

MA 3030 Spring 2019 Slides

Last compiled: Wednesday 28th August, 2019 at 06:23

Chapter 2: The Logic of Compound Statements

- ▶ 2.1 Logical form and logical equivalence
- ▶ 2.2 Conditional Statements
- ▶ 2.3 Valid and Invalid Arguments

Chapter 2

Section 2.1 Logical form and logical equivalence

The words **sentence**, **true**, and **false** are undefined terms.
Sometimes we will abbreviate *true* by *T* and *false* by *F*.

Definition

A **statement** is a sentence to which we have assigned a value of either **true** or **false**, but not both.

Definition

A **model** is an assignment of a meaning or definition to the undefined terms *sentence, true, and false*.

Example

In the model of the natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$

- ▶ an example of a sentence and a statement is “ $2 + 2 = 4$ ”, and it is assigned a value of true.
- ▶ “ $2 + 2 = 5$ ” is also a sentence and a statement and it is assigned a value of false.
- ▶ an example of a sentence with no assigned truth value (and therefore not a statement) is “ $x = 2$ ”, because we don’t assign a value of true or false to it.

Compound statements

We will typically use letters like $p, q, r \dots$ to denote a statement, and call these *statement variables* in much the same way that in algebra variables x, y are used to represent numbers.

For example, p could be the statement $2 + 2 = 4$ and q could stand for the statement $2 + 2 = 5$.

Since we can use conjunctions such as *and*, *or*, *not* in ordinary English language to form new sentences from old sentences, we want to do the same in for our logic framework/language.

The logical connectives we will use are $\vee, \wedge, \neg, \rightarrow$ (there are others, and you can even create your own!)

Statement forms

Definition

A **statement form** is an expression that is built out of letters and logical connectives and if necessary parentheses. Examples of statement forms are

$p, q, p \vee q, p \wedge q, \neg p, p \rightarrow q, (p \rightarrow q) \rightarrow q, (p \rightarrow q) \rightarrow r$. This definition is a bit imprecise, but don't worry about it.

Let p and q be statement variables. We can form three new *statements forms*

1. $p \vee q$, read “ p or q ”
2. $p \wedge q$, read “ p and q ”
3. $\neg p$, read “not p ”

Minor difference between statements and statement forms:

Recall *statements* are sentences that have been assigned a true or false value (but not both).

The expression $p \vee q$ is not quite a statement but instead it is a statement *form* - the truth value we assign to it that depends on the truth values of p and q .

Since p can take 2 possible values (T/F), and q can also take 2 possible truth values, there are a total of $2 \times 2 = 4$ possible combinations of truth values of p and q , and that's why the tables that follow for *or* and *and* have 4 rows.)

The difference between a statement and statement form

$S(p, q, r, \dots)$ is similar to the difference between a number like 2 and a function like x^3 .

logical or: \vee

Definition

We *define* the statement form $p \vee q$ to take truth values according to the table below. In words, “**or** is always true except in false-false case”:

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

logical and: \wedge

We *define* the statement form $p \wedge q$ to take truth values according to the table below. In words, “**and** is always false except in true-true case” :

Definition

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

Negation: \neg

We *define* the statements form $\neg p$ to take truth values according to the table below. In words, not/negation just flips the truth values:

Definition

p	$\neg p$
T	F
F	T

Once we have these basic definitions in place, we can figure out truth values of more complicated statement forms such as $\neg(p \vee q)$ and $\neg p \wedge \neg q$ (which means $(\neg p) \vee (\neg q)$ since \neg takes precedence over \vee and \wedge) by making truth tables (which are simply listing all possible combinations of the truth values of the variables involved):

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

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

Logical Equivalence

Now look at the columns $\neg(p \vee q)$ and $\neg p \wedge \neg q$ in the previous two tables. They are identical!

We thus say that the statement forms $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are *logically equivalent*, and we write

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

Logical equivalence is the analogue in logic for equal in algebra: for example the expressions/functions $2(x + 1)$ and $2x + 2$ are equal because for every value of x that you plug in, both functions gives the same output:

x	$2(x + 1)$	$2x + 2$
0	2	2
1	4	4
2	6	6
:	:	:

Definition

Informally, two statement forms $S_1(p, q, r, \dots)$ and $S_2(p, q, r, \dots)$ are **logically equivalent** if they have the same truth tables.

More formally, for all possible combinations of T/F that the variables p, q, r, \dots take on, the truth values of $S_1(p, q, r, \dots)$ and $S_2(p, q, r, \dots)$ are the same. If $S_1(p, q, r, \dots)$ and $S_2(p, q, r, \dots)$ are logically equivalent, we write

$$S_1(p, q, r, \dots) \equiv S_2(p, q, r, \dots)$$

Theorem (De Morgan's laws)

The following are logical equivalences:

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

Proof.

We simply check the truth tables are the same. We did this above for the first line, and the second line is similarly done. □

Truth tables with p, q, r

A truth table for a statement form involving three variables, say p, q, r , will involve $2 \times 2 \times 2 = 8$ rows. A systematic way to list all 8 rows is to first list the 4 rows with p equal to T , and then the four rows with p equal to F .

p	q	r
T		
F		

Then for q , begin with 2 T 's and then 2 F 's, and continue alternating:

p	q	r
T	T	
T	T	
T	F	
T	F	
F	T	
F	T	
F	F	
F	F	

Then for r , begin with 1 T and then 1 F , and continue alternating:

p	q	r
T	T	T
T	T	F
T	F	T
T	F	F
F	T	T
F	T	F
F	F	T
F	F	F

Chapter 2

Section 2.2 Conditional statements. i.e. $p \rightarrow q$

if-then: \rightarrow

Let p and q be statement variables.

We define a new statement form $p \rightarrow q$, (the book calls these conditional statement forms, I'll call them if-then statements), and read "if p then q " (or " p implies q ") by the following table:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

In words, "**implication/arrow is always true except in true-false case**". This will be a fact that is very often used!! And the last two lines of that truth table are a bit counterintuitive: $F \rightarrow T$ and $F \rightarrow F$ are both assigned a value of **true**!

So for example, the statement "If $2 + 2 = 5$ then $2 + 2 = 6$ " is assigned a value of true! It is a bit nonsensical, but just take my word that this *choice* makes things easier later on.

Here is a fact that will be used fairly often:

Theorem (if-then equals not-or)

$$p \rightarrow q \equiv \neg p \vee q$$

Proof.

We simply make a truth table and check the columns labelled $p \rightarrow q$ and $\neg p \vee q$ are identical:

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



Taking negations of the *if-then equals not-or* theorem and applying De Morgan's law gives the following result that will be useful when we do proof by contradiction:

Corollary (Negation of an if-then statement)

$$\neg(p \rightarrow q) \equiv p \wedge \neg q$$

In particular, *the negation of an if-then statement is NOT an if-then statement, instead it is an AND statement!*

Proof.

$$\neg(p \rightarrow q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$$



example

What is the negation of the statement
“If I win the lottery, then I will be happy”?

- a) If I don't win the lottery, then I won't be happy
- b) I don't win the lottery and I won't be happy
- c) I win the lottery and I won't be happy
- d) If I win the lottery, then I won't be happy

Answer: (c).

Definition

- ▶ The **converse** of $p \rightarrow q$ is $q \rightarrow p$
- ▶ The **contrapositive** of $p \rightarrow q$ is $\neg q \rightarrow \neg p$.

Let's figure out the truth tables of the converse and contrapositive:

p	q	$p \rightarrow q$	$\neg p$	$\neg q$	$q \rightarrow p$	$\neg q \rightarrow \neg p$
T	T	T	F	F	T	T
T	F	F	F	T	T	F
F	T	T	T	F	F	T
F	F	T	T	T	T	T

What do you notice? The contrapositive is logically equivalent to the original if-then $p \rightarrow q$. This observation will be the basis of proof by contrapositive. (We also see that the converse is *not* logically equivalent to the original if-then. One consequence is that proving an if-then is different from proving its converse).

Theorem

An if-then and its contrapositive are logically equivalent. In symbols:

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

Proof.

See truth table above.



Order of operations

The logical operators have order of precedence as follows:

1. \neg
2. $\wedge \vee$
3. \rightarrow

So for example, $\neg p \wedge q$ means $(\neg p) \wedge q$, and it does not mean $\neg(p \wedge q)$.

Also, $p \vee q \rightarrow r$ means $(p \vee q) \rightarrow r$, and not $p \vee (q \rightarrow r)$.

Section 2.3 Valid and Invalid arguments

Mathematical reasoning is based on something called “valid arguments”, which we will now explain.

The following three lines are a famous example (so famous that it gets a Latin name **modus ponens**, or “method positive”) of a *valid argument form*:

$$\begin{array}{|c|} \hline p \rightarrow q \\ p \\ \therefore q \\ \hline \end{array}$$

Definition

An **argument (form)** is simply a list of statement (forms), and where the very last begins with a therefore symbol \therefore . The last line is called the **conclusion** of the argument, and all the lines except the last form what is called the **hypotheses/premises/assumptions** of the argument.

premises	$p \rightarrow q$
	p
conclusion{	$\therefore q$

So in the modus ponens argument form above, $p \rightarrow q$ and p are the premises, and q is the conclusion.

Valid argument

Definition

An argument form is **valid** if in the truth table for the premises and conclusion, for every row in which the premises are all true, the conclusion is also true. (Note that we do not require the premises to be true in all the rows.). Otherwise, we say the argument is **invalid** - in other words, there is at least one row where the premises are all true, but the conclusion is false.

Modus ponens is valid

Let's make a truth table to see why modus ponens

$$\begin{array}{c} p \rightarrow q \\ p \\ \therefore q \end{array}$$

is a valid argument.

First for brevity, instead of making the truth table with columns

p	q	$p \rightarrow q$	p	q
-----	-----	-------------------	-----	-----

we omit the repeated columns and fill out the following truth table:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

premises	$p \rightarrow q$
	p
conclusion{	$\therefore q$

The premises of our argument form are $p \rightarrow q$ and p , and so to check if the argument is valid, we only care about those rows where $p \rightarrow q$ is true and p is true. In this example there is only one row - the first row of the table (highlighted) - but other arguments often have more. And then we ask, in that row(s), is the conclusion (q in this case) also true? In this case, the answer is yes: q is T in row 1. Hence our argument is **valid**.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Converse error

Here is a famous *invalid* argument form, called the **converse error**:

$$\begin{array}{c} p \rightarrow q \\ q \\ \therefore p \end{array}$$

Why is it **invalid**?

Simply look at the truth table! Which rows in truth table (copied below) do we have to look at? In other words, which rows of the truth table have all the premises true?

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

The answer is rows 1 and 3, since those are all the rows where the premises $p \rightarrow q$ and q are both true. In row 1 the conclusion p is true, so no problem so far. But in row 3, the conclusion p is *false*, and hence the entire argument is declared *invalid*.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Modus Tollens

There are infinitely many valid arguments forms (you can make your own one!), but there are a few basic ones. We saw earlier modus ponens (method positive). There is also a *valid* argument called **modus tollens** (method negative)

$$\begin{array}{c} p \rightarrow q \\ \neg q \\ \therefore \neg p \end{array}$$

Why is modus tollens a *valid* argument? Simply fill in the relevant truth table:

p	q	$p \rightarrow q$	$\neg q$	$\neg p$
T	T	T		
T	F	F		
F	T	T		
F	F	T		

p	q	$p \rightarrow q$	$\neg q$	$\neg p$
T	T	T	F	F
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

The highlighted columns are the premises. We have to find the rows (in the highlighted columns) that consists of only T 's. There is only one - the last row. In that row, the conclusion p is T (highlighted in slightly darker blue), so the modus tollens argument is valid.

Epp p.60 Table

The following table from p.60 of Epp records some *simple* (and frequently used) valid arguments forms (the book also uses the term “rules of inference” for valid argument forms):

Table 2.3.1 Valid Argument Forms

Modus Ponens	$p \rightarrow q$ p $\therefore q$	Elimination	a. $p \vee q$ $\sim q$ $\therefore p$ b. $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \rightarrow q$ $\sim q$ $\therefore \sim p$	Transitivity	$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$
Generalization	a. p $\therefore p \vee q$ b. q $\therefore p \vee q$	Proof by Division into Cases	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\therefore r$
Specialization	a. $p \wedge q$ $\therefore p$ b. $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	Contradiction Rule	$\sim p \rightarrow c$ $\therefore p$

Again, the fact that all these are *valid* argument forms can be quickly checked via a truth table - we've done modus pollens and modus tollens, and mathematicians have done the rest (and you can do so quickly).

What is the point of this table 2.3.1 in Epp? It is that these basic valid argument forms (which one checked via truth table) can be used to show more complicated argument forms are valid, *without using a truth table*.

Example (Epp p.62 #42)

Show using table 2.3.1 that the following is a valid argument:

- | |
|------------------------------------|
| 1. $p \vee q$ |
| 2. $q \rightarrow r$ |
| 3. $p \wedge s \rightarrow t$ |
| 4. $\neg r$ |
| 5. $\neg q \rightarrow u \wedge s$ |
| $\therefore t$ |

Solution:

There are 5 variables p, q, r, s, t , so checking validity via a truth table would require building one with $2^5 = 32$ rows - possible but very tedious and not advised! Fortunately, there is an easier way: use the basic valid arguments in Table 2.3.1 (especially modus ponens (MP) and modus tollens (MT)) to write down statement forms that **must be true** when the premises are all true. Also, several correct solutions are possible, mainly differing in the order the Table 2.3.1 valid arguments are invoked.

(One) Solution

1	$p \vee q$	given/premise
2	$q \rightarrow r$	given
3	$p \wedge s \rightarrow t$	given
4	$\neg r$	given
5	$\neg q \rightarrow u \wedge s$	given
6	$\neg q$	MT (modus tollens) 2, 4
7	p	Elimination 1, 6
8	$u \wedge s$	MP (modus ponens) 5, 6
9	s	Specialization 8
10	$p \wedge s$	Conjunction
11	t	MP 3, 10

Table 2.3.1 Valid Argument Forms

Modus Ponens	$p \rightarrow q$ p $\therefore q$	Elimination	a. $p \vee q$ $\sim q$ $\therefore p$ b. $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \rightarrow q$ $\sim q$ $\therefore \sim p$	Transitivity	$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$
Generalization	a. p $\therefore p \vee q$ b. q $\therefore p \vee q$	Proof by Division into Cases	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\therefore r$
Specialization	a. $p \wedge q$ $\therefore p$ b. $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	Contradiction Rule	$\sim p \rightarrow c$ $\therefore p$

Some terminology that I won't use too much, but appears sometimes in the text:

Definition

A tautology is a statement form $S(p, q, r, \dots)$ whose truth value is always true. We use the symbol \top to denote a tautology, and write $S(p, q, r, \dots) \equiv \top$ if $S(p, q, r)$ is a tautology.

example

$p \vee \neg p$ is a tautology, because look at its truth table:

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

Definition

Given two statement forms $S_1(p, q, r, \dots)$ and $S_2(p, q, r, \dots)$, we write

$$S_1 \implies S_2$$

if

$$\boxed{\begin{array}{c} S_1 \\ \therefore S_2 \end{array}}$$

is a valid argument form. In other words, for every row of the truth table for S_1 in which S_1 is true, we also have S_2 true. Since the conditional \rightarrow is always true except in $T \rightarrow F$, we have that $S_1 \implies S_2$ means $S_1 \rightarrow S_2$ is always has all truth values (in truth table) true ... i.e. $S_1 \rightarrow S_2$ is a tautology.

example

Modus ponens allows us to write

$$(p \rightarrow q) \wedge p \implies q$$

Equivalently,

$$(p \rightarrow q) \wedge p \rightarrow q$$

is a tautology.

Chapter 3 Logic of Quantified Statements

This chapter is basically the same as the previous chapter, but introduces two quantifiers:

1. \forall read as “for all” (upside down A is supposed to remind you of All)
2. \exists read as “there exists” (backwards E is supposed to remind you of Exists)

Sets of numbers

Set	Name	Examples
\mathbb{N}	natural numbers	1, 2, 3, ...
\mathbb{Z}	integers (=zahlen in German)	..., -2, -1, 0, 1, 2, ...
\mathbb{Z}^+	positive integers	1, 2, 3, ...
\mathbb{Q}	rational numbers (fractions or quotients of integers)	$\frac{1}{2}, 0 = \frac{0}{1}, 1, \frac{-2}{1}$
\mathbb{R}	real numbers (decimals)	$\pi, \frac{1}{3}, -e, 4$

$x \in \mathbb{N}$ is read “ x in \mathbb{N} ” and means x is a natural number, such as 1, 2, 3,

For example, $1 \in \mathbb{N}$ is true, while $\frac{1}{3} \in \mathbb{N}$ is false - in which case we write $\frac{1}{3} \notin \mathbb{N}$ and say “ $\frac{1}{3}$ is not in \mathbb{N} ”

Throughout this chapter we will write $x \in D$ to mean x is in some set D . (More precisely, $x \in D$ is a statement, and is assigned a value of *true* if x is in the set D , and a value of *false* if x is not in D .)

3.1 Predicates and Quantified Statements 1

Statements

Recall that a *statement* is a sentence to which we assign a truth value of either true or false, but not both. Is the following line a *statement*?

x is an even integer

No, because we don't know what the number x is, so we can't decide if the sentence above is true or false:

- ▶ If x is 1, then the sentence x is an even number is false,
- ▶ If x is 2 then the x is an even number is true,

Predicate

Let

$$P(x) = x \text{ is an even number}$$

$P(x)$ is an example of a *predicate* - a sentence involving variables such as x, y, \dots , whose truth value (i.e. T/F) *depends upon* the value these variables take.

