial with rational coefficients. Prove using Choice (or any of its consequences that we proved) that the set of algebraic numbers is countable.

(Hint: fundamental theorem of algebra.)

(iv) (Optional) Prove (iii) without using Choice.

Solution.

(i) The Cartesian product of two countable sets is countable, so $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is countable.

Consider the canonical projection $\pi \colon \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ defined by $\pi(p, q) = [(p, q)]$, which is surjective. Hence $\mathbb{Q}$ is countable.

(ii) Let $\mathbb{Q}[x]$ be the set of all single variable polynomials with rational coefficients.

Define a map $\mathbb{Q}^{<\mathbb{N}} \to \mathbb{Q}[x]$ by

$$(a_0, a_1, \dots, a_{n-1}, a_n) \mapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n$$

which maps each sequence of rationals to the polynomial whose coefficients are elements of the sequence.

This map is surjective. Since $\mathbb{Q}^{<\mathbb{N}}$ is countable, this implies that $\mathbb{Q}[x]$ is countable.

(iii) Let A denote the set of algebraic real numbers.

For each polynomial $p \in \mathbb{Q}[x]$, let R_p denote the set of real roots of p. By the fundamental theorem of algebra, $|R_p| \leq \deg p$, so each R_p is finite.

Since every algebraic real number is a root of some polynomial,

$$A = \bigcup_{p \in \mathbb{Q}[x]} R_p$$

which is a countable union of finite (hence countable) sets. By Choice, A is countable.

(iv)

□

Exercise 4.7.2. Prove the following statements without using Choice. (They have easy proofs using Choice.)

(a) The set of injections from $\mathbb{N}$ to $\mathbb{N}$ is uncountable.

(b) If A is Dedekind infinite and $A \preceq B$, then B is Dedekind infinite.

(c) If A is infinite, then $\mathbb{N} \preceq \mathcal{P}(\mathcal{P}(A))$.

Solution.

(a) Let $\mathcal{I}$ denote the set of injections from $\mathbb{N}$ to $\mathbb{N}$. For each subset $S \subseteq \mathbb{N}$, let $\chi_S \colon \mathbb{N} \to \{0,1\}$ be its characteristic function, and define

$$f_S(n) = \chi_S(n) + 2n \qquad (n \in \mathbb{N}).$$

Claim: The map $S \mapsto f_S$ is an injection from $\mathcal{P}(\mathbb{N})$ into $\mathcal{I}$.

If $S \neq T$, then $\chi_S \neq \chi_T$, so $f_S \neq f_T$.

Hence $\mathcal{P}(\mathbb{N}) \preceq \mathcal{I}$. Since $\mathcal{P}(\mathbb{N})$ is uncountable, so is $\mathcal{I}$.

(b) Let A be Dedekind infinite, and $A \preceq B$.

Then A is infinite; by Choice, $\mathbb{N} \preceq A$. Then $\mathbb{N} \preceq B$, so B is infinite; by Choice, B is Dedekind infinite.

Without Choice: Fix $A' \subsetneq A$ such that $A \approx A'$. Fix an injection $f \colon A \to B$.

By injectivity of f, we have $A \approx f[A]$ and $A' \approx f[A']$, so $f[A] \approx f[A']$. Then

$$B = (B \setminus f[A]) \cup f[A] \approx (B \setminus f[A]) \cup f[A'] \subsetneq B$$

since the union is disjoint (so this bijection leaves elements of $B \setminus f[A]$ unchanged, and sends elements of $f[A]$ to $f[A']$).

[include diagram]

(c) Let A be infinite. By Choice, $\mathbb{N} \preceq A$. Then $\mathbb{N} \preceq A \preceq \mathcal{P}(A) \preceq \mathcal{P}(\mathcal{P}(A))$.

Without Choice: The injection $n \mapsto \{\text{subsets of } A \text{ with cardinality } n\}$ for $n \in \mathbb{N}$ witnesses $\mathbb{N} \preceq \mathcal{P}(\mathcal{P}(A))$.

(For instance, if $A = \{1,2\}$, then $1 \mapsto \{\{1\},\{2\}\}$ and $2 \mapsto \{\{1,2\}\}$.)

□

Exercise 4.7.3. Assume that for every set Y and every **partition** P of Y, there is a choice function $G \colon P \to Y$. Prove that for every set X with $\emptyset \notin X$, there is a choice function $F \colon X \to \bigcup X$.

(Hint: X may not be a partition but there is a trick to "transform" it into one.)

This exercise tells us that if we have a choice function for partitions, then we have a choice function for arbitrary sets.

Ideally, if X is a partition (of $\bigcup X$), then we can apply the hypothesis in the question to obtain a choice function $X \to \bigcup X$.

Solution. Fix a set X with $\emptyset \notin X$. Since X may not be a partition, i.e., its parts are not disjoint, we want to make elements that lie in two parts different temporarily.

For each $A \in X$, define $P_A = A \times \{A\}$. (For instance, if $X = \{\{1,2\},\{2,3\}\}$, where $A = \{1,2\}$ and $B = \{2,3\}$, then transform $2 \in A$ to $(2, A)$, and $2 \in B$ to $(2, B)$.)

Let P be the collection of the transformed parts:

$$P = \{P_A \mid A \in X\}.$$

Then P is a partition. By assumption, there exists a choice function $G\colon P \to \bigcup P$ such that $G(P_A) \in P_A$ for every $A \in X$. Thus for each $A \in X$, $G(P_A) = (a, A)$ for some $a \in A$.

Define $F\colon X \to \bigcup X$ by

$$F(A) = \pi_1(G(P_A))$$

where π_1 is the projection onto the first coordinate. Then for each $A \in X$, we have $F(A) = a \in A$. Hence F is a choice function on X. □

Exercise 4.7.4. Suppose X is a set with $\emptyset \notin X$. Consider the set $\mathcal{S}$ consisting of all $G \subseteq X \times \bigcup X$ such that G is a graph of a function F with $\mathrm{dom}(F) \subseteq X$ and $F(A) \in A$ for every $A \in \mathrm{dom}(F)$.

(i) Prove that if $\mathcal{C} \subseteq \mathcal{S}$ is a chain, then $\bigcup \mathcal{C} \in \mathcal{S}$.

(ii) Use Zorn's lemma to prove that there is a choice function for X.

Solution.

(i) Let $\mathcal{C} \subseteq \mathcal{S}$ be a chain.

- Each $G \in \mathcal{C}$ is a subset of $X \times \bigcup X$, hence so is their union $\bigcup \mathcal{C}$. Thus $\bigcup \mathcal{C} \subseteq X \times \bigcup X$.
- Let $\bigcup \mathcal{C}$ be the graph of F. We want to show that F is a function.

  Let $(A, x), (A, y) \in \bigcup \mathcal{C}$. Fix $G_1, G_2 \in \mathcal{C}$ such that $(A, x) \in G_1$ and $(A, y) \in G_2$. Since $\mathcal{C}$ is a chain, either $G_1 \subseteq G_2$ or $G_2 \subseteq G_1$; WLOG assume $G_1 \subseteq G_2$.

  Then $(A, x), (A, y) \in G_2$. Since G_2 be the graph of a function, we have $x = y$. Hence F is a function. It follows that $\mathrm{dom}(F) \subseteq X$.
- Let $A \in \mathrm{dom}(F)$. Then $(A, x) \in \bigcup \mathcal{C}$ for some $x \in \bigcup X$, i.e., $x = F(A)$.

  Fix $G \in \mathcal{C}$ such that $(A, x) \in G$. Since $G \in \mathcal{S}$ is the graph of a function whose value at A lies in A, we have $x \in A$.

  Hence $F(A) \in A$ for all $A \in \mathrm{dom}(F)$.

Therefore $\bigcup \mathcal{C} \in \mathcal{S}$.

(ii) By (i), $\mathcal{S}$ satisfies the assumptions of ZL. Let G^* denote the maximal element of $\mathcal{S}$.

Let F^* denote the function whose graph is G^*; its domain is $\mathrm{dom}(F^*) \subseteq X$ and $F^*(A) \in A$ for all $A \in \mathrm{dom}(F^*)$.

Claim: $\mathrm{dom}(F^*) = X$ (this will show that F^* is a choice function for X).

Suppose, towards a contradiction, that $\mathrm{dom}(F^*) \neq X$. Then there exists some $A_0 \in X \setminus \mathrm{dom}(F^*)$. Since $A_0 \neq \emptyset$, fix some $a_0 \in A_0$. Define

$$G' = G^* \cup \{(A_0, a_0)\}.$$

Then $G' \subseteq X \times \bigcup X$. Let F' be the function with graph G'; then it has domain $\mathrm{dom}(F') = \mathrm{dom}(F^*) \cup \{A_0\} \subseteq X$ and $F'(A) \in A$ for every $A \in \mathrm{dom}(F')$. Thus $G' \in \mathcal{S}$. This contradicts the maximality of G^*.

□

Exercise 4.7.5 (MA1100T AY24/25)**.** Prove using Choice that for any two non-empty sets A and B, there is either a surjection from A to B, or a surjection from B to A.

Solution. By Comparability (which holds by Choice), we have either $A \preceq B$ or $B \preceq A$.

- If $A \preceq B$, then there is an injection from A to B, so there is a surjection from B to A.
- Similarly, if $B \preceq A$, then there is an injection from B to A, so there is a surjection from A to B.

□

Exercise 4.7.6 (MA1100T AY24/25)**.** Determine whether the following sets are finite, countably infinite, or uncountable:

(a) the set A of functions from $\mathbb{N}$ to $\mathbb{N}$ with finite range;

(b) the set B of functions from $\mathbb{N}$ to $\mathbb{N}$ such that for each $n \in \mathbb{N}$, the preimage of n is finite (possibly empty);

(c) the set C of strictly decreasing functions from $\mathbb{N}$ to $\mathbb{N}$ (a function $f \colon \mathbb{N} \to \mathbb{N}$ is strictly decreasing if whenever $x < y$, we have $f(x) > f(y)$);

(d) the set D of finite subsets of $\mathbb{Q}$.

Solution.

(a) A is uncountable, since it has an uncountable subset $\mathrm{Maps}(\mathbb{N}, \{0, 1\})$.

(b) B is uncountable; it suffices to show that B contains an uncountable subset. Consider the set of all bijections of $\mathbb{N}$:

$$\mathrm{Sym}(\mathbb{N}) = \{f \colon \mathbb{N} \to \mathbb{N} : f \text{ is bijective}\} .$$

If f is bijective, for each $n \in \mathbb{N}$, the fibre $f^{-1}(\{n\})$ is a singleton and thus finite. Hence $\mathrm{Sym}(\mathbb{N}) \subseteq B$.

Claim: $\mathrm{Sym}(\mathbb{N})$ is uncountable.

We shall embed the Cantor space $\{0, 1\}^{\mathbb{N}}$ into $\mathrm{Sym}(\mathbb{N})$. Given any binary sequence

$$x = (x_0, x_1, x_2, \dots) \in \{0, 1\}^{\mathbb{N}},$$

define a permutation f_x of $\mathbb{N}$ as follows: for each $n \in \mathbb{N}$,

- if $x_n = 0$, keep the pair $(2n, 2n + 1)$ in the same order;
- if $x_n = 1$, swap them.

It remains to check injectivity.

(c) $C = \emptyset$, so C is finite. It suffices to show that $\mathbb{N}$ has no infinite strictly descending chains.

Suppose, towards a contradiction, that there exists such a sequence $(a_n)_{n\in\mathbb{N}}$. Consider the set containing all of its elements. Since this is a nonempty set of natural numbers, by well-ordering, it contains a least element $a_k \in \mathbb{N}$. Since the sequence is strictly decreasing, we have $a_{k+1} < a_k$, which contradicts the minimality of a_k.

(d) Since

$$D = \bigcup_{n\geq 0} \{n\text{-element subsets of } \mathbb{Q}\},$$

D is a countable union of countable sets, so D is countable. In particular, D is infinite (e.g. there are infinitely many singletons $\{q\}$ with $q \in \mathbb{Q}$), so D is countably infinite.

□

Exercise 4.7.7 (MA1100T AY22/23)**.**

(a) Use Choice to prove that if P is a partition, then $P \preceq \bigcup P$.

(b) Prove that there is a set X such that $X \not\preceq \bigcup X$.

Solution.

(a) Let P be a partition. By the Axiom of Choice, there exists a choice function $F\colon P \to \bigcup P$ such that $F(S) \in S$ for every $S \in P$.

Claim: F is the required injection.

Suppose $F(S_1) = F(S_2)$. Then $F(S_1) \in S_1$ and $F(S_2) \in S_2$, so $F(S_1) = F(S_2) \in S_1 \cap S_2$. Since P is a partition, $S_1 = S_2$ since they are not disjoint.

(b) Let Y be any set, and take $X = \mathcal{P}(Y)$. Then $\bigcup X = \bigcup \mathcal{P}(Y) = Y$.

By Cantor's theorem, $Y \not\approx \mathcal{P}(Y)$, i.e., $\bigcup X \not\approx X$, so there is no injection from X to $\bigcup X$.

Alternative: Let $X = \{\{1\}, \{2\}, \{1, 2\}\}$. Observe that $\bigcup X = \{1, 2\}$. Since $|X| > |\bigcup X|$, there is no injection from X to $\bigcup X$.

□

Exercise 4.7.8 (MA1100T AY21/22)**.** For any infinite set A, the power set $\mathcal{P}(A)$ is infinite.

