Student's Guide to MATH 2000

Mathematical Concepts

A neophyte's guide to proofs, sets, and other fundamental concepts to become a mathematical wizard in the 21st century

So you want to be a mathematical wizard with the dream of winning the prestigious Fields Medal or Turing award. Unlike in earlier courses where you learned the math version of cantrips, success in advanced math (and to a lesser extent CS) courses does not depend so much on being able to find the right answer to a question, but providing a convincing explanation that the answer is correct. Here you will learn what the math version of spell-casting beyond cantrips would be like. You will learn the basics of logic, proofs, set theory, relations and functions, finite and countable sets, induction, and examples of axiomatic mathematical theories.

Disclaimer: This book is not responsible for the consequences of faulty proofs, attempting to cast a mathematical fireball, speaking math cant in an examination or saying yes when the professor asks, "Are you really sure about this proof?"

Contents

Part 1

Introduction to Logic and Proofs

Chapter 1: Introduction and Logical Deduction

1.1 Course Description

This course can be viewed as a "math as a second language" course. It introduces basic concepts such as logic, set theory, and techniques of proof that form the foundation of mathematics. The course acts as a bridge between computational courses like calculus, and later theoretical courses, like analysis and number theory.

1.2 Course Objective

The main goal in this course is to develope the ability to learn to write proofs and form mathematical arguments. We want to make the transition from *using* mathematics - for example, computing a derivative using established rules - and *doing* mathematics - establishing those rules in the first place, and explaining why they're valid. You will learn the precise logical meaning of words like 'and, 'or', and 'if', and why a precise meaning is necessary. While we will be stressing the importance of proper syntax, the primary focus will be on learning to produce writing that is clear and concise, and easily understood by the rest of your classmates. Even if you not planning to continue to higher-level math courses, this course should prepare you for any situation where clear technical writing or convincing arguments are needed.

1.3 Logic

Logic includes a hypothesis (assumptions), and a conclusion. For example, today is tuesday and you have Math 2000 on tuesday and thursday. Therefore, you have Math 2000 today.

Definition 1.3.1 (Assertion)**.** *An assertion is a sentence which is either* ***True*** *or* ***False*** *(has a truth value) proposition. For example, today is a tuesday, this is an assertion, Is today a tuesday? is not an assertion.*

Definition 1.3.2 (Deduction)**.** *is a series of hypothesis or assumptions followed by a conclusion, where each of the hypothesis and the conclusion are assertion. For example, Socrates is a man, and all man are mortal, therefore Socrates is mortal.*

A deduction is valid if its conclusion is true whenever all it's hypothesis is true. In other words it is impossible to have a situation where all the hypothesis is true but the conclusion is false.

Chapter 2: Propositional Logic

Notation
in propositional logic, capital letters are used to represent assertion. Considered only as a symbol of propositional logic, the letter 'A' could represent any assertion. Therefore, it is important to provide a symbolization key when translating english to PL.

For example let:

A	There is an apple on the desk
B	If there is an apple on the desk then Jenny made it to class
C	Jenny made it to class

This is our symbolization key.

We can write this as: A, B, Therefore C.

Note
Assertions that are represented by a single letter are called atomic assertions. These are the building blocks from which more complex assertions are made.

2.1 Connectives

Symbol	'read as'	meaning
~/-	Not	is not the case __
& /∧	And	both __ and __
∨	Or	Either __ or __
→	implies	if __ then __
↔	iff	__ if and only if __

The following holds for any assertion P.

1. If P is true then ¬P is false
2. If P is false then ¬P is true

Note
- ∨ and ∧ are commutative, while → is not.

2.2 Tautologies and Contradictions

Tautologies are true values by their logical structure and their truth values are independent from their atomic assertions. **Contradictions** follows the same idea as tautologies but with false values instead.

For example:

- $P \vee \neg P$ = tautology also called the law of excluded middle since it says that every assertion true or false
- $P \wedge \neg P$ = contradiction

2.3 Logical equivalences

Definition 2.3.1 (Logical equivalences). *Two assertions P and Q are said to be logically equivalent provided by both obtain the same truth value for every possible truth value assignment for their atomic assertion.*

Denoted as $\equiv$.

Rules for equivalence:

- $\neg\neg P = P$
- $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
- $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
- $\neg(P \to Q) \equiv \neg P \wedge \neg Q$
- $\neg(P \leftrightarrow Q) \equiv P \leftrightarrow \neg Q$
- $P \vee Q \equiv Q \vee P$
- $P \wedge Q \equiv Q \wedge P$
- $P \leftrightarrow Q \equiv Q \leftrightarrow P$
- $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$ *same with* $\vee$
- $P \wedge (Q \vee R) \equiv P \wedge Q \vee P \wedge R$
- $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
- $P \Rightarrow R \equiv \neg P \vee Q$

Follows the same algbraic rules

Definition 2.3.2 (Converse). *For an implication $P \to Q$ its converse is the implication $Q \to P$*

Definition 2.3.3 (Contrapositive). *For an implication $P \to Q$ its contrapositive is the implication $\neg Q \to \neg P$*

Note
Implication is not logically equivalent to its converse.

Definition 2.3.4 (Inverse). *For an implication $P \to Q$ its inverse is the implication $\neg P \to \neg Q$*

Note
- an implication is not logically equivalent to its inverse
- an implication is logically equivalent to its contrapositive.

2.4 Rules for Propositional Logic

1. Repeat: $A \therefore A$
2. ANDIntro: $A, B \therefore A \wedge B$
3. AND-Elim: $A \wedge B \therefore A$ / $A \wedge B \therefore B$
4. OR-Intro: $A \therefore A \vee B$
5. OR-Elim: $A \vee B, -A \therefore B$ (Modus Ponens)

6. Implicit-Elim: $A \to B, A \therefore B$
7. IFF-Intro: $A \to B, B \to A \therefore A \leftrightarrow B$
8. IFF-Elim: $A \leftrightarrow B \therefore A \to B$
9. Proof by cases: $A \vee B, A \to C, B \to C \therefore C$

Intro combines the atomic assertions into the binary operator for its conclusion

Elim turns the binary operator into an atomic assertion that has to be true

$P \to Q$ can be expressed in a number of ways

- If P, then Q, Q if P
- P implies Q, whenever P is true then Q is true
- P only if Q, Q is true whenever P is true
- Q is necessary for P, P is sufficient for Q

$P \leftrightarrow Q$ could mean: P if and only if Q, P implies Q and Q implies P, P is necessary and sufficient for Q.

Question(s)

1. Explain Why MP is valid?

Answer(s)

1. If we know that A is true and we know that A is a sufficient condition for B to be true, then B must be true.

Prove that $A \leftrightarrow B$

Proof. $A \to B$ s false if A is true and B is false, $B \to A$ is false if B is T and A is false. Hence, we see that $A \to B$, and $B \to A$ are both true whenever A and B have the same truth value, These are precisely the conditions for which $A \leftrightarrow B$ are true. □

Chapter 3: Two-Column Proofs

3.1 Proof

The aim of a proof is to show that a deduction is valid. We do this by putting together, a number of simpler deduction which we already know to be valid.

Here is an example

hypotheses:

1. $P \Rightarrow (Q \wedge R)$
2. P

Conclusion: R

Formally, a proof is a sequence of assertions. The first few assertions are the assumptions of the deduction, and each subsequent line is an immediate column in our 2 column proof, consequence of the preceding lines must contain two pieces with the final line begin our conclusion of information.

Format of 2-column-proof

Assertion in PL	Justification
Assertion	Justification

So for the example above we have this assumption

$P \Rightarrow (Q \wedge R)$	assumption
P	assumption
$(Q \wedge R)$	implicit elim
R	AND elim

Note
In this example everything was done in the language of PL. However, the deduction might be given in English, in which case we must first translate the deduction into PL using a symbolization key.

Assumptions and theorems

A two column proof starts off by listing each of the assumptions. These are justified by writing assumptions in the second column. We then draw a line to separate our assumptions from the rest of the proof. Any deduction which is already known to be valid is called a theorem. They can be used for justification, in a proof, provided that the assumptions of the theorem have already been established or assumed to be true.

Example:

$P \vee S$	Assumption
$P \rightarrow (Q \wedge R)$	assumption
$\neg S$	assumption
P	OR-elim
R	e.x 2.1

Note
Each line in a 2-column proof (after the assumption) is an assertion which is true whenever all the assumptions are true. Since tautologies are always true we can introduce a tautology into our two-col-proof whenever it is convenient. These are justified as tautologies when writing.

3.2 Sub-proof into implicit intro

Consider the deduction $P \rightarrow R \therefore (P \wedge Q) \rightarrow R$. This is a valid deduction. Intuitively we can see that if $P \wedge Q$ is true then P is true, and it follows from MP that R is true. That is, R is a necessary consequence of $P \wedge Q$.

Proof.

1. $P \Rightarrow R$: This is our assumption
2. Here is the beginning of our sub-proof
   (a) $P \wedge Q$: Assumption, we want R
   (b) P, AND-Elim
   (c) R, MP
3. $(P \wedge Q) \Rightarrow R$, implicit intro

2. Was our the beginning of our sub-proof. 4. was our ending. □

We can add a new assumption within a sub proof for the sake of argument to create an implicit intro

We created a new implciate statement based on the subproof and the assumption from the main proof

Note
Once you closed the sub-proof you cannot go back.

3.3 Proof by Contradiction

We need to be able to prove that an assertion is false, the usual way of doing this is to show that it cannot be true. We do this by considering what would happen if the assertion were true. If, by using logic, we can show that this assumption leads to a contradiction, then we can conclude that the assumption must be wrong This is a proof by contradiction.

Example

Prove that there is no largest natural number

Proof. Suppose that there is a largest natural number called n. Then $n + 1 \in \mathbb{N}$, and $n + 1 > n$. This contradicts our assumptions that n is the largest natural number.

$\therefore$ our assumption cannot be true hence there is no largest natural number. □

3.4 Proof strategies

We are told our starting condition and our end goal. We also have a set of rules which tells us what our acceptable or valid moves are. At each step there are several valid moves and we just need to choose the right one. However, there is no procedure on what that is.

1. Work forward from what you have
2. Work backward from what you want
3. Break our proof into cases: if it looks like your proof requires an additional assumption, try considering multiple cases.
4. Use logical equivalences to change what we are looking at: We can use replacement rules to make life easier, or use a different substitution something like DeMorgans, or what not.
5. Look for useful sub-goals: If you have establish or maybe assumed it. $P \to Q$, you should think about how you might obtain P or $\neg P$ so you can use implicit elim/MP
6. Proof by contradiction: if you have trouble establishing P directly, consider assuming $negP$, and deducing a contradiction. Eg,m instead of deducing P or Q directly, it might be easier to show $negP \wedge \neg Q$ and deduce a contradiction.
7. Repeat as necessary: after you made some progress (either deriving new assertion or deciding on a new sub-goal that represent significant progress) use the strategies above to plan our next move.
8. Don't give up (seriously): stop, backtrack and try something else.

3.5 Counterexamples

Consider the deduction:

$P \vee Q$, $P \to Q$, $\therefore P$, this is not valid, why?

To prove something not being valid we need a **counter example**. To do this, it suffices to show that it is possible to have a false conclusion when all our assumption(s) are true. This should be done by finding and assignment for our variables which makes the conclusion false and our assumption(s) true.

Proof. Let P be false and let Q be true. Then we have

- $P \vee Q = F \vee T = T$
- $P \to Q = F \to T = T$

So both our assumptions are true but our conclusion is false therefore the deduction is not valid □

Definition 3.5.1 (Counterexample)**.** *Any situation in which all our assumptions are true but our conclusion is false is called a* ***Counterexample****.*

Part 2

Sets and First-Order-Logic

Chapter 4: Sets

Consider the following deduction

Assumption:

- Merlin is a wizard
- All wizards wear funny hats

Conclusion: Merlin is wearing a funny hat.

This type of language is called first order logic

A predicate is an expression like "__ is wearing a funny hat." This is not an assertion on its own, because it is neither true nor false until we fill in the blank, to specify who it is that we claim is wearing a funny hat.

The words "all" and "some" are *quantifiers*, and we will have symbols that represent them. For instance, "∃" will mean "There exists some __, such that." Thus, to say that someone is wearing a funny hat, we can write $\exists x, H(x)$ where $H(x)$ is "x is wearing a funny hat." This mean that there exist a person x that is wearing a funny hat. ∀ will mean "For all __, such that." Thus, to say that everyone is wearing a funny hat, we can write $\forall x, H(x)$.

4.1 Sets

A set is a collection of unique, unordered objects. The objects in the set are called elements or members of the set.

Roster method

An easy way to describe a set is simply list all the elements in the set. Let X be a set, then we can write it like this $X = \{1, 2, 3, 4, 5\}$, $\in$ means the element is in the set, while $\notin$ means the element is not in the set. For example, $1 \in X$ while $8 \notin X$

There is a unique set called the **empty set** which is a set that has no elements, it is written like this $\emptyset$ or $\{\}$

A set is determined by its elements, we cannot have two distinct sets with identical elements.

List of common sets

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ - Natural Numbers
- $\mathbb{N}+ = \{1, 2, 3, \dots\}$ - Positive Natural Numbers
- $\mathbb{Z} = \{\dots, -2, 1, 0, 1, 2, \dots\}$ - Integers
- $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, and\ b \neq 0\}$ - Rational Numbers
- $\mathbb{R} = \{\pi, e, 12.3, 1, 2, -1, 2029\}$ - Real Numbers
- $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ - Complex Numbers

Cardinality

Definition 4.1.1 (Cardinality). *The number of elements within a set.*

Notation: *Let A be a set. $\#A$ or $|A|$ means the cardinality of A*

Note

Infinity is a valid "number" within this context. Also the set A is said to be finite if and only if there exist some natural number n such that |A| = n.