In the above example, $P(1)$ is false, $P(2)$ is true, $P(3)$ is false, and so on.

Definition

A **predicate** $P(x, y, \dots)$ is a sentence involving variables x, y, \dots , which becomes a statement (i.e. can be assigned a value of true/false) once the variables x, y, \dots are assigned specific values. The word *predicate* in ordinary English means “depends upon”; the reason we use this word here in logic is that the truth value of $P(x, y, \dots)$ *depends upon* the values of x, y, \dots .

Definition

The **domain** D of a predicate $P(x)$ is the set of values that x takes on.

Definition

The **truth set** of a predicate $P(x)$ with domain D is the subset of D where $P(x)$ is true:

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

which is read as “the set of x in D such that $P(x)$ is true. Notice that the vertical line $|$ is read as “such that”.

Example

Let $P(x) = x \text{ is an even integer}$ be a predicate with domain $D = \mathbb{Z}$. In other words, $x \in D$. The truth set of this predicate is

$$\{x \in \mathbb{Z} \mid x \text{ is an even integer}\} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

simply the set of even integers; sometimes denoted $2\mathbb{Z}$.

Universal Statement

\forall is read “for all” and is called the **universal quantifier**

Let $P(x)$ be a predicate with domain D . Recall that $P(x)$ is not a statement (i.e. is not true or false). We define a *statement*

$$\boxed{\forall x \in D, P(x)}$$

read “for all (or every) x in D , $P(x)$.” Because it is a statement, it is assigned a value of either true or false, and I now tell you how that is defined:

- ▶ $\forall x \in D, P(x)$ is TRUE if for all $x \in D$, $P(x)$ is true
- ▶ $\forall x \in D, P(x)$ is FALSE if there is at least one $x \in D$ with $P(x)$ false.

example

- ▶ The statement

$$\forall x \in \mathbb{Z}, x \text{ is even}$$

is false

- ▶ The statement

$$\forall x \in \mathbb{Z}, x^2 \geq 0$$

is true

Counterexample to a universal statement

Definition

If $\forall x \in D, P(x)$ is false, any value of $x \in D$ for which $P(x)$ is false is called a **counterexample**.

Example: The statement

$$\forall x \in \mathbb{R} \mid x^2 \geq x$$

is false. Find a counterexample.

Answer: any x with $0 < x < 1$ is a counterexample. For example $x = \frac{1}{2}$.

Universal Conditional Statement

A universal statement of the form

$$\boxed{\forall x \in D, \text{if } P(x) \text{ then } Q(x)}$$

or

$$\boxed{\forall x \in D, P(x) \rightarrow Q(x)}$$

is called a **universal conditional statement** - recall that $p \rightarrow q$ is a conditional statement.

Since $p \rightarrow q$ is always true except when p is true and q is false, to determine the truth value of

$$\forall x \in D, P(x) \rightarrow Q(x)$$

we do not need to check all $x \in D$, but only those $x \in D$ for which $P(x)$ is true, i.e. only those x in the truth set of the predicate $P(x)$. In symbols we have the logical equivalence:

$$\boxed{\forall x \in D, P(x) \rightarrow Q(x)} \quad \equiv \quad \boxed{\forall x \in D \text{ with } P(x) \text{ true, } Q(x)}$$

example

Determine if the following universal conditional statement is true or false:

" $\forall x \in \mathbb{Z}$, if x is odd then $x + 4$ is odd."

Solution: The universal conditional is logically equivalent to

" $\forall x \in \mathbb{Z}$ with x odd, $x + 4$ is odd."

So we just have to check for x an odd integer $1, 3, 5, \dots$ (and their negatives), whether $x + 4$ is odd. If $x = 1$, then $x + 4 = 1 + 4 = 5$, which is odd. But because we have a "for all" statement we would also need to check $x = 3, 5, \dots$ - it's impossible to check infinitely many values each by explicit computation. Instead notice, $x + 4$ has the form odd + even, and such a sum is always odd (we'll prove this carefully in chapter 4). So the given statement is **true**.

example

Determine if the following universal conditional statement is true or false:

“ $\forall x \in \mathbb{Z}$, if x is odd then $x + 4$ is **even**.”

Solution: The universal conditional is logically equivalent to

“ $\forall x \in \mathbb{Z}$ with x odd, $x + 4$ is even.”

So we just have to check for x an odd integer $1, 3, 5, \dots$ (and their negatives), whether $x + 4$ is even. If $x = 1$, then

$x + 4 = 1 + 4 = 5$, which is not even. A universal statement is false if we find just one value of x making the predicate false; we don't need to check any more values. So the given statement is **false**.

Existential Statement

\exists is read “there exists” and is called the **existential quantifier**

Let $P(x)$ be a predicate with domain D . Recall that $P(x)$ is not a statement (i.e. is not true or false because its truth value depends on x). We define a *statement*

$$\boxed{\exists x \in D, P(x)}$$

read “there exists x in D , $P(x)$.” Because it is a statement, it is assigned a value of either true or false, and I now tell you how that is assigned:

- ▶ $\boxed{\exists x \in D, P(x)}$ is TRUE if there exists $x \in D$ for which $P(x)$ is true
- ▶ $\boxed{\exists x \in D, P(x)}$ is FALSE if for all $x \in D$ we have $P(x)$ is false (equivalently, there does not exist an $x \in D$ for which $P(x)$ is true).

example

- ▶ The statement

$$\exists x \in \mathbb{Z}, x \text{ is even}$$

is **true**. By contrast, the statement “ $\forall x \in \mathbb{Z}, x \text{ is even}$ ” is false.

- ▶ The statement

$$\exists x \in \mathbb{Z}, x^2 \geq 10$$

is **true**. By contrast, the statement “ $\forall x \in \mathbb{Z}, x^2 \geq 10$ ” is false.

- ▶ The statement

$$\exists x \in \mathbb{Z}, x^2 < 0$$

is false (by the way, “ $0 < 0$ ” is false).

- ▶ The statement

$$\exists x \in \mathbb{Z}, x^2 \leq 0$$

is true (take $x = 0$).

(Minor) Fact:

$$\forall x \in D, P(x)$$

can be written as

$$\forall x, x \in D \rightarrow P(X)$$

The " \implies " notation for predicates

\implies and \rightarrow are both read as “implies” and are closely related but slight different:

Let $P(x)$, $Q(x)$ be predicates with domain D . Then $P(x) \rightarrow Q(x)$ is not a statement (because its truth value depends on x , so it's another predicate), but if we put either the \forall or \exists quantifiers in front of it, we get statements: $\boxed{\forall x, P(x) \rightarrow Q(x)}$ and

$\boxed{\exists x, P(x) \rightarrow Q(x)}$ are statements (i.e. have a truth value).

We form a new *statement* $\boxed{P(x) \implies Q(x)}$ and declare it to mean the statement

$\boxed{\forall x \in D, P(x) \rightarrow Q(x)}$

So $P(x) \implies Q(x)$ is assigned a value of true if $\forall x \in D, P(x) \rightarrow Q(x)$ is true, and likewise for false.

Example

Determine if the following statement is true or false, where the domain of x is set \mathbb{R} of real numbers:

$$x^2 \geq 4 \implies x \geq 2$$

Solution: We have to figure out if

$$\forall x \in \mathbb{R}, (x^2 \geq 4) \rightarrow (x \geq 2)$$

In other words, if $x^2 \geq 4$, does that force $x \geq 2$? Taking square roots of both sides of $x^2 \geq 4$ you might think the answer is yes, but you also have to remember the possibility of negative square roots.

A counterexample is $x = -3$: in that case, $x^2 \geq 4 \rightarrow x \geq 2$ becomes $(9 \geq 4) \rightarrow (-3 \geq 2)$, which is of the form $T \rightarrow F$ which is *false*. So since $x^2 \geq 4 \rightarrow x \geq 2$ is not true for *all* values of $x \in \mathbb{R}$ (although it is true for many values), we conclude that $\forall x \in \mathbb{R}, x^2 \geq 4 \rightarrow x \geq 2$ is false and therefore $x^2 \geq 4 \implies x \geq 2$ is **false**.

Terminology: Necessary, sufficient, if, only if

Definition

Let $P(x)$, $Q(x)$ be predicates with domain D

We say ...	if this is true
$P(x)$ is a necessary condition for $Q(x)$	$Q(x) \implies P(x)$
$P(x)$ is a sufficient condition for $Q(x)$	$P(x) \implies Q(x)$
$P(x)$ if $Q(x)$	$Q(x) \implies P(x)$
$P(x)$ only if $Q(x)$	$P(x) \implies Q(x)$

Section 3.2 Predicates and Quantified Statements II

Later in Chapter 4 on indirect proof techniques, we will need to form the negation and contrapositive of quantified if-then statements. So in this section we explain how.

Negation of Quantified Statements

When taking negations of quantified statements, the *for all* \forall changes to *there exists* \exists , and vice-versa:

Theorem

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

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

example

Find negation of “*For all $x \in \mathbb{N}$, $x^2 + 1$ is prime*”

Solution: “*There exists $x \in \mathbb{N}$, $x^2 + 1$ is not prime*”

example

Find the negation of $\exists y, Q(y) \wedge R(y)$.

Solution:

$$\neg(\exists y, Q(y) \wedge R(y)) \equiv \forall y, \neg(Q(y) \wedge R(y))$$

$$\equiv \boxed{\forall y, \neg Q(y) \vee \neg R(y)}$$

Negation of Quantified Conditional Statements

Recall $\neg(p \rightarrow q) \equiv p \wedge \neg q$, which we checked via a truth table.
Hence

Theorem

$$\neg(\forall x \in D, P(x) \rightarrow Q(x)) \equiv \exists x \in D, P(x) \wedge \neg Q(x)$$

$$\neg(\exists x \in D, P(x) \rightarrow Q(x)) \equiv \forall x \in D, P(x) \wedge \neg Q(x)$$

example

Consider the following statement:

For all integers n , if n is odd, then $n^2 - 1$ is a multiple of 4.

Write down its negation.

Solution: *There exists an integer n such that n is odd and $n^2 - 1$ is not a multiple of 4.*

Notice that the negation of an *if-then* is NOT an if-then, it is an *and* statement.

A more complicated example

Let $P(x)$, $Q(x, y)$, $R(y)$ be predicates (doesn't matter what exactly they are). Write down the negation of the statement

$$\forall x, P(x) \rightarrow \exists y, Q(x, y) \wedge R(y)$$

Solution:

$$\begin{aligned} & \neg(\forall x, P(x) \rightarrow \exists y, Q(x, y) \wedge R(y)) \\ & \equiv \exists x, \neg(P(x) \rightarrow \exists y, Q(x, y) \wedge R(y)) \\ & \equiv \exists x, P(x) \wedge \neg(\exists y, (Q(x, y) \wedge R(y))) \quad \text{since } \neg(p \rightarrow q) \equiv p \wedge \neg q \\ & \equiv \exists x, P(x) \wedge \forall y, \neg(Q(x, y) \wedge R(y)) \\ & \equiv \boxed{\exists x, P(x) \wedge \forall y, \neg Q(x, y) \vee \neg R(y)} \quad \text{since } \neg(p \wedge q) \equiv \neg p \vee \neg q \end{aligned}$$

Converse and Contrapositive of Universal (i.e. for all) Conditional (i.e. $p \rightarrow q$) Statements

Definition

Consider a universal conditional statement $\forall x \in D, P(x) \rightarrow Q(x)$.

- ▶ Its **contrapositive** is $\forall x \in D, \neg Q(x) \rightarrow \neg P(x)$.
- ▶ Its **converse** is $\forall x \in D, Q(x) \rightarrow P(x)$.

Note that when forming the contrapositive or converse the quantifier $\forall x \in D$ stays as $\forall x \in D$, it does **not** change to $\exists x \in D$. By contrast, when forming the *negation* of $\forall x \in D, P(x) \rightarrow Q(x)$ one changes the \forall to \exists :

$$\begin{aligned}\neg(\forall x \in D, P(x) \rightarrow Q(x)) &\equiv \exists x \in D, \neg(P(x) \rightarrow Q(x)) \\ &\equiv \exists x \in D, P(x) \wedge \neg Q(x)\end{aligned}$$

We saw via a truth table in Chapter 2 that $p \rightarrow q$ is logically equivalent to its contrapositive $\neg q \rightarrow \neg p$, so the same holds for quantified versions:

$$\boxed{\forall x \in D, P(x) \rightarrow Q(x)} \quad \equiv \quad \boxed{\forall x \in D, \neg Q(x) \rightarrow \neg P(x)}$$

$$\boxed{\exists x \in D, P(x) \rightarrow Q(x)} \quad \equiv \quad \boxed{\exists x \in D, \neg Q(x) \rightarrow \neg P(x)}$$

example

Consider the following statement:

For all integers n , if n is odd, then $n^2 - 1$ is a multiple of 4. Write down its contrapositive, converse, and negation.

Solution:

1. Contrapositive: *For all integers n , if $n^2 - 1$ is not a multiple of 4, then n is not odd.*
2. Converse: *For all integers n , if $n^2 - 1$ is a multiple of 4, then n is odd.*
3. Negation *There exists an integer n such that n is odd and $n^2 - 1$ is not a multiple of 4.*

3.3 Statements with Multiple Quantifiers

In this section, we find truth values of statements with multiple quantifiers, such as

$$\forall x \in D, \exists y \in E, P(x, y)$$

$$\exists x \in D, \forall y \in E, P(x, y)$$

where $P(x, y)$ is a predicate involving two variables.

example

$x + y = 2$ is not a statement, it is a predicate - its truth value depends on the value of x, y .

Also $\exists y \in \mathbb{Z}, x + y = 2$ is still not a statement - its truth value depends on value of x .

But

$$\forall x \in \mathbb{N}, \exists y \in \mathbb{Z}, x + y = 2$$

is a statement - i.e. has a definite truth value.

Let's figure out if it is a true statement or a false statement.

$$\forall x \in \mathbb{N}, \exists y \in \mathbb{Z}, x + y = 2$$

Theoretically, to find out the truth value of a “for all” statement “

$$\forall x \in \mathbb{N}, \dots$$

we have to go one by one through the values of x , in this case $1, 2, 3 \dots$, and check if the \dots is true for that value of x . In the example above, \dots is $\exists y \in \mathbb{Z}, x + y = 2$.

So let's start with $x = 1$. Then the \dots becomes

$\exists y \in \mathbb{Z}, 1 + y = 2$. Does there exist such a y ? Yes, take $y = 1$ (because by algebra if $1 + y = 2$, then we must have $y = 2 - 1$.) So when $x = 1$, we found that the \dots was true. But we can't stop there, because in a *for all* statement, we have to check all possible values of x .

Then we go to the next value $x = 2$. Then the \dots becomes

$\exists y \in \mathbb{Z}, 2 + y = 2$. Does there exist such a y ? Yes, take $y = 2 - 2 = 0$. Notice the $y = 0$ we found this time is different from the $y = 1$ we found in the $x = 1$ case - that is allowed because the y comes after the universally quantified x .

$$\forall x \in \mathbb{N}, \exists y \in \mathbb{Z}, x + y = 2$$

In general, for any value of x , we can find a value y making $x + y = 2$ - just take $y = 2 - x$. So the final answer is that the statement

$$\forall x \in \mathbb{N}, \exists y \in \mathbb{Z}, x + y = 2$$

is a **true** statement.

The main point of this example is that an existentially (\exists) quantified variable y is allowed to depend on variable(s) that are quantified before it.

new example

Now let's switch the order of the \forall and \exists quantifiers and consider the different statement

$$\exists x \in \mathbb{N}, \forall y \in \mathbb{Z}, x + y = 2$$

Is it true or false?

To show it is true, we would have to find a specific fixed value of x such that for every value of y , we would have $x + y = 2$. But this is impossible. So the given statement is *false*.

example

Now let's consider the statement

$$\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, xy = 0$$

Is it true or false?

To show it is true, we would have to find a specific fixed value of x such that for every value of y , we would have $xy = 0$. The value $x = 1$ doesn't work (because then we would need that for all $y \in \mathbb{Z}$, we have $1 \cdot y = 0$, which is clearly false). But for a *there exists* statement, we just need to find one value of x that "works". And $x = 0$ works: $\forall y \in \mathbb{Z}, 0 \cdot y = 0$ is true. So the final answer is that the given statement

$$\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, xy = 0$$

is *true*.

Chapter 4: Elementary Number Theory and Methods of Proof

Chapter 4 Elementary Number Theory and Methods of Proof

109

4.1 Direct Proof and Counterexample I: Introduction 110

Definitions; Proving Existential Statements; Disproving Universal Statements by Counterexample; Proving Universal Statements; Directions for Writing Proofs of Universal Statements; Variations among Proofs; Common Mistakes; Getting Proofs Started; Showing That an Existential Statement Is False; Conjecture, Proof, and Disproof

4.2 Direct Proof and Counterexample II: Rational Numbers 127

More on Generalizing from the Generic Particular; Proving Properties of Rational Numbers; Deriving New Mathematics from Old

4.3 Direct Proof and Counterexample III: Divisibility 134

Proving Properties of Divisibility; Counterexamples and Divisibility; The Unique Factorization of Integers Theorem

4.4 Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem 144

Discussion of the Quotient-Remainder Theorem and Examples; *div* and *mod*; Alternative Representations of Integers and Applications to Number Theory; Absolute Value and the Triangle Inequality

4.5 Indirect Argument: Contradiction and Contraposition 154

Proof by Contradiction; Argument by Contraposition; Relation between Proof by Contradiction and Proof by Contraposition; Proof as a Problem-Solving Tool

4.6 Indirect Argument: Two Classical Theorems 163

The Irrationality of $\sqrt{2}$; Are There Infinitely Many Prime Numbers?; When to Use Indirect Proof; Open Questions in Number Theory

Prove

The *prove* a statement means to show/deduce that it is true. To *disprove* a statement means to show that it is false. One shows/deduces statements by using definitions, axioms (statements which we agree to assign a value of true), and previously proven statements, rules of inference.