Solution. Let A be infinite. Then $\mathbb{N} \preceq A$, so $\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \preceq \mathcal{P}(A)$. □

II
Real Analysis

Real analysis deals with the real numbers and real-valued functions of a real variable (but we will generalise when appropriate). In this part, we shall prove the various theorems of calculus, which you should be acquainted with in high school.

- Chapter 5: This chapter defines the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and Euclidean space $\mathbb{R}^k$.
- **??**: Defining a notion of distance on a set gives rise to a metric space. This chapter discusses various structures in a metric space. We then
- **??**: We study the behaviour of sequences and series.
- **??**:
- **??**:
- **??**:
- **??**:

References: [Rud76; Apo57]

5
Real and Complex Number Systems

5.1 Ordered Sets and Boundedness

5.1.1 Definitions

Let S be a set.

Definition 5.1. An **order** on S is a binary relation $<$ such that

(i) for all $x, y \in S$, exactly one of $x < y$, $x = y$, or $y < x$ holds; (trichotomy)

(ii) if $x, y, z \in S$ are such that $x < y$ and $y < z$, then $x < z$. (transitivity)

We write $x \leq y$ if $x < y$ or $x = y$. We define $>$ and $\geq$ in the obvious way.

Definition 5.2. An **ordered set** is a set in which an order is defined.

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

Definition 5.3. Let $E \subseteq S$, where S is an ordered set.

- β is an **upper bound** of E if $x \leq \beta$ for all $x \in E$; if E has an upper bound, we say that E is **bounded above**.
- β is a **lower bound** of E if $x \geq \beta$ for all $x \in E$; if E has a lower bound, we say that E is **bounded below**.
- If E is bounded above and below, we say that E is **bounded**.

A set may have multiple upper and lower bounds. We give special names to the *least* upper bound and the *greatest* lower bound.

Definition 5.4. Let $E \subseteq S$, where S is an ordered set. We say that $\alpha \in S$ is the **supremum** of E if

(i) α is an upper bound for E;

(ii) if $\beta < \alpha$, then β is not an upper bound of E.

We say that $\alpha \in S$ is the **infimum** of E if

(i) α is a lower bound for E;

(ii) if $\beta > \alpha$, then β is not a lower bound of E.

Remark. By considering the contrapositive of (ii), we see that the supremum is the **least upper bound**, and the infimum is the **greatest lower bound**.

If a set has a supremum, then it is unique (see Exercise 5.1.1). We denote the supremum of a set E by $\sup E$, the infimum by $\inf E$.

Example. Let $E = \left\{\frac{1}{n} : n \in \mathbb{N}\right\}$. Then $\sup E = 1$, $\inf E = 0$.

Proof. It is clear that 1 is an upper bound for E. Suppose $\beta < 1$. Since $1 \in E$, evidently β is not an upper bound for E. Hence $\sup E = 1$.
It is clear that 0 is a lower bound for E. Suppose $\beta > 0$. Pick $n = \left\lfloor \frac{1}{\beta} \right\rfloor + 1$, then $\beta > \frac{1}{n}$, so β is not a lower bound for E. Hence $\inf E = 0$. □

This shows that the supremum and infimum of a set may not belong to the set itself.

5.1.2 Least-upper-bound Property

Definition 5.5. An ordered set S has the **least-upper-bound property** (l.u.b.) if every non-empty subset of S that is bounded above has a supremum in S.

We define the **greatest-lower-bound property** similarly.

Remark. If a set has the l.u.b. property, we sometimes say that it is **Dedekind complete**.

Proposition 5.6. *Let S be an ordered set. If S has the least-upper-bound property, then S has the greatest-lower-bound property.*

Proof. Let $B \subseteq S$ be non-empty and bounded below. We want to show that $\inf B \in S$.
Let $L \subseteq S$ be the set of all lower bounds of B:

$$L := \{y \in S \mid y \le x \text{ for all } x \in B\}.$$

Since B is bounded below, B has a lower bound, so $L \neq \emptyset$. Since every $x \in B$ is an upper bound of L, L is bounded above. By the l.u.b. property of S, $\sup L \in S$.

Claim: $\inf B = \sup L$.

To show that $\sup L = \inf B$ (greatest lower bound), we need to show that (i) $\sup L$ is a lower bound of B, (ii) and $\sup L$ is the greatest of the lower bounds.

(i) Suppose $\gamma < \sup L$. Then γ is not an upper bound of L. Since B is the set of upper bounds of L, $\gamma \notin B$. Considering the contrapositive, if $\gamma \in B$, then $\gamma \ge \sup L$. Hence $\sup L$ is a lower bound of B, and thus $\sup L \in L$.

(ii) If $\beta > \sup L$, then $\beta \notin L$, since $\sup L$ is an upper bound of L. In other words, $\sup L$ is a lower bound of B, but β is not if $\beta > \sup L$. This means that $\sup L$ is the greatest of the lower bounds.

Hence $\inf B = \sup L \in S$. □

Corollary 5.7. *If S has the greatest-lower-bound property, then it has the least-upper-bound property.*

Hence a set has the least-upper-bound property if and only if it has the greatest-lower-bound property.

5.1.3 Properties of Suprema and Infima

There is a corresponding set of properties of the infimum that the reader should formulate for himself.

The next result shows that a set with a supremum contains numbers arbitrarily close to its supremum.

Lemma 5.8 (Approximation property)**.** *Let S be non-empty, $b = \sup S$. Then for every $a < b$, there exists $x \in S$ such that*

$$a < x \leq b.$$

Proof. Since $b = \sup S$ is an upper bound of S, it follows that $x \leq b$ for all $x \in S$.

Next we show that there exists $x \in S$ such that $a < x$. Suppose, towards a contradiction, that $x \leq a$ for every $x \in S$. Then a is an upper bound for S, so $a \geq b$, a contradiction. □

For the rest of this section, suppose S has the least-upper-bound property.

Lemma 5.9 (Additive property)**.** *Let $A, B \subseteq S$ be non-empty, and*

$$C = A + B := \{x + y \mid x \in A,\ y \in B\}.$$

If A and B have suprema, then C has a supremum, and

$$\sup C = \sup A + \sup B.$$

Proof. Since A and B are non-empty, C is non-empty.

Let $a = \sup A$, $b = \sup B$. Let $z \in C$, then $z = x + y$ for some $x \in A$, $y \in B$.

Since $x \leq a$ and $y \leq b$, we have $z = x + y \leq a + b$, so $a + b$ is an upper bound for C. Since C is non-empty and bounded above, let $c = \sup C$. To show $a + b = c$, we need to show (i) $a + b \geq c$, and (ii) $a + b \leq c$.

(i) Since $a + b$ is an upper bound for C, and c is the *least* upper bound for C, we have $c \leq a + b$.

(ii) Let $\varepsilon > 0$ be arbitrary. By 5.8, there exist $x \in A$, $y \in B$ such that

$$a - \varepsilon < x, \qquad b - \varepsilon < y.$$

Adding these inequalities gives

$$a + b - 2\varepsilon < x + y \leq c.$$

Thus $a + b < c + 2\varepsilon$. Since $\varepsilon > 0$ is arbitrary, we have $a + b \leq c$.

□

Lemma 5.10 (Comparison property)**.** *Let non-empty $A, B \subseteq S$ such that $a \leq b$ for every $a \in A$, $b \in B$. If B has a supremum, then A has a supremum, and*

$$\sup A \leq \sup B.$$

Proof. Let $\beta = \sup B$. Then $b \leq \beta$ for all $b \in B$.

For each $a \in A$, choose any $b \in B$. Then $a \leq b \leq \beta$. Thus β is an upper bound for A.

Since A is non-empty and bounded above, by the lub property of S, A has a supremum in S; let $\alpha = \sup A$. Since β is an upper bound for A, and α is the *least* upper bound for A, we have that $\alpha \leq \beta$, as desired. □

Lemma 5.11. *Let $B \subseteq S$ be non-empty and bounded below. Let*

$$A = -B := \{-b \mid b \in B\}.$$

Then A is non-empty and bounded above. Furthermore, $\inf B$ *exists, and* $\inf B = -\sup A$.

Proof. Since B is non-empty, so is A. Since B is bounded below, let β be a lower bound for B. Then $b \geq \beta$ for all $b \in B$, which implies $-b \leq -\beta$ for all $b \in B$. Hence $a \leq -\beta$ for all $a \in A$, so $-\beta$ is an upper bound for A. By the l.u.b. property, A has a supremum.

Then $a \leq \sup A$ for all $a \in A$, so $b \geq -\sup A$ for all $b \in B$. Thus $-\sup A$ is a lower bound for B.

Also, we saw before that if β is a lower bound for B then $-\beta$ is an upper bound for A. Then $-\beta \geq \sup A$ (since $\sup A$ is the least upper bound), so $\beta \leq -\sup A$. Therefore $-\sup A$ is the greatest lower bound of B. □

5.1.4 Fields

Definition 5.12. A field F is called an **ordered field** if there exists an order $<$ on F such that for all $x, y, z \in F$,

(i) if $y < z$ then $x + y < x + z$;

(ii) if $x > 0$ and $y > 0$ then $xy > 0$.

We call x **positive** if $x > 0$, and **negative** if $x < 0$.

All the familiar rules for working with inequalities apply in every ordered field: Multiplication by positive [negative] quantities preserves [reverses] inequalities, no square is negative, etc. The following result lists some of these.

Lemma 5.13 (Basic properties)**.** *Let F be an ordered field, $x, y, z \in F$.*

(i) If $x > 0$ then $-x < 0$, and vice versa.

(ii) If $x > 0$ and $y < z$, then $xy < xz$.

(iii) If $x < 0$ and $y < z$, then $xy > xz$.

(iv) If $x \neq 0$, then $x^2 > 0$. In particular, $1 > 0$.

(v) If $0 < x < y$, then $0 < \frac{1}{y} < \frac{1}{x}$.

Proof.

(i) If $x > 0$, by (i) of Definition 5.12, we have

$$-x = -x + 0 < -x + x = 0.$$

Similarly, if $x < 0$, then $0 = -x + x < -x + 0$. Hence $-x > 0$.

(ii) Since $z > y$, we have $z - y > y - y = 0$. By (i) of Definition 5.12, $x(z - y) > 0$. Hence

$$xz = x(z - y) + xy > 0 + xy = xy.$$

(iii) By (i) and (ii),

$$-[x(z - y)] = (-x)(z - y) > 0,$$

so that $x(z-y)<0$. Hence $xz<xy$.

(iv) If $x>0$, by (ii) of Definition 5.12, we have $x^2=x\cdot x>0$.

If $x<0$, then $-x>0$, so $x^2=(-x)^2>0$.

Since $1\neq 0$, it follows that $1=1^2>0$.

(v) If $y>0$ and $v\le 0$, then $yv\le 0$. But $y\left(\frac{1}{y}\right)=1>0$, so $\frac{1}{y}>0$. Likewise, $\frac{1}{x}>0$.

Multiplying both sides of the inequality $x<y$ by the positive quantity $\left(\frac{1}{x}\right)\left(\frac{1}{y}\right)$, we obtain $\frac{1}{y}<\frac{1}{x}$.

□

— Exercises —

★ **Exercise 5.1.1.** Show that if a set has a supremum, then it is unique.

Proof. Let α and β be suprema of a set E.

Since β is a supremum, it is an upper bound for E. Since α is a supremum, it is the *least* upper bound, so $\alpha\le\beta$.

Interchanging the roles of α and β gives $\beta\le\alpha$. Hence $\alpha=\beta$. □

★ **Exercise 5.1.2** ([Rud76] 1.4)**.** Let E be a non-empty subset of an ordered set. Suppose α is a lower bound of E, and β is an upper bound of E. Prove that $\alpha\le\beta$.

Solution. Since E is non-empty, fix $x\in E$. Since α is a lower bound of E, we have $\alpha\le x$. Since β is an upper bound of E, we have $x\le\beta$.

Combining these two inequalities gives $\alpha\le x\le\beta$; thus $\alpha\le\beta$. □

★ **Exercise 5.1.3** (Finite sets always have suprema)**.** Let S be an ordered set (not assumed to have the l.u.b. property).

(i) Show that every two-element subset $\{x,y\}\subseteq S$ has a supremum.

(ii) Deduce (using induction) that every finite subset of S has a supremum.

Solution.

(i) Use trichotomy: if $x\le y$, the supremum is y; if $x>y$, the supremum is x.

(ii) We will show that for each $n\in\mathbb{N}$, every n-element subset of S has a supremum.

The case of a singleton is trivial. The case where $n=2$ has been shown in (i).

Suppose the desired result holds for n. Let $A=\{x_1,\dots,x_n,x_{n+1}\}\subseteq S$. By induction hypothesis, $\{x_1,\dots,x_n\}$ has a supremum x_k for some $k\in\{1,\dots,n\}$.

- If $x_k\le x_{n+1}$, then $\sup A=x_{n+1}$.
- If $x_k>x_{n+1}$, then $\sup A=x_k$.

□

★ **Exercise 5.1.4** (If one set lies above another)**.** Let S be a set with the l.u.b. property and the g.l.b. property, and let X and Y be non-empty subsets of S.

(i) If every element of $X\le$ every element of Y, show that $\sup X\le\inf Y$.

(ii) If every element of $X<$ every element of Y, is is true that $\sup X<\inf Y$? (Give a proof or a counterexample.)

Solution.

(i) Since X is non-empty and bounded above by elements of Y, let $\alpha = \sup X$.

Similarly, since Y is non-empty and bounded below by elements of X, let $\beta = \inf Y$.