Subset

Suppose A and B are sets, we say that A is a subset of B and write $A \subseteq B$ if and only if for every x if x is in A then x must be in B.

Definition 4.1.2 (Subset). $A \subseteq B \leftrightarrow \forall x(x \in A \rightarrow x \in B)$.

We can say that A is contained in B, B contains A, or B is a superset of A.

Note

We write $A \subset$ if A is a proper subset of B but A and B are different. $A \not\subseteq B$ means A is not a subset of B.

1. For all set A, then $A \subseteq A$
2. For every set A, then $\emptyset \subseteq A$
3. If $A \subseteq B$ then $|A| \leq |B|$
4. Let A and B bet sets. $A = B$ if and only if they are a subset of each other. i.e., $A \subseteq B$ and $B \subseteq A$

4.2 Predicates

The simplest predicates are things we can say about on individual objects. for example "x is a dog" or "x is tall" could be symbolize as D(x): "x is a dog" or T(x): "x is tall". Predicates such as these are called unary or one-place predicates, they only have one object for their predicates. Other predicates are about relations between objects i.e., x = y, or x > y. These are examples of two-place or binary predicates. By convention, when we are writing our symbolization key specific objects (constant) go to the end. So for example

- S(x): "x is a Skaven"
- xAy: "x assassinated y"
- i: Ikit Claw
- m: Malekith

Set Builder Notation

Rather than listing all the elements of a set, it is often more convenient to use predicates to build sets.

Suppose A is a set, and P(x) is a predicate. Then $\{z \in A; P(a)\}$ denotes the set of all elements in A, for which P(a) is true.

If A is a set, P(x) is a predicate, $B = \{a \in A; P(a)\}$ then the assertion $b \in B$ is logically equivalent to the assertion $b \in A \wedge P(b)$. In a proof this $\equiv$ could be justified as the definition of B.

When we are talking about sets or predicates we usually assume a universe of discord (U) has been agreed upon. This means all element of the sets are assumed to be elements of (U). Then x|P(x) could be short hand to $\{x \in U | P(x)\}$. Instead of writing D(x) for "x is a dog" we might let D denote the set of all dogs and we can say $x \in D$.

4.3 Set Operations

Theorem 4.3.1 (Set Operations)**.**

- *Union:* $A \bigcup B = \{x | x \in A \vee x \in B\}$
- *Intersection:* $A \bigcap B = \{x | x \in A \wedge x \in B\}$
- *Set Difference:* $A \backslash B = \{x | x \in A \wedge x \notin B\}$
- *Complements:* $\bar{A} = \{x \in U | x \notin A\} = U \backslash A$

Definition 4.3.1 (Disjoint Set)**.** *Two sets A and B are said to be disjoint if and only if* $A \wedge B = \emptyset$*. Meaning there is nothing common between the two sets.*

Definition 4.3.2 (Power Set)**.** *The power set of set A is the set of all subsets of A:* $\mathcal{P}(A) = \{B | B \subseteq A\}$*. For example if* $A = \{a, b, c\}$*. The power set of A* **denoted** *P(A) would be this:*
$\{\emptyset,\ \{a\}, \{b\}, \{c\},\ \{a, b\}, \{a, c\}, \{b, c\},\ \{a, b, c\}\}$

4.4 Example

Let A and B be sets, prove that if $x \in \bar{A} \bigcup \bar{B}$, then $x \in \overline{(A \bigcap B)}$. DeMorgans for sets.

Proof. Let $x \in \bar{A} \bigcup \bar{B}$, then by definition of union we have x be either $x \in \bar{A}$ or $X \in \bar{B}$. We will solve by cases.

1. if $x \in \bar{A}$, then by definition of complements, $x \notin A$, and therefore $x \notin A \bigcap B$, then by definition of complement we have $x \in \overline{A \bigcap B}$
2. if $x \in \bar{B}$, then by definition of complements, $x \notin B$, and therefore $x \notin A \bigcap B$, then by definition of complement we have $x \in \overline{A \bigcap B}$

In either case we see that $x \in \overline{A \bigcap B}$ and therefore conclude that if $x \in \bar{A} \bigcup \bar{B}$ then $x \in \overline{A \bigcap B}$. □

Chapter 5: First Order Logic

5.1 Quantifiers

Earlier, we observed that Propositional Logic cannot fully express ideas involving quantity, such as "some" or "all." In this chapter, we will fill this gap by introducing quantifier symbols. Together with predicates and sets, which have already been discussed, this completes the language of First-Order-Logic. We will then use this language to translate assertions from English into mathematical notation.

Consider the following symbolization key

U : The set of all people.
L : The set of all people in Lethbridge.
A : The set of all angry people.
H : The set of all happy people.
xRy : x is richer than y
d : Donald
g : Gregor
m : Marybeth

Now consider these assertions

- Everybody is happy
- Everyone in Lethbridge is happy
- Everyone in Lethbridge is richer than Donald
- Someone in Lethbridge is angry

It might be tempting to translate Assertion 1 as $(d \in H)$ & $(g \in H)$ & $(m \in H)$. Yet this would only say that Donald, Gregor, and Marybeth are happy. We want to say that *everyone* is happy, even if we have not listed them in our symbolization key. In order to do this, we introduce the "$\forall$" symbol. This is called the **universal quantifier**.

Definition 5.1.1 (Universal Quantifier). *$\forall x$ mean "for all x"*
$\forall x \in X$ mean "for all x in X", where X is any set.

For example this "$\forall x,\ x \in H$" means that everyone is happy.

Note
Each quantifier much have a variable that the quantifier affect. This variable could be from a set that is not the universe.

To translate Assertion 4, we introduce another new symbol: the **existential quantifier** $\exists$.

Definition 5.1.2 (Existential quantifier). *$\exists x$ means "there exists some x, such that"*
$\exists x \in X$ means "there exists some x in X, such that", where X is any set.

Consider the following:

S : The set of all students.
B : The set of all books.
N : The set of all novels.
xLy : x likes to read y.

$\forall n \in N, (n \in B)$ means "every novel is a book," and $\forall s \in S, \big(\exists b \in B, (s\ L\ b)\big)$ means "for every student, there is some book that the student likes to read."

It is important to have proper ordering of quantifiers, as having them in different order means different things.

Consider the following:

U : everything

1. $\forall x(\exists y, x = y)$
2. $\exists x(\forall y, x = y)$

1 and 2 looks the same except for the ordering however 1 means "everything is equal to something" while 2 means "there exist something that equals to every other thing". The ordering is done from left to right manner.

Theorem 5.1.1 (Demorgans of Quantifiers).
$\neg\forall x, X(x) \equiv \exists x, \neg X(x)$
$\neg\exists x, X(x) \equiv \forall x, \neg X(x)$

Vacuous Truth

Note that if the assertion

$$\exists x \in A, \neg P(x)$$

is true (where A is any set and $P(x)$ is any unary predicate), then there must exist an element a of A, such that $P(a)$ is false. Ignoring the last condition (about $P(a)$), we know that $a \in A$, so $A \neq \emptyset$. That is, we know:

If the assertion $\exists x \in A, \neg P(x)$ is true, then $A \neq \emptyset$.

So the contrapositive is also true:

If $A = \emptyset$, then the assertion $\exists x \in A, \exists P(x)$ is false.

Therefore, the assertion $\exists x \in \emptyset, \neg P(x)$ is false, so its negation is true:

The Assertion
$\forall x \in \emptyset, P(x)$ is true.

Since $P(x)$ is an arbitrary predicate, this means that any assertion about *all* of the elements of the empty set is true; we say it is **vacuously true**. The

point is that there is nothing in the empty set to contradict whatever assertion you care to make about all of the elements.

Summary

Any assertion about *all* of the elements of the empty set is *vacuously true.*

Uniqueness

Saying "there is a **unique** so-and-so" means not only that there is a so-and-so, but also that there is only one of them—there are not two different so-and-so's. For example, to say that "there is a *unique* person who owes Hikaru money" means

> some person owes Hikaru *and* no other person owes Hikaru.

This translates to

$$\exists h \in H, (\forall y, (y \neq h \Rightarrow y \notin H));$$

or, equivalently,

$$\exists h \in H, (\forall y, (y \in H \Rightarrow y = h)).$$

Unfortunately, both of these are quite complicated expressions (and are examples of "multiple quantifiers," because they use both $\exists$ and $\forall$). To simplify the situation, mathematicians introduce a special notation:

Definition 5.1.3 (Uniqueness Quantifier)**.**
"$\exists! \, x$" means "there is a unique x, such that..."
If X is any set, then "$\exists! \, x \in X$" means "there is a unique x in X, such that..."

5.2 The introduction and elimination rules for quantifiers

As you know, there are two quantifiers ($\exists$ and $\forall$). Each of these has an introduction rule and an elimination rule, so there are 4 rules to present in this section. Proofs in First-Order Logic can use both of these rules, plus all of the rules of Propositional Logic (such as the rules of negation and the basic theorems, including introduction and elimination rules), and also any other theorems that have been previously proved.

$\exists$-introduction

We need to determine how to prove a conclusion of the form $\exists x \in X, \ldots$. For example, in a murder mystery, perhaps Inspector Thinkright gathers the suspects in a room and tells them, "Someone in this room has red hair." That is a $\exists$-statement. (With an appropriate symbolization key, in which P is the set of all of the the people in the room, and $R(x)$ is the predicate "x has red hair," it is the assertion $\exists p \in P, R(p)$.) How would the Inspector convince a skeptic that the claim is true? The easiest way would be to exhibit an explicit example of a person in the room who has red hair. For example, if Jim is in the room, and he has red hair, the Inspector might say,

> "Look, Jim is sitting right there by the door, and now, when I take off his wig, you can see for yourself that he has red hair. So I am right that someone in this room has red hair."

In general, the most straightforward way to prove $\exists p \in P, R(p)$ is true is to find a specific example of a p that makes $R(p)$ true. That is the essence of the $\exists$-intro rule.

Here is a principle to remember:

Principle

The proof of an assertion that begins "there exists $x \in X$, such that..." will usually be based on the statement "Let $x = \square$," where the box is filled with an appropriate element of X

Example

Prove that there exist a real number c, such that $n^2 = 64$

Proof. Let $n = 8 \in \mathbb{R}$. Then $n^2 = 8^2 - 64$. □

$\exists$-elimination

Perhaps Inspector Thinkright knows that one of the men lit a match at midnight, but does not know who it was. The Inspector might say,

> "We know that one of the men lit a match at midnight. Let us call this mysterious gentleman 'Mr. X.' Because right-handed matches are not allowed on the island, we know that Mr. X is left handed. Hence, Mr. X is not a butler, because all of the butlers in this town are right handed. ..."

and so on, and so on, telling us more and more about Mr. X, based only on the assumption that he lit a match at midnight.

The situation in mathematical proofs is similar. Suppose we know there exists an element of the set A. Then it would be helpful to have a name for this mysterious element, so that we can talk about it. But a mathematician would not call the element "Mr. X": if it is an element of the set A, then he or she would probably call it a (or a_1 if there are going to be other elements of A to talk about). In general, the idea of the $\exists$-elimination rule is:

Principle

If $\exists x \in X, P(x)$ is known to be true, then we may let x be an element of X, such that $P(x)$ is true.

Example

Show that if there exists $a \in \mathbb{R}$, such that $a^3 + a + 1 = 0$, then there exists $b \in \mathbb{R}$, such that $b^3 + b - 1 = 0$.

Proof. Assume there exists $a \in \mathbb{R}$, such that $a^3+a+1 = 0$. Let $b = -a$. Then $b \in \mathbb{R}$, and

$$\begin{aligned} b^3 + b - 1 &= (-a)^3 + (-a) - 1 \\ &= -a^3 - a - 1 \\ &= -(a^3 + a + 1) \\ &= -0 \qquad \text{(by the definition of } a\text{)} \\ &= 0, \end{aligned}$$

as desired. □

∀-ELIMINATION

Perhaps Inspector Thinkright knows that Jeeves is a butler in the town, and that all of the butlers in the town are right handed. Well, then it is obvious to the Inspector that Jeeves is right handed. This is an example of ∀-elimination: if you know something is true about every element of a set, then it is true about any particular element of the set.

Principle

If $\forall x \in X, P(x)$ is true, and $a \in X$, then $P(a)$ is true.

Example

Suppose

1. $C \subset \mathbb{R}$, and
2. $\forall x \in \mathbb{R}, \big((x^2 = 9) \Rightarrow (x \in C)\big)$.

Show $\exists c \in \mathbb{R}, c \in C$.

Proof. Let $c = 3 \in \mathbb{R}$. Then $c^2 = 3^2 = 9$, and letting $x = c$ in Hypothesis 2 tells us that

$$(c^2 = 9) \Rightarrow (c \in C).$$

Therefore $c \in C$. □

∀-INTRODUCTION

If Inspector Thinkright needs to verify that all of the butlers in town have seen the aurora borealis, he would probably get a list of all the butlers, and check them one-by-one. That is a valid approach, but it could be very time-consuming if the list is very long. In mathematics, such one-by-one checking is often not just time-consuming, but impossible. For example, the set $\mathbb{N}$ is infinite, so, if we wish to show $\forall n \in \mathbb{N}, (2n$ is even), then we would never finish if we tried to go through all of the natural numbers one-by-one. So we need to deal with many numbers at once.

Consider the following simple deduction:

Deduction Example

Hypotheses:
Every butler in town got up before 6am today.
Everyone who got up before 6am today, saw the aurora.
Conclusion:
Every butler in town saw the aurora.