Types of statements encountered in math:

1. $\exists x, P(x)$ (existence statement)
2. $\forall x, P(x)$ (universal or a for-all statement)
3. $\boxed{\forall x, P(x) \rightarrow Q(x)}$. (universal conditional). Most mathematical statements are of this form, and this chapter will be about techniques to prove them.

familiar definitions

Definition

1. An integer n is **even** if there exists an integer k such that $n = 2k$.
2. An integer n is **odd** if there exists an integer k such that $n = 2k + 1$.
3. An integer n is **prime** if $n > 1$, and if n factors into positive integers as $n = rs$, then r or s equals n . First few prime numbers are 2, 3, 5, 7, 11, 13, 17, There is no known formula that gives all the primes. Prime numbers are incredibly mysterious and fascinating to professional mathematicians to this day. One of the most important unsolved math problem (the Riemann hypothesis) is about them.
4. An integer n is **composite** if $n > 1$ and n factors as $n = rs$ with integers r, s with $1 < r < n$ and $1 < s < n$. First few composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, ...

$$\exists x \in D, P(x)$$

To prove an exists statement ($\exists x \in D, P(x)$), usually (but not always) the easiest way is to find a number x in the set D making the statement true:

Example

Prove $\exists a \in \mathbb{Z}, a + 1$ is prime. (read as *There exists an a in the set of integers such that $a + 1$ is prime*).

Solution: Take $a = 1$ (or $2, 4, \dots$). Then $1 + 1 = 2$ which is prime.

Done.

But there are existence statements that are easier to prove indirectly (i.e. without finding a specific number); we'll talk about indirect proofs at the end of chapter 4, but let me just give here an example:

Example

The following is a true statement, but the easiest way to prove it is not by finding a example:

"There exists a prime number bigger than 2^{85} trillion"

(As of 2018, largest known prime number that computers have found is about 2^{85} million, but we will prove in this chapter there exist bigger ones, but we won't be able to say exactly what they are! In other words, we will prove an existence statement without actually saying exactly what the prime number is!

Existence statement $\exists x \in D, P(x)$

Back to an easy existence statement and proof:

Example

Prove that there exists an integer a greater than or equal to 3, such that $a^2 - 1$ is composite.

Solution: Take $a = 3$ (or 4, 5, ...). Then

$$a^2 - 1 = 3^2 - 1 = 9 - 1 = 8, \text{ which is composite. Done.}$$

Universal statement $\forall x \in D, P(x)$

Now let's change the there exists to a for all:

Example

Prove that FOR ALL integers a greater than or equal to 3, such that $a^2 - 1$ is composite.

Bogus Solution: *Take $a = 3$ (or 4, 5, ...). Then*

$a^2 - 1 = 3^2 - 1 = 9 - 1 = 8$, which is composite. Done.

NOOOOO!!!! In a “for all” statement, it is not enough to pick a specific value to prove the statement.

Correct solution:

1. Let a be an arbitrary integer greater than or equal to 3. (*we are not picking a specific value!*)
2. $a^2 - 1 = (a + 1)(a - 1)$ is a factorization of $a^2 - 1$ as required in the definition of composite.

Method of Direct Proof for $\forall x \in D, P(x) \rightarrow Q(x)$

To prove a universal conditional statement i.e. one of the form

$$\boxed{\forall x \in D, P(x) \rightarrow Q(x)} \quad (\text{read as for all } x \text{ in } D, \text{ if } P(x) \text{ then } Q(x))$$

begin with the following steps

1. Let $x \in D$ be arbitrary (you are not allowed to pick a specific value of x !!)
2. Assume x is such that $P(x)$ is true. (we can do this because if x makes $P(x)$ false, then $P(x) \rightarrow Q(x)$ is $F \rightarrow Q(x)$ which is *true* - recall conditional/arrow is always true except in tunafish $T \rightarrow F$ case - so there is nothing more to do).
3. Work to show $Q(x)$ is true.

example

Prove that for all integers a , if a is even, then a^3 is even.

Proof

- ▶ Let a be an arbitrary integer.
- ▶ Assume a is even. So $a = 2k$ for some integer k .
- ▶ $a^3 = (2k)(2k)(2k) = 8k^3$
- ▶ $a^3 = 2(4k^3)$ so a^3 is even.



example

Prove that if a and b are both even integers, then ab is an even integer.

Two possible interpretations:

1. $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}$, if a and b are both even integers, then ab is even.
2. $\exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}$, if a and b are even, then ab is even.

The intended interpretation is (1) because proving (2) is too easy. So let's prove the statement (1), by writing down statements we know are true.

Prove

$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}$, if a and b are both even integers, then ab is even.

Proof:

- ▶ Let a, b be arbitrary integers.
- ▶ Assume a and b are even integers.
- ▶ $a = 2k$ for some integer k (definition of a is even)
- ▶ $b = 2l$ for some integer l (definition of b is even). The letter k was already taken in previous line, so we have to use a different letter.
- ▶ $ab = (2k)(2l)$
- ▶ $ab = 2(2kl)$ so ab is even.



Disproving a statement means showing it is false

. To show a statement is false is equivalent to showing its negation is true.

So take its negation, remembering

- ▶ \forall changes to \exists and vice versa
- ▶ $\neg(p \rightarrow q) \equiv p \wedge \neg q$
- ▶ $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- ▶ $\neg(p \wedge q) \equiv \neg p \vee \neg q$

and use proof techniques we just discussed.

example

Disprove the following statement: *For all integers n , if n is even then $n + 1$ is prime*

Solution. Disprove means prove negation is true, so first take the negation, so we want to show:

There exists $n \in \mathbb{Z}$ such that n is even and $n + 1$ is not prime.

This is a \exists -statement, so easiest to try finding an n . Many choices are possible, for example $n = 8$. (but not $n = 2$ or $n = 3$).

Prove or disprove

Example

Prove or disprove the following statement: *For all integers n , if n is even then $3n + 2$ is even*

Solution: The statement is a *for all* statement, so picking a number is not enough for a proof. However, privately picking a few numbers to get an idea of if the statement is true is fine if you don't know immediately how to get started. $n = 1, 2, 3 \dots$ all give true statements. (For $n = 1$, the statement becomes $F \rightarrow F$, which is true. Odd values of n will obviously make the statement true, so really we are only interested in even values). So we try proving the statement.

Proof:

- ▶ Let n be an arbitrary integer.
- ▶ Assume n is even. So $n = 2k$ for some integer k .
- ▶ We want to show $3n + 2$ is even.
- ▶ $3n + 2 = 3(2k) + 2 = 2(3k + 1)$ is even.



Prove or disprove

Example

Prove or disprove the following statement: *For all integers n , if $n \geq 1$ then $6n - 1$ is a prime number*

Solution: The statement is a *for all* statement, so picking a number is not enough for a proof. However, privately picking a few numbers to get an idea of if the statement is true is fine if you don't know immediately how to get started.

$n = 1, 2, 3, 4, 5$, the numbers $6n - 1$ are $5, 11, 17, 23, 29$, which are all prime. So you might suspect the statement is true. But for $n = 6$, we get $6n - 1 = 35 = 5 \times 7$, which is not prime! So we have found a **counterexample** (a number showing that a universal (i.e. for all) statement is false). Remember there is no simple formula that gives just primes.

example continued

So we disprove the statement: *For all integers n , if $n \geq 1$ then $6n - 1$ is a prime number*

Solution: The disprove means show negation is true, so first we need to find negation,

Use

$$\neg(\forall n \in \mathbb{Z}, P(n) \rightarrow Q(n)) \quad \equiv \quad \exists n \in \mathbb{Z}, P(n) \wedge \neg Q(n)$$

So we need to prove *There exists integer n such that $n \geq 1$ and $6n - 1$ is not prime number*

Proof:

$n = 6$ gives $6n - 1 = 35 = 5 \times 7$ which is not prime.



4.2 Direct proof II: Rational Numbers

Definition

1. A real number r is a **rational number** if it is a **ratio of two integers** a and b with $b \neq 0$:

$$r = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$$

2. A real number that is not rational is called **irrational**.

The set of rational number is denoted \mathbb{Q} (q for quotient; recall \mathbb{R} is the set of real numbers).

Examples of rational numbers are $\frac{1}{2}, \frac{-1}{3}, 0 = \frac{0}{1}, 1 = \frac{1}{1}$.

Any integer n is a rational number as $n = \frac{n}{1}$.

Examples of irrational numbers are $\pi, e, \sqrt{2}, \sqrt{3}, \dots$ we will see in Chapter 7 that there are many more irrational numbers than rational numbers.

Example 1

Prove that the sum of two rational numbers is a rational number.

You can't pick specific rational numbers because the question really means sum of ANY two rational numbers. In other words, we have to prove a "for all" statement.

Pick variables - for example r, s - to denote the two arbitrary rational numbers.

We have to prove:

$$\forall r \in \mathbb{Q}, \forall s \in \mathbb{Q}, r + s \text{ is rational}$$

Prove

$$\forall r \in \mathbb{Q}, \forall s \in \mathbb{Q}, r + s \text{ is rational}$$

Proof

1. Let r and s be arbitrary rational numbers.
2. $r = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ (by definition that r is rational)
3. $s = \frac{c}{d}$, $c, d \in \mathbb{Z}, d \neq 0$ (by definition that s is rational)
- 4.

$$\begin{aligned}r + s &= \frac{a}{b} + \frac{c}{d} \\&= \frac{ad}{bd} + \frac{bc}{bd} \quad \text{make common denominator} \\&= \frac{ad + bc}{bd}\end{aligned}$$

which shows that $r + s$ is rational since we have expressed $r + s$ as a ratio of two integers $ad + bc$ and bd , and $bd \neq 0$ since $b \neq 0$ and $d \neq 0$.

Example 2

Prove that the product of any two rational numbers is a rational number.

Proof:

1. Let r and s be arbitrary rational numbers.
2. $r = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ (by definition that r is rational)
3. $s = \frac{c}{d}$, $c, d \in \mathbb{Z}, d \neq 0$ (by definition that s is rational)
4. $rs = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. So rs is rational (since it is a ratio of two integers ac, bd with $bd \neq 0$.)

Example 3

Once we have proven certain statements, we can use them in subsequent proofs:

Example

Prove that for all rational numbers r, s , the number $3r + 4s$ is rational.

Proof:

1. Let r, s be arbitrary rational numbers.
2. $3 = \frac{3}{1}$ is a rational number.
3. $3r$ is rational since we have proved that a product of rational numbers is rational.
4. $4s$ is rational (same reason as above)
5. $3r + 4s$ is rational since a sum of rational number is rational.



What about irrational numbers?

It's hard to work directly with irrational numbers because we can't turn them into an equation like $r = \frac{a}{b}$ for rational numbers r . We will see later in chapter 4 how to prove statements about them using *indirect* proofs. But here's something we can do now:

Disprove the (false) statement:

"For any two real numbers, if they are both irrational then their sum is irrational."

Disprove means prove the negation of the statement is true.

The statement to disprove can be written as

$\forall r \in \mathbb{R}, \forall s \in \mathbb{R}$, if r and s are irrational, then $r + s$ is irrational.

To find its negation, we switch the \forall 's to \exists 's and use

$\neg(p \rightarrow q) \equiv p \wedge \neg q$, to get:

$\exists r \in \mathbb{R}, \exists s \in \mathbb{R}$, r and s are irrational AND $r + s$ is RATIONAL

So the statement we want to prove is:

$$\exists r \in \mathbb{R}, \exists s \in \mathbb{R}, \text{ } r \text{ and } s \text{ are irrational AND } r + s \text{ is RATIONAL}$$

It is an existence statement, so we are allowed to pick specific numbers. Many choices work. For example take $r = \pi, s = -\pi$. Then $\pi + -\pi = 0$ is an example of two irrational numbers $\pi, -\pi$ adding to a rational number 0. (On the other hand, it is apparently still unknown if $\pi + e$ is irrational or rational!)

4.3 Direct Proof III: Divisibility

Definition

Let n and d be integers, with $d \neq 0$. We introduce a predicate $d | n$, read “ d divided n ”. We assign $d | n$ a value of

- ▶ true if n/d is an integer
- ▶ false if n/d is not an integer

$$d | n \iff \frac{n}{d} \in \mathbb{Z}$$

If $d | n$ is true, we say any of the following things are true:

1. d divides n
2. d is a factor of n
3. d is a divisor of n
4. n is a multiple of d

Example:

- ▶ $3 \mid 15$ is true, since $\frac{15}{3} = 5 \in \mathbb{Z}$
- ▶ $15 \mid 3$ is false, since $\frac{3}{15} = \frac{1}{5} = 0.2 \notin \mathbb{Z}$.
So $15 \nmid 3$ is true.

We write $d \nmid n$ (read d does not divide n) to mean $\neg(d \mid n)$, or equivalently $\frac{n}{d} \notin \mathbb{Z}$.

Note $d \mid n$ and d/n are completely different things despite looking very similar:

- ▶ $d \mid n$ has a value of true or false (once d and n are chosen) according to $\frac{n}{d} \in \mathbb{Z}$ or not,
- ▶ $d/n = \frac{d}{n}$ is a rational number (assuming $n \neq 0$).

Direct proofs involving divisibility

Example 1.

Prove that for all integers a, b, c , if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof.

1. Let a, b, c be arbitrary integers.
2. Assume $a \mid b$ and $b \mid c$ are true.
3. (Want to show $a \mid c$ i.e. $\frac{c}{a} \in \mathbb{Z}$)
4. So $\frac{b}{a} = k$ and $\frac{c}{b} = l$ for some $k, l \in \mathbb{Z}$.
5. So $b = ak$ and $c = bl$.
6.
$$\frac{c}{a} = \frac{bl}{a} = \frac{(ak)l}{a} = kl \in \mathbb{Z}$$
7. So $a \mid c$. □



Example 2

Prove: For all integers a, b , if $3 \mid (a + b)$ then $3 \mid (4a - 5b)$.

Proof:

1. Let a, b be arbitrary integers.
2. Assume $3 \mid (a + b)$.
3. (Want to show $3 \mid (4a - 5b)$).
4. $\frac{a+b}{3} \in \mathbb{Z}$, so $a + b = 3k$ for some integer k .
5. So $a = 3k - b$.
- 6.

$$\begin{aligned}4a - 5b &= 4(3k - b) - 5b \\&= 12k - 4b - 5b \\&= 12k - 9b \\&= 3(4k - 3b)\end{aligned}$$

7. So $3 \mid (4a - 5b)$.



Fundamental Theorem of Arithmetic

Here is a theorem that just says you can factor any integer $n > 1$ into a product of primes:

Theorem (Fundamental Theorem of Arithmetic/ Unique Factorization of Integers)

Given any integer $n > 1$, there exists a positive k and distinct prime numbers p_1, p_2, \dots, p_k and positive integers e_1, e_2, \dots, e_k such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and any other expression for n as a product of prime numbers is identical tho this except, perhaps, for the order in which the factors are written.

Example

Take $n = 48$ and keep factoring it: $48 = 2 \cdot 24 = 2 \cdot 2 \cdot 12 = \dots$ and eventually we get

$$48 = 2^4 \cdot 3^1$$

Section 4.4 Direct proof IV: Quotient Remainder Theorem and Modular Arithmetic

When you divide an integer n by 2, the possible remainders are 0 or 1; and these give rise to the two cases of even or odd integers. In this section, we extend this idea by replacing 2 by other positive integers.

For example, when you divide a integer n by 3, the possible remainders are 0, 1, 2. If there is a larger remainder, you can divide n by more copies of 3 to (eventually) get a remainder of 0, 1, or 2.

Quotient Remainder Theorem

More generally, when you divide an integer n by an integer $d \geq 1$, you get a (possibly zero) remainder r satisfying $0 \leq r \leq d - 1$. This is the content of the *Quotient-Remainder Theorem*.

Theorem (Quotient-Remainder Theorem)

Given any integer n and a positive integer d , there are unique integers q (called the quotient) and r (called the remainder) such that

$$n = dq + r \quad \text{and} \quad 0 \leq r \leq d - 1$$

example $n=14$, $d=3$

What equation does the quotient-remainder theorem give when $n = 14$ is divided by $d = 3$?

In other words, we need to find integers q, r such that $14 = 3q + r$, and $0 \leq r \leq 2$. To find q , we calculate $\frac{14}{3} = 4.666\dots$

Hence we must have $q = \lfloor 4.666 \rfloor \dots = 4$.

Here $\lfloor x \rfloor$ is the “floor function”, also known as the greatest integer function, gives the greatest/largest integer less than or equal to x .

Once $q = 4$, since we solve $14 = 3q + r$ for r to get $14 - 12 = r$.

So the quotient remainder theorem says

$$14 = 3 \cdot 4 + 2$$

which in words says when 14 divided by 3, the quotient is 4 and the remainder of 2.

example $n=-14$, $d=3$

The integer n can be negative in the quotient remainder theorem. Note that if we multiply the answer from the previous example by -1 we get

$$-14 = 3(-4) + (-2)$$

While that is a true equation, the value of $r = -2$ does not satisfy $0 \leq r \leq 2$, and so it not what the quotient remainder theorem says.

Instead we divide $n = -14$ by $d = 3$, we get $\frac{-14}{3} = -4.666$ and once again the quotient $q = \lfloor -4.666 \rfloor \dots = -5$.

(Note $\lfloor -4.666 \rfloor \dots = -5$ since -5 is largest integer less than or equal to -4.666 - the answer is not -4 since -4 is bigger than -4.666).