Since every $y \in Y$ is an upper bound for X, and α is the *least* upper bound, we must have $\alpha \leq y$ for all $y \in Y$. Thus α is a lower bound of Y.

But β is the *greatest* lower bound of Y, so $\alpha \leq \beta$.

(ii) Let $X = (0,1)$ and $Y = (1,2)$. Then $\sup X = 1 = \inf Y$.

□

★★ **Exercise 5.1.5** (Least upper bounds of least upper bounds)**.** Let S be an ordered set with the l.u.b. property, and let $\{A_i\}_{i\in I}$ be a non-empty family of non-empty subsets of S.

(i) Suppose each A_i is bounded above, let $\alpha_i = \sup A_i$, and suppose further that $\{\alpha_i\}_{i\in I}$ is bounded above. Show that $\bigcup_{i\in I} A_i$ is bounded above, and $\sup\left(\bigcup_{i\in I} A_i\right) = \sup_{i\in I} \alpha_i$.

(ii) On the other hand, suppose either (a) not all of the A_i are bounded above, or (b) they are all bounded above, but writing $\alpha_i = \sup A_i$ for each i, the set $\{\alpha_i\}_{i\in I}$ is unbounded above. Show in each of these cases that $\bigcup_{i\in I} A_i$ is unbounded above.

(iii) Again suppose each A_i is bounded above, with $\alpha_i = \sup A_i$. Show that $\bigcap_{i\in I} A_i$ is also bounded above. Must it be non-empty? If it is non-empty, what can be said about the relationship between $\sup(\bigcap_{i\in I} A_i)$ and the numbers α_i $(i \in I)$.

Solution.

(i) Let $A = \bigcup_{i\in I} A_i$. Denote $\alpha = \sup_{i\in I} a_i$. Let $a \in A$ be arbitrary. Then $a \in A_i$ for some A_i, so $a \leq \alpha_i \leq \alpha$. Thus A is bounded above, so $\sup A$ exists.

We already shown that α is an upper bound of A. It remains to show that α is the *least* upper bound. Let $u < \alpha$; we will show that u is not an upper bound of A.

Since $u < \alpha = \sup_{i\in I} \alpha_i$, by definition of supremum, $\alpha_{i_0} > u$ for some $i_0 \in I$.

But $\alpha_{i_0} = \sup A_{i_0}$, so $u < \sup A_{i_0}$; by definition of supremum, $a > u$ for some $a \in A_{i_0}$.

Since $a \in A$ but $a > u$, this means that u is not an upper bound of A.

(ii) Let $A = \bigcup_{i\in I} A_i$.

(a) Suppose A_{i_0} is not bounded above for some $i_0 \in I$. Then for any $u \in S$, there exists $a \in A_{i_0} \subseteq A$ such that $a > u$. Hence A is unbounded above.

(b) Let $u \in S$. Since $\{\alpha_i\}_{i\in I}$ is unbounded above, $\alpha_{i_0} > u$ for some $i_0 \in I$. But $\alpha_{i_0} = \sup A_{i_0}$; by definition of supremum, there exists $a \in A_{i_0} \subseteq A$ such that $a > u$. Hence A is unbounded above.

(iii) Let $A = \bigcap_{i\in I} A_i$. For each $i \in I$, since A_i is bounded above and $\alpha_i = \sup A_i$, we have $a_i \leq \alpha_i$ for all $a_i \in A_i$.

If $A \neq \emptyset$, let $x \in A$. Then $x \in A_i$ for every $i \in I$, so $x \leq \alpha_i$ for all $i \in I$. Since every element of A is bounded above by every α_i, we conclude that A is bounded above by each α_i.

$\bigcap_{i\in I} A_i$ need not be non-empty; let $A_n := (0, \frac{1}{n})$ for $n \in \mathbb{N}$. Then $\bigcap_{n=1}^{\infty} A_n = \emptyset$.

If $A = \bigcap_{i\in I} A_i \neq \emptyset$, then $\sup A \leq \alpha_i$ for all $i \in I$. Thus $\sup\left(\bigcap_{i\in I} A_i\right) \leq \inf_{i\in I} \alpha_i$.

□

★★★ **Exercise 5.1.6** (Fixed points for increasing functions)**.** Let S be a non-empty ordered set such that every non-empty subset $E \subseteq S$ has both a supremum and an infimum. (A closed interval $[a, b]$ in $\mathbb{R}$ is an example of such an S.)

Let $f \colon S \to S$ be monotonically increasing. Show that there exists $x \in S$ such that $f(x) = x$.

Solution. Consider the set $A := \{x \in S \mid f(x) \geq x\}$.

Case 1: $A \neq \emptyset$**.** Let $\alpha = \sup A$.

Claim: $f(\alpha) = \alpha$.

Since f is monotonically increasing and $x \leq \alpha$ for all $x \in A$, we have

$$f(x) \leq f(\alpha) \quad \text{for all } x \in A.$$

In particular, since $f(x) \geq x$, we obtain $f(\alpha) \geq x$ for all $x \in A$; thus

$$f(\alpha) \geq \sup A = \alpha.$$

Suppose, towards a contradiction, that $f(\alpha) > \alpha$. Since $f(\alpha) > \alpha$, and S is an ordered set, there exists $\alpha' \in S$ such that $\alpha < \alpha' < f(\alpha)$. Since f is increasing, we have $f(\alpha') \geq f(\alpha) > \alpha'$, so $\alpha' \in A$. But this contradicts the assumption that $\alpha = \sup A$, since $\alpha' > \alpha$ and $\alpha' \in A$.

Thus we must have $f(\alpha) \leq \alpha$. Combined with the earlier inequality $f(\alpha) \geq \alpha$, it follows that $f(\alpha) = \alpha$.

Case 2: $A = \emptyset$**.** Define $B := \{x \in S \mid f(x) \leq x\}$.

Then $B \neq \emptyset$, and we can apply a symmetric argument to the infimum $\beta := \inf B$. Using similar reasoning, we conclude that $f(\beta) = \beta$.

In either case, a fixed point of f exists. □

★ **Exercise 5.1.7.**

(a) Prove that $\inf\{x + y + z \mid x, y, z \in \mathbb{R},\ 0 < x < y < z\} = 0$.

(b) Determine the values of each of the following (some may not exist).

$$\begin{aligned}
a &= \inf\{x + y + z \mid x, y, z \in \mathbb{R},\ 1 < x < y < z\},\\
b &= \inf\{x + y - z \mid x, y, z \in \mathbb{R},\ 1 < x < y < z\},\\
c &= \inf\{x - y + z \mid x, y, z \in \mathbb{R},\ 1 < x < y < z\},\\
d &= \sup\{x + y + z \mid x, y, z \in \mathbb{R},\ 1 < x < y < z\},\\
e &= \sup\{x + y - 2z \mid x, y, z \in \mathbb{R},\ 1 < x < y < z\}.
\end{aligned}$$

Solution.

(a) Let $A = \{x + y + z \mid x, y, z \in \mathbb{R},\ 0 < x < y < z\}$.

Evidently 0 is a lower bound of A. Let $s > 0$; evidently s is not a lower bound of A, since we can choose $x < y < z < \frac{s}{3}$ such that $x + y + z < s$.

(b) $a = 3$, b does not exist since the set is not bounded below, $c = 1$, d does not exist since the set is not bounded above, $e = 0$.

□

★ **Exercise 5.1.8.** Let $A \subseteq \mathbb{R}$ be non-empty and bounded above, and let $c \in \mathbb{R}$. Define the set $c + A$ by

$$c + A = \{c + a : a \in A\}.$$

Show that $\sup(c + A) = c + \sup A$.

Solution. Let $s = \sup A$. We will show that $\sup(c + A) = c + s$.

(i) Since s is an upper bound for A, we have $a \leq s$ for all $a \in A$.

Thus $c + a \leq c + s$ for all $a \in A$, so $c + s$ is an upper bound for $c + A$.

(ii) Let b be an arbitrary upper bound for $c + A$, i.e., $c + a \leq b$ for all $a \in A$.

This is equivalent to $a \leq b - c$ for all $a \in A$. Thus $b - c$ is an upper bound for A. Since s is the *least* upper bound of A, we have $s \leq b - c$, so $c + s \leq b$.

□

★ **Exercise 5.1.9** ([Abb16] 1.3.5)**.** Let $A \subseteq \mathbb{R}$ be non-empty and bounded above, and let $c \in \mathbb{R}$. Define the set

$$cA = \{ca : a \in A\}.$$

(i) If $c \geq 0$, show that $\sup(cA) = c \sup A$.

(ii) Postulate a similar type of statement for $\sup(cA)$ for the case $c < 0$.

Solution.

(i) The result trivially holds for $c = 0$. Thus assume $c > 0$. Let $s = \sup A$. We will show that $\sup(cA) = cs$.

Since s is an upper bound of A, we have $s \geq a$ for all $a \in A$, so $cs \geq ca$ for all $a \in A$. Thus cs is an upper bound of cA.

Let b be an upper bound of cA. Then $b \geq ca$ for all $a \in A$, i.e., $\frac{b}{c} \geq a$, so $\frac{b}{c}$ is an upper bound of A. Since s is the *least* upper bound of A, we have $s \leq \frac{b}{c}$, so $cs \leq b$, as desired.

(ii)

□

★ **Exercise 5.1.10** ([Abb16] 1.3.7)**.** Prove that if α is an upper bound for A, and if α is also an element of A, then it must be that $\alpha = \sup A$.

Solution. Let b be an upper bound of A. Then $a \leq b$ for all $a \in A$.
In particular, since $\alpha \in A$, we have $\alpha \leq b$. □

★ **Exercise 5.1.11** ([Abb16] 1.3.9)**.**

(a) If $\sup A < \sup B$, show that there exists an element $b \in B$ that is an upper bound for A.

(b) Give an example to show that this is not always the case if we only assume $\sup A \leq \sup B$.

Solution.

(a) Let $s = \sup B$. Then for any $\varepsilon > 0$, there exists $b \in B$ such that $s - \varepsilon < b$. Choose $\varepsilon = s - \sup A > 0$. Then $\sup A < b$, so for all $a \in A$, $a \leq b$.

(b) Take $A = B = (0, 1)$. Clearly no element of B is an upper bound for B (i.e., A), since 1 is the least upper bound but it does not belong to the set, nor does any larger bound.

□

5.2 Construction of the Real Numbers

$\mathbb{Q}$ has some problems, the first of which being **algebraic incompleteness**: there exists equations with coefficients in $\mathbb{Q}$ but do not have solutions in $\mathbb{Q}$ (in fact $\mathbb{R}$ has this problem too, but $\mathbb{C}$ is algebraically complete, by the fundamental theorem of algebra).

Lemma 5.14. *$x^2 - 2 = 0$ has no solution in $\mathbb{Q}$.*

Proof. Suppose, towards a contradiction, that $x^2 - 2 = 0$ has a solution $x = \frac{p}{q}$, $q \neq 0$. We also assume $\frac{p}{q}$ is in lowest terms, i.e., p and q are coprime.

Then $\frac{p^2}{q^2} = 2$, or $p^2 = 2q^2$. Observe that p^2 is even, so p is even; let $p = 2m$ for some integer m. This then implies $4m^2 = 2q^2$, or $2m^2 = q^2$. Similarly, q^2 is even so q is even.

Since p and q share a common factor of 2, we have reached a contradiction. □

Proposition 5.15. *$\mathbb{Q}$ does not have the least-upper-bound property.*

Proof. Consider the sets

$$\begin{aligned} A &:= \{p \in \mathbb{Q} : p > 0,\ p^2 < 2\}, \\ B &:= \{p \in \mathbb{Q} : p > 0,\ p^2 > 2\}. \end{aligned}$$

Claim: A contains no largest number, and B contains no smallest number.

For each rational $p > 0$, let

$$q := p - \frac{p^2 - 2}{p + 2} = \frac{2p + 2}{p + 2}.$$

Then

$$q^2 - 2 = \frac{2(p^2 - 2)}{(p + 2)^2}.$$

Let $p \in A$. Then $p^2 < 2$, so $q^2 - 2 < 0$, i.e., $q^2 < 2$. Thus $q \in A$. Hence A has no largest number.

Let $p \in B$. Then $p^2 > 2$, so $q^2 - 2 > 0$, i.e., $q^2 > 2$. Thus $q \in B$. Hence B has no smallest number.

Note that B is the set of all upper bounds of A, and B does not have a smallest element. Hence $A \subseteq \mathbb{Q}$ is bounded above, but has no least upper bound in $\mathbb{Q}$. □

Remark. The formula for p might seem to be "rabbit-out-of-hat". We motivate it as such: If $p^2 < 2$ we want to increase p slightly, while if $p^2 > 2$ we want to decrease it, so the amount we should change it by should be obtained from $p^2 - 2$. A denominator is needed to prevent overshooting, especially when p is large, so we use one that grows with p; the actual choice of denominator $p + 2$ can be regarded as the result of trial and error.

The second problem that $\mathbb{Q}$ has is **analytic incompleteness**: there exists a sequence in $\mathbb{Q}$ which converges to a point that is not in $\mathbb{Q}$; for example, the sequence $1, 1.4, 1.41, 1.414, 1.4142, \dots$ converges to $\sqrt{2}$.