This is clearly a valid deduction in English. Let us translate it into First-Order-Logic to analyze how we were able to reach a conclusion about all of the butlers, without checking each of them individually. Here is a symbolization key:

B : The set of all of the butlers in town.
P : The set of all people.
U(x) : x got up before 6am today.
S(x) : x saw the aurora.

We can now translate our English deduction, as follows:

Hypotheses

$\forall b \in B, U(b)$.
$\forall p \in P, \big(U(p) \Rightarrow S(p)\big)$.

Conclusion: $\forall b \in B, S(b)$.

How do we justify the conclusion? Well, suppose for a moment that we start to check every butler in town, and that j represents Jimmy, who is one of the butlers in town. Then our first hypothesis allows us to conclude $U(j)$. Since Jimmy is a person, our second hypothesis allows us to conclude that $U(j) \Rightarrow S(j)$. Then, using $\Rightarrow$-elimination, we conclude $S(j)$. But there was nothing special about our choice of Jimmy. All that we know about him, is that he is a butler in the town. So we could use exactly the same argument to deduce $S(b)$ for any butler b in the town.

This is how we justify a ∀-introduction. If we can prove that the desired conclusion is true for an *arbitrary* element of a set, when we assume *nothing* about the element except that it belongs to the set, then the conclusion must be true for every element of the set.

We write the above deduction as follows:

Theorem 5.2.1. *Assume that every butler in town got up before 6am today. Also assume that everyone who got up before 6am today, saw the aurora. Then every butler in town saw the aurora.*

Proof. Let b represent an arbitrary butler in town. Then, since all of the butlers got up before 6am, we know that b got up before 6am. By hypothesis, this implies that b saw the aurora. Since b is an arbitrary butler in town, we conclude that every butler in town saw the aurora. □

This reasoning leads to the ∀-introduction rule: in order to prove that *every* element of a set X has a certain property, it suffices to show that an *arbitrary* element of X has the desired property. For example, if we wish to prove $\forall b \in B, P(b)$, then our proof should start with the sentence "Let b be an arbitrary element of B." (However, this can be abbreviated to: "Given $b \in B, \dots$") After this, our task will be to prove that $P(b)$ is true, without assuming anything about b other than it is an element of B.

Principle

The proof of an assertion that begins "for all $x \in X$," will usually begin with "Let x be an arbitrary element of X" (or, for short, "Given $x \in X$,").

Note

It is important not to assume anything about x other than that it is an element of X. If you choose x to be a particular element of X that has some special property, then your deduction will not be valid for *all* elements of the set.

This is the proof proof subsection: The pain in the ass that makes math people win Fields medal.

Example

Suppose we would like to justify the following deduction:

> All of the butlers in town dislike Jimmy, and Jimmy is a butler in town. Therefore, all of the butlers in town dislike themselves.

Then it suffices to show, for an arbitrary butler b, that b dislikes b. We might try the following proof:

Proof attempt. Let b be Jimmy, who is a butler in town. Then, since all of butlers in town dislike Jimmy, we know that b dislikes Jimmy. Since Jimmy $= b$, this means b dislikes b, as desired. So every butler in town dislikes himself. □

This proof is certainly *not* valid, however. Letting $b =$ Jimmy does not make b an *arbitrary* butler; rather, it makes b a very special butler — the one that everybody dislikes. In this case, conclusions that are true about b are not necessarily true about the other butlers.

Example

Assume A and B are sets. We have $A = B$ if and only if $A \subset B$ and $B \subset A$.

Proof. ($\Rightarrow$) Assume $A = B$. Every set is a subset of itself, so we have

$$A = B \subset B \quad \text{and} \quad B = A \subset A,$$

as desired.

($\Leftarrow$) Assume $A \subset B$ and $B \subset A$. We wish to show $A = B$; in other words, we wish to show

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

Let x be arbitrary.

($\Rightarrow$) Suppose $x \in A$. Since $A \subset B$, this implies $x \in B$.

($\Leftarrow$) Suppose $x \in B$. Since $B \subset A$, this implies $x \in A$.

Therefore, $x \in A \Leftrightarrow x \in B$. Since x is arbitrary, this implies $\forall x, (x \in A \Leftrightarrow x \in B)$, as desired. □

5.3 Counterexample (reprise)

Recall: to show deduction is valid, we provided a proof: to prove its valid.

Definition 5.3.1 (Counterexample)**.** *To show a deduction that is not valid we provided a counterexample. We only need a single example that the proof is not valid. That is the assumption(s) are correct but the conclusion is not.*

Example

Show that the following deduction is not valid:

$$\exists x, (x \in A), \qquad \therefore \ \forall x, (x \in A).$$

Scratchwork. We could consider what this says if A is the set of Flyers fans. So our universe could be all people A where A could be Flyers fans in this room.

Then the deduction becomes. There exist a Flyer fan in this room. Therefore everyone in this room is a Flyers fan.

Which is clearly not valid.

Counterexample. Let

$$\mathcal{U} = \{1, 2\} \text{ and } A = \{1\}.$$

Then:

$1 \in A$ is true, so $\exists x, (x \in A)$ is true, so the hypothesis is true,

but

$2 \notin A$, so $\forall x, (x \in A)$ is false, so the conclusion is false.

Since we have a situation in which the hypothesis is true, but the conclusion is false, the deduction is not valid. □

5.4 Proof strategies

The strategies we used in Propositional Logic is the same strategies we use in First-Order-Logic

1. If you have $\exists x, A(x)$ you probably want to do an $\exists$-elimination, assume A(c) for some undeclared 'c'.
2. If you're trying to deduce an assertion: $\forall x, A(x)$, you probably want to use a $\forall$-intro, use the form Let $x \in X$ or given $x \in X$.
3. If you have $\forall x, A(x)$, and it might be useful to know A(c) for some constant c, then you can use $\forall$-elimination

Chapter 6: Sample Topics

Up to this point, our valid deductions have been called "theorems," but mathematicians usually reserve this name for the ones that are particularly important, and apply some other name to the others. The terminology allows some flexibility, but here are general guidelines

Definition 6.0.1 (Terminologies)**.**

- *Any valid deduction can be referred to as a "result"*
- *A* ***theorem*** *is an important result*
- *A* ***proposition*** *is a result that is not sufficiently important to be called a theorem*
- *A* ***corollary*** *is a result that is proved as an easy consequence of some other result*
- *A* ***lemma*** *is a minor result that is not interesting for its own sake, but will be used as part of the proof of theorem (or other more significant result)*

6.1 Number Theory: divisibility and congruence

In this section, we will get some practice with proving properties of integers.

Divisibility

Definition 6.1.1 (Divisibility)**.** *Suppose $a, b \in \mathbb{Z}$. We say a is a* ***divisor*** *of b (and write "$a \mid b$") if and only if there exists $k \in \mathbb{Z}$, such that $ak = b$. (Since multiplication is commutative and equality is symmetric, this equation can also be written as $b = ka$.)*

These means the same

- *a is a* ***divisor*** *of b*
- *a is a* ***factor*** *of b*
- *b is a* ***multiple*** *of a*
- *b is* ***divisible*** *by a*

Definition 6.1.2 (Even and Odd)**.** *Let $n \in \mathbb{Z}$. We say n is* ***even*** *if and only if $2 \mid n$. We say n is* ***odd*** *if and only if $2 \nmid n$.*

We will assume the well-known fact that the sum, dif and only iference, and product of integers are integers: for all $k_1, k_2 \in \mathbb{Z}$, we know that $k_1 + k_2 \in \mathbb{Z}$, $k_1 - k_2 \in \mathbb{Z}$, and $k_1 k_2 \in \mathbb{Z}$. Also, the negative of any integer is an integer: for all $k \in \mathbb{Z}$, we have $-k \in \mathbb{Z}$.

Our first result is a generalization of the well-known fact that the sum of two even numbers is even.

Proposition 6.1.1. *Suppose $a, b_1, b_2 \in \mathbb{Z}$. If $a \mid b_1$ and $a \mid b_2$, then $a \mid (b_1 + b_2)$.*

Proof. Assume $a \mid b_1$, and $a \mid b_2$. By definition, it follows that there exists $k_1, k_2 \in \mathbb{Z}$ such that $ak_1 = b_1$ and $ak_2 = b_2$. Let $k = k_1 + k_2$, then $k \in \mathbb{Z}$, and we have $ak = a(k_1 + k_2) = ak_1 + ak_2 = b_1 + b_2$. Therefore, we have $a \mid (b_1 + b_2)$ as desired. □

Proposition 6.1.2. *Suppose $a, b \in \mathbb{Z}$. We have $a \mid b$ if and only if $a \mid -b$.*

Proof.

($\Rightarrow$) By assumption, there is some $k \in \mathbb{Z}$, such that $ak = b$. Then $-k \in \mathbb{Z}$, and we have $a(-k) = -ak = -b$, Therefore, a divides $-b$.

($\Leftarrow$) Assume $a \mid -b$. From the preceding paragraph, we conclude that $a \mid -(-b) = b$, as desired. □

Proposition 6.1.3. *Suppose $a, b_1, b_2 \in \mathbb{Z}$, if $a \mid b_1$, and $a \mid b_2$ then $a \mid (b_1 - b_2)$.*

Proof. Assume $a \mid b_1$ and $a \mid b_2$ then there exist $k_1, k_2 \in \mathbb{Z}$ such that $k = k_1 + k_2$ because $-k \in \mathbb{Z}$ and $) \; - \; k \; = \; k_1 \; - \; k_2$, and we have $-ak = a(k_1 - k_2) = ak_1 - ak_2 = b_1 - b_2$. Therefore, we have $a \mid (b_1 - b_2)$ as desired. □

Proposition 6.1.4. *Suppose $a, b_1, b_2 \in \mathbb{Z}$. If $a \mid b_1$ and $a \nmid b_2$, then $a \nmid (b_1 + b_2)$.*

Proof. Assume $a \mid b_1$ and $a \nmid b_2$.

Suppose $a \mid (b_1 + b_2)$. (This will lead to a contradiction.) Then a is a divisor of both $b_1 + b_2$ and (by assumption) b_1. So Proposition 6.1.4 tells us

$$a \mid \big((b_1 + b_2) - b_1\big) = b_2.$$

This contradicts the assumption that $a \nmid b_2$.

Because it leads to a contradiction, our hypothesis that $a \mid (b_1 + b_2)$ must be false. This means $a \nmid (b_1 + b_2)$. □

Congruence modulo n

Definition 6.1.3 (Congruence)**.** *Suppose $a, b, n \in \mathbb{Z}$. We say a is* ***congruent to*** *b* ***modulo*** *n if and only if $a - b$ is divisible by n. The notation for this is: $a \equiv b \pmod{n}$.*

Examples

1. We have $22 \equiv 0 \pmod 2$, because $22 - 0 = 22 = 11 \times 2$ is a multiple of 2. (More generally, for $a \in \mathbb{Z}$, one can show that $a \equiv 0 \pmod 2$ if and only if a is even.)
2. We have $15 \equiv 1 \pmod 2$, because $15-1 = 14 = 7\times 2$ is a multiple of 2. (More generally, for $a \in \mathbb{Z}$, one can show that $a \equiv 1 \pmod 2$ if and only if a is odd.)
3. We have $28 \equiv 13 \pmod 5$, because $28 - 13 = 15 = 3 \times 5$ is a multiple of 5.
4. For any $a, n \in \mathbb{Z}$, it is not difficult to see that $a \equiv 0$

$(\mod n)$ if and only if a is a multiple of n.

Theorem 6.1.1 (Division Algorithm). *Suppose $a, n \in \mathbb{Z}$, and $n \neq 0$. Then there exist unique integers q and r in $\mathbb{Z}$, such that:*

1. $a = qn + r$, *and*
2. $0 \leq r < |n|$.

Definition 6.1.4. *In the situation of 6.1.1, the number r is called the* **remainder** *when a is divided by n.*

Proposition 6.1.5. *Suppose $a, b \in \mathbb{Z}, n \in \mathbb{Z}^+$,*

1. *Let r be the remained when $a \mid n$, then $a \equiv r \pmod n$.*
2. *$a \equiv b \pmod n$ if and only if a and b have the same remainder when divided by n.*

It follows from 6.1.1 and 6.1.5 that every $\mathbb{Z}$, is congruent to either 0 or 1 module 2 exclusively that is

Even and Odd

n is even if and only if $n \equiv 0 \pmod 2$.

n is odd if and only if $n \equiv 1 \pmod 2$.

More generally we can say if $n \in \mathbb{N}^+$ then we have $\forall x \in \mathbb{Z}, \exists r \in \{0, 1, 2, 3, \ldots, n-1\}$ such that $a \equiv r \pmod n$

Theorem 6.1.2 (Properties of modulo arithmetic)**.** *Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $n \in \mathbb{N}^+$, with $a_1 \equiv b_1 \pmod n$ and $a_2 \equiv b_2 \pmod n$. We have the following*

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod n$
2. $a_1 - a_2 \equiv b_1 - b_2 \pmod n$
3. $a_1 \times a_2 \equiv b_1 \times b_2 \pmod n$

Proof. Exercise □

Proposition 6.1.6. *Let $n \in \mathbb{Z}$. Then $n^2 + n$ is even.*

Proof. From 6.1, we know that n is congruent to either 0 or 1 modulo 2. We consider these two possibilities as separate cases.

1. Assume $n \equiv 0 \pmod 2$. By the assumption of this case, we have $n = 2q$, for some $q \in \mathbb{Z}$. Therefore

$$n^2 + n = (2q)^2 + 2q = 4q^2 + 2q = 2(2q^2 + q)$$

is divisible by 2.