Then $r = n - dq = -14 - 3(-5) = -14 + 15 = 1$. So the quotient remainder theorem says

$$-14 = 3(-5) + 1$$

Modular arithmetic

Definition (mod)

Let $d > 0$ be an integer. We write

$$a \equiv b \pmod{d}$$

and say “ a and b are equivalent mod d ”, if any of the following equivalent conditions are true.

1. $d|(a - b)$ (d divides $a - b$)
2. $a - b = dk$ for some integer k .
3. $a = b + dk$ for some integer k .
4. a and b differ by a multiple of d , e.g. you can get to b by starting from a and repeatedly adding or subtracting multiples of d .

Our textbook uses the notation $a \pmod{d} = b$ to mean $a \equiv b \pmod{d}$ and $0 \leq b \leq d - 1$, i.e. b is the remainder when a is divided by d .

example

1. Find numbers that are equivalent to $14 \bmod 3$.

Solution: (lots of correct answers) we have

$$14 \equiv 11 \equiv 8 \equiv 5 \equiv 2 \equiv -1 \bmod 3$$

Also $14 \equiv 17 \equiv 20 \bmod 3$. Our book would write
 $14 \bmod 3 = 2$.

2. Consider $14 \bmod 4$. We have

$$14 \equiv 10 \equiv 6 \equiv 2 \equiv -2 \equiv -6 \bmod 4$$

Our book would write $14 \bmod 4 = 2$.

3. if $n = dq + r$ then $n \equiv r \bmod d$. In words, n is equivalent mod d to its remainder r upon division by d .

example

1. Find $1000 \bmod 7$ i.e. find the remainder when 1000 is divided by 7.

Solution:

$$1000 \equiv 1000 - 700 \bmod 7$$

$$= 300 \bmod 7$$

$$\equiv 300 - 280 \bmod 7 \quad (\text{since } 280 = 28 \cdot 10 = 7 \cdot 4 \cdot 10 \text{ is a multiple of 7})$$

$$= 20 \bmod 7$$

2. If today is Wednesday, what day of the week will it be 1000 days from today?

Answer: above calculation tells us $1000 \equiv 6 \equiv -1 \bmod 7$, so the answer is Tuesday.

Modular Arithmetic Theorem

So modular arithmetic basically focuses on the *remainders* after dividing by d . Here's why it is useful ... roughly, mod respects the basic operations of arithmetic:

Theorem (Modular arithmetic theorem)

Suppose $a \equiv a' \pmod{d}$ and $b \equiv b' \pmod{d}$. Then

1. $a + b \equiv a' + b' \pmod{d}$
2. $a - b \equiv a' - b' \pmod{d}$
3. $ab \equiv a'b' \pmod{d}$
4. $a^n \equiv (a')^n \pmod{d}$ for any positive integer n .

example

Before giving a proof, let's see how this modular arithmetic theorem can be useful:

Find the remainder when 2017×2019 is divided by 5, without multiplying out 2017×2019

Solution: The question is asking us to consider remainders after dividing by 5, i.e. it's asking us to work mod 5. So

$$2017 \equiv 2 \pmod{5}$$

(think about why - basically because 2015 is a multiple of 5 and 2017 is 2 more than it) and

$$2019 \equiv 4 \pmod{5}$$

The theorem allows us to replace 2017 and 2019 by their remainders 2 and 4 when working mod 5. Hence

$$2017 \cdot 2019 \equiv 2 \cdot 4 = 8 \equiv 3 \pmod{5}$$

So the answer is 3.

example

Prove that the square of any integer has the form $4k$ or $4k + 1$ for some integer k . In other words, $n^2 \equiv 0$ or $1 \pmod{4}$. We say that 0 and 1 are the **quadratic residues mod 4**

Proof: Let n be an arbitrary integer. The question is asking us to show that $n^2 \equiv 0$ or $1 \pmod{4}$.

The idea is to consider the possibilities for $n \pmod{4}$: We have $n \equiv 0, 1, 2$ or $3 \pmod{4}$ (by quotient remainder theorem). Hence the modular arithmetic theorem tells us that

$n^2 \equiv 0^2, 1^2, 2^2$, or $3^2 \pmod{4}$. These squares are $0, 1, 4, 9$, and $\pmod{4}$ these are $0, 1, 0, 1$ (the last one is from $9 \pmod{4} = 1$).

example

Here a typical application of how modular considerations are used in elementary number theory.

Prove that there are no integers x, y such that $x^2 + y^2 = 2019$.

Proof: The trick is to consider the equation mod4 (the first several times you this trick you might feel it comes out of nowhere ... but it is employed so often that it becomes a standard thing to do in number theory).

We have

$$2019 = 2016 + 3 \equiv 3 \pmod{4}$$

since $2016 = 4(504)$ is a multiple of 4.

Suppose there were integers x, y such that $x^2 + y^2 = 2019$. Then mod4 this equation becomes

$$x^2 + y^2 \equiv 3 \pmod{4}$$

But x^2, y^2 can only be equivalent to 0 or 1 mod 4, so there is no way any of the four numbers $0+0, 0+1, 1+0, 1+1$ add up to 3, so the equation $x^2 + y^2 \equiv 3 \pmod{4}$ can't be satisfied.

Proof of the modular arithmetic theorem

Proof: Suppose $a \equiv a' \pmod{d}$ and $b \equiv b' \pmod{d}$. Then $a = a' + dk$ and $b = b' + dl$ for some integers k, l . Then

1.

$$a + b = (a' + dk) + (b' + dl) = a' + b' + d(k + l)$$

so $a + b \equiv a' + b' \pmod{d}$.

2.

$$a - b = (a' + dk) - (b' + dl) = a' - b' + d(k - l)$$

so $a - b \equiv a' - b' \pmod{d}$.

3.

$$ab = (a' + dk)(b' + dl) = a'b' + a'dl + dk b' + d^2 kl = a'b' + d(a'l + kb' + dkl)$$

so $ab \equiv a'b' \pmod{d}$.

4. a^n is multiplication of a with itself n times, so the claim that $a^n \equiv (a')^n \pmod{d}$ follows from the fact that equivalence mod d is preserved under multiplication.

example

Prove that for all integers a, b if $a \bmod 7 = 4$ and $b \bmod 7 = 6$, then $ab \bmod 7 = 3$.

Proof: By the modular arithmetic theorem, we have
 $ab \equiv 4 \cdot 6 = 24 \bmod 7$. Working mod 7, we have

$$24 \equiv 17 \equiv 10 \equiv 3 \bmod 7$$

Section 4.5 Indirect Argument: Contradiction and Contraposition

Sometimes direct proof won't work, and we have to take an indirect approach. There are two indirect approaches: proof by contradiction, and proof by contraposition.

Summary of proof techniques

To prove

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x)$$

1. Direct proof: Assume $P(x)$ is true, work to show $Q(x)$ is true
2. Proof by Contrapositive: Assume $\neg Q(x)$ is true, work to show $\neg P(x)$ is true.
3. Proof by Contradiction: Assume $P(x)$ and $\neg Q(x)$ are both true (for some $x \in D$). Work to come up with a statement that is both true and false.

Proof by Contradiction

Recall that a statement is true or false but not both.

Suppose we want to show a certain statement S is true.

In proof by contradiction,

1. we assume the statement S is *false* (equivalently, its negation $\neg S$ is true)
2. we show (somehow) that this assumption (that $\neg S$ is true) leads us to conclude that **some other statement S' is both true and false**.

Equivalently, **both S' and $\neg S'$ are true**. When this happens, we say *we have reached a contradiction*.

3. But a statement cannot both be true and false, so we conclude that our original assumption that S was false was incorrect, and so S is must be true.

It is usually not clear when beginning the proof what the statement S' that gives rise to contradiction will be! That's what makes proof by contradiction a bit tricky.

Proof by contradiction is useful when

1. you want to show there is *no* object satisfying a certain property (so the proof would begin, “Assume there exists such an object ...”)
2. you want to show that an object does *not* have a certain property (e.g. being rational number). So the proof would begin “Assume the object has that property. ”

example

Prove that the sum of any rational and any irrational number is irrational.

Proof:

1. Proof by contradiction.
2. The statement S we want to show is true is

For any rational number r , for any irrational number s , $r+s$ is irrational.

3. so we assume the negation $\neg S$ is true:

There exists rational number r , there exists irrational number s , $r+s$ is not irrational.

4. r rational
5. s irrational
6. $r+s$ rational
7. The difference (as well as sum or product) of two rational numbers is rational (proved in section 4.3)
8. So $s = (r+s) - r$ is rational since it is the difference of two rational numbers.
9. We have contradiction: s is irrational, and s is rational.
10. (So the statement S must be true.)

example

Prove that for all integers m, n , if mn is even, then m is even or n is even.

Proof:

1. Proof by contradiction.
2. So we form the negation and assume it's true:
3. There exist integers m, n such that mn is even and m is odd and n is odd (note we are used $\neg(p \rightarrow q) \equiv p \wedge \neg q$, and $\neg(p \vee q) \equiv \neg p \wedge \neg q$)
4. m odd
5. n odd
6. mn even
7. Product of odd integers is odd (proved in section 4.1, or by modular arithmetic theorem working mod2: being odd is being 1 mod 2, so $mn \equiv 1 \cdot 1 = 1 \text{ mod } 2$) so m odd and n odd imply mn is odd.
8. We have a contradiction: mn is odd and mn is even.

As a special case ($m = n$) of the theorem we just proved we record the following result for use in the next section on irrationality of $\sqrt{2}$:

Theorem

For all integers n , if n^2 is even then n is even.

Proof by Contraposition

The second technique of indirect proof is called *Proof by Contrapositive*, and is easier - it is simply **direct proof applied to the contrapositive** of a conditional (i.e. if-then) statement. Recall in chapters on logic we saw via a truth table that the contrapositive is logically equivalent to the original conditional statement.

Proof by Contraposition

To prove

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x)$$

1. Take the contrapositive:

$$\forall x \in D, \text{ if } \neg Q(x) \text{ then } \neg P(x)$$

2. Then use Direct Proof strategy on the contrapositive, meaning:
3. Let $x \in D$ be arbitrary.
4. Assume $\neg Q(x)$ is true.
5. Goal: work to show $\neg P(x)$ is true.

Note that in proof by contrapositive, there is a clear goal: show $\neg P(x)$ is true.

By contrast in proof by contradiction, the goal - to find a statement S' that is both true and false - is often not clear at the outset what S' will turn out to be.

example

Here's an example we did by contradiction; now let's do it by contrapositive:

For all integers m, n , if mn is even, then m is even or n is even.

Proof:

1. Proof by contrapositive. Form the contrapositive:

For all integers m, n , if $\neg(m \text{ is even or } n \text{ is even})$ then mn is odd.

\equiv *For all integers m, n , if m is odd AND n is odd then mn is odd.*

2. Let m, n be arbitrary integers.
3. Assume m is odd and n is odd.
4. (Want to show mn is odd.)
5. We have $m \equiv 1 \pmod{2}$ and $n \equiv 1 \pmod{2}$, so by modular arithmetic theorem, $mn \equiv 1 \cdot 1 = 1 \pmod{2}$, i.e. mn is odd.

example

Prove by contraposition:

If the sum of two real numbers is less than 60, then at least one of the numbers is less than 30.

1. Proof by contrapositive. The contrapositive is:

If two numbers are both greater than or equal to 30, then their sum is greater than or equal to 60.

2. Let x, y be two numbers and assume $x \geq 30$ and $y \geq 30$.
3. Then $x + y \geq 30 + 30 = 60$.

Section 4.6: Two famous indirect proofs

In this section, proof by contradiction can be used to give famous and elegant proofs of the following two facts:

1. The $\sqrt{2}$ is irrational
2. There are infinitely many prime numbers

Theorem

$\sqrt{2}$ is irrational.

Traditional proof:

1. Proof by contradiction. Assume $\sqrt{2}$ is rational.
2. So

$$\sqrt{2} = \frac{a}{b}$$

where $a, b \in \mathbb{Z}$ and $b \neq 0$

3. We can assume further that $\frac{a}{b}$ is a reduced fraction, i.e. a and b have greatest common divisor of 1.
4. Squaring both sides and clearing denominators we have

$$\sqrt{2} = \frac{a}{b}$$

$$2 = \frac{a^2}{b^2}$$

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

5. $2b^2$ is even, therefore a^2 is even.

Proof continued

6. Since a^2 is even, a is even by a previous theorem.
7. So $a = 2a_1$ for some $a_1 \in \mathbb{Z}$. So we get

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

$$2b^2 = (2a_1)^2$$

$$2b^2 = 4a_1^2$$

$$b^2 = 2a_1^2$$

8. Since $2a_1^2$ is even, the last equation tells us that b^2 is even.
9. Once again, since b^2 is even, we conclude b is even.
10. So a and b are both even, they have a common factor of 2, contradicting the earlier statement that a and b have gcd 1.

□

Second proof of irrationality of $\sqrt{2}$

Here is a second proof (similar to the previous one) but we use the **fundamental theorem of arithmetic**, which says that any positive integer has a *unique* factorization into powers of distinct primes (up to order the prime powers are listed).

Theorem

$\sqrt{2}$ is irrational.

Proof.

1. Proof by contradiction. Assume $\sqrt{2}$ is rational.
2. So

$$\sqrt{2} = \frac{a}{b}$$

where $a, b \in \mathbb{Z}$ and $b \neq 0$

3. Squaring both sides and clearing denominators we have

$$\sqrt{2} = \frac{a}{b}$$

$$2 = \frac{a^2}{b^2}$$

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

- In the equation $2b^2 = a^2$ consider the exponent of 2 in the prime factorization of each side.
- The exponent of 2 in a^2 will be even, since it will be twice the exponent of 2 in prime power factorization a :

$$a = 2^x \cdot 3^y \cdot 5^z \dots$$

$$a^2 = (2^x \cdot 3^y \cdot 5^z \dots)^2 = 2^{\boxed{2x}} 3^{2y} 5^{2z} \dots$$

- The exponent of 2 in prime factorization of $2b^2$ will be odd (because it will 1 plus the even exponent of 2 in b^2).

$$b = 2^x 3^y 5^z \dots$$

$$2b^2 = 2(2^x 3^y 5^z \dots)^2 = 2^{\boxed{2x+1}} 3^{2y} 5^{2z} \dots$$

- To summarize: exponent of 2 in prime factorization of $2b^2$ is **odd**, while in a^2 it is **even**. But $a^2 = 2b^2$ are the same number, and we have found two different prime factorizations of it. This contradicts uniqueness of the prime factorizations guaranteed by fundamental theorem of arithmetic.

The previous proof generalizes easily to the following result

Theorem

Let m, n be positive integers. Then the n -th root of m

$$\sqrt[n]{m}$$

is irrational unless m is an n -th power of an integer (i.e. $m = a^n$ for some $a \in \mathbb{Z}$)

For example, $\sqrt[3]{2}, \sqrt{3}, \sqrt{6}, \sqrt[4]{12}, \sqrt{15} \dots$ are irrational
but $\sqrt[3]{8}, \sqrt{16}$ are (obviously) rational as they are integers.

Show that $\sqrt{3} + \sqrt{5}$ is irrational. Proof

1. Proof by contradiction. Assume $\sqrt{3} + \sqrt{5}$ is rational.
2. So $\sqrt{3} + \sqrt{5} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$, $b \neq 0$.
3. Squaring plus some algebra to solve for the $\sqrt{15}$ gives

$$\sqrt{3} + \sqrt{5} = \frac{a}{b}$$

$$(\sqrt{3} + \sqrt{5})^2 = \frac{a^2}{b^2}$$

$$3 + 2\sqrt{3}\sqrt{5} + 5 = \frac{a^2}{b^2} \quad \text{since } (x + y)^2 = x^2 + 2xy + y^2$$

$$3 + 2\sqrt{15} + 5 = \frac{a^2}{b^2}$$

$$2\sqrt{15} = \frac{a^2}{b^2} - 3 - 5$$

$$\sqrt{15} = \frac{1}{2} \left(\frac{a^2}{b^2} - 3 - 5 \right)$$

4. Look at last equation. Left hand side $\sqrt{15}$ is irrational (by previous theorem), while right hand side is rational.
Contradiction.

example

Prove that $\log_2 3$ is irrational.

Proof:

1. Proof by contradiction. Assume $\log_2 3$ is rational.
2. So $\log_2 3 = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$, $b \neq 0$. Since $\log_2 3$ is positive (in fact, greater than 1 since $\log_2 2 = 1$), we can further assume a, b are both *positive* integers.
- 3.

$$\log_2 3 = \frac{a}{b}$$

$$3 = 2^{a/b} \quad \text{definition of } \log_2$$

$$3^b = (2^{a/b})^b$$

$$3^b = 2^a$$

4. Last line $3^b = 2^a$ contradicts unique prime factorization of the integer $3^b = 2^a$.

Here is a second very famous proof by contradiction, due to Euclid.

Theorem

The set of prime numbers is infinite.

Proof

1. Proof by contradiction. Assume that the set of prime numbers is finite.
2. So some prime number p is the largest, and we can list *all* the prime numbers:
 $2, 3, 5, \dots, p$

3. **The ingenious trick is to consider the number**

$$N = (2 \cdot 3 \cdot 5 \cdots p) + 1$$

4. By prime factorization of integers, there must be a prime q dividing N .
5. But because $2 \cdot 3 \cdot 5 \cdots p$ includes q somewhere in there, N is one more than a multiple of q . I.e. N has remainder of 1 when divided by q .
6. To summarize: N is divisible by q , yet also N is not divisible by q , a contradiction.