Definition 5.16. We say that $\alpha \subseteq \mathbb{Q}$ is a **Dedekind cut** if

(i) $\alpha \neq \emptyset$, $\alpha \neq \mathbb{Q}$; (non-trivial)

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

(iii) if $p \in \alpha$, then there exists $r \in \alpha$ such that $p < r$. (no largest member)

Remark. (ii) implies two facts which will be used freely:

- If $p \in \alpha$ and $q \notin \alpha$, then $p < q$. (This is the contrapositive of (ii).)
- If $p \notin \alpha$ and $p < q$, then $q \notin \alpha$.

Example. Let $r \in \mathbb{Q}$. Define

$$r^* := \{p \in \mathbb{Q} \mid p < r\}.$$

We check that r^* is a Dedekind cut:

(i) Since $p = r - 1 \in r^*$, we get $r^* \neq \emptyset$.

Since $p = 1 + r \notin r^*$, we get $r^* \neq \mathbb{Q}$.

(ii) Let $p \in r^*$, and $q \in \mathbb{Q}$ be such that $q < p$.

Then $q < p < r$ implies that $q < r$. Thus $q \in r^*$.

(iii) Let $p \in r^*$. Put $q = \frac{p+r}{2} \in \mathbb{Q}$. Then $p < q < r$. Thus $q \in r^*$.

This shows that we can associate every $r \in \mathbb{Q}$ with the cut r^*; we call such cuts **rational cuts**.

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

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

(i) Since $1 \in \alpha$, we get $\alpha \neq \emptyset$. Since $2 \notin \alpha$, we get $\alpha \neq \mathbb{Q}$.

(ii) Let $p \in \alpha$, and $q \in \mathbb{Q}$ be such that $q < p$. Monotonicity of the cubic function implies that $q^3 < p^3 < 2$. Thus $q \in \alpha$.

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

Definition 5.17. The set of **real numbers** $\mathbb{R}$ is the set of all Dedekind cuts:

$$\mathbb{R} := \{\alpha \subseteq \mathbb{Q} \mid \alpha \text{ is a Dedekind cut}\}.$$

Notice that $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$. Hence a subset of $\mathbb{R}$ is a collection of Dedekind cuts.

Remark. Intuitively, a real number r is the set of all rational numbers strictly less than r.

Proposition 5.18. *For all $\alpha, \beta \in \mathbb{R}$, define*

$$\alpha < \beta \iff \alpha \subsetneq \beta.$$

Then $<$ is an order on $\mathbb{R}$.

Proof.

Trichotomy: We want to show that for all $\alpha, \beta \in \mathbb{R}$, exactly one of the following holds:

$$\alpha \subsetneq \beta, \quad \alpha = \beta, \quad \beta \subsetneq \alpha.$$

If $\alpha = \beta$, then it is clear that $\alpha \subsetneq \beta$ and $\beta \subsetneq \alpha$ do not hold.

Thus suppose that $\alpha \neq \beta$. We need to show exactly one of $\alpha \subsetneq \beta$ and $\beta \subsetneq \alpha$ holds. Suppose, towards a contradiction, that this is false.

- If none of $\alpha \subsetneq \beta$ and $\beta \subsetneq \alpha$ hold, then there exists $q \in \alpha$ such that $q \notin \beta$, and there exists $q' \in \beta$ such that $q' \notin \alpha$.

  Since $q \notin \beta$, we must have $q \geq q'$. Similarly, we must have $q' \geq q$. Thus, $q = q'$, a contradiction.
- It is not possible that both $\alpha \subsetneq \beta$ and $\beta \subsetneq \alpha$ hold, since if $\alpha \subsetneq \beta$, then there exists $q \in C$ such that $q \notin \beta$, contradicting $\beta \subsetneq \alpha$.

Transitivity: Suppose $\alpha < \beta$ and $\beta < \gamma$. Then $\alpha \subsetneq \beta$ and $\beta \subsetneq \gamma$, so $\alpha \subsetneq \gamma$. Thus $\alpha < \gamma$.

□

Theorem 5.19. *The ordered set $\mathbb{R}$ has the least-upper-bound property.*

Proof. Let S be a non-empty subset of $\mathbb{R}$ bounded above.

Claim: $\sup(S) = \bigcup S$.

First, we need to show that $\bigcup S \in \mathbb{R}$, i.e., $\bigcup S$ is a Dedekind cut.

- $\bigcup S$ is non-empty, since S is non-empty and each element of S is non-empty.
- Since S is bounded, every $\alpha \in S$ is a proper subset of some Dedekind cut β. Thus $\bigcup S \subseteq \beta \subsetneq \mathbb{Q}$.
- Let $p \in \bigcup S$, and $q \in \mathbb{Q}$ be such that $q < p$. Fix $\alpha \in S$ such that $p \in \alpha$. Since α is a Dedekind cut, $q \in \alpha$. Thus $q \in \bigcup S$.
- Let $p \in \bigcup S$. Fix $\alpha \in S$ such that $p \in \alpha$. Since α is a Dedekind cut, there exists $r \in \alpha$ such that $r > p$.

  Thus we have $r \in \bigcup S$ and $r > p$.

Second, by definition of union, for all $\alpha \in S$, we have $\alpha \subseteq \bigcup S$. Thus $\bigcup S$ is an upper bound for S (in $\mathbb{R}$). Finally, we need to show that $\bigcup S$ is the *least* upper bound of S. Let $\gamma \subsetneq \bigcup S$. Fix a rational $p \in \bigcup S \setminus \gamma$. Fix $\alpha \in S$ such that $p \in \alpha$. Then α is not a subset of γ (because $p \in \alpha \setminus \gamma$), so by trichotomy, $\gamma \subsetneq \alpha$. Thus γ is not an upper bound of S.

□

We now make $\mathbb{R}$ into an ordered field by defining addition and multiplication on $\mathbb{R}$.

Definition 5.20. For all $\alpha, \beta \in \mathbb{R}$, define addition as

$$\alpha + \beta := \{r \in \mathbb{Q} \mid r = a + b, a \in \alpha, b \in \beta\}.$$

We check that addition is closed in $\mathbb{R}$: for all $\alpha, \beta \in \mathbb{R}$, $\alpha + \beta \in \mathbb{R}$.

(i) Since $\alpha \neq \emptyset$ and $\beta \neq \emptyset$, there exists $a \in \alpha$ and $b \in \beta$. Hence $r = a + b \in \alpha + \beta$, so $\alpha + \beta \neq \emptyset$.

Since $\alpha \neq \mathbb{Q}$ and $\beta \neq \mathbb{Q}$, there exist $c \notin \alpha$ and $d \notin \beta$. Thus $r' = c + d > a + b$ for any $a \in \alpha$, $b \in \beta$, so $r' \notin \alpha + \beta$. Hence $\alpha + \beta \neq \mathbb{Q}$.

(ii) Let $r \in \alpha + \beta$ and $r' \in \mathbb{Q}$ be such that $r' < r$. We want to show that $r' \in \alpha + \beta$.

Write $r = a + b$ for some $a \in \alpha$, $b \in \beta$. Then $r' - a < b$. Since $\beta \in \mathbb{R}$ is downward closed, we have $r' - a \in \beta$. Thus $r' - a = b_1$ for some $b_1 \in \beta$.

Hence $r' = a + b_1 \in \alpha + \beta$.

(iii) Let $r \in \alpha + \beta$. Then $r = a + b$ for some $a \in \alpha$, $b \in \beta$.

Since $\alpha, \beta \in \mathbb{R}$ have no largest member, there exist $a' \in \alpha$, $b' \in \beta$ such that $a < a'$ and $b < b'$. Then $r = a + b < a' + b'$, where $a' + b' \in \alpha + \beta$.

Take $r' = a' + b' \in \alpha + \beta$, such that $r < r'$.

Lemma 5.21. *$\mathbb{R}$ with addition defined above is an Abelian group.*

(i) Addition is commutative: $\alpha + \beta = \beta + \alpha$ for all $\alpha, \beta \in \mathbb{R}$.

(ii) Addition is associative: $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for all $\alpha, \beta, \gamma \in \mathbb{R}$.

(iii) Additive identity: Define $0^* := \{p \in \mathbb{Q} \mid p < 0\}$. Then $\alpha + 0^* = \alpha$ for all $\alpha \in \mathbb{R}$.

(iv) Additive inverse: For each $\alpha \in \mathbb{R}$, define $\beta = \{p \in \mathbb{Q} \mid (\exists r > 0)\ -p - r \notin \alpha\}$. Then $\alpha + \beta = 0^*$.

Proof.

(i) $\boxed{\subseteq}$ Let $r \in \alpha + \beta$. Then $r = a + b$ for some $a \in \alpha$, $b \in \beta$.

By commutativity of $+$ on $\mathbb{Q}$, we have $r = b + a$. Hence $r \in \beta + \alpha$.

$\boxed{\supseteq}$ Similar as above.

(ii) $\boxed{\subseteq}$ Let $r \in \alpha + (\beta + \gamma)$. Then $r = a + (b + c)$ for some $a \in \alpha$, $b \in \beta$, $c \in \gamma$.

By associativity of $+$ on $\mathbb{Q}$, we have $r = (a + b) + c$. Hence $r \in (\alpha + \beta) + \gamma$.

$\boxed{\supseteq}$ Similar as above.

(iii) It is clear that 0^* is a cut, since 0^* is a rational cut.

$\boxed{\subseteq}$ Let $r \in \alpha + 0^*$. Then $r = a + p$ for some $a \in \alpha, p \in 0^*$.

Thus $r = a + p < a + 0 = a$, so $r \in \alpha$ by downward closure.

$\boxed{\supseteq}$ Let $r \in \alpha$. Then there exists $r' \in \alpha$ where $r' > r$. Thus $r - r' < 0$, so $r - r' \in 0^*$.

Note that $r = r' + (r - r')$, where $r' \in \alpha$, $r - r' \in 0^*$. Hence $r \in \alpha + 0^*$.

(iv) Fix some $\alpha \in \mathbb{R}$. We first show that β is a cut:

(i) Fix some $s \notin \alpha$, and let $p = -s - 1$. Then $-p - 1 \notin \alpha$. Hence $p \in \beta$, so $\beta \neq \emptyset$.
Let $q \in \alpha$. Then $-q \notin \beta$, so $\beta \neq \mathbb{Q}$.

(ii) Let $p \in \beta$. Then there exists $r > 0$ such that $-p - r \notin \alpha$. If $q < p$, then $-q - r > -p - r$ so $-q - r \notin \alpha$. Hence $q \in \beta$.

(iii) Let $t = p + \frac{r}{2}$. Then $t > p$, and $-t - \frac{r}{2} = -p - r \notin \alpha$. Hence $t \in \beta$.

$\boxed{\subseteq}$ Let $r \in \alpha$, $s \in \beta$. Then $-s \notin \alpha$. This implies $r < -s$ (since α is closed downwards) so $r + s < 0$. Hence $\alpha + \beta \subseteq 0^*$.

$\boxed{\supseteq}$ Let $v \in 0^*$, and let $w = -\frac{v}{2}$. Then $w > 0$. By the Archimedean property on $\mathbb{Q}$, there exists $n \in \mathbb{N}$ such that $nw \in \alpha$ but $(n + 1)w \notin \alpha$. Let $p = -(n + 2)w$. Then

$$-p - w = (n + 2)w - w = (n + 1)w \notin \alpha$$

so $p \in \beta$. Since $v = nw + p$ where $nw \in \alpha$, $p \in \beta$, $v \in \alpha + \beta$. Hence $0^* \subseteq \alpha + \beta$.

□

Notation. β is denoted by the more familiar notation $-\alpha$.

Lemma 5.22. *If $\alpha, \beta, \gamma \in \mathbb{R}$ and $\beta < \gamma$, then $\alpha + \beta < \alpha + \gamma$.*

Proof. □

We say that a cut α is **positive** if $0 \in \alpha$, and **negative** if $0 \notin \alpha$. If α is neither positive nor negative, then $\alpha = 0^*$.

Multiplication is a little more bothersome than addition in the present context, since products of negative rationals are positive. For this reason, we first confine ourselves to $\mathbb{R}^+$, the set of all positive cuts.

Definition 5.23. Given $\alpha, \beta \in \mathbb{R}^+$, define multiplication as

$$\alpha\beta := \{p \in \mathbb{Q} \mid p \leq rs \text{ for some } r \in \alpha,\ s \in \beta,\ r, s > 0\}.$$

We also define $1^* := \{q \in \mathbb{Q} \mid q < 1\}$.

We check that multiplication is closed in $\mathbb{R}^+$: for all $\alpha, \beta \in \mathbb{R}^+$, $\alpha\beta \in \mathbb{R}^+$.

(i) Since $\alpha \neq \emptyset$, fix $r \in \alpha, r > 0$. Since $\beta \neq \emptyset$, fix $s \in \beta, s > 0$.

Then $rs \in \mathbb{Q}$ and $rs \leq rs$, so $rs \in \alpha\beta$. Hence $\alpha\beta \neq \emptyset$.

Since $\alpha \neq \mathbb{Q}$, there exists $r' \notin \alpha$ such that $r' > r$ for all $r \in \alpha$. Since $\beta \neq \mathbb{Q}$, there exists $s' \in \beta$ such that $s' > s$ for all $s \in \beta$.

Then $r's' > rs$ for all $r \in \alpha, s \in \beta$, so $r's' \notin \alpha\beta$. Hence $\alpha\beta \neq \mathbb{Q}$.

(ii) Let $p \in \alpha\beta$. Then $p \leq ab$ for some $a \in \alpha, b \in \beta$, $a, b > 0$.

If $q < p$, then $q < p \leq ab$, so $q \in \alpha\beta$.