2. Assume $n \equiv 1 \pmod 2$. By the assumption of this case, we have $n = 2q + 1$, for some $q \in \mathbb{Z}$. Therefore

$$\begin{aligned} & n^2 + n \\ &= (2q+1)^2 + (2q+1) \\ &= (4q^2 + 4q + 1) + (2q + 1) \\ &= 4q^2 + 6q + 2 \\ &= 2(2q^2 + 3q + 1) \end{aligned}$$

is divisible by 2.

□

Let $n \in \mathbb{Z}$.

1. Show that if n is even, then $n^2 \equiv 0 \pmod 4$. *hint:* We have $n = 2q$, for some $q \in \mathbb{Z}$.
2. Show that if n is odd, then $n^2 \equiv 1 \pmod 8$. *hint:* We have $n = 2q + 1$, for some $q \in \mathbb{Z}$.
3. Show that if n^2 is even, then n is even.

Irrational Numbers

Recall: $\mathbb{Q} = \{\frac{p}{q} | \text{where } p \in \mathbb{Z}, q \in \mathbb{Z} \wedge q \neq 0\}$

Note that every rational number is a real number $\mathbb{Q} \subseteq \mathbb{R}$. However, it is not so clear that not all $\mathbb{Q}$ are rational. That is $\mathbb{R} \nsubseteq \mathbb{Q}$

Proposition 6.1.7. *$\sqrt{2}$ is irrational.*

Proof by contradiction. Suppose $\sqrt{2}$ is rational. (This will lead to a contradiction.) By definition, this means $\sqrt{2} = a/b$ for some $a, b \in \mathbb{Z}$, with $b \neq 0$. By reducing to lowest terms, we may assume that a and b have no common factors. In particular,

it is not the case that both a and b are even.

We have

$$\frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 = \sqrt{2}^2 = 2,$$

so $a^2 = 2b^2$ is even. Then 3 from the previous subsection tells us that

a is even,

so we have $a = 2k$, for some $k \in \mathbb{Z}$. Then

$$2b^2 = a^2 = (2k)^2 = 4k^2,$$

so $b^2 = 2k^2$ is even. Then 3 from the previous subsection tells us that

b is even.

We have now shown that a and b are even, but this contradicts the fact, mentioned above, that it is not the case that both a and b are even. □

Part 3

Other Fundamental Concepts

Chapter 7: Functions

7.1 Cartesian product

Notation: For any objects x and y, mathematicians use (x, y) to denote the **ordered pair** whose first coordinate is x and whose second coordinate is y. It is important to know that the order matters: (x, y) is usually not the same as (y, x). (That is why these are called *ordered* pairs. Notice that sets are not like this: sets are unordered, so $\{x, y\}$ *is* always the same as $\{y, x\}$.) It is important to realize that:

ordered pair

$$(x_1, y_1) = (x_2, y_2) \quad \Leftrightarrow \quad x_1 = x_2 \text{ and } y_1 = y_2$$

Definition 7.1.1 (Cartesian Product)**.** *For any sets A and B, we let*

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

This notation means, for all x, that

$$x \in A \times B \text{ if and only if } \exists a \in A, \exists b \in B,\ x = (a, b).$$

The set $A \times B$ is called the ***Cartesian product*** *of A and B.*

Examples

1. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.
2. $\{1, 2, 3\} \times \{\mathsf{a}, \mathsf{b}\} = \big\{(1, \mathsf{a}), (1, \mathsf{b}), (2, \mathsf{a}), (2, \mathsf{b}), (3, \mathsf{a}), (3, \mathsf{b})\big\}$.
3. $\{\mathsf{a}, \mathsf{b}\} \times \{1, 2, 3\} = \big\{(\mathsf{a}, 1), (\mathsf{a}, 2), (\mathsf{a}, 3), (\mathsf{b}, 1), (\mathsf{b}, 2), (\mathsf{b}, 3)\big\}$.

By comparing 2 and 3, we see that $\times$ is *not* commutative: $A \times B$ is usually *not* equal to $B \times A$.

Note

Cardinality of Cardinality Product We will prove in later that

$$\#(A \times B) = \#A \cdot \#B.$$

Informal proof. Suppose $\#A = m$ and $\#B = n$. Then, by listing the elements of these sets, we may write

$$A = \{a_1, a_2, a_3, \ldots, a_m\} \quad \text{and} \quad B = \{b_1, b_2, b_3, \ldots, b_n\}.$$

The elements of $A \times B$ are:

$$\begin{array}{ccccc} (a_1, b_1), & (a_1, b_2), & (a_1, b_3), & \cdots & (a_1, b_n), \\ (a_2, b_1), & (a_2, b_2), & (a_2, b_3), & \cdots & (a_2, b_n), \\ (a_3, b_1), & (a_3, b_2), & (a_3, b_3), & \cdots & (a_3, b_n), \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (a_m, b_1), & (a_m, b_2), & (a_m, b_3), & \cdots & (a_m, b_n). \end{array}$$

In this array,

- each row has exactly n elements, and
- there are m rows,

so the number of elements is the product $mn = \#A \cdot \#B$. □

Question(s)

1. If A and B are non empty sets, and $A \times B = B \times A$, then we have $A = B$.
2. If B is disjoint from C, then $A \times B$ is disjoint from $A \times C$.
3. Assume A, B, and C are sets. Prove $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Answer(s)

1. *Proof.* We assume A and B are non-empty sets and $A \times B = B \times A$. We need to show that $A \subseteq B$ and $B \subseteq A$, however, due to symmetry we only need to show that $A \subseteq B$.

   Let $a_0 \in A_0$. Since $B \neq \emptyset$, there exists some $b_0 \in B$ and we have $(a_0, b_0) \in A \times B = B \times A = \{(b, a); b \in B, a \in A\}$. Hence there exist some $b \in B$ and $a \in A$ with $(a_0, b_0) = (a_1, b_1)$, and therefore $a_0 = b \in B$. □
2. *Proof.* We prove the contrapositive: Assume $A \times B$ is *not* disjoint from $A \times C$, and we will show B is *not* disjoint from C.

   By assumption, the intersection of $A \times B$ and $A \times C$ is not empty, so we may choose some

   $$x \in (A \times B) \cap (A \times C).$$

   Then:

   - Since $x \in A \times B$, there exist $a_1 \in A$ and $b \in B$, such that $x = (a_1, b)$.
   - Since $x \in A \times C$, there exist $a_2 \in A$ and $c \in C$, such that $x = (a_2, c)$.

   Hence $(a_1, b) = x = (a_2, c)$, so $b = c$. Now $b \in B$ and $b = c \in C$, so $b \in B \cap C$. Therefore $B \cap C \neq \emptyset$, so, as desired, B and C are *not* disjoint. □
3. *Proof.* ($\supset$) Given $x \in (A \times B) \cup (A \times C)$, we have $x \in A \times B$ or $x \in A \times C$. By symmetry, we may assume $x \in A \times B$, so $x = (a, b)$ for some $a \in A$ and $b \in B$. Note that $b \in B \cup C$, so we have $a \in A$ and $b \in B \cup C$. Therefore

   $$x = (a, b) \in A \times (B \cup C).$$

   Since x is an arbitrary element of $(A \times B) \cup (A \times C)$, this implies $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$.

   ($\subset$) Given $(a, x) \in A \times (B \cup C)$, we have $a \in A$, and either $x \in B$ or $x \in C$. By symmetry, we may assume $x \in B$. Then $(a, x) \in A \times B \subset (A \times B) \cup (A \times C)$, so $(a, x) \in (A \times B) \cup (A \times C)$. Since (a, x) is an arbitrary element of $A \times (B \cup C)$, this implies $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$. □

7.2 Informal Introduction to Functions

Ever since junior high you have seen functions in the form of a formula i.e., $f(x) = x^2$. However there are other ways to define a function. The key property of a function is that it accepts inputs, and provides a corresponding output value for each possible input.

Definition 7.2.1 (Informal Def of a Functions)**.** *Suppose f is any function.*

1. *The set of allowable inputs of f is called the* ***domain*** *of f.*
2. *If A is the domain of f, and B is any set that contains all of the possible outputs of f, then we say that f is a* ***function from*** *A* ***to*** *B. In the case of the function $f(x) = x^3$, we may take A and B to both be the set of real numbers; thus, f is a function from to .*

Ways to describe a function

There are many ways to describe a function

1. A table

item	price in cents
apple	65
banana	83
cherry	7
⋮	⋮

2. A set of ordered pairs: The price function would be represented as : $\{(Apple, 65), (Banana, 83), (Cherry, 7), \dots\}$

3. An arrow diagram: we can also do this $f : A \to B$
   - A dot is drawn for each element in set A and B
   - An arrow is drawn from a to f(a), for each $a \in A$.

7.3 Official Functions

Definition 7.3.1 (Function)**.** *Suppose A and B are sets.*

1. *A set f is a* ***function from*** *A* ***to*** *B if and only if*
   (a) *each element of f is an ordered pair (a, b), such that $a \in A$ and $b \in B$, and*
   (b) *for each $a \in A$, there is a* unique *$b \in B$, such that $(a, b) \in f$.*
2. *If f is a function from A to B, then*
   - *A is called the* ***domain*** *of f, and*
   - *B is a* ***codomain*** *of f.*
3. *We write "$f : A \to B$"to denote that f is a function from A to B.*

Note

we write $f(a) = b$ if and only if $(A, b) \in f$.

Definition 7.3.2 (Range)**.** *Let $f : A \to B$, then the range of f is the set $\{f(a); a \in A\}$.*

7.4 One-to-One Functions

Definition 7.4.1 (One-to-One function)**.** *Suppose $f : A \to B$ we say $f : A \to B$ is* ***one-to-one*** *or (injective) if and only if $\forall a_1, a_2 \in A; f(a_1) = f(a_2) \Rightarrow a_1 = a_2$*

Example

Let $F : \mathbb{R} \to \mathbb{R}$, be defined as $f(x)x^2$. Then f is not one-to-one, since $f(2) = 2^2 = 4 = (-2^2) = f(-2)$ but $2 \neq -2$.

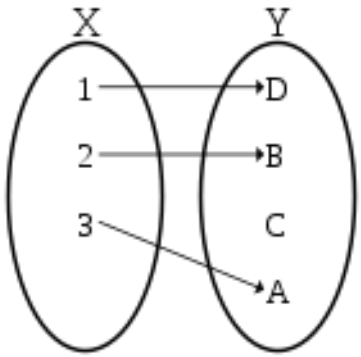

Figure 7.1: one-to-one functions

Example

Prove that $f(x) = x + 1$ is one-to-one

Proof. let $x_1, x_2 \in \mathbb{R}$ such that $f(x_1) = f(x_2)$. Then we have $x_1 + 1 = x_2 + 1$ hence $x_1 = x_2$ as desired. □

Theorem 7.4.1. *If a function $f : A \to B$ is one-to-one, then*

$$\forall a_1, a_2 \in A, \big(a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)\big).$$

Proof. Let $f : A \to B$ be one-to-one. Given $a_1, a_2 \in A$, we know, from the definition of one-to-one, that

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

So the contrapositive of this implication is also true. That is,

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2).$$

□

7.5 Onto Functions

Definition 7.5.1 (Onto Function)**.** *Suppose $f\colon A \to B$. We say f is **onto** if and only if, for all $b \in B$, there is some $a \in A$, such that $f(a) = b$.*

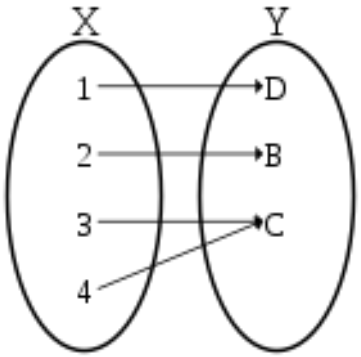

Figure 7.2: Onto

Example

$f : \mathbb{R} \to \mathbb{R}$ be $f(x) = |x|$ prove that its not onto.

Proof. Note that $-1 \in \mathbb{R}$. Then $f(x) = |-1| = 1 \geq 0 > -1$, so there does not exist $x \in \mathbb{R}$ for which $f(x) = -1$ hence f is not onto. □

7.6 Bijection

Definition 7.6.1 (Bijection)**.** *We say a function has a bijection if and only if the function is one-to-one* **and** *onto.*

Moreover, if the function $f : A \to B$ then the two sets A and B must have exactly the same number of elements.

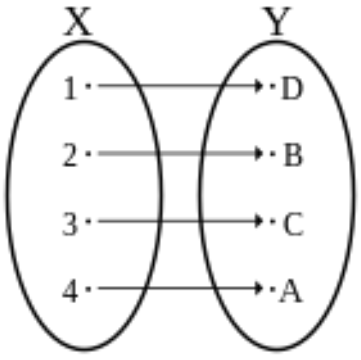

Figure 7.3: Bijection

Note

Let $f : A \to B$ we have the following

1. If f is one-to-one, then each element of A gets mapped to a unique element of B. Therefore, $\#A \leq \#B$.
2. If f is onto, then all elements of B is mapped to at least one element from A. Therefore, $\#A \geq \#B$.

In general to prove a function $f : A \to B$ that is

1. one-to-one, we let $a_1, a_2 \in A$ for which $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.
2. Not one-to-one, we provide a counterexample
3. onto, we prove that $\forall b \in B, \exists a \in A$ such that $f(a) = b$.
4. not onto, we provide a counterexample where given a element from B there does not exist an element from A such that $f(a) = b$.

Definition 7.6.2 (Identity map)**.** *or any set A, define the **identity map** $I_A\colon A \to A$ by $I_A(a) = a$ for every $a \in A$.*

Example

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 7x - 3$. Prove f is a bijection.

Proof.

(one-to-one) Set $x_1, x_2 \in \mathbb{R}$ and assume that $f(x_1) = f(x_2)$ then we have , $7x_1 - 3 = 7x_2 - 3 \Rightarrow 7x_1 = 7x_2 \Rightarrow x_1 = x_2$, therefore f is one-to-one.