Summary of proof techniques

To prove

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x)$$

1. Direct proof: Assume $P(x)$ is true, work to show $Q(x)$ is true
2. Proof by Contrapositive: Assume $\neg Q(x)$ is true, work to show $\neg P(x)$ is true.
3. Proof by Contradiction: Assume $P(x)$ and $\neg Q(x)$ are both true (for some $x \in D$). Work to come up with a statement that is both true and false.

Chapter 5: Sequences, Mathematical Induction, and Recursion

Chapter 5 Sequences, Mathematical Induction, and Recursion 171

5.1 Sequences 171

Explicit Formulas for Sequences; Summation Notation; Product Notation; Properties of Summations and Products; Change of Variable; Factorial and n Choose r Notation

5.2 Mathematical Induction I 185

Principle of Mathematical Induction; Sum of the First n Integers; Proving an Equality; Deducing Additional Formulas; Sum of a Geometric Sequence

5.3 Mathematical Induction II 199

Comparison of Mathematical Induction and Inductive Reasoning; Proving Divisibility Properties; Proving Inequalities; A Problem with Trominoes

5.4 Strong Mathematical Induction and the Well-Ordering Principle for the Integers 209

Strong Mathematical Induction; Binary Representation of Integers; The Well-Ordering Principle for the Integers

5.5 Defining Sequences Recursively 222

Definition of Recurrence Relation; Examples of Recursively Defined Sequences; Recursive Definitions of Sum and Product

5.6 Solving Recurrence Relations by Iteration 236

The Method of Iteration; Using Formulas to Simplify Solutions Obtained by Iteration; Checking the Correctness of a Formula by Mathematical Induction; Discovering That an Explicit Formula Is Incorrect

5.1 Sequences

Let m, n be two integers with $m < n$ and in this chapter let

$[m, n]$ be the set of *integers* (not real numbers) starting from m and ending at n .

So for example $[2, 5] = \{2, 3, 4, 5\}$.

Let $[m, \infty)$ be the set of integers greater than or equal to m . So for example, $[2, \infty) = \{2, 3, 4, 5, 6, \dots\}$

Definition (Sequence)

1. A **sequence** is just a list of numbers, e.g. $2, 3, -1, \frac{3}{2}, \dots$
2. It can be finite or infinite list, and the order the numbers are listed in matters - different order means a different sequence.
3. More abstractly a **sequence** (of real numbers) is a function $a : [m, n] \rightarrow \mathbb{R}$ or a function $a : [m, \infty) \rightarrow \mathbb{R}$. This is the book's definition, and is correct and precise, but not really the way we think about sequences (see below).
4. Instead of using the function notation $a(x)$ for the function/sequence a , we use subscript notation a_k to denote the value of $a(k) \in \mathbb{R}$.
5. Instead of writing $a : [m, n] \rightarrow \mathbb{R}$ we write instead

$$(a_k)_{k=m}^n$$

6. We think of a sequence $(a_k)_{k=m}^n$ as a finite list of numbers

$$a_m, a_{m+1}, \dots, a_n$$

7. We think of a sequence $(a_k)_{k=m}^{\infty}$ as an infinite list of real numbers

$$a_m, a_{m+1}, \dots,$$

8. The subscript k in a_k is called the **index**, and the set $[m, n]$ or $[m, \infty)$ is called the **indexing set**.

example

Let $(a_k)_{k=-1}^5$ be the sequence defined by

$$a_k = 2^k$$

for $k \in [-1, 5]$ (for example). Then a is the sequence of numbers

$$a_{-1}, a_0, a_1, a_2, a_3, a_4, a_5$$

$$\frac{1}{2}, 1, 2, 4, 8, 16, 32$$

where $a_{-1} = 2^{-1} = \frac{1}{2}$, $a_0 = 2^0 = 1$, $a_1 = 2$, \dots , $a_5 = 2^5 = 32$.

This was an example of a sequence given by a formula.

Fibonacci sequence

Here is an famous example of a sequence defined *recursively*: the Fibonacci Sequence Let $(f_k)_{k=0}^{\infty}$ be the sequence defined by

- ▶ $f_0 = 1$
- ▶ $f_1 = 1$
- ▶ For $k \geq 2$, $f_k = f_{k-1} + f_{k-2}$

The last condition says that the k th term of the sequence is the sum of the previous two terms. So $f_2 = f_1 + f_0 = 1 + 1 = 2$ and so on. So the terms of the Fibonacci sequence are

$$1, 1, 2, 3, 5, 8, 13, 21, \dots$$

Summation Notation

Let $(a_k)_{k=0}^{\infty}$ or a_0, a_1, \dots be a sequence. Often times we will want to find the sum of a bunch of terms of the sequence, for example $a_0 + a_1 + a_2 + \dots + a_5$, or maybe $a_2 + a_4 + a_6 + \dots + a_{20}$. We use summation notation involving the symbol \sum as a shorthand to avoid writing \dots and also to specify the precisely the terms of the sequence we are adding.

Definition

Here is the definition of $\sum_{k=\ell}^m a_k$:

$$\sum_{k=\ell}^m a_k = a_\ell + a_{\ell+1} + a_{\ell+2} + \dots + a_{m-1} + a_m$$

In words, we add up the numbers a_k where k starts at the number ℓ appearing below the \sum , and ends at the number m appearing above the \sum , and increases by 1 each time.

Some examples of summation notation

$$\sum_{k=0}^5 a_k = a_0 + a_1 + a_2 + \cdots + a_5$$

$$\sum_{k=1}^6 a_{k-1} = a_0 + a_1 + a_2 + \cdots + a_5$$

$$\sum_{k=1}^{10} a_{2k} = a_2 + a_4 + a_6 + \cdots + a_{20}$$

Product Notation

Product notation \prod is basically the same idea as summation notation \sum but instead of adding a bunch of terms, we are interested in *multiplying* the terms together:

Definition

Here is the definition of $\prod_{k=\ell}^m a_k$:

$$\prod_{k=\ell}^m a_k = a_\ell \cdot a_{\ell+1} \cdot a_{\ell+2} \cdots a_{m-1} \cdot a_m$$

In words, we *multiply* the numbers a_k where k starts at the number ℓ below the \prod , and ends at the number m above the \prod , and increases by 1 each time.

example: factorials $n!$

For a positive integer n , define **n -factorial** by

$$n! = \prod_{k=1}^n k = 1 \cdot 2 \cdots n$$

For example $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

It turns out to be very useful to define $0! = 1$ (in particular, $0!$ is not 0).

Arithmetic Sequence

Definition

An **arithmetic sequence** with first term a_1 and common difference d is a sequence $(a_k)_{k=1}^{\infty}$ such that

$$a_{k+1} = a_k + d$$

for all integers $k \geq 1$. In words, we get each successive term by adding the same number d to the previous term.

Example

The arithmetic sequence with first term 3 and common difference 5 is

$$3, 8, 13, 18, \dots$$

The arithmetic sequence with first term 1 and common difference 1 is

$$1, 2, 3, 4, \dots$$

Story: In 1800s, an elementary school teacher wanted to keep his/her class busy for a while and asked them to add up the integers beginning at 1 and ending at 100, i.e. find the value of

$$\sum_{k=1}^{100} k = 1 + 2 + 3 + \dots + 99 + 100$$

The teacher was surprised when after a few moments, a student named Carl Gauss (who would end up becoming a great mathematician) found the answer!

Gauss' trick

Let $S = 1 + 2 + 3 + \dots + 99 + 100$ be the number we want to find.
The number S is also the sum of the numbers from 100 down to 1:

$$S = 1 + 2 + 3 + \dots + 99 + 100$$

$$S = 100 + 99 + 98 + \dots + 2 + 1$$

Add these two equations to get

$$2S = (1 + 100) + (2 + 99) + (3 + 98) + \dots + (99 + 2) + (100 + 1)$$

$$2S = 101 + 101 + 101 + \dots + 101 + 101$$

$$2S = 101 \times 100$$

$$S = 101 \cdot \frac{100}{2} = 101 \cdot 50 = \boxed{5050}$$

We can use this trick to find a formula for the sum of the first n terms of an arithmetic sequence:

Theorem

Let $(a_k)_{k=1}^{\infty}$ be an arithmetic sequence with first term a_1 and common difference d . Let a_n denote the n term, and let

$S_n = \sum_{k=1}^n a_k = a_1 + a_2 + \dots + a_n$ denote the sum of the first n terms. Then

$$a_n = a_1 + (n - 1)d$$

$$S_n = \frac{(a_1 + a_n)}{2}n$$

Section 5.2: Mathematical Induction

Let $\mathbb{Z}_{\geq 0} = \{x \in \mathbb{Z} \mid x \geq 0\} = \{0, 1, 2, 3, \dots\}$ denote the set of non-negative integers, ordered by the usual order:
 $0 < 1 < 2 < 3 < \dots$.

Mathematical Induction is a principle/technique to prove statements roughly of the form

$$\forall n \in \mathbb{Z}_{\geq 0}, P(n)$$

Typical examples of statements that we will see can be proven by mathematical induction are

1.

$$\forall n \in \mathbb{Z}_{\geq 0}, \sum_{j=0}^n j = \frac{n(n+1)}{2}$$

2. For all positive integers n ,

$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

3. For all integers $n \geq 3$, we have $2n+1 < 2^n$.

First, let's recall the truth table of an if-then statement:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

So if you know $p \rightarrow q$ is true, you cannot conclude p and/or q are true - they could both be false, while $p \rightarrow q$ is true!

Before explaining what mathematical induction is, let me ask question that I hope will help understand the logic behind mathematical induction:

question

Let $P(n)$ be some predicate (it doesn't matter exactly what) where the domain of n is $\mathbb{Z}_{\geq 0}$. So $P(n)$ might be true for some values of n , and false for some other values of n . Suppose we know the following three statements are all true:

- (a) $P(3)$ is true
- (b) $P(4)$ is false
- (c) for all integers $n \geq 0$, if $P(n)$ is true, then $P(n + 2)$ is true.

Question: For what values of n can you conclude that $P(n)$ is true? For what values of n can you conclude $P(n)$ is false? For what values of n do you not have enough information to decide the truth value of $P(n)$?

Answer

Recall (c) is “for all integers $n \geq 0$, if $P(n)$ is true, then $P(n + 2)$ is true.”

1. $P(3)$ is true is given.
2. Plug in $n = 3$ into (c), we know the statement " $P(3) \rightarrow P(3 + 2)$ " is true, i.e. " $P(3) \rightarrow P(5)$ " is true.
3. Hence $P(5)$ is true (by modus ponens, or because if $P(5)$ was false, then $P(3) \rightarrow P(3 + 2)$ would be of the form $T \rightarrow F$, which has truth value false).
4. We can then repeat the process: we know $P(5) \rightarrow P(7)$ is true (set $n = 5$ in (c)), and also now know $P(5)$ is true, hence $P(7)$ is true.
5. Continuing in this way, we see that $P(9), P(11), P(13), \dots$ are true.
6. **More precisely, $P(n)$ is true for all odd integers $n \geq 3$.**

What about $P(1)$? We know $P(1) \rightarrow P(3)$ is true, i.e. $P(1) \rightarrow T$ is true. But this does not allow us to figure out the truth value of $P(1)$, because $F \rightarrow T$ and $T \rightarrow T$ both have truth value true, so $P(1)$ could be true or it could be false. There is not enough information given.

Answer continued

For what values of n can we conclude $P(n)$ is false?

Recall (c) is “for all integers $n \geq 0$, if $P(n)$ is true, then $P(n + 2)$ is true.”

1. We are given $P(4)$ false.
2. If we try and plug in $n = 4$ into (c) we get “If $P(4)$ then $P(6)$ ” has truth value true. This becomes $F \rightarrow P(6)$ is true, but this does not allow us to conclude the exact truth value of $P(6)$ since $F \rightarrow T$ and $F \rightarrow F$ both have truth value true. To summarize, $n = 4$ into (c) gave us no information.
3. Let’s plug in $n = 2$ into (c). Then we get $P(2) \rightarrow P(4)$ is true; we are given $P(4)$ is false, and so $P(2)$ is false by modus tollens (or noticing by truth table that $P(2) \rightarrow F$ being true forces $P(2)$ to be false).
4. Similarly, we know $P(0) \rightarrow P(2)$ is true, and now we know $P(2)$ is false, so $P(0)$ is false.
5. To summarize, the answer is $P(0), P(2), P(4)$ are false.

Finally, there is not enough information to figure out the truth values of $P(n)$ for even integers $n \geq 6$ or for $n = 1$.

Question again

Let's do a similar question that is precisely the hypothesis of mathematical induction:

Suppose we know the following three statements are all true:

- (a) $P(0)$ is true
- (b) for all integers $n \geq 0$, if $P(n)$ is true, then $P(n + 1)$ is true.

Question: For what values of n can you conclude that $P(n)$ is true?

Answer

1. $P(0)$ is true is given
2. $P(0) \rightarrow P(1)$ is true (plug in $n = 0$ into (b)),
3. hence by modus ponens $P(1)$ is true.
4. Now repeat the process: we know $P(1) \rightarrow P(2)$ is true (plug in $n = 1$ into (b)), and $P(1)$ is true, so hence by modus ponens $P(2)$ is true.
5. And so on. We see that $P(n)$ is true for all values of $n \geq 0$.

Mathematical Induction principle

Let's summarize this as a theorem:

Theorem (Principle of Mathematical Induction)

Let $P(n)$ be a predicate, where the domain of n is $\mathbb{Z}_{\geq 0}$. The following if-then statement is true:

If

1. $P(0)$ is true
2. $\forall n \in \mathbb{Z}_{\geq 0}, P(n) \rightarrow P(n + 1)$ is true

then

$$\forall n \in \mathbb{Z}_{\geq 0}, P(n)$$

So to prove

$$\forall n \in \mathbb{Z}_{\geq 0}, \quad P(n)$$

by mathematical induction, follow these steps:

1. (Base case) Show $P(0)$ is true (generally very easy by direct calculation).
2. (Inductive step) Show the following if-then statement is true, by direct proof:

$$\text{"}\forall n \in \mathbb{Z}_{\geq 0}, \text{ if } P(n) \text{ then } P(n + 1)\text{"}$$

- 2.1 Let $n \in \mathbb{Z}_{\geq 0}$ be arbitrary integer.
- 2.2 Assume $P(n)$ is true.
- 2.3 Work to show $P(n + 1)$ is true. A rule of thumb: if $P(n + 1)$ is an equation or inequality, start from *one* side, write down things you know are true, until you get to the other side.

Summary

To prove

$$\forall n \in \mathbb{Z}_{\geq 0}, \quad P(n)$$

by mathematical induction, follow these steps:

1. (Base case) Show $P(0)$ is true (generally very easy by direct calculation).
2. (Inductive step) Let $n \in \mathbb{Z}_{\geq 0}$ be arbitrary but fixed integer. (You are not allowed to pick a specific number for n ; it will remain some unspecified number throughout the proof).
3. Assume $P(n)$ is true (not for all n , but only for the unspecified value of n appearing in the previous step. In particular, we cannot assume $P(n + 1)$ is true!! That's what we are trying to prove).
4. Work to show $P(n + 1)$ is true. A rule of thumb: if $P(n + 1)$ is an equation or inequality, start from *one* side, write down things you know are true, until you get to the other side.

example

Prove by mathematical induction that

$$\forall n \in \mathbb{Z}_{\geq 0}, \sum_{j=0}^n j = \frac{n(n+1)}{2}$$

In other words, $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Let $P(n)$ be the predicate (i.e. true or false depending on n)

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

We have to show that $P(n)$ is actually true for *all* values of non-negative integers n

proof

1. Proof by mathematical Induction
2. Base case: $P(0)$ is the statement $\sum_{j=0}^n j \stackrel{?}{=} \frac{n(n+1)}{2}$. The left hand side is 0, while the right hand side is $\frac{0 \cdot 1}{2} = 0$. So $P(0)$ becomes $0 \checkmark = 0$ which is true.
3. Let $n \in \mathbb{Z}_{\geq 0}$ be arbitrary integer.
4. Assume $P(n)$ is true, i.e. assume

$$\sum_{j=0}^n j \stackrel{?}{=} \frac{n(n+1)}{2}$$

(the checkmark is not necessary but I use it to emphasize we know/assume the equation is true)

5. We want to show $P(n + 1)$ is true, i.e. that the following equation is true:

$$\sum_{j=0}^{n+1} j \stackrel{?}{=} \frac{(n+1)(n+1+1)}{2}$$

Notice how we replaced each instance of n in $P(n)$ by $n + 1$. Also the $\stackrel{?}{=}$ indicates we do not know yet that the equation is true.