(iii) Let $p \in \alpha\beta$. Then $p \leq ab$ for some $a \in \alpha, b \in \beta$, $a, b > 0$.

Pick $a' \in \alpha$ and $b' \in \beta$ with $a' > a$ and $b' > b$.

Since $p \leq ab < a'b'$, we have $a'b' \in \alpha \cdot \beta$.

We now complete the definition of multiplication by setting $\alpha 0^* = 0^* = 0^* \alpha$, and by setting

$$\alpha\beta = \begin{cases} (-\alpha)(-\beta) & \text{if } a < 0^*,\ \beta < 0^*, \\ -[(-\alpha)\beta] & \text{if } a < 0^*,\ \beta > 0^*, \\ -[\alpha(-\beta)] & \text{if } \alpha > 0^*,\ \beta < 0^*. \end{cases}$$

where we make negative numbers positive, multiply, and then negate them as needed.

Lemma 5.24.

(i) Multiplication is commutative: $\alpha\beta = \beta\alpha$ for all $\alpha, \beta \in \mathbb{R}$.

(ii) Multiplication is associative: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for all $\alpha, \beta, \gamma \in \mathbb{R}$.

(iii) Multiplicative identity: $1\alpha = \alpha$ for all $\alpha \in \mathbb{R}$.

(iv) Multiplicative inverse: For each $\alpha \in \mathbb{R}$, $\alpha \neq 0^*$, there exists $\beta \in \mathbb{R}$ such that $\alpha\beta = 1^*$.

Therefore $\mathbb{R}$ is a field.

Proposition 5.25. *The replacement of $r \in \mathbb{Q}$ by the corresponding rational cuts preserves sums, products and order: for all $r^*, s^* \in \mathbb{R}$,*

(i) $r^* + s^* = (r + s)^*$;

(ii) $r^* s^* = (rs)^*$;

(iii) $r^* < s^*$ if and only if $r < s$.

Proof.

(i) $\boxed{\subseteq}$ Let $p \in r^* + s^*$. Then $p = u + v$ for some $u \in r^*$, $v \in s^*$, where $u < r$, $v < s$. Then $p < r + s$. Hence $p \in (r+s)^*$, so $r^* + s^* \subseteq (r+s)^*$.

$\boxed{\supseteq}$ Let $p \in (r+s)^*$. Then $p < r + s$. Let $t = \dfrac{(r+s)-p}{2}$, and let

$$r' = r - t, \quad s' = s - t.$$

Since $t > 0$, $r' < r$ so $r' \in r^*$; $s' < s$ so $s' \in s^*$. Then $p = r' + s'$, so $p \in r^* + s^*$. Hence $(r+s)^* \subseteq r^* + s^*$.

(ii)

(iii) Suppose $r < s$. Then $r \in s^*$, but $r \notin r^*$. Hence $r^* < s^*$.

Conversely, suppose $r^* < s^*$. Then there exists $p \in s^*$ such that $p \in r^*$. Hence $r \leq p < s$, so $r < s$.

□

This shows that the ordered field $\mathbb{Q}$ is isomorphic to the ordered field $\mathbb{Q}^* = \{q^* \mid q \in \mathbb{Q}\}$ whose elements are rational cuts. It is this identification of $\mathbb{Q}$ with $\mathbb{Q}^*$ which allows us to regard $\mathbb{Q}$ as a subfield of $\mathbb{R}$.

Remark. In fact, $\mathbb{R}$ is the unique ordered field with the l.u.b. property up to isomorphism; any other ordered field with the l.u.b. property is isomorphic to $\mathbb{R}$.
Proof sketch: Let $(F_1, +_1, \cdot_1, <_1)$ and $(F_2, +_2, \cdot_2, <_2)$ be complete ordered fields.

- Map the additive identity of F_1 to the additive identity of F_2.
- Same for multiplicative identity.
- Extend to a bijection ϕ from the rationals $\mathbb{Q}_1$ of F_1 to the rationals $\mathbb{Q}_2$ of F_2.
- Finally, use the ordering and Dedekind completeness to extend ϕ, i.e., for each $x \in F_1 \setminus \mathbb{Q}_1$, define

$$\phi(x) = \sup_{F_2}\{\phi(y) \in \mathbb{Q}_2 \mid y <_1 x,\ y \in \mathbb{Q}_1\}.$$

One then checks that ϕ is an isomorphism.

Therefore we have proven 5.26.

Theorem 5.26 (Existence of real field)**.** *There exists an ordered field* $\mathbb{R}$ *that*

(i) contains $\mathbb{Q}$ *as a subfield, and*

(ii) has the least-upper-bound property.

5.2.1 Extended Real Number System

Definition 5.27. Define the **extended real number system** as $\overline{\mathbb{R}} := \mathbb{R} \cup \{-\infty, +\infty\}$.

Notation. We sometimes write $[-\infty, \infty]$ in place of $\overline{\mathbb{R}}$.

We preserve the original order in $\mathbb{R}$, and define

$$-\infty < x < +\infty$$

for all $x \in \mathbb{R}$.

Defining $\overline{\mathbb{R}}$ is convenient since the following result holds.

Lemma 5.28. *Any non-empty $E \subseteq \overline{\mathbb{R}}$ has a supremum and infimum in $\overline{\mathbb{R}}$.*

Proof. If E is bounded above in $\mathbb{R}$, then by the l.u.b. property of $\mathbb{R}$, it has a supremum in $\mathbb{R} \subseteq \overline{\mathbb{R}}$. If E is not bounded above in $\mathbb{R}$, then $\sup E = +\infty \in \overline{\mathbb{R}}$.

Exactly the same remarks apply to lower bounds. □

$\overline{\mathbb{R}}$ does not form a field, but it is customary to make the following conventions for arithmetic on $\overline{\mathbb{R}}$:

(i) If x is real or ∞, then $x + \infty = +\infty$.

If x is real or $-\infty$, then $x - \infty = -\infty$.

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

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

If x is real, then $\dfrac{x}{+\infty} = \dfrac{x}{-\infty} = 0$.

(Note that addition and multiplication are understood to be commutative on the extended reals, so that the definitions also imply further cases such as $+\infty + x = +\infty$.)

— Exercises —

★ **Exercise 5.2.1.** Say whether each of the following statements is true or false.

(a) In the extended real numbers, $(+\infty) \cdot 0 = 1$.

(b) In the extended real numbers, $(-\frac{1}{2}) \cdot (-\infty) = +\infty$.

Solution.

(a) False.

(b) True.

□

★ **Exercise 5.2.2** (MA1100 AY04/05)**.** Prove that $\sqrt[3]{2}$ is irrational.

Solution. Suppose, towards a contradiction, that $\sqrt[3]{2}$ is rational, i.e., $\sqrt[3]{2} = \frac{m}{n}$, where $m, n \in \mathbb{Z}$, $n \neq 0$ and m, n are coprime.

Then $2 = \frac{m^3}{n^3}$, or $2n^3 = m^3$, so m is even.

Let $m = 2p$. Then $2n^3 = (2p)^3 = 8p^3$, so $n^3 = 4p^3$. Since $4p^3$ is even, n^3 is even, so n is even. This is a contradiction. □

5.3 Properties of the Real Numbers

Henceforth, we shall view $\mathbb{R}$ as the set of numbers that we are familiar with.

5.3.1 Archimedean Property

Let F be an ordered field with additive identity 0_F, multiplicative identity 1_F. The **set of natural numbers** in F is

$$\{0_F, 1_F, 1_F + 1_F, \dots\}.$$

We say that F has the **Archimedean property** if the set of natural numbers in F is unbounded in F.

Hence if F does not have the Archimedean property, then the natural numbers are bounded in F, i.e., there exists $x \in F$ which is an upper bound for the natural numbers.

This is equivalent to the existence of some infinitesimal x, i.e., $x > 0$ yet for all $n \in \mathbb{N}$, $x < 1/n$.

Example. $\mathbb{Q}$ has the Archimedean property: For each $m/n \in \mathbb{Q}$, we have $m/n < |m| + 1$.

Example. There are ordered fields where the Archimedean property fails. Consider

$$\mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in \mathbb{Q}[x],\ q(x) \neq 0 \right\}.$$

Addition and multiplication are defined in the usual way.
We will only define part of the ordering: To compare $\frac{p(x)}{q(x)}$ with $\frac{0}{1}$, make $q(x)$ have leading coefficient 1 and say that $\frac{p(x)}{q(x)} \succ \frac{0}{1}$ if the leading coefficient of $p(x)$ is positive.
One can check that $Q(x)$ forms an ordered field under the above operations.
The natural numbers of $\mathbb{Q}(x)$ have the form $\frac{n}{1}$ for $n \in \mathbb{N}$.
The Archimedean property fails ($\mathbb{N}$ is bounded in $\mathbb{Q}(x)$): $\frac{x}{1} \succ \frac{n}{1}$ for every $n \in \mathbb{N}$, because the numerator of $\frac{x-n}{1}$ has positive leading coefficient (hence $\frac{x-n}{1} \succ \frac{0}{1}$).

Proposition 5.29. *$\mathbb{R}$ has the Archimedean property.*

Proof. Suppose, towards a contradiction, that $\mathbb{R}$ does not satisfy the Archimedean property. Then $\mathbb{N}$ is bounded in $\mathbb{R}$.

Since $\mathbb{N}$ is a non-empty bounded subset of $\mathbb{R}$, $\sup(\mathbb{N})$ exists (and is an element of $\mathbb{R}$). Since $\sup(\mathbb{N}) - 1 < \sup(\mathbb{N})$, by definition of supremum, $\sup(\mathbb{N}) - 1$ is not an upper bound of $\mathbb{N}$. Thus there exists $n \in \mathbb{N}$ such that $n > \sup(\mathbb{N}) - 1$.

Now $n + 1 > \sup(\mathbb{N})$ and $n + 1 \in \mathbb{N}$, contradicting the fact that $\sup(\mathbb{N})$ is an upper bound of $\mathbb{N}$. □

Corollary 5.30. *For every $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that $0 < \frac{1}{n} < \varepsilon$.*

5.3.2 Density

Definition 5.31. Let F be an ordered field. The ordering on F is **dense** if for every two distinct $x, y \in F$, there exists $z \in F$ between them.
We say $\mathbb{Q}$ is **dense in** $\mathbb{R}$ if for every two distinct $x, y \in \mathbb{R}$, there is $z \in \mathbb{Q}$ in between them.

Example.

- The standard ordering on $\mathbb{Q}$, $\mathbb{R}$ is dense.
- The standard ordering on the set of irrationals is dense. (Note that $\mathbb{R} \setminus \mathbb{Q}$ is not an ordered field).

  Given two distinct irrationals x and y, consider $z = \frac{x+y}{2}$. If z is irrational, then we are done. Otherwise, consider $w = \frac{x+z}{2}$. If w is irrational, then we are done. Otherwise, since w and z are two distinct rational numbers, there is an irrational number in between them.

Proposition 5.32. *$\mathbb{Q}$ is dense in $\mathbb{R}$.*

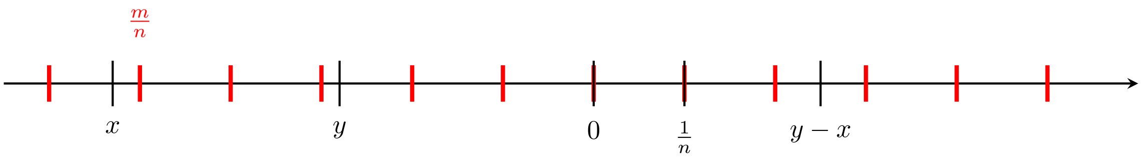
Proof. Let $x, y \in \mathbb{R}$ with $x < y$. Then $y - x > 0$. By the Archimedean property, fix $n \in \mathbb{N}$ such that

$$\frac{1}{n} < y - x.$$

Consider integer multiples of $\frac{1}{n}$; choose the smallest $m \in \mathbb{Z}$ such that $\frac{m}{n} > x$.
Claim: $x < \frac{m}{n} < y$.
We only need to show $\frac{m}{n} < y$. Suppose, towards a contradiction, that this does not hold. Then

$$\frac{m-1}{n} \leq x \quad \text{and} \quad \frac{m}{n} \geq y,$$

where the first inequality follows from the minimality of m. But these two statements combined imply that $\frac{1}{n} \geq y - x$, a contradiction. □



Corollary 5.33. *$\mathbb{R} \setminus \mathbb{Q}$ is dense in $\mathbb{R}$.*

Proof. Let $x, y \in \mathbb{R}$ with $x < y$.
By 5.32, there exists $p \in \mathbb{Q}$ such that $p \neq 0$ and $\dfrac{x}{\sqrt{2}} < p < \dfrac{y}{\sqrt{2}}$. Thus

$$x < p\sqrt{2} < y$$

and $p\sqrt{2}$ is irrational. □

Corollary 5.34. *Every interval $I \subseteq \mathbb{R}$ contains infinitely many rational numbers and infinitely many irrational numbers.*

5.3.3 Existence of Roots

Proposition 5.35 ($\mathbb{R}$ is closed under taking roots)**.** *For every $x \in \mathbb{R}^+$ and every $n \in \mathbb{N}$, there exists a unique $y \in \mathbb{R}^+$ such that $y^n = x$.*

We call the number y the positive n-th root of x, and denote it by $\sqrt[n]{x}$ or $x^{1/n}$.