(onto) Given $y \in \mathbb{R}$, let $x = \frac{y+3}{7} \in \mathbb{R}$. Then we have

$$\begin{aligned} f(x) &= 7x - 3 \\ &= 7\left(\frac{y+3}{7}\right) - 3 \\ &= y + 3 - 3 \\ &= y \end{aligned}$$

Since y was arbitrary we conclude that f is onto

Since f is both one-to-one and onto we conclude that f is bijective by definition. □

7.7 Inverse Function

Definition 7.7.1 (Inverse Function)**.** *Suppose*

- *$f\colon A \to B$, and*
- *$g\colon B \to A$.*

We say that g is the **inverse** *of f if and only if:*

1. *$g\big(f(a)\big) = a$ for all $a \in A$, and*
2. *$f\big(g(b)\big) = b$ for all $b \in B$.*

The inverse of the function f is denoted by f^{-1}

$$f^{-1}(x) = \frac{1}{f(x)}$$

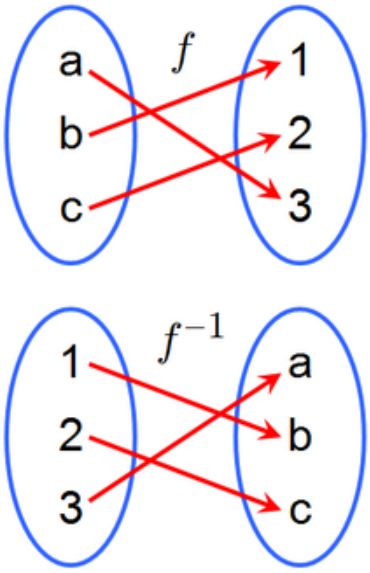

Figure 7.4: Inverse

Example

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 7x - 4$, and let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = \frac{x+4}{7}$. Prove that g is the inverse of f.

Proof. it suffice to show two things

1. $g(f(x)) = x \quad \forall x \in \mathbb{R}$
2. $f(g(y)) = y \quad \forall y \in \mathbb{R}$

1. Let $x \in \mathbb{R}$. Then we have $g(f(x)) = \frac{f(x)+4}{7} = \frac{(7x-4)+4}{7}$
2. Let $y \in \mathbb{R}$. Then we have $f(g(y)) = 7g(y) - 4 = 7\left(\frac{y+4}{7}\right) - 4 = y + 4 - 4 = y$

□

Theorem 7.7.1. *Suppose $f : A \to B$. If f has an inverse $f^{-1} : B \to A$, then f is a bijection.*

7.8 Composition of a Function

Definition 7.8.1 (Composition of a Function)**.** *Suppose that $f : A \to B$ and $g : B \to C$ the composition of g and f is the function gof. $gof : A \to C$, defined by $gof(x) = g(f(a))$*

Define $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ by $f(x) = 3x$ and $g(x) = x^2$. Then $g \circ f$ and $f \circ g$ are functions from $\mathbb{R}$ to $\mathbb{R}$. For all $x \in \mathbb{R}$, we have

$$(g \circ f)(x) = g\big(f(x)\big) = g(3x) = (3x)^2 = 9x^2$$

and

$$(f \circ g)(x) = f\big(g(x)\big) = f(x^2) = 3(x^2) = 3x^2.$$

Notice that (in this example) $f \circ g \neq g \circ f$, so *composition is **not** commutative.*

Proposition 7.8.1. *Let $f : A \to B$ and let $f^{-1} : B \to A$ be the inverse of f. Then, we have*

1. $f^{-1} \circ f = I_A$
2. $f \circ f^{-1} = I_B$

Example

Suppose $f : A \to B$ and $g : B \to C$. Show that if f and $g \circ f$ are bijections, then g is a bijection.

Proof. It suffices to show that g is both one-to-one and onto.

(one-to-one) Let b_1 and b_2 be arbitrary elements of B, such that $g(b_1) = g(b_2)$. Since f is a bijection, it is onto, so there exist $a_1, a_2 \in A$, such that $f(a_1) = b_1$ and $f(a_2) = b_2$. Then

$$(g \circ f)(a_1) = g\big(f(a_1)\big) = g(b_1) = g(b_2) = g\big(f(a_2)\big) = (g \circ f)(a_2).$$

Since $g \circ f$ is a bijection, it is one-to-one, so we conclude that $a_1 = a_2$. Therefore

$$b_1 = f(a_1) = f(a_2) = b_2.$$

Since b_1 and b_2 are arbitrary elements of B, such that $g(b_1) = g(b_2)$, this implies that g is one-to-one.

(onto) Let c be an arbitrary element of C. Since $g \circ f$ is a bijection, it is onto, so there exists $a \in A$, such that $(g \circ f)(a) = c$. Let $b = f(a)$. Then

$$g(b) = g\big(f(a)\big) = (g \circ f)(a) = c.$$

Since c is an arbitrary element of C, we conclude that g is onto. □

7.9 Image and Preimage

Definition 7.9.1 (Image)**.** *Suppose $f : A \to B$, and $A_1 \subset A$. The **image** of A_1 under f is*

$$f(A_1) = \{f(a);\ a \in A_!\} \subseteq B$$

It is a subset of B. The notation means that, for all x, we have

$$x \in f(A_1) \quad \Leftrightarrow \quad \exists a \in A_1, \big(x = f(a)\big).$$

Example

Assume $f : A \to B$. Show that if A_1 and A_2 are subsets of A, and f is one-to-one, then $f(A_1) \cap f(A_2) \subset f(A_1 \cap A_2)$.

Proof. Given $b \in f(A_1) \cap f(A_2)$, we know $b \in f(A_1)$ and $b \in f(A_2)$. Therefore, since $b \in f(A_1)$, we know there is some $a_1 \in A_1$, such that $b = f(a_1)$. Also, since $b \in f(A_2)$, we know there is some $a_2 \in A_2$, such that $b = f(a_2)$. Then

$$f(a_1) = b = f(a_2).$$

Since f is one-to-one, this implies $a_1 = a_2 \in A_2$. Since we also know that $a_1 \in A_1$, this implies $a_1 \in A_1 \cap A_2$. So $f(a_1) \in f(A_1 \cap A_2)$. Since $b = f(a_1)$, this means $b \in f(A_1 \cap A_2)$. Since b is an arbitrary element of $f(A_1) \cap f(A_2)$, we conclude that $f(A_1) \cap f(A_2) \subset f(A_1 \cap A_2)$. □

Definition 7.9.2 (Preimage)**.** *Suppose $f\colon A \to B$, and $B_1 \subset B$. The **pre-image** (or **inverse image**) of B_1 under f is*

$$f^{-1}(B_1) = \{\forall a \in A; f(a) \in B_1\} \subseteq A.$$

It is a subset of A. When $B_1 = \{b\}$ has only one element, we usually write $f^{-1}(b)$, instead of $f^{-1}\big(\{b\}\big)$.

Example

Suppose $f\colon A \to B$ and $B_1 \subset B$.

1. We have $f\big(f^{-1}(B_1)\big) \subset B_1$.
2. If f is onto, then $f\big(f^{-1}(B_1)\big) = B_1$.

Proof. 1 Let $b \in f\big(f^{-1}(B_1)\big)$. By definition, we have

$$f\big(f^{-1}(B_1)\big) = \{f(a); a \in f^{-1}(B_1)\},$$

so we must have $b = f(a_1)$, for some $a_1 \in f^{-1}(B_1)$. From the definition of $f^{-1}(B_1)$, we know that $f(a_1) \in B_1$. Therefore $b = f(a_1) \in B_1$. Since b is an arbitrary element of $f\big(f^{-1}(B_1)\big)$, this implies that $f\big(f^{-1}(B_1)\big) \subset B_1$, as desired.

2 Assume f is onto. We know, from 1, that $f\big(f^{-1}(B_1)\big) \subset B_1$, so it suffices to show that $B_1 \subset f\big(f^{-1}(B_1)\big)$.

Let $b \in B_1$ be arbitrary. Because f is onto, we know there exists $a_1 \in A$, such that $f(a_1) = b$. Then $f(a_1) = b \in B_1$, so $a_1 \in f^{-1}(B_1)$. Therefore

$$f(a_1) \in \{f(a); a \in f^{-1}(B_1)\} = f\big(f^{-1}(B_1)\big).$$

Since $f(a_1) = b$, we conclude that $b \in f\big(f^{-1}(B_1)\big)$. Since b is an arbitrary element of B_1, this implies that $B_1 \subset f\big(f^{-1}(B_1)\big)$, as desired. □

Chapter 8: Equivalence Relations

8.1 Binary relations

Definition 8.1.1 (Binary relations)**.** *Suppose A and B are sets*

1. *Any subset of $A \times B$ is called a* ***relations from A to B***
2. *For the special case where $A = B$, any subset of $A \times A$ is called a* ***binary relations*** *on A.*

Notation: Let R be any notation.

1. if $(x, y) \in R$ we write xRy
2. if $x, y) \in R$ we write $x \not R\ y$

There are other relations like $>$ and $<$.

Definition 8.1.2. *Suppose R is a binary relation on a set A.*

1. *We say that R is* ***reflexive*** *if and only if $\forall a \in A, (aRa)$.*
2. *We say that R is* ***symmetric*** *if and only if $\forall a, b \in A, \big((aRb) \implies (bRa)\big)$.*
3. *We say that R is* ***transitive*** *if and only if $\forall a, b, c \in A, \Big(\big((aRb)\ \&\ (bRc)\big) \implies (aRc)\Big)$.*

Definition 8.1.3 (digraph)**.** *We can draw a picture to represent any given binary relation on any given set A:*

- *Draw a dot for each element of A.*
- *For $a, b \in A$, draw an arrow from a to b if and only if (a, b) is an element of the relation.*

The resulting picture is called a ***digraph****.*

Example

Consider the relation $R = \{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3),(3,2)\}$ we can represent this relation by drawing a digraph

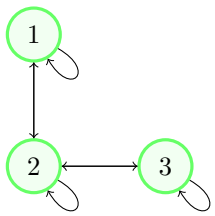

Figure 8.1: Digraph of the relation above

This relation is:

1. reflexive since $1R1$,$2R2$,$3R3$
2. symmetric since $\forall_{(a,b)} \in R$ we have $(b, a) \in R$, $\forall a, b \in \{1, 2, 3\}\ (aRb) \implies (bRa)$
3. not transitive, since 1R2, 2R3, but 1 is not related to 3

8.2 Definition and basic properties of equivalence relations

Definition 8.2.1 (equivalence relation)**.** *An* ***equivalence relation*** *on a set A is a binary relation on A that is reflexive, symmetric, and transitive.*

Instead of representing an equivalence relation by a letter, it is traditional to use the symbol $\sim$(or sometimes $\equiv$or $\cong$).

Question(s)

1. Define a binary relation $\sim$ on $\mathbb{R}$ by $x \sim y$ if and only if $x^2 = y^2$. Then $\sim$ is an equivalence relation.
2. Define a binary relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by $(a_1, b_1) \sim (a_2, b_2)$ if and only if $a_1 + b_2 = a_2 + b_1$. Then $\sim$ is an equivalence relation.

Answer(s)

1. *Proof.* We wish to show that $\sim$ is reflexive, symmetric, and transitive.
   (reflexive) Given $x \in \mathbb{R}$, we have $x^2 = x^2$, so $x \sim x$.
   (symmetric) Given $x, y \in \mathbb{R}$, such that $x \sim y$, we have $x^2 = y^2$. Since equality is symmetric, this implies $y^2 = x^2$, so $y \sim x$.
   (transitive) Given $x, y, z \in \mathbb{R}$, such that $x \sim y$ and $y \sim z$, we have $x^2 = y^2$ and $y^2 = z^2$. Therefore $x^2 = y^2 = z^2$, so $x^2 = z^2$. Hence $x \sim z$. □
2. *Proof.* We wish to show that $\sim$ is reflexive, symmetric, and transitive.
   (reflexive) Given $(a, b) \in \natural \times \natural$, we have $a + b = a + b$, so $(a, b) \sim (a, b)$.
   (symmetric) Given $(a_1, b_1), (a_2, b_2) \in \natural \times \natural$, such that $(a_1, b_1) \sim (a_2, b_2)$, the definition of $\sim$ tells us that $a_1 + b_2 = a_2 + b_1$. Since equality is symmetric, this implies $a_2 + b_1 = a_1 + b_2$, so $(a_2, b_2) \sim (a_1, b_1)$.
   (transitive) Given $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \natural \times \natural$, such that

   $$(a_1, b_1) \sim (a_2, b_2) \quad \text{and} \quad (a_2, b_2) \sim (a_3, b_3),$$

   we have

   $$a_1 + b_2 = a_2 + b_1 \text{ and } a_2 + b_3 = a_3 + b_2. \qquad (8.1)$$

   Therefore

   $$\begin{aligned} &(a_1 + b_3) + (a_2 + b_2) \\ &= (a_1 + b_2) + (a_2 + b_3) && \text{(rearrange terms)} \\ &= (a_2 + b_1) + (a_3 + b_2) && 8.1 \\ &= (a_3 + b_1) + (a_2 + b_2) && \text{(rearrange terms)} \end{aligned}$$

   Subtracting $a_2 + b_2$ from both sides of the equation, we conclude that $a_1 + b_3 = a_3 + b_1$, so $(a_1, b_1) \sim (a_3, b_3)$. □

8.3 Equivalence classes

Definition 8.3.1 (Equivalence classes). *Suppose $\sim$ is an equivalence relation on a set A. For each $a \in A$, the* ***equivalence class*** *of a is the following subset of A:*

$$[a] = \{\, a' \in A \mid a' \sim a \,\}.$$

Example

Suppose $A = \{1, 2, 3, 4, 5\}$ and

$$R = \left\{ \begin{matrix} (1,1), (1,3), (1,4), (2,2), (2,5), (3,1), (3,3), \\ (3,4), (4,1), (4,3), (4,4), (5,2), (5,5) \end{matrix} \right\}.$$

One can verify that R is an equivalence relation on A. The equivalence classes are:

$$[1] = \{1, 3, 4\}, \qquad [2] = \{2, 5\}, \qquad [3] = \{1, 3, 4\}$$

$$[4] = \{1, 3, 4\}, \qquad [5] = \{2, 5\}.$$

Theorem 8.3.1 (Equivalence relations properties). *Suppose $\sim$ is an equivalence relation on a set A. Then:*

1. *For all $a \in A$, we have $a \in [a]$.*
2. *For all $a \in A$, we have $[a] \neq \emptyset$.*
3. *The union of the equivalence classes is all of A. That is, we have $A = \bigcup_{a \in A} [a]$, where*

$$\bigcup_{a \in A} [a] = \{x \mid \exists a \in A, \big(x \in [a]\big)\}.$$

4. *For any $a_1, a_2 \in A$, such that $a_1 \sim a_2$, we have $[a_1] = [a_2]$.*
5. *For any $a_1, a_2 \in A$, such that $a_1 \not\sim a_2$, we have $[a_1] \cap [a_2] = \emptyset$.*

Proof. Left as an exercise □

Note

That if $\sim$ is a equivalence relation on a set A, and $a_1, a_2 \in A$ for which $a_1 \sim a_2$, it is tempting to think of a_1 and a_2 as being equal but this is not technically correct. However, we have that $a_1 \sim a_2$ if and only if $[a_1] = [a_2]$

8.4 Modular arithmetic

The integers modulo 3

Recall that if $n \in \mathbb{N}^+$, then congruence modulo n is an equivalence relation. We will work with $n = 3$.