- Start with *one* (not both!) sides of $P(n+1)$. Let's start with $\sum_{j=0}^{n+1} j$, which when written out is $0 + 1 + 2 + \cdots + n + (n+1)$
- The idea is to split off the last summand $n+1$

$$\sum_{j=0}^{n+1} j \stackrel{?}{=} \left(\sum_{j=0}^n j \right) + (n+1)$$

The reason we do this is we have we somehow should use our assumption that $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

- 8.

$$\begin{aligned}\sum_{j=0}^{n+1} j &= \left(\sum_{j=0}^n j \right) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1)\end{aligned}$$

9. The goal is to end up with the right hand side of $P(n + 1)$, i.e. with $\frac{(n+1)(n+1+1)}{2}$, or $\frac{(n+1)(n+2)}{2}$ which has an $(n + 1)$ factored out. So let's factor out an $(n + 1)$ in the last line of the previous step

$$\begin{aligned}\sum_{j=0}^{n+1} j &\stackrel{\checkmark}{=} \left(\sum_{j=0}^n j \right) + (n + 1) \\ &\stackrel{\checkmark}{=} \frac{n(n + 1)}{2} + (n + 1) \\ &\stackrel{\checkmark}{=} (n + 1) \left(\frac{n}{2} + 1 \right) \\ &\stackrel{\checkmark}{=} (n + 1) \left(\frac{n}{2} + \frac{2}{2} \right) \\ &\stackrel{\checkmark}{=} (n + 1) \left(\frac{n + 2}{2} \right)\end{aligned}$$

To summarize, we have shown $P(n + 1)$ is true:

$$\sum_{j=0}^{n+1} j \leq \frac{(n+1)(n+1+1)}{2}$$

so by the principle of mathematical induction we have proven the statement

$$\forall n \in \mathbb{Z}_{\geq 0}, \sum_{j=0}^n j = \frac{n(n+1)}{2}$$

example

Prove by mathematical induction that

$$\forall n \in \mathbb{Z}_{\geq 1}, \sum_{j=1}^n j^2 = \frac{n(n+1)(2n+1)}{6}$$

In other words, $1^2 + 2^2 + 3^2 \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof by mathematical Induction

- Let $P(n)$ be the predicate

$$\sum_{j=1}^n j^2 = \frac{n(n+1)(2n+1)}{6}$$

- Base case: $P(1)$ is the statement $\sum_{j=1}^1 j^2 \stackrel{?}{=} \frac{n(n+1)(2n+1)}{6}$. The left hand side is $1^2 = 1$, while the right hand side is $\frac{1 \cdot 2 \cdot (2 \cdot 1 + 1)}{6} = \frac{6}{6} = 1$. So $P(1)$ becomes $1 \stackrel{?}{=} 1$ which is true.
- Let $n \in \mathbb{Z}_{\geq 1}$ be arbitrary fixed but unspecified integer.
- Assume $P(n)$ is true for our fixed unspecified value of n , i.e. assume

$$\sum_{j=1}^n j^2 \stackrel{?}{=} \frac{n(n+1)(2n+1)}{6}$$

- We want to show $P(n+1)$ is true, i.e. that the following equation is true:

$$\sum_{j=1}^{n+1} j^2 \stackrel{?}{=} \frac{(n+1)(n+1+1)(2(n+1)+1)}{6}$$

Notice how we replaced each instance of n in $P(n)$ by $n+1$. Also the $\stackrel{?}{=}$ indicates we do not know yet that the equation is true.

6. Start with *one* (not both!) sides of $P(n+1)$. Let's start with $\sum_{j=1}^{n+1} j^2$, which when written out is $1^2 + 2^2 + \cdots + n^2 + (n+1)^2$
7. The idea is to split off the last summand $(n+1)^2$

$$\sum_{j=1}^{n+1} j^2 \leq \left(\sum_{j=1}^n j^2 \right) + (n+1)^2$$

The reason we do this is we have somehow should use our assumption that $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

8.

$$\begin{aligned} \sum_{j=1}^{n+1} j^2 &= \left(\sum_{j=1}^n j^2 \right) + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \end{aligned}$$

9. The goal is to end up with the right hand side of $P(n+1)$, i.e. with $\frac{(n+1)(n+1+1)(2(n+1)+1)}{6}$, or $\frac{(n+1)(n+2)(2n+3)}{6}$ which has an $(n+1)$ factored out. So let's factor out an $(n+1)$ in the last line of the previous step

$$\begin{aligned}
\sum_{j=1}^{n+1} j^2 &\stackrel{\checkmark}{=} \left(\sum_{j=1}^n j^2 \right) + (n+1)^2 \\
&\stackrel{\checkmark}{=} \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&\stackrel{\checkmark}{=} (n+1) \left(\frac{n(2n+1)}{6} + (n+1) \right) \\
&\stackrel{\checkmark}{=} (n+1) \left(\frac{2n^2 + n}{6} + \frac{6n + 6}{6} \right) \\
&\stackrel{\checkmark}{=} (n+1) \left(\frac{2n^2 + 7n + 6}{6} \right) \\
&\stackrel{\checkmark}{=} (n+1) \left(\frac{(n+2)(2n+3)}{6} \right)
\end{aligned}$$

To summarize, we have shown $P(n + 1)$ is true:

$$\sum_{j=1}^{n+1} j^2 \leq \frac{(n+1)(n+1+1)(2(n+1)+1)}{6}$$

so by the principle of mathematical induction we have proven the statement

$$\forall n \in \mathbb{Z}_{\geq 0}, \sum_{j=1}^n j^2 \leq \frac{n(n+1)(2n+1)}{6}$$

example

For all integers $n \geq 3$, we have $2n + 1 < 2^n$.

Proof by mathematical Induction

1. Base case $n = 3$. We need to determine if $2(3) + 1 < 2^3$. Left hand side is 7, while right hand sides is 8 and indeed $7 < 8$.
2. Let $n \geq 3$ be an arbitrary integer.
3. Assume $2n + 1 < 2^n$ for that specific but unspecified value of n .
4. We want to show $2(n + 1) + 1 < 2^{n+1}$. Let's start with the left hand side $2(n + 1) + 1$ and write down inequalities we know for sure are true, and eventually try to end up with the right hand side 2^{n+1} .
- 5.

$$\begin{aligned}2(n + 1) + 1 &= 2n + 2 + 1 \\&= 2n + 1 + 2 \\&< 2^n + 2 \quad \text{by our assumption } 2n + 1 < 2^n \\&< 2^n + 2^n \quad \text{since } 2 < 2^n \\&= 2 \cdot 2^n = 2^{n+1}\end{aligned}$$

6. To summarize $2(n + 1) + 1 < 2^{n+1}$, which is what we wanted to show.

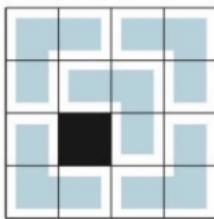
Mathematical Induction is a versatile principle can be used in problems besides those involving sums and inequalities.

A L-shaped tromino is like a domino but consists of three squares



in a shape of L:

The following picture shows that if a particular square (shaded in black) is removed from a 4×4 checkerboard, the remaining squares can be completely covered by L-shaped trominoes (blue), without any overlap.

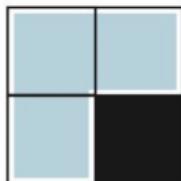


It turns out that induction can be used to prove the following tiling result:

Prove that for any integer $n \geq 1$, if *any* single square is removed from a $2^n \times 2^n$ checkerboard, the remaining squares can be completely covered by L-shaped trominoes (without any overlap).

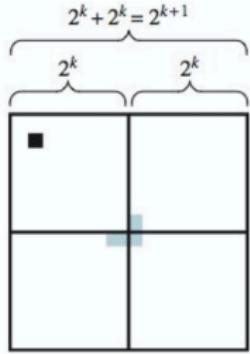
proof

1. Proof by mathematical induction,
2. Base case $n = 1$. We have to show that a 2×2 checkerboard with one square removed can be covered with a tromino. Yes, exactly one tromino will do the job; for example if the removed square is the one in the lower right, the picture is:



3. (Inductive step). Let $n \geq 1$ be an arbitrary fixed integer. Assume we can tile (i.e. cover without overlaps) a $2^n \times 2^n$ checkerboard that has any one square removed with L-shaped trominoes.
4. Suppose we are given a $2^{n+1} \times 2^{n+1}$ checkerboard with one square removed. We have to show it can be tiled by L-shaped trominos.

- Divide the $2^{n+1} \times 2^{n+1}$ into four $2^n \times 2^n$ smaller checkerboards. The missing tile is going to be in one of the four $2^n \times 2^n$ checkerboards.
- Place a L-shaped tromino at the center of the big $2^{n+1} \times 2^{n+1}$ checkerboard so that it covers one square of each of the three other $2^n \times 2^n$ sub-checkerboards.



- Now we can apply the inductive hypothesis: the four $2^n \times 2^n$ sub-checkerboards each have a square we don't have to cover, so by the inductive hypothesis they can be tiled by L-shaped trominos. Then we get a tiling of the whole $2^{n+1} \times 2^{n+1}$ checkerboard.

Turn in next time

Epp Section 5.3 exercise 34

34. a. Use mathematical induction to prove that any checkerboard with dimensions $2 \times 3n$ can be completely covered with L-shaped trominoes for any integer $n \geq 1$.
- b. Let n be any integer greater than or equal to 1. Use the result of part (a) to prove by mathematical induction that for all integers m , any checkerboard with dimensions $2m \times 3n$ can be completely covered with L-shaped trominoes.

Section 5.4 Strong mathematical Induction

There is a slight variant of mathematical induction called “strong” induction (although it turns out to be logically equivalent usual mathematical induction), where in the inductive step,

- ▶ instead of assuming only $P(n)$ is true (and then working to show $P(n + 1)$ is true),
- ▶ we assume something (seemingly) stronger - namely that $P(0), P(1), \dots, P(n - 1), P(n)$ are *all* true,
- ▶ and then as before working to show $P(n + 1)$ is true.

Strong Mathematical Induction summary

To prove

$$\forall n \in \mathbb{Z}_{\geq 0}, \quad P(n)$$

by **strong** mathematical induction, follow these steps:

1. (Base case) Show $P(0)$ is true (generally very easy by direct calculation).
2. (Inductive step begins) Let $n \in \mathbb{Z}_{\geq 0}$ be arbitrary but fixed integer. (You are not allowed to pick a specific number for n ; it will remain some unspecified number throughout the proof).
3. (Inductive hypothesis/assumption) Assume $P(0), P(1), \dots, P(n)$ are **all** true (not for all n , but only for the unspecified value of n appearing in the previous step. In particular, we cannot assume $P(n + 1)$ is true!! That's what we are trying to prove).
4. Work to show $P(n + 1)$ is true.

Strong induction can be useful for problems involving recurrence relations and representation problems.

By a representation problem, I mean problems where you are asked to show how to represent something (like a number) in a particular manner. For example, here is a theorem we saw in chapter 4 but did not prove:

Theorem (Fundamental Theorem of Arithmetic - existence part)

Any integer greater than 1 can be written as a product of prime numbers (or is prime itself - which we consider a product of primes).

proof

1. Proof by strong mathematical induction.
2. Base case $n = 2$: since 2 is prime itself, so we are done.
3. Let $n > 1$ be an arbitrary integer. Assume all the integers from 2 up through n can be written as a product of primes or are prime themselves (inductive hypothesis).
4. Consider the number $n + 1$. If $n + 1$ is prime, then we are done, there is nothing to prove.
5. If $n + 1$ is not prime, then it can be factored $n + 1 = ab$ where $1 < a < n + 1$ and $1 < b < n + 1$ are integers greater than 1 and less than $n + 1$.
6. Hence by the inductive hypothesis, a and b can be written as a product of primes (or are prime themselves). Then $n + 1 = ab$ can be written as a product of primes by multiplying together the representations of a and b as products of primes.

Here is an example with recurrence relations:

Example

Define a sequence $(a_n)_{n=0}^{\infty}$ by

$$a_0 = 2$$

$$a_1 = 8$$

$$a_n = 8a_{n-1} - 15a_{n-2} \quad \text{for all } n \geq 2$$

Prove by strong induction that for all integers $n \geq 0$, $a_n = 3^n + 5^n$.

proof

1. Proof by strong mathematical induction.
2. Base case $n = 0$. Then $a_0 = 2$ and $3^0 + 5^0 = 1 + 1 = 2$, so we indeed have $a_0 = 3^n + 5^n$.
3. Let $n \geq 0$ be an integer. Assume $a_k = 3^k + 5^k$ for all integers k with $0 \leq k \leq n$.
4. We want to show $a_{n+1} \stackrel{?}{=} 3^{n+1} + 5^{n+1}$.
5. If $n + 1 = 1$ then $a_1 = 8$ and $3^{n+1} + 5^{n+1} = 3 + 5 = 8$ so we are done. (We have to treat the case $n + 1 = 1$ separately since the recurrence relation $a_n = 8a_{n-1} - 15a_{n-2}$ requires $n \geq 2$).

6. So we may assume $n + 1 \geq 2$, in which case we may use the recurrence relation:

$$a_{n+1} = 8a_{(n+1)-1} - 15a_{(n+1)-2} = 8a_n - 15a_{n-1}$$

7. We now use the inductive hypothesis that $a_n = 3^n + 5^n$ and $a_{n-1} = 3^{n-1} + 5^{n-1}$ (notice that *strong* induction allows us to assume the last equation).

$$\begin{aligned}a_{n+1} &= 8a_n - 15a_{n-1} \\&= 8(3^n + 5^n) - 15(3^{n-1} + 5^{n-1}) \\&= 3^{n-1}(8 \cdot 3 - 15) + 5^{n-1}(8 \cdot 5 - 15) \quad (\text{factored out } 3^{n-1} \text{ & } 5^{n-1}) \\&= 3^{n-1}(9) + 5^{n-1}(25) \\&= 3^{n-1}(3^2) + 5^{n-1}(5^2) \\a_{n+1} &\stackrel{\checkmark}{=} 3^{n+1} + 5^{n+1}\end{aligned}$$

The theory (as opposed to practice) behind principle of Mathematical Induction

Recall mathematical Induction is a principle/technique to prove statements roughly of the form

$$\forall n \in \boxed{\mathbb{Z}_{\geq 0}}, P(n)$$

- ▶ The crucial point is that the domain of n is the *non-negative* integers (or minor variants, like positive integers $\mathbb{Z}_{\geq 1}$, or $\mathbb{Z}_{\geq 3}$).
- ▶ Mathematical induction typically does not apply to statements $\forall x \in D, P(x)$ where the domain D of x is \mathbb{Z}, \mathbb{Q} , or \mathbb{R} .
- ▶ There is a special property called the Well-Ordering Principle, that (mathematicians assume) the set $\mathbb{Z}_{\geq 0}$ has; it is clear that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (each with their usual ordering of numbers) don't have this property:

Well-Ordering Principle

Well-Ordering Principle/Axiom Every non-empty subset S of $\mathbb{Z}_{\geq 0}$ has a smallest/least element.

- ▶ By contrast, not every non-empty subset of \mathbb{Z} , \mathbb{Q} , or \mathbb{R} (each with their usual order) has a least element.
- ▶ For example, \mathbb{Z} itself does not have a least element:
 $-1 > -2 > -3, \dots$ are smaller and smaller numbers.
- ▶ The subset of positive rational numbers also does not have a smallest element - if $r \in \mathbb{Q}_{>0}$ is a positive rational number, then $\frac{r}{2}$ is a smaller positive rational number.

Assuming the Well-Ordering Principle of $\mathbb{Z}_{\geq 0}$, we can prove the following Principle of Mathematical Induction. (And if we assume the Principle of Mathematical Induction as an axiom, then we can prove the Well Ordering Principle. So the two statements are equivalent).

Theorem (Principle of Mathematical Induction)

Let $P(n)$ be a predicate, where the domain of n is $\mathbb{Z}_{\geq 0}$. The following if-then statement is true:

If

1. $P(0)$ is true
2. $\forall n \in \mathbb{Z}_{\geq 0}, P(n) \rightarrow P(n + 1)$ is true

then

$$\forall n \in \mathbb{Z}_{\geq 0}, P(n)$$

proof

1. Proof by Contradiction. We assume the negation of what we want to show (which is an if-then statement); using $\neg(p \rightarrow q) \equiv p \wedge \neg q$, we assume

1.1 $P(0)$ is true

1.2 $\forall n \in \mathbb{Z}_{\geq 0}, P(n) \rightarrow P(n + 1)$ is true

1.3 **and**

$$\exists n \in \mathbb{Z}_{\geq 0}, \neg P(n) \text{ is true.}$$

2. Let

$$S = \{n \in \mathbb{Z}_{\geq 0} \mid \neg P(n) \text{ (is true)}\}$$

be the set of non-negative integers n for which $\neg P(n)$ is true, or equivalently $P(n)$ is false.

3. Part (c) says that S is non-empty.
4. By the Well-ordering principle, S has a smallest element, call it n_0 .
5. So $P(n_0)$ is false (since $n_0 \in S$)

proof continued

6. n_0 cannot equal 0 since $P(0)$ is true by part (a).
7. Since $n_0 \geq 1$, we have $n_0 - 1 \in \mathbb{Z}_{\geq 0}$
8. Also $n_0 - 1 \notin S$ since n_0 is smallest element in S .
9. So $P(n_0 - 1)$ is true (since $n_0 - 1 \notin S$).
10. Hence the if-then statement $P(n_0 - 1) \rightarrow P(n_0)$ is false because it is of the form $T \rightarrow F$. Contradiction to assumption (b).

Chapter 6 Set theory

section 6.1 Set theory: definitions and element method of proof

Set theory has become the underlying language of the mathematics: nearly all mathematical objects (e.g. numbers, functions, ordered pairs, etc) can be represented/constructed as a set.

Just like *sentence*, *true* and *false* are the undefined terms of logic, the undefined terms of set theory are

1. *set*
2. *element of*, denoted by the symbol \in

These two undefined terms interact with each other as follows:

Given two sets S, T , the sentence

$$S \in T \quad (\text{read "S is an element of } T\text{"})$$

is a statement (i.e. is either true or false but not both). Also, we define $S \notin T \equiv \neg(S \in T)$ and read it as S is not an element of T .

What is a set? That's a trick question - there is no answer as *set* is an undefined term. But mathematicians think of sets as a collection of objects; these objects themselves are sets. For example, these objects can be numbers (we will see shortly how numbers themselves are sets).

We use curly brackets $\{\}$ as the notation for a set, and within the brackets we list elements of the set, separated by commas.

$$S = \{\dots, x, \dots\} \iff x \in S \text{ is true}$$

Also given a set S and a predicate $P(x)$ with domain S , we are allowed to define a new set

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

whose elements are those elements x of S such that $P(x)$ is true. The vertical line $|$ is read “such that”.