Proof. Let $x \in \mathbb{R}^+$, fix $n \in \mathbb{N}$.
$\boxed{\text{Existence}}$ Consider the set $E = \left\{t \in \mathbb{R}^+ : t^n < x\right\}$.
Claim: $y = \sup E$ satisfies $y^n = x$.
We first show that E has a supremum.

(i) Set $t = \frac{x}{1+x}$. Then $0 \le t < 1$, so $t^n \le t < x$ implies $t^n < x$. Hence $t \in E$, so $E \neq \emptyset$.

(ii) We claim that $1+x$ is an upper bound for E. If $t > 1+x$, then $t^n \ge t > x$ implies $t^n > x$, so $t \notin E$. Hence $1+x$ is an upper bound of E, so E is bounded above.

Hence E has a supremum; let $y = \sup E$.
To prove $y^n = x$, we show that both $y^n < x$ and $y^n > x$ lead to a contradiction.
Consider the identity $b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \cdots + a^{n-1})$. If $0 < a < b$, then

$$b^n - a^n < (b-a)nb^{n-1}. \tag{1}$$

Case 1: $y^n < x$**.** The idea is to find a *small* $h > 0$ such that $(y+h)^n < x$.

Choose h so that $0 < h < 1$ and $h < \dfrac{x - y^n}{n(y+1)^{n-1}}$. In (1), take $b = y+h$, $a = y$. Then

$$\begin{aligned}(y+h)^n - y^n &< hn(y+h)^{n-1} \\ &< hn(y+1)^{n-1} \\ &< \frac{x-y^n}{\cancel{n(y+1)^{n-1}}}\cancel{n(y+1)^{n-1}} \\ &= x - y^n.\end{aligned}$$

Thus $(y+h)^n < x$, and $y+h \in E$. Since $y+h > y$, this contradicts the fact that y is an upper bound of E.

Case 2: $y^n > x$**.** The idea is to find a *small* $k > 0$ such that $(y-k)^n > x$.

Let $k = \dfrac{y^n - x}{ny^{n-1}}$. Then $0 < k < y$, by (1). If $t \ge y - k$,

$$\begin{aligned}y^n - t^n &\le y^n - (y-k)^n \\ &< kny^{n-1} \\ &= \frac{y^n - x}{\cancel{ny^{n-1}}}\cancel{ny^{n-1}} \\ &= y^n - x.\end{aligned}$$

Thus $t^n > x$, and $t \notin E$. It follows that $y-k$ is an upper bound of E. But $y - k < y$, which contradicts the fact that y is the *least* upper bound of E.

$\boxed{\text{Uniqueness}}$ Suppose, towards a contradiction, that there exist distinct y_1, y_2 which are both n-th roots of x. WLOG assume that $0 < y_1 < y_2$. Then taking the n-th power gives ${y_1}^n < {y_2}^n$.
Since y_1 is a n-th root of x, then $x = {y_1}^n$, so $x < {y_2}^n$ implies $x \neq {y_2}^n$. Hence y_2 cannot be a n-th root of x, a contradiction. □

Corollary 5.36. *Let $a, b \in \mathbb{R}^+$ and $n \in \mathbb{N}$. Then*

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

Proof. Let $\alpha = a^{1/n}$, $\beta = b^{1/n}$. Then

$$ab = \alpha^n \beta^n = (\alpha\beta)^n$$

where the last line follows from commutativity of multiplication. The uniqueness assertion of the previous result allows us to take the n-th root on both sides:

$$(ab)^{\frac{1}{n}} = \alpha\beta = a^{\frac{1}{n}} b^{\frac{1}{n}}.$$

□

Lemma 5.37. *Let $a \in \mathbb{R}^+$ and $m, n \in \mathbb{N}$. Then*

$$(a^{1/n})^m = (a^m)^{1/n}.$$

Proof. We have

$$((a^{1/n})^m)^n = (a^{1/n})^{mn} = ((a^{1/n})^n)^m = a^m.$$

By definition, this yields the desired result. □

For $a \in \mathbb{R}^+$ and $m, n \in \mathbb{N}$, we define **rational exponents**

$$a^{m/n} := (a^{1/n})^m \quad \text{and} \quad a^{-m/n} := \frac{1}{a^{m/n}}.$$

(We also define $a^0 = 1$.)

We need to check that the above definition of a^r is well defined. That is, if $m, n, p, q \in \mathbb{N}$ are such that $\frac{m}{n} = \frac{p}{q}$, then $(a^{1/n})^m = (a^{1/q})^p$. To see this, note that $mq = np$, and thus

$$((a^{1/n})^m)^q = (a^{1/n})^{mq} = (a^{1/n})^{np} = a^p.$$

Hence $(a^{1/n})^m$ is the q-th root of a^p, i.e.,

$$(a^{1/n})^m = (a^p)^{1/q}.$$

Lemma 5.38 (Properties of rational exponents)**.**

(i) If $a > 0$ and $r, s \in \mathbb{Q}$, then $a^{r+s} = a^r a^s$ and $(a^r)^s = a^{rs}$.

(ii) If $0 < a < b$ and $r \in \mathbb{Q}$ with $r > 0$, then $a^r < b^r$.

(iii) If $a > 1$, $r, s \in \mathbb{Q}$ with $r < s$, then $a^r < a^s$.

— Exercises —

★ **Exercise 5.3.1** ([Rud76] 1.1)**.** Let $r \in \mathbb{Q} \setminus \{0\}$ and $x \in \mathbb{R} \setminus \mathbb{Q}$. Prove that $r + x \in \mathbb{R} \setminus \mathbb{Q}$ and $rx \in \mathbb{R} \setminus \mathbb{Q}$.

Solution. Prove by contradiction. If r and $r + x$ were both rational, then $x = (r + x) - r$ would also be rational. Similarly if rx were rational, then $x = \frac{rx}{r}$ would also be rational. □

★ **Exercise 5.3.2** ([Rud76] 1.2)**.** Prove that there is no rational number whose square is 12.

Solution. Prove by contradiction. □

★ **Exercise 5.3.3.** Prove that for every two distinct rational numbers, there is an irrational number in between them.

Solution. Let p, q be two distinct rational numbers; WLOG assume $p < q$. Consider $r = p + \frac{q-p}{\sqrt{2}}$. □

★★ **Exercise 5.3.4** (MA1100T AY22/23)**.** Prove that for every two distinct irrational numbers, there is an irrational number between them.

Solution. Let p, q be two distinct irrational numbers; WLOG assume $p < q$.

Consider the average of p and q; we have $p < \frac{p+q}{2} < q$.

Case 1: If $\frac{p+q}{2}$ is irrational, take $x = \frac{p+q}{2}$ and we are done.

Case 2: If $\frac{p+q}{2}$ is rational, let $r = \frac{p+q}{2}$, and consider the average of p and r:

$$x = \frac{p+r}{2} = \frac{p + \frac{p+q}{2}}{2} = \frac{3p+q}{4}.$$

Evidently $p < x < r < q$. Since p is irrational and r is rational, $x = \frac{p+r}{2}$ is irrational.

□

★ **Exercise 5.3.5.** Prove or disprove: The sum of two irrational numbers is irrational.

Solution. Disprove. $\sqrt{2} + (-\sqrt{2}) = 0$. □

★★ **Exercise 5.3.6** (MA1100T AY23/24)**.** Prove that for every pair of real numbers $q < r$, there exists an irrational number that is strictly between them.

Solution. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there is a rational number x strictly between q and r.

By the same argument, there is a rational number y strictly between x and r.

By Exercise 5.3.3, there is an irrational number strictly between two rational numbers, so we are done, as there is an irrational z such that $q < x < z < y < r$. □

Exercise 5.3.7. Prove that $\mathbb{Q}$ is dense in $\mathbb{R}$ using Dedekind cuts.

Solution. Let $\alpha, \beta \in \mathbb{R}$, where $\alpha < \beta$. Then $\alpha \subsetneq \beta$. Thus $\beta \setminus \alpha$ is non-empty; fix $r \in \beta \setminus \alpha$.

Consider $\gamma = \{p \in \mathbb{Q} \mid p < r\}$.

We first show that γ is a Dedekind cut:

- Obviously $\gamma \neq \emptyset$, since there must exist rationals smaller than r.

  Since $r \notin \gamma$ and $r \in \mathbb{Q}$, we have $\gamma \neq \mathbb{Q}$.
- Downward closed: If $p \in \gamma$ and $q \in \mathbb{Q}$ is such that $q < p$, then $q < p < r$, so $q \in \gamma$.
- No largest member: If $p \in \gamma$, then $p < r$. Since $\mathbb{Q}$ is dense, there exists $t \in \mathbb{Q}$ such that $p < t < r$; thus $t \in \gamma$ and p is not largest.

Next we show that $\alpha < \gamma < \beta$:

- Suppose, towards a contradiction, that there exists $p \in \alpha$ such that $p \geq r$.

  If $p > r$, since α is downward closed and $p \in \alpha$, we would have $r \in \alpha$, a contradiction. If $p = r$, then $r = p \in \alpha$, a contradiction.

  Hence every $p \in \alpha$ satisfies $p < r$, so $\alpha \subseteq \gamma$.
- Let $p \in \gamma$. Then $p < r$ and $r \in \beta$, so $p \in \beta$ (since β is downward closed). Hence $\gamma \subseteq \beta$.

  Since $r \in \beta$ but $r \notin \gamma$, we get $\gamma \subsetneq \beta$.

What if we choose r such that its Dedekind cut coincides with α (alpha is a rational cut)? Then take a rational in $\beta \setminus \alpha$ whose Dedekind cut is strictly greater than α. □

★★ **Exercise 5.3.8.** Prove that for each real number r, there is some integer n such that $n \leq r < n+1$. (Henceforth, we will refer to n by $\lfloor r \rfloor$.)

Solution. Let $r \in \mathbb{R}$. By the Archimedean property, there exists $N \in \mathbb{N}$ such that $N > r$.
Consider the set

$$S = \left\{ a \in \mathbb{Z} \mid a \leq r \right\}.$$

Since S is non-empty and bounded above by N, by well-ordering, S has a maximum $M \in \mathbb{Z}$.
By construction, $M \leq r$, and for any integer $k > M$, we have $k \notin S$, so $k > r$. In particular, $M+1 > r$.
Hence we have

$$M \leq r < M+1,$$

and the integer $n = M$ satisfies the desired property.

Remark. After checking the uniqueness of $\lfloor r \rfloor$, then we can define the **floor function**.

□

★★ **Exercise 5.3.9.** Let A be a non-empty bounded subset of $\mathbb{R}$. Prove that $s = \sup A$ if and only if for every $n \in \mathbb{N}$, $s + \frac{1}{n}$ is an upper bound of A and $s - \frac{1}{n}$ is not an upper bound of A.

Solution. Let A be a non-empty bounded subset of $\mathbb{R}$.
$\boxed{\Rightarrow}$ Let $s = \sup A$. Let $n \in \mathbb{N}$ be arbitrary.
Since s is an upper bound of A, and $s < s + \frac{1}{n}$, it follows that $s + \frac{1}{n}$ is an upper bound of A.
Since $s - \frac{1}{n} < s$, by definition of supremum, $s - \frac{1}{n}$ is not an upper bound of A.
$\boxed{\Leftarrow}$ Suppose the given property holds. We will show that $s = \sup A$.

- First we show that s is an upper bound of A, i.e., $a \leq s$ for all $a \in A$.

  Suppose, towards a contradiction, that $a > s$ for some $a \in A$.

  Then $a - s > 0$; by the Archimedean property, fix $n \in \mathbb{N}$ such that $\frac{1}{n} < a - s$. Thus $s + \frac{1}{n} < a$, contradicting the assumption that $a \leq s + \frac{1}{n}$ for all $n \in \mathbb{N}$.

- Next we show s is the *least* such upper bound.

  Let u be an upper bound of A. We want to show that $s \leq u$.

  For each $n \in \mathbb{N}$, since $s - \frac{1}{n}$ is not an upper bound of A, there exists $a_n \in A$ such that $a_n > s - \frac{1}{n}$. Since u is an upper bound of A, we have $a_n \leq u$ for all $n \in \mathbb{N}$, so $s - \frac{1}{n} < u$.

  Suppose, towards a contradiction, that $s > u$. Then $s - u > 0$. By the Archimedean property, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < s - u$. Then $s - \frac{1}{n} > u$, a contradiction. Hence $s \leq u$.

(The idea is that we can stuff in some $1/n$.) □

★★ **Exercise 5.3.10** (MA1100T AY22/23)**.** Prove that for every real number x, there is a set A of rational numbers such that $\sup A = x$.

Solution. Let $x \in \mathbb{R}$. Define

$$A = \{q \in \mathbb{Q} : q < x\} \subseteq \mathbb{Q}.$$

Claim: $\sup A = x$.

Since A is non-empty and bounded above by x, by completeness, $\sup A$ exists.

Let $y < x$. By density, there exists $q \in \mathbb{Q}$ such that $y < q < x$. By definition, $q \in A$. But $q > y$, so y is not an upper bound of A. Hence $x = \sup A$. □

5.4 Complex Field

Lemma 5.39. *Let $(a,b),(c,d)\in\mathbb{R}^2$. Define addition and multiplication on $\mathbb{R}^2$ as*

$$\begin{aligned}(a,b)+(c,d)&=(a+c,b+d),\\(a,b)\cdot(c,d)&=(ac-bd,ad+bc).\end{aligned}$$

Then $\mathbb{R}^2$ is a field, with additive identity $(0,0)$ and multiplicative identity $(1,0)$.

We call this structure $\mathbb{C}$, the **complex field**; its elements are called **complex numbers**.