Note

That when $\mathbb{Z}, k$ is divided by 3. The remainder is either 0,1,2. Hence $[k]_3$ is either $[0]_3, [1]_3, [2]_3$.

Thus the congruence modulo 3 gives 3 distinct equivalence classes. The set $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ is called the integers modulo 3. Rather than writing $[k]_3$ it si often more convenient to write k like this $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.

We can do arithmetic (add, subtract, and multiply) on these equivalence classes, just as we do for ordinary integers. This is called **arithmetic modulo** 3. The rules are:

- $[a]_3 + [b]_3 = [a + b]_3$ (or $\overline{a} + \overline{b} = \overline{a + b}$),
- $[a]_3 - [b]_3 = [a - b]_3$ (or $\overline{a} - \overline{b} = \overline{a - b}$), and
- $[a]_3 \times [b]_3 = [ab]_3$ (or $\overline{a} \times \overline{b} = \overline{ab}$).

(Actually, we should write $+_3$, $-_3$, and $\times_3$, to indicate that the arithmetic is being done modulo 3, but we will usually not bother.)

Example

We have $[1]_3 + [2]_3 = [1 + 2]_3 = [3]_3$. However, since $3 \equiv 0 \pmod 3$, we have $[3]_3 = [0]_3$, so the above equation can also be written as $[1]_3 + [2]_3 = [0]_3$. Equivalently, $\overline{1} + \overline{2} = \overline{0}$.

This is an example of the following general principle:

The result of any arithmetic operation (modulo 3) will be either $[0]_3$, $[1]_3$, or $[2]_3$:

If r is the remainder when $a + b$ is divided by 3,

then $\overline{a} +_3 \overline{b} = \overline{r}$.

Here is a table that shows the results of addition modulo 3:

$+_3$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Definition 8.4.1. *Fix some nonzero natural number $n \in \mathbb{N}^+$.*

1. *For any integer k, we use $[k]_n$ to denote the equivalence class of k under congruence modulo n. When n is clear from the context, we may write $\overline{k}$, instead of $[k]_n$.*
2. *The set of these equivalence classes is called the* ***integers modulo*** *n. It is denoted $\mathbb{Z}_n$.*
3. *Addition, subtraction, and multiplication modulo n are defined by:*
   - $\overline{a} +_n \overline{b} = \overline{a+b}$,
   - $\overline{a} -_n \overline{b} = \overline{a-b}$, *and*
   - $\overline{a} \times_n \overline{b} = \overline{ab}$.

   (When n is clear from the context, we usually write $+$, $-$, and $\times$, rather than $+_n$, $-_n$, and $\times_n$.)

Proposition 8.4.1. *For any $n \in \mathbb{N}^+$, we have*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

and $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ are all distinct.

Question(s)

1. Simplify $(\overline{17} - \overline{5}) \times (\overline{21} + \overline{11})$ in $\mathbb{Z}_7$.

Answer(s)

1. We have

$$\begin{aligned}(\overline{17} - \overline{5}) \times (\overline{21} + \overline{11}) &= (\overline{3} - \overline{5}) \times (\overline{0} + \overline{4}) \\ &= (\overline{3-5}) \times (\overline{0+4}) \\ &= \overline{-2} \times \overline{4} = \overline{5} \times \overline{4} \\ &= \overline{5 \times 4} = \overline{20} = \overline{6}.\end{aligned}$$

Chapter 9: Proof by Induction

9.1 The Principle of Mathematical Induction

Proposition 9.1.1 (Principle of Mathematical Induction)**.** *Suppose $P(n)$ is a predicate of natural numbers. If*

(i) *$P(1)$ is true, and*

(ii) *for every $k \geq 2$, $\big(P(k-1) \implies P(k)\big)$,*

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

pretty much like recursion but upward instead of downwards

Definition 9.1.1 (Terminology)**.**

- *In a proof using Mathematical Induction, establishing (i) is called the* ***base case****, and establishing (ii) is the* ***induction step****.*
- *In the induction step, we are proving $P(k-1) \implies P(k)$, so we assume that $P(k-1)$ is true (and establish $P(k)$). This assumption $P(k-1)$ is called the* ***induction hypothesis****.*

Proposition 9.1.2 (Sum of Natural Numbers)**.** *For every $n \in \mathbb{N}^+$, we have* $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$.

Proof by induction. Define $P(n)$ to be the assertion

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}.$$

(i) *Base case.* For $n = 1$, we have

$$1+2+3+\cdots+n = 1 \quad \text{and} \quad \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1.$$

Since these are equal, $P(1)$ is true.

(ii) *Induction step.* Assume $P(k-1)$ is true (and $k \geq 2$). This means that

$$1+2+3+\cdots+(k-1) = \frac{(k-1)\big((k-1)+1\big)}{2}.$$

Hence

$$\begin{aligned}
&1+2+3+\cdots+k \\
&\quad = \big(1+2+3+\cdots+(k-1)\big)+k \\
&\quad = \frac{(k-1)\big((k-1)+1\big)}{2}+k \\
&\quad \text{(Induction Hypothesis)} \\
&\quad = \frac{(k-1)k}{2}+k \\
&\quad = k\left(\frac{k-1}{2}+1\right) \\
&\quad = k\left(\frac{k+1}{2}\right) \\
&\quad = \frac{k(k+1)}{2},
\end{aligned}$$

so $P(k)$ is true.

Therefore, by the Principle of Mathematical Induction, we know $P(n)$ is true for all n. This means

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}$$

for every $n \in \mathbb{N}^+$. □

Proposition 9.1.3 $(2n^2+n)$**.** *For every $n \in \mathbb{N}^+$, we have*

$$3+7+11+\cdots+(4n-1) = 2n^2+n.$$

Proof by induction. Define $P(n)$ to be the assertion

$$3+7+11+\cdots+(4n-1) = 2n^2+n.$$

(i) *Base case.* For $n = 1$, we have

$$3+7+11+\cdots+(4n-1) = 3 \quad \text{and} \quad 2n^2+n = 2(1^2)+1 = 3.$$

Since these are equal, $P(1)$ is true.

(ii) *Induction step.* Assume $P(k-1)$ is true (and $k \geq 2$). This means that

$$3+7+11+\cdots+\big(4(k-1)-1\big) = 2(k-1)^2+(k-1).$$

Hence

$$\begin{aligned}
&3+7+11+\cdots+(4k-1) \\
&\quad = \Big(3+7+11+\cdots+\big(4(k-1)-1\big)\Big)+(4k-1) \\
&\quad = \Big(2(k-1)^2+(k-1)\Big)+(4k-1) \\
&\quad \text{(Induction Hypothesis)} \\
&\quad = \Big(2(k^2-2k+1)+(k-1)\Big)+(4k-1) \\
&\quad = (2k^2-4k+2)+(k-1)+(4k-1) \\
&\quad = 2k^2+k,
\end{aligned}$$

so $P(k)$ is true.

Therefore, by the Principle of Mathematical Induction, we know $P(n)$ is true for all n. This means

$$3+7+11+\cdots+(4n-1) = 2n^2+n$$

for every $n \in \mathbb{N}^+$. □

9.2 Other proofs by induction

Example on Mondulo Operations

Suppose $a, b, n \in \mathbb{Z}$, with $a \equiv b \pmod{n}$. Show $a^k \equiv b^k \pmod{n}$, for all $k \in \mathbb{N}^+$.

Proof by induction. We induct on k. Define $P(k)$ to be the assertion

$$a^k \equiv b^k \pmod{n}.$$

(i) *Base case.* Since $a^1 = a$ and $b^1 = b$, the hypothesis $a \equiv b \pmod{n}$ tells us that

$$a^1 \equiv b^1 \pmod{n},$$

so $P(1)$ is true.

(ii) *Induction step.* Assume $P(k-1)$ is true. This means that

$$a^{k-1} \equiv b^{k-1} \pmod{n}.$$

By assumption, we also have

$$a \equiv b \pmod{n}.$$

We can multiply the above congruences, to conclude that

$$(a^{k-1})(a) \equiv (b^{k-1})(b) \pmod{n}.$$

In other words,

$$a^k \equiv b^k \pmod{n},$$

so $P(k)$ is true.

Therefore, by the Principle of Mathematical Induction, $P(k)$ is true for every $k \in \mathbb{N}^+$. □

Definition 9.2.1 (Fibonacci Numbers). *The **Fibonacci numbers** $F_1, F_2, F_3, \ldots$ are defined by:*

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

(For example, $F_3 = F_{3-1} + F_{3-2} = F_2 + F_1 = 1 + 1 = 2$.) In general, each Fibonacci number (after F_2) is the sum of the two preceding Fibonacci numbers, so the first few Fibonacci numbers are:

n	1	2	3	4	5	6	7	$\cdots$
F_n	1	1	2	3	5	8	13	$\cdots$

Example on Fibonacci Numbers

Prove $\sum_{k=1}^{n} F_k = F_{n+2} - 1$ for all $n \in \mathbb{N}^+$.

Proof by induction. Define $P(n)$ to be the assertion

$$\sum_{k=1}^{n} F_k = F_{n+2} - 1.$$

(i) *Base case.* For $n = 1$, we have

$$\sum_{k=1}^{n} F_k = \sum_{k=1}^{1} F_k + = F_1 = 1 = 2 - 1 = F_3 - 1$$
$$= F_{1+2} - 1 = F_{n+2} - 1,$$

so $P(1)$ is true.

(ii) *Induction step.* Assume $P(n-1)$ is true (and $n \geq 2$). Then

$$\begin{aligned}
\sum_{k=1}^{n} F_k &= \left(\sum_{k=1}^{n-1} F_k\right) + F_n \\
&= \Big(F_{(n-1)+2} - 1\Big) + F_n \quad \text{(Induction Hypothesis)} \\
&= (F_{n+1} - 1) + F_n \\
&= (F_{n+1} + F_n) - 1 \\
&= F_{n+2} - 1 \qquad \left(\begin{array}{c}\text{definition of} \\ \text{Fibonacci number}\end{array}\right).
\end{aligned}$$

Therefore, by the Principle of Mathematical Induction, $P(n)$ is true for every n. This means $\sum_{k=1}^{n} F_k = F_{n+2} - 1$ for all $n \in \natural^+$. □

9.3 Other versions of induction

There are other versions of induction that works better in solving other cases.

Proposition 9.3.1. *Suppose $P(n)$ is a predicate of natural numbers, and $m \in \mathbb{N}^+$.*

1. (Strong induction) *If*
   (i) $P(1)$ is true, and
   (ii) for every $n \geq 2$,
   $$\Big(\big(\text{for every } k \in \{1, 2, \ldots, n-1\}, P(k)\big) \implies P(n)\Big),$$
   then $P(n)$ is true for all $n \in \mathbb{N}^+$.
2. (Generalized induction) *If*
   (i) $P(m)$ is true, and
   (ii) for every $n > m$, $\big(P(n-1) \implies P(n)\big)$,
   then $P(n)$ is true for all $n \geq m$.
3. (Strong induction with multiple base cases) *If*
   (i) $P(k)$ is true for all $k \in \{1, 2, \ldots, m\}$, and
   (ii) for every $n > m$,
   $$\Big(\big(\text{for every } k \in \{1, 2, \ldots, n-1\}, P(k)\big) \implies P(n)\Big),$$
   then $P(n)$ is true for all $n \in \mathbb{N}^+$.
4. *If*
   (i) $P(1)$ is true, and
   (ii) for every $k \in \mathbb{N}^+$, $P(k) \Rightarrow P(k+1)$,
   then $P(n)$ is true for all $n \in \mathbb{N}^+$.
5. *Suppose $S \subset \mathbb{N}^+$. If*
   (i) $1 \in S$, and
   (ii) for every $n \in S$, $\big(n+1 \in S\big)$,
   then $S = \mathbb{N}^+$.

Strong induction goes down to the base case

Example

Prove $F_n < 2^n$, for every $n \in \mathbb{N}^+$.