Equality of sets

Definition

We say two sets S, T are **equal**, and write $S = T$, if they have the same elements:

$$S = T \iff \forall x, x \in S \leftrightarrow x \in T$$

Here the biconditional “ \leftrightarrow ” is defined by

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ and has the following truth table:

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

So $p \leftrightarrow q$ is true if p, q have the same truth values (i.e. p, q are both true or both false); $p \leftrightarrow q$ is false if p, q have different truth values.

The definition of equality of sets given above implies that the order which elements are listed in does not matter, and repeatedly listed elements are the same as the set where those elements are listed once. Here are some examples (the $::=$ means “define”):

1. $A := \{1, 2\} = \{2, 1\} = \{1, 1, 1, 2\}$ is a set with 2 (distinct) elements.
2. $B := \{3, A\} = \{3, \{1, 2\}\}$ is a set with 2 elements; the elements are 3 and A . Note that $2 \in B$ is false i.e. 2 is not an element of B , although 2 is an element of A . Meanwhile $A \in B$ and $3 \in B$ are both true.
3. $\{2\}$ and $\{\{2\}\}$ both have a single element but are not equal sets. The statements $2 \notin \{\{2\}\}$ and $\{2\} \in \{\{2\}\}$ are true.

numbers as sets

1. $\emptyset := \{\}$ (empty set) is a set with no elements
2. Define $0 := \emptyset = \{\}$ so the number 0 is a set!
3. Define $1 := \{0\} = \{\emptyset\}$ is a set with one element; so the number 1 is a set.
4. $2 := \{0, 1\} = \{\underbrace{\emptyset}_0, \underbrace{\{\emptyset\}}_1\}$ is a set with two elements
5. $3 := \{0, 1, 2\} = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{\underbrace{\emptyset}_0, \underbrace{\{\emptyset\}}_1, \underbrace{\{\emptyset, \{\emptyset\}\}}_2\}$
6. Given a set n , define the successor set

$$S(n) = n \cup \{n\}$$

where we add one more element to the set n , namely the set n . So $3 = S(2)$.

7. $\mathbb{N} := \{0, 1, 2, \dots\}$ is defined as the smallest set containing 0 and closed under the successor function S . This means that if $n \in \mathbb{N}$ then $S(n) \in \mathbb{N}$.

Subsets

Definition

Given two sets S, T ,

1. we say S is a **subset** of T , and write $S \subseteq T$ is true, if all elements of S are also elements of T :

$$S \subseteq T \iff \forall x, x \in S \rightarrow x \in T$$

2. We write $S \not\subseteq T$ (and say S is not a subset of T) to mean $\neg(S \subseteq T)$, the negation of $S \subseteq T$. Recalling that $\neg(p \rightarrow q) \equiv p \wedge \neg q$, we see that

$$S \not\subseteq T \iff \exists x, x \in S \wedge x \notin T$$

3. Notice that $(S = T) \iff (S \subseteq T) \wedge (T \subseteq S)$. So a very common strategy for showing two sets S, T are equal is to show $S \subseteq T$ and $T \subseteq S$.

example

\in and \subseteq are different.

$\{2\} \in \{\{2\}\}$ is true but $\{2\} \subseteq \{\{2\}\}$ is false since $2 \notin \{\{2\}\}$.
 $n \in S(n)$ and $n \subseteq S(n)$ are both true, where $S(n) = n \cup \{n\}$.

example

Let $A = \{n \in \mathbb{Z} \mid n \equiv 2 \pmod{4}\}$ and $B = \{n \in \mathbb{Z} \mid n/2 \in \mathbb{Z}\}$. Show that $A \subseteq B$ and $B \not\subseteq A$

Proof:

1. First we show $A \subseteq B$. We have to show $\forall x, x \in A \rightarrow x \in B$.
2. Use direct proof. Assume $x \in A$. Want to show $x \in B$.
3. By definition of $x \in A$, we have $x \equiv 2 \pmod{4}$, so $x = 2 + 4k$ for some integer k .
4. Then $x/2 = 1 + 2k \in \mathbb{Z}$, so $x \in B$. Done.
5. Next we show $B \not\subseteq A$. We have to show $\exists x, x \in B \wedge x \notin A$.
6. Take $x = 4$. Then $x \in B$ but $x \equiv 0 \pmod{4}$ so $x \notin A$.

New sets from old

Definition

Given two sets A, B that are subsets of some set U (for universal set) we define the sets

1. intersection:

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

2. union:

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

3. set minus:

$$A - B = \{x \in U \mid x \in A \wedge x \notin B\}$$

4. complement (in U)

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

We can take unions and intersections of more than two sets. Let I be a set, and suppose for each $i \in I$, we are given a set A_i ; that is a subset of some set U . So we have a collection/set/family of sets indexed by I (i.e. labelled by the elements of I).

Definition

1. Define the **union** of the $(A_i)_{i \in I}$ by

$$\bigcup_{i \in A} A_i := \{x \in U \mid \exists i \in I, x \in A_i\}$$

2. Define the **intersection** of the A_i by

$$\bigcap_{i \in A} A_i := \{x \in U \mid \forall i \in I, x \in A_i\}$$

Power set

Definition

Given a set A , there exists a set called the **power set**, denoted $\mathcal{P}(A)$, whose elements are all the subsets of A , including the empty set:

$$x \in \mathcal{P}(A) \iff x \subseteq A$$

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}$$

example

1. If $A = \{1, 2\}$ then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ has $2^2 = 4$ elements.
2. If $A = \emptyset$ has 0 elements, then $\mathcal{P}(A) = \{\emptyset\}$ has $2^0 = 1$ element.
3. In general, the power set of a set with n elements will have 2^n elements including the empty set (because to form a subset S of a set A , for each element $x \in A$, you can make 2 choices - either $x \in S$ or $x \notin S$).

ordered pairs

Recall that $\{a, b\} = \{b, a\}$, i.e. sets do not record the order of elements. Mathematicians use the round bracket notation (a, b) to denote *ordered pairs*, where order matters. For example, in the xy-coordinate system, the point $(3, 4)$ and $(4, 3)$ are different points. By definition, two ordered pairs (a, b) and (c, d) are **equal** if and only if $a = c$ and $b = d$.

(Caution: if a, b are real numbers, unfortunately we use the same notation (a, b) to denote the interval $(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$ of real numbers between a and b . This is completely different from the order pair. The context should tell you whether (a, b) means the ordered pair or the interval.)

Cartesian Product

Definition

Let A, B be two sets. The (Cartesian) **product** $A \times B$ is the set of ordered pairs:

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

Example

If $A = \{1, 2, 3\}$ and $B = \{x, y\}$ then

$$A \times B = \{(1, x), (2, x), (3, x), (1, y), (2, y), (3, y)\}$$

ordered n-tuples

One can generalize ordered pairs to ordered n-tuples (x_1, x_2, \dots, x_n) . Two n-tuples (x_1, x_2, \dots, x_n) and (y_1, y_2, \dots, y_n) are equal if and only if $x_1 = y_1, x_2 = y_2, \dots$ and $x_n = y_n$. And one can similarly define the Cartesian product $A_1 \times A_2 \times \dots \times A_n$ of n sets A_1, \dots, A_n :

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid \forall i \ a_i \in A_i\}$$

Theoretically, one can use sets to define ordered pairs as follows, but this is not really convenient in practice:

Definition (Not important)

Given two sets a, b define the **ordered pair** (a, b) to be the set

$$(a, b) := \{a, \{a, b\}\}$$

to be the underlying set of the ordered pair (a, b) .

Mathematicians don't really think about the ordered pair (a, b) in terms of its underlying set $\{a, \{a, b\}\}$! Instead they just use the following result:

Theorem

For any sets a, b, c, d , we have

$$(a, b) = (c, d) \iff a = c \text{ and } b = d$$

Section 6.2 Properties of Sets

Given two sets S, T , recall that $S \subseteq T$ means

$\forall x, x \in S \rightarrow x \in T$. Hence to prove $S \subseteq T$, use direct proof to show $\forall x, x \in S \rightarrow x \in T$:

To show $S \subseteq T$:

1. Assume $x \in S$ is arbitrary.
2. Work to show $x \in T$.

To show two sets S, T are equal $S = T$, use the above strategy to show $S \subseteq T$ and $T \subseteq S$.

example

Show that for all sets A, B, C ,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

(Distributive law for sets)

Proof:

1. First we show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.
2. Assume $x \in A \cup (B \cap C)$. We have to show $x \in (A \cup B) \cap (A \cup C)$
3. So $x \in A$ or $x \in B \cap C$ (by definition of union). We consider these two cases separately:
4. Case 1: $x \in A$. Then $x \in A \cup B$ and $x \in A \cup C$, and hence $x \in (A \cup B) \cap (A \cup C)$.
5. Case 2: $x \in B \cap C$. Then $x \in B$ and $x \in C$.
6. $x \in B$ implies $x \in A \cup B$, and similarly $x \in C$ implies $x \in A \cup C$.
7. Hence $x \in (A \cup B) \cap (A \cup C)$, completing Case 2.
8. So we have shown $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

9. Next we show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$
10. Let $x \in (A \cup B) \cap (A \cup C)$. We want to show $x \in A \cup (B \cap C)$.
11. We have $x \in A \cup B$ and $x \in A \cup C$.
12. If $x \in A$, then $x \in A \cup (B \cap C)$, so we may assume $x \notin A$.
13. $x \notin A$ and $x \in A \cup B$ imply $x \in B$ (by elimination).
14. Similarly $x \notin A$ and $x \in A \cup C$ imply $x \in C$ (by elimination).
15. So $x \in B$ and $x \in C$ imply $x \in B \cap C$, and hence
 $x \in A \cup (B \cap C)$.
16. So we have shown $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

example

Show $(A \cap B)^c = A^c \cup B^c$. (DeMorgan's law for sets).

Proof

1. First we show $(A \cap B)^c \subseteq A^c \cup B^c$.
2. Assume $x \in (A \cap B)^c$.
3. So

$$\begin{aligned}x \notin (A \cap B) &\equiv \neg(x \in A \cap B) \\&\equiv \neg(x \in A \wedge x \in B) \\&\equiv x \notin A \vee x \notin B \quad \text{De Morgan's law} \\&\equiv x \in A^c \vee x \in B^c \\&\equiv x \in A^c \cup B^c\end{aligned}$$

4. So $x \in A^c \cup B^c$. So we have shown $(A \cap B)^c \subseteq A^c \cup B^c$.

5. Next we show $A^c \cup B^c \subseteq (A \cap B)^c$.
6. Let $x \in A^c \cup B^c$. Reversing the steps above argument shows $x \in (A \cap B)^c$.

Definition

An empty set E is a set such that $\forall x, x \notin E$ (equivalently, $x \in E$ is false).

Here's a simple result: the empty set is a subset of every set:

Theorem

If E is an empty set and A is any set, then $E \subseteq A$.

proof

1. By definition of subset, to show $E \subseteq A$ we have to show $\forall x, x \in E \rightarrow x \in A$.
2. since E is an empty set, $x \in E$ is false, so $\forall x, x \in E \rightarrow x \in A$ becomes $\forall x, F \rightarrow x \in A$
3. Recall $F \rightarrow (\text{anything})$ is always true, so $\forall x, F \rightarrow x \in A$ is true.
4. Hence $\forall x, x \in E \rightarrow x \in A$ is true.

Proof by contradiction is often a good strategy for proving a certain set A is the empty set. To say A is empty set means $\forall x, x \notin A$. Assume the negation, i.e. $\exists x, x \in A$. Then somehow find a contradiction.

Example

Show that for any set A , $A \cap A^c = \emptyset$.

Proof.

1. Proof by contradiction. Assume $A \cap A^c \neq \emptyset$, and hence there exists $x \in A \cap A^c$.
2. Hence $x \in A$ and $x \in A^c$.
3. $x \in A^c$ means $x \in A$ is false. Contradicts $x \in A$ is true.



Section 6.3 Disproofs and Algebraic Proofs

Recall from logic chapters:

1. To disprove a statement means to show it is false, or equivalently, to show its negation is true.
2. The negation of $\forall x$, $P(x)$ is $\exists x$, $\neg P(x)$.
3. Hence to disprove $\forall x$, $P(x)$, we have to show/prove $\exists x$, $\neg P(x)$ is true.
4. To show a there exists statement $\exists x$, $\neg P(x)$ is true, try to come up with an example of a number (or in this chapter, set) x making $\neg P(x)$ true, or equivalently, $P(x)$ false.
5. A specific number/set/example for x making $P(x)$ false is called a **counterexample** to the universal statement $\forall x$, $P(x)$
6. It may be helpful to use Venn Diagrams to come up with counterexamples.

See the book for examples.

In the previous section, to show two sets S, T were equal, we proceeded by showing

1. $S \subseteq T$ and
2. $T \subseteq S$.

And to show $S \subseteq T$, we

1. let $x \in S$ be arbitrary element of S
2. work to show $x \in T$.

In other words, we gave an *element* based proof because we worked with an element $x \in S$.

In this section we illustrate how to use some basic set identities - that are easily established via element based proof - to give “algebraic” proofs of more complicated set identities.

Next slide is table 6.2.2 from p. 267 of our textbook, Discrete Mathematics by Susanna Epp consisting of some basic set identities. You do not have to memorize these.

Of these, perhaps 3, 9, and 12 are worth remembering, the others are somewhat obvious.

Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U .

1. *Commutative Laws:* For all sets A and B ,

(a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$.

2. *Associative Laws:* For all sets A , B , and C ,

(a) $(A \cup B) \cup C = A \cup (B \cup C)$ and
(b) $(A \cap B) \cap C = A \cap (B \cap C)$.

3. *Distributive Laws:* For all sets, A , B , and C ,

(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

4. *Identity Laws:* For all sets A ,

(a) $A \cup \emptyset = A$ and (b) $A \cap U = A$.

5. *Complement Laws:*

(a) $A \cup A^c = U$ and (b) $A \cap A^c = \emptyset$.

6. *Double Complement Law:* For all sets A ,

$(A^c)^c = A$.

7. *Idempotent Laws:* For all sets A ,

(a) $A \cup A = A$ and (b) $A \cap A = A$.

8. *Universal Bound Laws:* For all sets A ,

(a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$.

9. *De Morgan's Laws:* For all sets A and B ,

(a) $(A \cup B)^c = A^c \cap B^c$ and (b) $(A \cap B)^c = A^c \cup B^c$.

10. *Absorption Laws:* For all sets A and B ,

(a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$.

11. *Complements of U and \emptyset :*

(a) $U^c = \emptyset$ and (b) $\emptyset^c = U$.

12. *Set Difference Law:* For all sets A and B ,

$$A - B = A \cap B^c.$$

example [Epp p.285 #40]

Show algebraically (i.e. using table 6.2.2) that for all sets A, B, C ,

$$(A - B) - (B - C) = A - B$$

Proof: Start from **one** side (not both!) side of the equation we wish to show (usually the more complicated side) and use table 6.2.2 to write down true equations, until we reach the other side.

$$\begin{aligned}(A - B) - (B - C) &= (A - B) \cap (B - C)^c \quad (12) \\&= (A \cap B^c) \cap (B \cap C^c)^c \quad (12) \\&= (A \cap B^c) \cap (B^c \cup C) \quad (9b, 6) \\&= \left((A \cap B^c) \cap B^c \right) \cup \left((A \cap B^c) \cap C \right) \quad (3 \text{ Distrib}) \\&= \left(A \cap (B^c \cap B^c) \right) \cup \left((A \cap B^c) \cap C \right) \quad (2b \text{ Assoc}) \\&= (A \cap B^c) \cup \left((A \cap B^c) \cap C \right) \quad (7b) \\&= (A \cap B^c) \quad (10a) \\&= A - B \quad (12)\end{aligned}$$

Chapter 7 Functions

In pre-calculus one defines a function $f : \mathbb{R} \rightarrow \mathbb{R}$ as a rule taking a real number $x \in \mathbb{R}$ as input and giving a real number $f(x) \in \mathbb{R}$ as output. In this course (and in math in general), we generalize the pre-calculus notion of function to $f : X \rightarrow Y$, where X and Y are arbitrary sets. Also, since everything in math is a set, a function is technically going to be a set, but the precalculus way of thinking of a function as a rule giving an output $f(x) \in Y$ for each input $x \in X$ is still how most mathematicians think of a function $f : X \rightarrow Y$ (as opposed to its underlying set).

Relations

Given two sets X, Y recall that the (Cartesian) product $X \times Y$ is the set of ordered pairs

$$X \times Y := \{(x, y) \mid x \in X, y \in Y\}$$

Definition

Let X, Y be two sets. A **relation** R from X to Y is simply a subset of $X \times Y$:

$$R \subseteq X \times Y$$

We define xRy to mean $(x, y) \in R$. So xRy is true if $(x, y) \in R$ is true, and xRy is false if $(x, y) \notin R$ is true.

Definition

Let X, Y be two sets. A **function** f from X to Y , denoted $f : X \rightarrow Y$, is a relation f from X to Y , i.e. a subset $f \subseteq X \times Y$, such that

- ▶ for every element $x \in X$, there is exactly one element $y \in Y$ such that $(x, y) \in f$

We write $f(x) = y$ to mean $(x, y) \in f$, and say that “ f maps x to y ”. Given a function $f : X \rightarrow Y$, the set X is called the **domain** and the set Y is called the **codomain** or **target**.

Caution: the above is a very confusing way to think of functions!

example

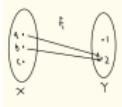
In precalculus, we have the function $f : \mathbb{R} \rightarrow \mathbb{R}$ given by the formula $f(x) = x^2$. What is the underlying set of this function f , considered as relation from \mathbb{R} to \mathbb{R} ?