Proof. Check the field axioms. □

The next result shows that the complex numbers of the form $(a,0)$ have the same arithmetic properties as the corresponding real numbers a. We can therefore identify $(a,0)\in\mathbb{C}$ with $a\in\mathbb{R}$. This identification implies that $\mathbb{R}$ is a **subfield** of $\mathbb{C}$.

Lemma 5.40. *For any $a,b\in\mathbb{R}$,*

$$\begin{aligned}(a,0)+(b,0)&=(a+b,0),\\(a,0)\cdot(b,0)&=(ab,0).\end{aligned}$$

Proof. Exercise. □

You may have noticed that we have defined the complex numbers without referring to the mysterious square root of -1. We now show that the notation (a,b) is equivalent to the more customary $a+bi$.
Define the imaginary number $i:=(0,1)$. See that

$$i^2=(0,1)(0,1)=(-1,0)=-1.$$

Lemma 5.41. *For any $a,b\in\mathbb{R}$, $(a,b)=a+bi$.*

Proof. $a+bi=(a,0)+(b,0)(0,1)=(a,0)+(0,b)=(a,b)$. □

For $a,b\in\mathbb{R}$, we write $z=a+bi$; we call a and b the **real part** and **imaginary part** of z respectively, denoted by $a=\operatorname{Re}(z)$, $b=\operatorname{Im}(z)$. We call $\overline{z}=a-bi$ the **conjugate** of z.
The next result summarises basic properties of the conjugate of a complex number.

Lemma 5.42. *For $z,w\in\mathbb{C}$,*

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

(ii) $\overline{zw}=\overline{z}\,\overline{w}$

(iii) $z+\overline{z}=2\operatorname{Re}(z)$, $z-\overline{z}=2i\operatorname{Im}(z)$

(iv) $z\overline{z}$ *is real, and* $z\overline{z}\ge 0$

Proof. Let $z=a+bi$, $w=c+di$.

(i) $\overline{z+w}=\overline{(a+c)+(b+d)i}=(a+c)-(b+d)i=(a-bi)+(c-di)=\overline{z}+\overline{w}$.

(ii) $\overline{zw} = \overline{(a+bi)(c+di)} = \overline{(ac-bd)+(ad+bc)i} = (ac-bd)-(ad+bc)i = (a-bi)(c-di) = \overline{z}\overline{w}$.

(iii) $z + \overline{z} = (a+bi)+(a-bi) = 2a = 2\operatorname{Re}(z)$.

$z - \overline{z} = (a+bi)-(a-bi) = 2bi = 2i\operatorname{Im}(z)$.

(iv) $z\overline{z} = (a+bi)(a-bi) = a^2+b^2 \in \mathbb{R}_{\geq 0}$.

□

Let $z \in \mathbb{C}$. The **absolute value** of z is defined as

$$|z| := (z\overline{z})^{1/2}.$$

The existence (and uniqueness) of $|z|$ follows from 5.35, and (iv) of the previous result. Note that when z is real, then $\overline{z} = z$; thus $|z| = \sqrt{z^2}$. Hence $|z| = z$ if $z \geq 0$, and $|z| = -z$ if $z < 0$.

Remark. Since the absolute value is defined as a square root, it is more useful to work with the *square* of the absolute value.

The next result summarises basic properties of the absolute value.

Lemma 5.43. *Let $z, w \in \mathbb{C}$. Then*

(i) $|z| \geq 0$.

(ii) $|\overline{z}| = |z|$.

(iii) $|zw| = |z||w|$.

(iv) $|\operatorname{Re}(z)| \leq |z|$.

Proof. Let $z = a+bi$, $w = c+di$ where $a,b,c,d \in \mathbb{R}$.

(i) The square root is non-negative, by definition.

(ii) The conjugate of $\overline{z}$ is z, and the rest follows by the definition of absolute value.

(iii) We have

$$\begin{aligned} |zw|^2 &= (ac-bd)^2 + (ad-bc)^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= |z|^2|w|^2 = (|z||w|)^2. \end{aligned}$$

Taking square roots on both sides yields the desired result.

(iv) Note that $a^2 \leq a^2+b^2$. Hence

$$|\operatorname{Re}(z)| = |a| = \sqrt{a^2} \leq \sqrt{a^2+b^2} = |z|.$$

□

Proposition 5.44 (Triangle inequality)**.** *For $z, w \in \mathbb{C}$,*

$$|z+w| \leq |z|+|w|. \tag{5.1}$$

Proof. Let $z, w \in \mathbb{C}$. Note that the conjugate of $z\overline{w}$ is $\overline{z}w$, so $z\overline{w} + \overline{z}w = 2\operatorname{Re}(z\overline{w})$. Hence

$$\begin{aligned}
|z+w|^2 &= (z+w)(\overline{z+w}) = (z+w)(\overline{z}+\overline{w}) \\
&= z\overline{z} + z\overline{w} + \overline{z}w + w\overline{w} \\
&= |z|^2 + 2\operatorname{Re}(z\overline{w}) + |w|^2 \\
&\le |z|^2 + 2|z\overline{w}| + |w|^2 \\
&= |z|^2 + 2|z||w| + |w|^2 \\
&= (|z|+|w|)^2
\end{aligned}$$

and taking square roots yields the desired result. □

Corollary 5.45 (Generalised triangle inequality)**.** *For $z_1, \dots, z_n \in \mathbb{C}$,*

$$|z_1 + \cdots + z_n| \le |z_1| + \cdots + |z_n|.$$

Proof. Induct on n. The case when $n = 1$ is trivial. We have proven the case when $n = 2$. Assume the statement holds for $n - 1$. Then

$$|z_1 + \cdots + z_{n-1} + z_n| \le |z_1 + \cdots + z_{n-1}| + |z_n| \le |z_1| + \cdots + |z_n|.$$

□

Corollary 5.46. *For $x, y, z \in \mathbb{C}$,*

(i) $\big||x| - |y|\big| \le |x - y|$*;*

(ii) $|x - y| \le |x - z| + |z - y|$.

Proof.

(i) By the triangle inequality,

$$|x| = |(x-y) + y| \le |x-y| + |y|$$

so that

$$|x| - |y| \le |x - y|.$$

Interchanging the roles of x and y in the above gives

$$|y| - |x| \le |x - y|.$$

Hence

$$\big||x| - |y|\big| \le |x - y|.$$

(ii) In the triangle inequality, replace x by $x - y$ and y by $y - z$.

□

Proposition 5.47 (Cauchy–Schwarz inequality)**.** *If $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{C}$, then*

$$\left|\sum_{i=1}^n a_i\overline{b_i}\right|^2 \le \sum_{i=1}^n |a_i|^2 \sum_{i=1}^n |b_i|^2. \tag{5.2}$$

Proof. For simplicity, we shall drop the upper and lower limits of the sums. Let

$$A = \sum |a_i|^2, \quad B = \sum |b_i|^2, \quad C = \sum a_i \overline{b_i}.$$

Then (5.2) becomes

$$|C|^2 \leq AB.$$

If $B = 0$, then $b_1 = \cdots = b_n = 0$, and the conclusion is trivial. Now assume that $B > 0$. Then consider the sum

$$\begin{aligned}\sum |Ba_i - Cb_i|^2 &= \sum (Ba_i - Cb_i)(\overline{Ba_i - Cb_i}) \\ &= \sum (Ba_i - Cb_i)(B\overline{a_i} - \overline{Cb_i}) \\ &= B^2 \sum |a_i|^2 - B\overline{C} \sum a_i \overline{b_i} - BC \sum \overline{a_i} b_i + |C|^2 \sum |b_i|^2 \\ &= B^2 A - B|C|^2 \\ &= B(AB - |C|^2).\end{aligned}$$

Each term in $\sum |Ba_i - Cb_i|^2$ is non-negative, so $\sum |Ba_i - Cb_i|^2 \geq 0$. Thus

$$B(AB - |C|^2) \geq 0.$$

Since $B > 0$, it follows that $AB - |C|^2 \geq 0$, or $|C|^2 \leq AB$. This is the desired inequality.
(when does equality hold?) □

Define

$$\mathbb{C}^n = \{(z_1, \ldots, z_n) \mid z_i \in \mathbb{C}\}.$$

We can define an inner product on $\mathbb{C}^n$: for $\mathbf{a}, \mathbf{b} \in \mathbb{C}^n$,

$$\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^{n} a_i \overline{b_i}.$$

We can also define the norm of $\mathbf{a} \in \mathbb{C}^n$:

$$|\mathbf{a}| = \langle \mathbf{a}, \mathbf{a} \rangle^{\frac{1}{2}}.$$

— Exercises —

★ **Exercise 5.4.1** ([Rud76] 1.8)**.** Prove that no order can be defined in $\mathbb{C}$ that turns it into an ordered field. *Hint*: -1 is a square.

Solution. By 5.13, an order $<$ that makes $\mathbb{C}$ an ordered field would have to satisfy $-1 = i^2 > 0$, contradicting $1 > 0$. □

Even though $\mathbb{C}$ cannot be made into an ordered field, the next exercise tells us that $\mathbb{C}$ can be made into an ordered set.

★★ **Exercise 5.4.2** ([Rud76] 1.9, lexicographic order)**.** Let $z = a + bi$, $w = c + di$. Define an order $<$ on $\mathbb{C}$ as follows:

$$z < w \iff \begin{cases} a < c, \text{ or} \\ a = c, b < d. \end{cases}$$

Prove that this turns $\mathbb{C}$ into an ordered set. Does this ordered set have the least upper bound property?

Solution. We show that this order turns $\mathbb{C}$ into an ordered set.

(i) Since the *real* numbers are ordered, we have $a < c$ or $a = c$ or $c < a$. In the first case $z < w$; in the third case $w < z$.

Now consider the second case where $a = c$. We must have $b < d$ or $b = d$ or $d < b$, which correspond to $z < w$, $z = w$, $w < z$ respectively.

Hence we have shown that either $z < w$ or $z = w$ or $w < z$.

(ii) We now show that if $z < w$ and $w < u$, then $z < u$. Let $u = e + fi$.

Since $z < w$, we have either $a < c$, or $a = c$ and $b < d$. Since $w < u$, we have either $c < f$, or $c = f$ and $d < g$. Hence there are four possible cases:

- $a < c$ and $c < f$. Then $a < f$ and so $z < u$, as required.
- $a < c$ and $c = f$, and $d < g$. Again $a < f$, so $z < u$.
- $a = c$, and $b < d$ and $c < f$. Once again $a < f$ so $z < u$.
- $a = c$ and $b < d$, and $c = f$ and $d < g$. Then $a = f$ and $b < g$, so $z < u$.

□

★★ **Exercise 5.4.3** ([Rud76] 1.10, square roots in $\mathbb{C}$)**.** Let $z = a + bi$, $w = u + iv$, and

$$a = \left(\frac{|w| + u}{2}\right)^{1/2}, \qquad b = \left(\frac{|w| - u}{2}\right)^{1/2}.$$

Prove that $z^2 = w$ if $v \geq 0$ and that $\overline{z}^2 = w$ if $v \leq 0$. Hence prove that every complex number (with one exception!) has two complex square roots.

Solution. We have

$$a^2 - b^2 = \frac{|w| + u}{2} - \frac{|w| - u}{2} = u,$$

and

$$2ab = (|w| + u)^{1/2}(|w| - u)^{1/2} = (|w|^2 - u^2)^{1/2} = (v^2)^{1/2} = |v|.$$

Hence if $v \geq 0$,

$$z^2 = (a^2 - b^2) + 2abi = u + |v|i = w;$$

if $v \leq 0$,

$$\overline{z}^2 = (a^2 - b^2) - 2abi = u - |v|i = w.$$

Hence every non-zero w has two square roots $\pm z$ or $\pm \overline{z}$. Of course, 0 has only one square root, itself. □

★★ **Exercise 5.4.4** ([Rud76] 1.11, $\mathbb{C} =$ (positive reals) $\cdot$ (unit circle))**.** If $z \in \mathbb{C}$, prove that there exists $r \geq 0$ and $w \in \mathbb{C}$ with $|w| = 1$ such that $z = rw$. Are w and r always uniquely determined by z?

Solution. If $z = 0$, take $r = 0$ and $w = 1$; in this case w is not unique.
Otherwise take $r = |z|$ and $w = \frac{z}{|z|}$; these choices are unique, since if $z = rw$, we must have $r = r|w| = |rw| = |z|$ so $w = \frac{z}{r} = \frac{z}{|z|}$ are unique. □

★ **Exercise 5.4.5** ([Rud76] 1.14, an identity on the unit circle)**.** If z is a complex number such that $|z| = 1$, compute

$$|1 + z|^2 + |1 - z|^2.$$

Solution. Since $z\overline{z} = 1$, we have

$$\begin{aligned}
|1+z|^2 + |1-z|^2 &= (1+z)(1+\overline{z}) + (1-z)(1-\overline{z}) \\
&= (1 + z + \overline{z} + z\overline{z}) + (1 - z - \overline{z} + z\overline{z}) \\
&= 4.
\end{aligned}$$

□

5.5 Euclidean Space

For $n \in \mathbb{N}$, define

$$\mathbb{R}^n := \{(x_1, \dots, x_n) \mid x_i \in \mathbb{R}\}$$

where $\mathbf{x} = (x_1, \dots, x_n)$, x_i's are called the coordinates of $\mathbf{x}$. The elements of $\mathbb{R}^n$ are called **points**, or **vectors**.