Proof by induction. Define $P(n)$ to be the assertion

$$F_n < 2^n.$$

We use strong induction with 2 base cases.

(i) *Base cases.* We have

$$F_1 = 1 < 2 = 2^1,$$

and

$$F_2 = 1 < 4 = 2^2,$$

so $P(1)$ and $P(2)$ are true.

(ii) *Induction step.* Assume $n \geq 3$, and that $P(n-1)$ and $P(n-2)$ are true. We have

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &< 2^{n-1} + 2^{n-2} \qquad \text{(Induction Hypotheses)} \\ &< 2^{n-1} + 2^{n-1} \\ &= 2^n, \end{aligned}$$

so $P(n)$ is true.

By the Principle of Mathematical Induction (in the form of strong induction with multiple base cases), we conclude that $P(n)$ is true for all $n \in \mathbb{N}^+$. □

9.4 Well-ordered

Definition 9.4.1 (Smallest)**.** *Let $S \subset$ and $a \in$. We say a is the **smallest** element of S if and only if:*

- *$a \in S$, and*
- *$\forall s \in S$, $a \leq s$.*

Theorem 9.4.1 ($\mathbb{N}$ is well-ordered)**.** *Every nonempty subset of $\mathbb{N}$ has a smallest element.*

Note

If $P(n)$ can be proven for all $n \in \mathbb{N}$ using induction, then it can also be proven by applying Theorem 9.4.1 ot the set

$$S = \{\, n \in \mathbb{N}^+ \mid \neg P(n) \,\}.$$

9.5 Application to Number Theory

Definition 9.5.1 (Prime)**.** *An element p of $\mathbb{N}^+$ is **prime** if and only if $p > 1$ and p is not divisible by any element of $\mathbb{N}^+$ other than 1 and p.*

Proposition 9.5.1. *If $n \in \mathbb{N}$ and $n > 1$, then n is divisible by a prime number.*

Proof. Suppose there is some natural number $n > 1$, such that n is not divisible by a prime number. (This will lead to a contradiction.) Since $\mathbb{N}$ is well-ordered, we may assume that n is the smallest such number, so:

If $1 < k < n$ (and $k \in \mathbb{N}$), then k is divisible by a prime number.

Since $n \mid n$, but (by assumption) n is not divisible by any prime number, we know that n is not prime. By definition, this means there exists $k \in \mathbb{N}$, such that $k \mid n$ and $1 < k < n$. From the minimality of n, we know that k is divisible by some prime number p. Then $p \mid k$ and $k \mid n$, so $p \mid n$. This contradicts the fact that n is not divisible by a prime number. □

Theorem 9.5.1 (Fundamental Theorem of Arithmetic)**.** *Every natural number (other than 0 and 1) is a product of prime numbers (or is itself a prime).*

Proof by contradiction. Suppose there is some natural number $n > 1$, such that n is not a product of prime numbers (and is not a prime). Since $\mathbb{N}$ is well-ordered, we may assume that n is the smallest such number, so:

If $1 < k < n$ (and $k \in \mathbb{N}$), then k is a product of prime numbers.

Since n is not prime, it is divisible by some natural number k, with $1 < k < n$. This means we may write $n = km$, for some $m \in \mathbb{N}^+$. Since $m = n/k$ and $1 < k < n$, we see that $1 < m < n$. Therefore, the minimality of n implies that k and m are products of prime numbers: say $k = p_1 p_2 \cdots p_r$ and $m = q_1 q_2 \cdots q_s$. Then

$$n = km = (p_1 p_2 \cdots p_r)(q_1 q_2 \cdots q_s)$$

is a product of prime numbers. This is a contradiction. □

Corollary 9.5.1.1. *Infinite many primes There are infinitely many prime numbers*

Proof by contradiction. Suppose there are only finitely many prime numbers. Then we can make a list of all of them:

The set of all prime numbers is $\{p_1, p_2, \ldots, p_n\}$.

Let

$$N = p_1 \times p_2 \times \cdots \times p_n.$$

From 9.5.1, we know there is some prime p, such that $p \mid (N + 1)$.

Since $p_1, p_2, \ldots, p_n$ is a list of all the prime numbers, we know $p = p_i$, for some i. Therefore $p = p_i$ is one of the factors in the product that defines N, so $p \mid N$. Therefore, p divides both N and $N + 1$, so we have

$$p \mid \big((N + 1) - N\big) = 1.$$

This implies $p = \pm 1$, which contradicts the fact that p, being a prime number, must be > 1. □

Definition 9.5.2 (relatively prime)**.** *Let $a, b \in \mathbb{N}^+$. We say a and b are **relatively prime** if and only if they have no divisors in common, other than 1. (I.e., if $k \in \mathbb{N}^+$, and k is a divisor of both a and b, then $k = 1$. In other words, the "greatest common divisor" of a and b is 1.)*

Theorem 9.5.2. *Let $a, b \in \mathbb{N}^+$. If a and b are relatively prime, then there exist $m, n \in \mathbb{Z}$, such that $ma + nb = 1$.*

Proof. Let

$$S = \{\, ma + nb \mid m, n \in \mathbb{Z}\ k = \} \cap \mathbb{N}^+.$$

It is easy to see that $a \in S$ (by letting $m = 1$ and $n = 0$), so $S \neq \emptyset$. Therefore, since $\mathbb{N}$ is well-ordered, we may let d be the smallest element of S. Then $d \in S$, so we have $d = m_0 a + n_0 b$ for some $m_0, n_0 \in \mathbb{Z}$.

By the Division Algorithm 6.1.1, we may write

$$a = qd + r \text{ with } 0 \leq r < d.$$

So

$$r = a - qd = a - q(m_0 a + n_0 b) = (1 - qm_0)a + qn_0 b = ma + nb,$$

where $m = 1 - qm \in \mathbb{Z}$ and $n = qn \in \mathbb{Z}$. On the other hand, since $r < d$, and d is the smallest element of S, we know $r \notin S$. From the definition of S, we conclude that $r = 0$. So $d \mid a$.

By repeating the same argument with a and b interchanged (and m_0 and n_0 also interchanged) we see that $d \mid b$.

Therefore, d is a divisor of both a and b. Since a and b are relatively prime, we conclude that $d = 1$. Since $d \in S$, this means $1 \in S$, which establishes the desired conclusion. □

Chapter 10: Cardinality

10.1 Definition and basic properties

Definition 10.1.1 (Cardinality). *1. Let A be a set and let n be a natural number, we say cardinality of A is n, and write $\#A$. $\#A = n$ if and only if there is a bijection from $A \to \{1, 2, 3, \ldots, N\}$*

2. A set is finite if and only if there exist a natural number for which the cardinality of A is n

3. A set is infinite if and only if the set is not finite.

Example

Show that $\#\{1, 2, 3, \ldots, n\} = n$ for each natural number n.

Proof. Let $n \in \mathbb{N}$, and set $A = \{1, 2, 3, \ldots, n\}$ note that $I_A : A \to A$ is a bijection from the set $\{1, 2, 3, \ldots, n\}$ to $\{1, 2, 3, \ldots, n\}$. □

Note

that the $\#\emptyset = 0$.

Proposition 10.1.1 (Cardinality A = Cardinality B). *Suppose A and B are finite sets. Then $\#A = \#B$ if and only if there is a bijection from A to B.*

Proof. ($\Rightarrow$) Let n be the cardinality of A. By definition, this means

$$\text{there is a bijection } f\colon A \to \{1, 2, \ldots, n\}.$$

By assumption, n is also the cardinality of B, so

$$\text{there is also a bijection } g\colon B \to \{1, 2, \ldots, n\}.$$

The inverse of a bijection is a bijection, and the composition of bijections is a bijection, so $g^{-1} \circ f$ is a bijection from A to B.

($\Leftarrow$) We leave this as an exercise. □

Proposition 10.1.2 (Cardinality of Disjoint Finite Sets). *If A and B are disjoint finite sets, then*

$$\#(A \cup B) = \#A + \#B.$$

Proof. Let $m = \#A$ and $n = \#B$. Then there exist bijections

$$f\colon \{1, 2, \ldots, m\} \to A \quad \text{and} \quad g\colon \{1, 2, \ldots, n\} \to B.$$

Define a function $h\colon \{1, 2, \ldots, m + n\} \to (A \cup B)$ by

$$h(k) = \begin{cases} f(k) & \text{if } k \le m \\ g(k - m) & \text{if } k > m \end{cases}$$

(Notice that if $k \in \{1, 2, \ldots, m + n\}$, and $k > m$, then $m + 1 \le k \le m + n$, so $1 \le k - m \le n$; therefore, $k - m$ is in the domain of g, so the expression $g(k - m)$ makes sense.)

To complete the proof, it suffices to show that h is a bijection; thus, we we need only show that h is one-to-one and onto.

(onto) Given $y \in A \cup B$, we have either $y \in A$ or $y \in B$, and we consider these two possibilities as separate cases.

1. Suppose $y \in A$. Since f is onto, there is some $k \in \{1, 2, \ldots, m\}$ with $f(k) = y$. Then, because $k \le m$, we have
$$h(k) = f(k) = y.$$
2. Suppose $y \in B$. Since g is onto, there is some $k \in \{1, 2, \ldots, n\}$ with $g(k) = y$. Then $k + m \in \{1, 2, \ldots, m + n\}$ and $k + m > m$, so
$$h(k + m) = g\big((k + m) - m\big) = g(k) = y.$$

Since y is an arbitrary element of $A \cup B$, we conclude that h is onto.

(one-to-one) We leave this as an exercise. □

Theorem 10.1.1 (Cardinality of Cartesian Products). *For any finite sets A and B, we have*

$$\#(A \times B) = \#A \cdot \#B.$$

Proof. Let $m = \#A$. Then there is no harm in assuming $A = \{1, 2, \ldots, m\}$. Therefore

$$A = \{1\} \cup \{2\} \cup \cdots \cup \{m\},$$

and the sets $\{1\}, \{2\}, \cdots, \{m\}$ are pairwise-disjoint, so

$$\begin{aligned} \#(A \times B) &= \#\big(\{1\} \times B\big) + \#\big(\{2\} \times B\big) + \cdots + \#\big(\{m\} \times B\big) \\ &= \#B + \#B + \cdots + \#B \qquad (m \text{ summands}) \\ &= m \cdot \#B \\ &= \#A \cdot \#B. \end{aligned}$$

□

10.2 Pigeonhole Principle

Proposition 10.2.1 (Pigeonhole Principle). *Let B and $A_1, A_2, \ldots, A_n$ be finite sets. If*

$$B \subset A_1 \cup A_2 \cup \ldots \cup A_n,$$

and $\#B > n$, then $\#A_i \ge 2$, for some i.

Corollary 10.2.0.1. *Suppose A and B are finite sets.*

1. If there exists a one-to-one function $f\colon A \to B$, then $\#A \le \#B$.

2. If there exists an onto function $f\colon A \to B$, then $\#A \ge \#B$.

Proof. Let $m = \#A$ and $n = \#B$.

(1) Suppose $f\colon A \to B$ is one-to-one, and $m > n$. Assume without loss of generality that $B = \{1, 2, \ldots, n\}$, so we may let

$$A_i = f^{-1}(i) \quad \text{for } i = 1, 2, \ldots, n.$$

For any $a \in A$, we have $a \in f^{-1}\big(f(a)\big) = A_{f(a)}$, so $a \in A_1 \cup A_2 \cup \cdots \cup A_n$. Since a is an arbitrary element of A, this implies $A \subset A_1 \cup A_2 \cup \ldots \cup A_n$. Because $\#A = m > n$, we conclude that $\#A_i \geq 2$ for some i. This means $\#f^{-1}(i) > 1$, which contradicts the fact that f is one-to-one.

(2) Suppose $f\colon A \to B$ is onto, and $m < n$. There is no harm in assuming $A = \{1, 2, \ldots, m\}$, and then we may let

$$B_i = \{f(i)\}$$

for $i = 1, 2, \ldots, m$. Since f is onto, we know, for any $b \in B$, there is some $i \in A$, such that $f(i) = b$. This means $b \in B_i$; hence, $b \in B_1 \cup B_2 \cup \cdots \cup B_m$. Since b is an arbitrary element of B, this implies $B \subset B_1 \cup B_2 \cup \ldots \cup B_m$. Because $\#B = n > m$, we conclude that $\#B_i \geq 2$ for some i. This contradicts the fact that $\#B_i = 1$ (because $B_i = \{f(i)\}$ has only one element). □

10.3 Cardinality of a union

Proposition 10.3.1 (Cardinality of a union)**.** *For any finite sets A and B, we have*

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

Proof. We know that $A \setminus B$, $B \setminus A$, and $A \cap B$ are pairwise-disjoint, and that their union is $A \cup B$, so

$$\begin{aligned} &\#(A \setminus B) + \#(B \setminus A) + \#(A \cap B) \\ &= \#\big((A \setminus B) \cup (B \setminus A) \cup (A \cap B)\big) \\ &= \#(A \cup B). \end{aligned}$$

Also, we have

$$\begin{aligned} \#A &= \#\big((A \setminus B) \cup (A \cap B)\big) \\ &= \#(A \setminus B) + \#(A \cap B). \end{aligned}$$

Similarly, we have

$$\#B = \#(B \setminus A) + \#(A \cap B).$$

Therefore

$$\begin{aligned} &\#A + \#B \\ &= \big(\#(A \setminus B) + \#(A \cap B)\big) + \big(\#(B \setminus A) + \#(A \cap B)\big) \\ &= \#(A \setminus B) + \#(B \setminus A) + 2\#(A \cap B) \\ &= \#(A \cup B) + \#(A \cap B). \end{aligned}$$

The desired conclusion is obtained by subtracting $\#(A \cap B)$ from both sides. □

10.4 Cardinality of infinite sets

Definition 10.4.1 (same cardinality)**.** *We say that two sets A and B have the* ***same cardinality*** *if and only if there is a bijection $f : A \to B$.*

Let A be a set

1. *A is said to be countably infinite if and only if there is a bijection $f : A \to \mathbb{N}^+$.*
2. *A is said to be countable if and only if it is either finite or countably infinite*
3. *A is said to be uncountable if and only if it is not countable.*

Note

Remark: A set is countable if and only if the elements of a set can be listed as a sequence. (either finite or infinite)

1. A set is finite if and only if its elements can be listed in a sequence as, $a_1, a_2, a_3, \ldots, a_n$ for some $n \in \mathbb{N}$.
2. If the elements of A can be listed in an infinite sequence like so $a_1, a_2, a_3, \ldots$
3. Conversely, if A is countable infinite, then there is a bijection $f : \mathbb{N}^+ \to A$. Then, letting $a_i = f(i)$, yields a infinite sequence $a_1, a_2, \ldots$ that lists all the elements of A.