Lemma 5.48. *Let* $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{y} = (y_1, \dots, y_n)$, $\alpha \in \mathbb{R}$. *Define addition and scalar multiplication on* $\mathbb{R}^n$ *as*

$$\begin{aligned} \mathbf{x} + \mathbf{y} &= (x_1 + y_1, \dots, x_n + y_n), \\ \alpha \mathbf{x} &= (\alpha x_1, \dots, \alpha x_n). \end{aligned}$$

Then $\mathbb{R}^n$ *is a vector space over* $\mathbb{R}$, *with zero element* $\mathbf{0} = (0, \dots, 0)$.

Proof. These two operations satisfy the commutative, associatives, and distributive laws (the proof is trivial, in view of the analagous laws for the real numbers). □

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

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

and the **norm** of $\mathbf{x}$ by

$$\|\mathbf{x}\| := \sqrt{\mathbf{x} \cdot \mathbf{x}}.$$

The structure now defined (the vector space $\mathbb{R}^n$ with the above inner product and norm) is called the **Euclidean n-space**.

The next result summarises basic properties of the norm on $\mathbb{R}^n$.

Lemma 5.49. *Suppose* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$.

(i) $\|\mathbf{x}\| \geq 0$, *where equality holds if and only if* $\mathbf{x} = \mathbf{0}$ *(positive definiteness)*

(ii) $\|\alpha \mathbf{x}\| = |\alpha| \|\mathbf{x}\|$ *(homogeneity)*

(iii) $|\mathbf{x} \cdot \mathbf{y}| \leq \|\mathbf{x}\| \|\mathbf{y}\|$ *(Cauchy–Schwarz inequality)*

(iv) $\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|$ *(triangle inequality)*

(v) $\|\mathbf{x} - \mathbf{z}\| \leq \|\mathbf{x} - \mathbf{y}\| + \|\mathbf{y} - \mathbf{z}\|$ *(triangle inequality)*

Proof.

(i) Since the square root is non-negative, we have $\|\mathbf{x}\| \geq 0$.

$\|\mathbf{x}\| = 0 \iff \mathbf{x} \cdot \mathbf{x} = 0 \iff \sum_{i=1}^{n} {x_i}^2 = 0 \iff x_i = 0$, since each ${x_i}^2 \geq 0$. Thus $\mathbf{x} = \mathbf{0}$.

(ii) We have

$$\|\alpha \mathbf{x}\|^2 = (\alpha \mathbf{x}) \cdot (\alpha \mathbf{x}) = \sum_{i=1}^{n} (\alpha x_i)^2 = \alpha^2 \sum_{i=1}^{n} {x_i}^2 = \alpha^2 \|\mathbf{x}\|^2.$$

Taking square roots on both sides yields the desired result.

(iii) By the Cauchy–Schwarz inequality (5.2), we have

$$(\mathbf{x} \cdot \mathbf{y})^2 = \left(\sum_{i=1}^{n} x_i y_i \right)^2 \leq \left(\sum_{i=1}^{n} {x_i}^2 \right) \left(\sum_{i=1}^{n} {y_i}^2 \right) = \|\mathbf{x}\|^2 \|\mathbf{y}\|^2.$$

Taking square roots on both sides yields the desired result.

(iv) By (iii), we have

$$\begin{aligned} \|\mathbf{x} + \mathbf{y}\|^2 &= (\mathbf{x} + \mathbf{y}) \cdot (\mathbf{x} + \mathbf{y}) \\ &= \mathbf{x} \cdot \mathbf{x} + 2\mathbf{x} \cdot \mathbf{y} + \mathbf{y} \cdot \mathbf{y} \\ &\leq \|\mathbf{x}\|^2 + 2\|\mathbf{x}\|\|\mathbf{y}\| + \|\mathbf{y}\|^2 \\ &= (\|\mathbf{x}\| + \|\mathbf{y}\|)^2. \end{aligned}$$

(v) This follows directly from (iv) by replacing $\mathbf{x}$ by $\mathbf{x} - \mathbf{y}$, and $\mathbf{y}$ by $\mathbf{y} - \mathbf{z}$.

□

5.6 *Size of $\mathbb{R}$

In this section, we answer the question: How big is $\mathbb{R}$?

Theorem 5.50. $\mathbb{R} \approx \mathcal{P}(\mathbb{N})$.

Proof. By Cantor-Schroder-Bernstein, it suffices to prove $\mathbb{R} \preceq \mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{N}) \leq \mathbb{R}$.

Since $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$, we have $\mathbb{R} \prec \mathcal{P}(\mathbb{Q})$ (as witnessed by the inclusion map). Since $\mathbb{Q} \approx \mathbb{N}$, it follows that $\mathcal{P}(\mathbb{Q}) \approx \mathcal{P}(\mathbb{N})$. Thus $\mathbb{R} \preceq \mathcal{P}(\mathbb{N})$.

With more work one can show $\mathcal{P}(\mathbb{N}) \preceq \mathbb{R}$. Sketch: Map $A \subseteq \mathbb{N}$ to the Dedekind cut

$$\left\{ p \in \mathbb{Q} : (\exists n \in \mathbb{N})\, p < \sum_{i \in A \cap [n]} 3^{-(i+1)} \right\}.$$

Informally, A is mapped to the real number $\sum_{i \in A \cap [n]} 3^{-(i+1)}$ (cf. ternary representation) (this is informal because we did not discuss convergence of infinite sums). To complete this sketch, one needs to prove that the above function is well-defined and injective.

We conclude by Cantor-Schroder-Bernstein that $\mathbb{R} \approx \mathcal{P}(\mathbb{N})$. In particular, $\mathbb{R}$ is uncountable. □

— Exercises —

Exercise 5.6.1. If $A \approx B$, then $\mathcal{P}(A) \approx \mathcal{P}(B)$.

Solution. Since $A \approx B$, fix a bijection $f \colon A \to B$. Consider the map $\mathcal{P}(A) \to \mathcal{P}(B)$ defined by $S \mapsto f[S]$; it remains to be shown that this map is a bijection. □

5.7 *Other Constructions of $\mathbb{R}$

5.7.1 Cauchy Sequences

5.7.2 The Eudoxus Real Numbers

The Eudoxus real numbers is an interesting construction of the real numbers; unlike the Dedekind construction, its construction proceeds directly from the integers to the real numbers, bypassing the intermediate construction of the rational numbers.

[The Efficient Real Numbers](http://maths.mq.edu.au/ street/EffR.pdf) - first two pages contain the first mention of it in the mathematical literature. See bottom of page 1 and top of page 2 for hint for (iv). [A natural construction for the real numbers](https://arxiv.org/abs/math/0301015) [The Eudoxus Real Numbers](https://arxiv.org/abs/math/0405454) - contains details

Exercise 5.7.1. Define a relation $\sim$ on $\text{Maps}(\mathbb{Z}, \mathbb{Z})$ as follows: $f \sim g$ if $f - g$ is bounded, i.e., there exists $b \in \mathbb{N}$ such that $|f(n) - g(n)| \leq b$ for all $n \in \mathbb{Z}$.

(i) Prove that $\sim$ is an equivalence relation.

(ii) We attempt to define a binary operator $+$ on $\text{Maps}(\mathbb{Z}, \mathbb{Z})/\sim$ as follows:

$$[f]_\sim + [g]_\sim = [f + g]_\sim$$

where $+$ on the RHS denotes pointwise addition of functions. Prove that $+$ (on $\text{Maps}(\mathbb{Z}, \mathbb{Z})/\sim$) is well-defined.

(iii) Let R be the set of all $f \in \text{Maps}(\mathbb{Z}, \mathbb{Z})$ such that the set $\{f(a + b) - f(a) - f(b) : a, b \in \mathbb{Z}\}$ is a bounded subset of $\mathbb{Z}$. We attempt to define a binary operator $\times$ on $R/\sim$ as follows:

$$[f]_\sim \times [g]_\sim = [f \circ g]_\sim$$

where $\circ$ denotes function composition. Prove that $\times$ is well-defined.

(iv) (Optional, hard) Prove that $\times$ (on $R/\sim$) is commutative.

Solution.

(i) Reflexivity: For any $f \in \text{Maps}(\mathbb{Z}, \mathbb{Z})$, we have $|f(n) - f(n)| = 0 \leq 0$ for all $n \in \mathbb{Z}$. Hence $f \sim f$.

Symmetry: Suppose $f \sim g$. Fix $b \in \mathbb{N}$ such that $|f(n) - g(n)| \leq b$ for all $n \in \mathbb{Z}$. Then

$$|g(n) - f(n)| = |f(n) - g(n)| \leq b.$$

Hence $g \sim f$.

Transitivity: Suppose $f \sim g$ and $g \sim h$. Fix $b_1, b_2 \in \mathbb{N}$ such that $|f(n) - g(n)| \leq b_1$ and $|g(n) - h(n)| \leq b_2$ for all $n \in \mathbb{Z}$. By triangle inequality,

$$|f(n) - h(n)| \leq |f(n) - g(n)| + |g(n) - h(n)| \leq b_1 + b_2.$$

Hence $f \sim h$.

(ii) Let $[f]_\sim = [f']_\sim$ and $[g]_\sim = [g']_\sim$. Then $f \sim f'$ and $g \sim g'$. Fix $b_1, b_2 \in \mathbb{N}$ such that

$$|f(n) - f'(n)| \leq b_1, \qquad |g(n) - g'(n)| \leq b_2 \qquad \text{for all } n \in \mathbb{Z}.$$

By triangle inequality,

$$\begin{aligned} |(f+g)(n)-(f'+g')(n)| &= |f(n)-f'(n)+g(n)-g'(n)| \\ &\le |f(n)-f'(n)|+|g(n)-g'(n)| \\ &\le b_1+b_2. \end{aligned}$$

Hence $f+g \sim f'+g'$, so $[f+g]_\sim = [f'+g']_\sim$.

(iii) We first show that $f \circ g \in R$ for all $f, g \in R$. Let $f, g \in R$. Fix $b_1, b_2 \in \mathbb{N}$ such that

$$|f(a+b)-f(a)-f(b) \le b_1|, \qquad |g(a+b)-g(a)-g(b)| \le b_2 \quad \text{for all } n \in \mathbb{Z}.$$

Denote $M = \{f(x) : -b_2 \le x \le b_2\}$. Since M is finite, M is bounded by some integer m. Then

$$\begin{aligned} &|f \circ g(a+b) - f \circ g(a) - f \circ g(b)| \\ &= |f(g(a+b)) - f(g(a)) - f(g(b))| \\ &= |f(g(a+b)) - f(g(a)+g(b)) + f(g(a)+g(b)) - f(g(a)) - f(g(b))| \\ &\le |f(g(a+b)) - f(g(a)+g(b))| + |f(g(a)+g(b)) - f(g(a)) - f(g(b))| \\ &\le |f(g(a+b)) - f(g(a)+g(b))| + b_1 \\ &= |f(g(a+b)) - f(g(a)+g(b)) - f(g(a+b)-g(a)-g(b)) + f(g(a+b)-g(a)-g(b))| + b_1 \\ &\le |f(g(a+b)) - f(g(a)+g(b)) - f(g(a+b)-g(a)-g(b))| + |f(g(a+b)-g(a)-g(b))| + b_1 \\ &\le b_1 + m + b_1. \end{aligned}$$

Thus $f \circ g \in R$.

Now suppose $[f] = [f']$ and $[g] = [g']$. Since $f \sim f'$ and $g \sim g'$, fix $c_1, c_2 \in \mathbb{N}$ such that

$$|f(x)-f'(x)| \le c_1, \qquad |g(x)-g'(x)| \le c_2 \quad \text{for all } x \in \mathbb{Z}.$$

Since $f, g \in R$, fix $c_3 \in \mathbb{N}$ such that

$$|f(a+b)-f(a)-f(b)| \le c_3.$$

Denote $A = \{f(x) : -c_2 \le x \le c_2\}$. Since A is finite, A is bounded by some $m \in \mathbb{N}$. We have

$$\begin{aligned} &|f \circ g(x) - f' \circ g'(x)| \\ &= |f(g(x)) - f'(g'(x))| \\ &= |f(g(x)) - f'(g(x)) + f'(g(x)) - f'(g(x)-g'(x)) - f'(g'(x)) + f'(g(x)-g'(x))| \\ &\le |f(g(x)) - f'(g(x))| + |f'(g(x)) - f'(g(x)-g'(x)) - f'(g'(x))| + |f'(g(x)-g'(x))| \\ &\le c_1 + c_3 + m. \end{aligned}$$

Hence $f \circ g \sim f' \circ g'$, so $[f \circ g] = [f' \circ g']$.

(iv)

□

(i) – (iii) show that $R/\!\sim$ is a ring, (iv) shows that $R/\!\sim$ is a (complete) field.

Bibliography

[Abb16] Stephen Abbott. *Understanding Analysis.* Springer, 2016.

[Apo57] T. M. Apostol. *Mathematical Analysis.* Addison-Wesley, 1957.

[End77] H. B. Enderton. *Elements of Set Theory.* Academic Press, Inc., 1977.

[HS65] E. Hewitt and K. Stromberg. *Real and Abstract Analysis.* Springer-Verlag, 1965.

[Lak16] T. J. Lakins. *The Tools of Mathematical Reasoning.* American Mathematical Society, 2016.

[Pól45] G. Pólya. *How to Solve It.* Princeton University Press, 1945.

[Rud76] W. Rudin. *Principles of Mathematical Analysis.* McGraw–Hill, 1976.

[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.

Index