Note that the "smallest" infinite sets are the countable ones.

10.5 Countable sets

Recall the definition 10.4.1

Theorem 10.5.1.

1. *Every infinite set contains a countably infinite subset.*
2. *Every subset of a countable set is countable.*

Proof.

1. Given an infinite set A, it suffices to construct an infinite sequence $a_1, a_2, \ldots$ of distinct elements of A. Then $\{a_1, a_2, \ldots\}$ is a countably infinite subset of A.
   (a) Since A is infinite, A is not empty, so we may choose $a_1 \in A$
   (b) Since A is infinite; $A \setminus \{a_1\}$ is not empty, so we may choose $a_2 \in A \setminus \{a_1\}$.

   ⋮

   i. Since A is infinite we have that $A \setminus \{a_1, a_2, \ldots, a_{i-1}\}$ is not empty. So we may take $a_i \in A \setminus \{a_1, a_2, \ldots, a_{i-1}\}$. Continuing this process uelds an infinite sequence $a_1, a_2, \ldots$ of distinct elements of A.
2. Given a subset M of a countable set A, we need to show that M is countable. Since A is countable, we may list the elements of A as $a_1, a_2, \ldots$

Since $M \subseteq A$ every $m \in M$ appears somewhere in the sequence $A = a_1, a_2, \ldots$ We let m_1 be the first element of M in the sequence. We let m_2 be the second and so on, and so forth. This produces a sequence $m_1, m_2, \ldots$ containing all the elements of M hence M is countable. □

Theorem 10.5.2 (Countability from set operations).

1. *A countable union of countable sets is countable.*
2. *The cartesian product of two countable sets is countable.*
3. *The image of a countable set is countable.*

Proof of Theorem. (1) Given either an infinite sequence $A_1, A_2, A_3, \ldots$ of countable sets, or a finite sequence $A_1, A_2, A_3, \ldots, A_n$ of countable sets, we wish to show that the the union of the sets is countable. Subsets of a countable set are countable, so there is no harm in assuming:

- the sequence is infinite (because adding additional terms to the sequence will make the union larger), and
- each of the sets is infinite (because replacing A_i with an infinite superset will make the union larger).

Now, the numbering method from the previous section shows there is an onto function $g\colon \mathbb{N}^+ \to \bigcup_{i=1}^{\infty} A_i$. So, from 3, we conclude that $\bigcup_{i=1}^{\infty} A_i$ is countable.

(2) Given countable sets A and B, we wish to show that $A \times B$ is countable. Subsets of a countable set are countable, so there is no harm in assuming that A and B are infinite (because replacing A and B with infinite supersets will make the cartesian product larger). Let

- $a_1, a_2, a_3, \ldots$ be a list of the elements of A, and
- $b_1, b_2, b_3, \ldots$ be a list of the elements of B,

Then the elements of $A \times B$ are listed in the following table (or matrix):

$$\begin{array}{cccccc}
(a_1,b_1) & (a_1,b_2) & (a_1,b_3) & (a_1,b_4) & (a_1,b_5) & \cdots \\
(a_2,b_1) & (a_2,b_2) & (a_2,b_3) & (a_2,b_4) & (a_2,b_5) & \cdots \\
(a_3,b_1) & (a_3,b_2) & (a_3,b_3) & (a_3,b_4) & (a_3,b_5) & \cdots \\
(a_4,b_1) & (a_4,b_2) & (a_4,b_3) & (a_4,b_4) & (a_4,b_5) & \cdots \\
(a_5,b_1) & (a_5,b_2) & (a_5,b_3) & (a_5,b_4) & (a_5,b_5) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

The numbering method from the previous section defines a bijection from $A \times B$ to $\mathbb{N}^+$. So $A \times B$ is countable.

(3) Suppose $f\colon A \to B$, and A is countable. By replacing B with $f(A)$, we may assume f is onto; then we wish to show that B is countable.

It suffices to define a one-to-one function $g\colon B \to A$. The function f is onto, so, for each $b \in B$, there is some $a \in A$, such that $f(a) = b$; thus, for each $b \in B$, we may choose $g(b)$ to be an element of A such that

$$f\big(g(b)\big) = b.$$

Then $g\colon B \to A$, and all that remains is to show that g is one-to-one. Given $b_1, b_2 \in B$, such that $g(b_1) = g(b_2)$, we have $f\big(g(b_1)\big) = b_1$ and $f\big(g(b_2)\big) = b_2$. Therefore

$$b_1 = f\big(g(b_1)\big) = f\big(g(b_2)\big) = b_2.$$

So g is one-to-one, as desired. □

Example

Show that $\mathbb{Z}$ is countably infinite

Proof. Lets consider $\mathbb{Z} = \{0, -1, 1, -2, 2, \ldots\}$

Define $f : \mathbb{Z} \to \mathbb{N}^+$, by

$$f(k) = \begin{cases} 2k+1, & \text{if } k \geq 0 \\ -2k, & \text{if } k < 0 \end{cases}$$

We need to show that f is a bijection.
(onto) let $n \in \mathbb{N}^+$, we wwill consider two cases

1. If n is odd, then we have $2k + 1 = n$ for some $k \in \mathbb{Z}$. Since n is a positive natural number so $n > 0$ and $2(1) + 1 > 0$ hence $f(k) = 2k + 1 = n$
2. If n is even, then we have $n = 2k$ for some $k \in \mathbb{Z}$ Since $n > 0$, $k > 0$. Then we have $-k \in \mathbb{Z}$ with $-k < 0$. Hence, $f(-k) = -2(-k) = 2k = n$

In either case there exist some integer for which $f(k) = n$ therefore f is onto.

(one-to-one) exercise. □

Note

It is very important to remember that $\mathbb{Q}$ is countable. Since $\mathbb{N}$ and $\mathbb{Z}$ are subsets of $\mathbb{Q}$, this implies that $\mathbb{N}$ and $\mathbb{Z}$ are also countable.

10.6 Uncountable sets

The real set

Theorem 10.6.1 ($\mathbb{R}$ are uncountable). *If $\mathbb{R}$ were countable, then all of its subsets would be countable. thus, in order to prove this theorem we will do a proof by contradiction. Assume that $\mathbb{R}$ is countable.*

Notation

For $a, b \in$ with $a < b$:

- **open interval**: $(a, b) = \{\, x \in | \; a < x < b \,\}$.
- **closed interval**: $[a, b] = \{\, x \in | \; a \leq x \leq b \,\}$.
- **half-open interval**: $[a, b) = \{\, x \in | \; a \leq x < b \,\}$ or $(a, b] = \{\, x \in | \; a < x \leq b \,\}$.

Proof by contradiction. We will prove the interval $[0,1)$ is uncountable.

Suppose $[0,1)$ is countable. (This will lead to a contradiction.) This means there is a list $x_1, x_2, x_3, \ldots$ of all the numbers in $[0,1)$. To obtain a contradiction, we will use a method called the *Cantor Diagonalization Argument*. It was discovered by the mathematician Georg Cantor in the 19th century.

Each number in $[0,1)$ can be written as a decimal of the form $0.d_1d_2d_3\ldots$, where each d_k is a digit (0, 1, 2, 3, 4, 5, 6, 7, 8, or 9). In particular, we can write each x_i in this form:

$$x_i = 0.x_{i,1}x_{i,2}x_{i,3}x_{i,4}x_{i,5}\ldots$$

Then we can make a list of all of these decimals (omitting the leading 0 in each one):

$$\begin{aligned} x_1 &= .x_{1,1}x_{1,2}x_{1,3}x_{1,4}x_{1,5}\ldots \\ x_2 &= .x_{2,1}x_{2,2}x_{2,3}x_{2,4}x_{2,5}\ldots \\ x_3 &= .x_{3,1}x_{3,2}x_{3,3}x_{3,4}x_{3,5}\ldots \\ x_4 &= .x_{4,1}x_{4,2}x_{4,3}x_{4,4}x_{4,5}\ldots \\ x_5 &= .x_{5,1}x_{5,2}x_{5,3}x_{5,4}x_{5,5}\ldots \\ &\vdots \qquad\qquad\quad \vdots \end{aligned}$$

The right-hand side can be thought of as an array of digits, and we now focus on the diagonal entries $x_{i,i}$ of this array, which are circled in the following picture:

$$\begin{aligned} x_1 &= .\textcircled{$x_{1,1}$}x_{1,2}x_{1,3}x_{1,4}x_{1,5}\ldots \\ x_2 &= .x_{2,1}\textcircled{$x_{2,2}$}x_{2,3}x_{2,4}x_{2,5}\ldots \\ x_3 &= .x_{3,1}x_{3,2}\textcircled{$x_{3,3}$}x_{3,4}x_{3,5}\ldots \\ x_4 &= .x_{4,1}x_{4,2}x_{4,3}\textcircled{$x_{4,4}$}x_{4,5}\ldots \\ x_5 &= .x_{5,1}x_{5,2}x_{5,3}x_{5,4}\textcircled{$x_{5,5}$}\ldots \\ &\vdots \qquad\qquad\quad \vdots \end{aligned}$$

They form a sequence $x_{1,1}, x_{2,2}, x_{3,3}, \ldots$.

The key to the proof is to make a new sequence $d_1, d_2, d_3, \ldots$ of digits, such that

$$d_1 \neq x_{1,1}, \quad d_2 \neq x_{2,2}, \quad d_3 \neq x_{3,3}, \quad \text{etc.}$$

This means that every term of the new sequence is different from the corresponding term of the diagonal sequence. (This idea of choosing a sequence that is completely different from the diagonal is called **Cantor diagonalization**, because it was invented by the mathematician Georg Cantor.) Also, to avoid problems coming from the fact that $.999\cdots = 1.000\cdots$, you should not use the digits 0 and 9. The sequence $\{d_i\}$ can be constructed in many ways: just be sure to choose each d_i to be a digit that is not $x_{i,i}$ (and is not 0 or 9). For example, we could let

$$d_i = \begin{cases} 1 & \text{if } x_{i,i} \neq 1 \\ 5 & \text{if } x_{i,i} = 1. \end{cases}$$

Now, let

$$d = 0.d_1d_2d_3\ldots \in [0,1).$$

For each i, we made sure that $d_i \neq x_{i,i}$, which means that the ith digit of d is different from the ith digit of x_i. Therefore, for each i, we have $d \neq x_i$.[1] So d is an element of $[0,1)$ that is not in the list $x_1, x_2, x_3, \ldots$. This contradicts the fact that $x_1, x_2, x_3, \ldots$ is a list of *all* the numbers in $[0,1)$. □

The cardinality of power sets

If A is a finite set, then the set $\mathcal{P}(A)$ of all subsets of A is also finite. (Indeed, $\#\mathcal{P}(A) = 2^{\#A}$.) However, this assertion does *not* remain true when the word "finite" is replaced with "countable".

Example

Show that $\mathcal{P}(\mathbb{N}^+)$ is uncountable.

Hint: For any $f\colon \mathbb{N}^+ \to \mathcal{P}(\mathbb{N}^+)$, the set $\{i \in \mathbb{N}^+; i \notin f(i)\}$ is not in the image of f.

For every set A, not just the countable ones, the same argument shows that the cardinality of $\mathcal{P}(A)$ is greater than the cardinality of A. Thus, there is no "largest" infinite set. For every set, there is always some set that has *much* larger cardinality.

Barber Paradox

Suppose

1. There is a town with only one barber
2. The barber is a man
3. The barber shaves precisely those men in the town who do not shave themselves

Now we ask:

> Does the barber shave himself?

This question is a paradox:

- If the answer is yes, then the barber shaves himself. But the barber does *not* shave men who shave themselves, so this means that the barber does not shave himself. But we already said that the barber does shave himself, so this is nonsense.
- If the answer is no, then the barber does not shave himself. But the barber *does* shave any man who does not shave himself, so this means that the barber does shave himself. But we already said that the barber does not shave himself, so this is nonsense.

The premise of this discussion is that the hypothesized situation leads to a contradiction, so it is impossible.

[1] The digits of d are only 1's and 5's, so it is not a problem that numbers ending $000\ldots$ can also be expressed as a different decimal that ends $999\ldots$.

Credits

General

- Created by: Jihoon Og, u/DnD_Notes
- Compiled on Monday 21st March, 2022 at 23:08
- Typesetting engine: LaTeX
- Dungeon and Dragon (5e) LaTeX Template
- Referenced from Proofs and Concepts, the fundamentals of abstract mathematics by Dave Witte Morris and Joy Morris

Art

- Gold Dragon and Wizard for the cover art is from D&D Beyond
- Andy the D&D Ampersand is from Dungeon and Dragons
- Cover art formatting and design done in Photoshop CC 2019

Disclaimer