Answer: $f = \{(x, x^2) \in \mathbb{R} \times \mathbb{R} \mid x \in \mathbb{R}\}$. So for example $(0, 0), (1, 1), (2, 4), (3, 9)$ are all elements of f , while $(3, 8)$ is not an element of f . Note the similarity to the graph of $f(x)$.

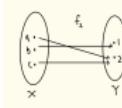
example

Let $X = \{a, b, c\}$ and $Y = \{1, 2\}$. Decide which of the following subsets of $X \times Y$ are functions $f : X \rightarrow Y$.

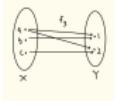
1. $f_1 = \{(a, 2), (b, 2)\}$



2. $f_2 = \{(a, 2), (b, 1), (c, 2)\}$



3. $f_3 = \{(a, 2), (b, 1), (c, 2), (a, 1)\}$



Answer

The set f_1 is not a function since $f(c)$ is not defined, i.e. there is no $y \in Y$ such that $(c, y) \in f_1$.

The set f_2 is a function.

The set f_3 is not a function since there are two distinct elements $y \in Y$ such that $(a, y) \in f_3$ namely, $(a, 2)$ and $(a, 1)$.

Definition

Let $f : X \rightarrow Y$ be a function. We define the **image** of f to be the set $\{f(x) \mid x \in X\}$. For $y \in Y$, the preimage $f^{-1}(y)$ is the set

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

of elements of x that map to y .

Section 7.2 Injective, surjective, bijective functions

Definition

Let $f : X \rightarrow Y$ be a function. We say f is

1. **injective** or **one-to-one** if the following statement is true:

$$\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2$$

Taking the contrapositive of the above statement, we get the following equivalent definition: f is injective if

$$\forall x_1, x_2 \in X, \text{ if } x_1 \neq x_2 \text{ then } f(x_1) \neq f(x_2)$$

In words, f is injective if different inputs lead to different outputs.

2. **surjective** or **onto** if the following statement is true:

$$\forall y \in Y, \exists x \in X \text{ such that } f(x) = y$$

In words, for every element y of the target is in the image of f .

3. **bijective** or **one-to-one correspondence** if it is injective and surjective.

Let's take negations to find what it means for a function to not be injective, surjective, or bijective:

A function $f : X \rightarrow Y$ is

1. *not injective* if the following statement is true:

$$\exists x_1, x_2 \in X \ f(x_1) = f(x_2) \wedge x_1 \neq x_2$$

In words, different inputs give the same output

2. *not surjective* if the following statement is true

$$\exists y \in Y, \forall x \in X, \ f(x) \neq y$$

In words, there exists an element $y \in Y$ that is not in the image of f .

Here is a nice diagram in Epp showing a function is injective or not:

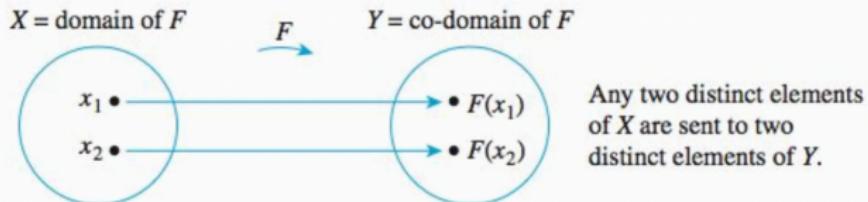


Figure 7.2.1(a) A One-to-One Function Separates Points
(Injective)

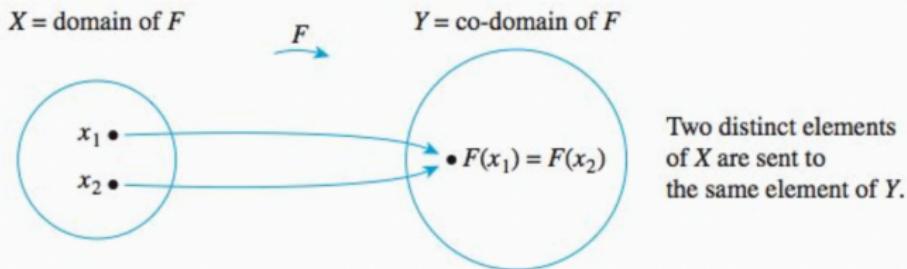
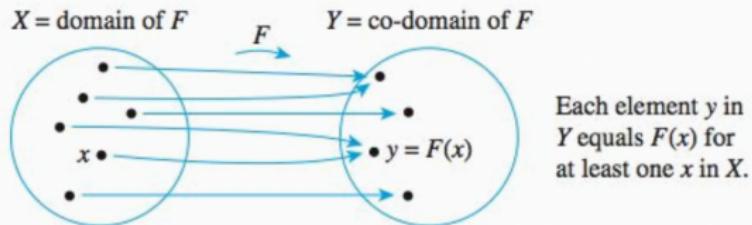


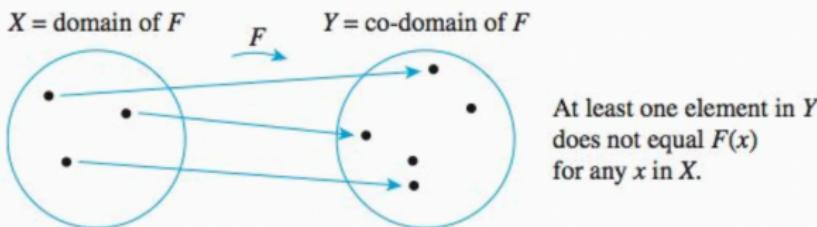
Figure 7.2.1(b) A Function That Is Not One-to-One Collapses Points Together
(Injective)

Here is a nice diagram in Epp showing a function is surjective or not:



Each element y in Y equals $F(x)$ for at least one x in X .

Figure 7.2.3(a) A Function That Is Onto
(Surjective)



At least one element in Y does not equal $F(x)$ for any x in X .

Figure 7.2.3(b) A Function That Is Not Onto
(Surjective)

example

Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by $f(n) = 5n - 1$. Show that f is injective but not surjective.

Proof: Use direct proof on the if-then statement appearing in the definition of injective:

$$\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2$$

1. Let $x_1, x_2 \in \mathbb{Z}$
2. Assume $f(x_1) = f(x_2)$. We want to show $x_1 = x_2$.
3. So $5x_1 - 1 = 5x_2 - 1$. Do some algebra:

$$5x_1 - 1 = 5x_2 - 1$$

$$5x_1 = 5x_2$$

$$x_1 = x_2$$

Hence f is injective.

To show $f : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $f(n) = 5n - 1$ is not surjective we have to show

$$\exists y \in Y, \forall x \in X, f(x) \neq y$$

This is an “exists” statement, so we should try to find a $y \in Y = \mathbb{Z}$ that is not in the image of f . General strategy to determine whether a function is surjective or not is to solve for x in terms of y :

1. Proof that f is not surjective by contradiction. So assume f is surjective.
2. So $\forall y \in \mathbb{Z}, \exists x \in \mathbb{Z}, | 5x - 1 = y$.
3. Solve for x in terms of y :

$$5x - 1 = y$$

$$5x = y + 1$$

$$x = \frac{y+1}{5}$$

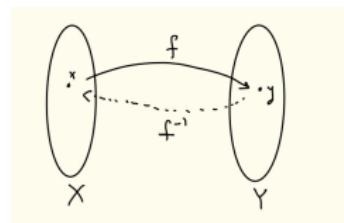
We must have $x \in \mathbb{Z}$, but the fraction tells us there are many choice of $y \in \mathbb{Z}$ for which $x \notin \mathbb{Z}$ a contradiction. For a specific counterexample, take $y = 0$, then $x = \frac{1}{5} \notin \mathbb{Z}$.

By contrast, the function $f : \mathbb{R} \rightarrow \mathbb{R}$ given by $f(n) = 5n - 1$ (for $n \in \mathbb{R}$) is injective and surjective, and hence bijective.

Inverse function

Definition

Suppose the function $f : X \rightarrow Y$ is bijective. Then f has an **inverse** function $f^{-1} : Y \rightarrow X$, defined by $f^{-1}(y) = x$ where $x \in X$ is the unique element of X such that $f(x) = y$.



example

Define $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ by

$$f(x, y) = (x + y, x - y)$$

- . Show that f is bijective, and find a formula for the inverse function f^{-1} .

Proof

1. The f is bijective means that f is injective and f is surjective.
2. First we show f is injective. Suppose we had two elements (x, y) and (x', y') of the domain $\mathbb{R} \times \mathbb{R}$ such that

$$f(x, y) = f(x', y')$$

We have to show $(x, y) = (x', y')$, i.e. $x = x'$ and $y = y'$.

3. The condition $f(x, y) = f(x', y')$ translates to $(x + y, x - y) = (x' + y', x' - y')$, and hence

$$x + y = x' + y' \text{ and}$$

$$x - y = x' - y'$$

4. Adding these two equations gives $2x = 2x'$, and hence $x = x'$.
5. The $x + y = x' + y'$ becomes $x + y = x + y'$, and hence $y = y'$. This finishes the proof f is injective.

6. Next we show f is surjective. Let $(a, b) \in \mathbb{R} \times \mathbb{R}$ be an element of the co-domain/target of $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$.
7. We have to show there exists $(x, y) \in \mathbb{R} \times \mathbb{R}$ such that $f(x, y) = (a, b)$.
8. Work backwards: assume there exists such an (x, y) , and solve for x, y in terms of a and b :
9. The condition $f(x, y) = (a, b)$ becomes $(x + y, x - y) = (a, b)$, i.e.

$$x + y = a \text{ and}$$

$$x - y = b$$

10. Adding these two equations gives $2x = a + b$, and hence

$$x = \frac{a+b}{2}$$

11. Solving $x + y = a$ for y gives $y = a - x$ and hence

$$y = a - \frac{a+b}{2} = \frac{2a}{2} - \frac{a+b}{2} = \frac{a-b}{2}$$

12. The above calculation shows that if $f(x, y) = (a, b)$ then we must have $x = \frac{a+b}{2}$ and $y = \frac{a-b}{2}$.
13. Technically, we want the converse - that if $x = \frac{a+b}{2}$ and $y = \frac{a-b}{2}$ then $f(x, y) = (a, b)$.

14. For $a, b \in \mathbb{R}$, we have $\frac{a+b}{2}$ and $\frac{a-b}{2}$ are in \mathbb{R} .
15. Finally we check that if $x = \frac{a+b}{2}$ and $y = \frac{a-b}{2}$ then $f(x, y) = (a, b)$:

$$f\left(\frac{a+b}{2}, \frac{a-b}{2}\right) = \left(\frac{a+b}{2} + \frac{a-b}{2}, \frac{a+b}{2} - \frac{a-b}{2}\right) = (a, b)$$

16. Hence f is surjective.
17. Finally the inverse function $f^{-1} : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ is given by

$$f^{-1}(a, b) = \left(\frac{a+b}{2}, \frac{a-b}{2}\right)$$

example

Define $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ by

$$f(x, y) = (x + y, x - y)$$

Show that f is injective but not surjective.

Proof:

1. The proof that f is injective is the same as in the previous example.
2. The proof of that f is not surjective follows like the previous example, but now, for $a, b \in \mathbb{Z}$, it is not necessarily the case that $\frac{a+b}{2}$ and $\frac{a-b}{2}$ are in \mathbb{Z} .
3. For a specific counterexample, take $a = 0, b = 1$. Then there is no $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(x, y) = (0, 1)$, since such an (x, y) must be $(\frac{1}{2}, -\frac{1}{2})$ which is not $\mathbb{Z} \times \mathbb{Z}$.

Section 7.3 Composition of functions

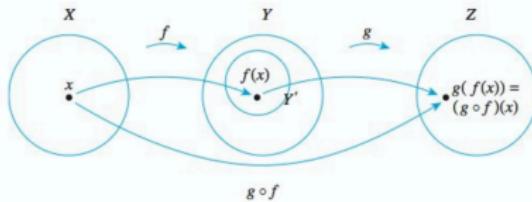
Definition

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be two functions. The **composite of f and g** is a function $g \circ f : X \rightarrow Z$ defined by

$$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X$$

Even though we say f first in “composite of f and g ”, but write $g \circ f$ - because given an element $x \in X$, we apply f first, then g .

Here's a schematic picture of the composite of f and g :



example

Let $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ be given by

$$f(x, y) = (y, x) \quad \text{for all } (x, y) \in \mathbb{R} \times \mathbb{R}$$

and $g : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ be given by

$$g(x, y) = (x + 2y, x^2)$$

Figure out what the functions $(g \circ f)$ and $(f \circ g)$ (they will be different).

Solution Let $(a, b) \in \mathbb{R} \times \mathbb{R}$. Then

$$(g \circ f)(a, b) = g\left(f(a, b)\right) = g\left((b, a)\right) = (b + 2a, b^2)$$

Notice the last equality - it is not a typo. I could have used (x, y) to represent an element in $\mathbb{R} \times \mathbb{R}$; in that case, we would have written

$$(g \circ f)(x, y) = g\left(f(x, y)\right) = g\left((y, x)\right) = (y + 2x, y^2)$$

Finally, for $f \circ g$:

$$(f \circ g)(x, y) = f\left(g(x, y)\right) = f(x + 2y, x^2) = (x^2, x + 2y)$$

The proof of the following result teaches you how to work with the definitions of injective and surjective.

Theorem

Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be two functions.

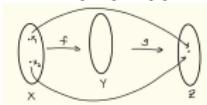
- a) If f and g are both injective, then $g \circ f$ is injective
- b) If f and g are both surjective, then $g \circ f$ is surjective.
- c) If f and g are both bijective, then $g \circ f$ is bijective.

Proof of part a

1. Assume $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are injective. We want to show $g \circ f$ is injective.
2. According to the definition of injective, we have to show

$\forall x_1, x_2 \in X$, if $(g \circ f)(x_1) = (g \circ f)(x_2)$ then $x_1 = x_2$

3. Do direct proof. Let $x_1, x_2 \in X$ be arbitrary. Assume $(g \circ f)(x_1) = (g \circ f)(x_2)$; we want to show $x_1 = x_2$.
4. So $g(f(x_1)) = g(f(x_2))$ by definition of $g \circ f$.



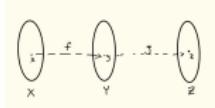
5. Since g is injective, the equation $g(f(x_1)) = g(f(x_2))$ implies $f(x_1) = f(x_2)$ is true.
6. Since f is injective, the equation $f(x_1) = f(x_2)$ implies we have $x_1 = x_2$.

Proof of Part b)

1. Assume $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are surjective. We want to show $g \circ f : X \rightarrow Z$ is surjective.
2. According to the definition of a function (in this case $g \circ f$) to be surjective, we have to show

$$\forall z \in Z, \exists x \in X \text{ such that } (g \circ f)(x) = z$$

3. Let $z \in Z$ be arbitrary. We want to find $x \in X$ with $(g \circ f)(x) = z$.



4. Since g is surjective, there exists $y \in Y$ such that $g(y) = z$.
5. Since f is surjective, there exists $x \in X$ such that $f(x) = y$.
6. Then $(g \circ f)(x) = g(f(x)) = g(y) = z$, so we have found an $x \in X$ with $(g \circ f)(x) = z$.

Section 7.4 Cardinality and Sizes of Infinity

- ▶ In the 1870s, the mathematician Georg Cantor realized there are different sizes of infinity!
- ▶ While

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

are three infinite sets, each containing the previous one, and so intuitively each should be “bigger” than the previous one.

- ▶ But a startling discovery (in the 1800s) was that \mathbb{Z} and \mathbb{Q} actually have the same “size” (the technical term for size is *cardinality*), even though \mathbb{Z} is a subset of \mathbb{Q} !
- ▶ \mathbb{R} is a bigger infinity than \mathbb{Z} and \mathbb{Q} . We will explain these things.

Continuum Hypothesis

One thing we won't explain is this famous question:

In 1878 Georg Cantor asked whether the following statement, called the **Continuum Hypothesis** was true or false:

There is no set whose cardinality (roughly, size) is between that of \mathbb{Z} and \mathbb{R}

The answer (which is too advanced to discuss in this course) was a surprise. Combining results of K. Gödel in 1940 and P. Cohen in 1963 shows that the Continuum Hypothesis can neither be proved or disproved using the most widespread framework of set theory (called Zermelo-Frankel + Choice). This means one can add the Continuum Hypothesis (or its negation, but not both) as an axiom, and develop a mathematical theory that will be consistent if Zermelo-Frankel + Choice is consistent.

Finite vs infinite sets

Definition

A set X is **finite** if it either has no elements or if there exists a positive integer n and a bijective function $f : X \rightarrow \{1, 2, \dots, n\}$. The bijection f implies that X has n elements.

A set X is **infinite** if it is not finite. In other words, an infinite set is not empty and for every positive integer n there is no bijective function $f : X \rightarrow \{1, 2, \dots, n\}$.

Example

The $\{4, 6, 8\}$ is a finite set since there is a bijection with $\{1, 2, 3\}$.

The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are infinite sets.

Cardinality

Definition

Let X, Y be two sets. We say X and Y **have the same cardinality** if there is a bijection $f : X \rightarrow Y$. The inverse $f^{-1} : Y \rightarrow X$ will then be a bijection from Y to X , so order doesn't matter: if X and Y have the same cardinality, then we have bijections $X \rightarrow Y$ and $Y \rightarrow X$.

Here is an easy fact:

Theorem

If X and Y have the same cardinality, and Y and Z have the same cardinality, then X and Z have the same cardinality.

proof

1. Assume X and Y have the same cardinality, and Y and Z have the same cardinality.
2. Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be bijective functions. Then $g \circ f : X \rightarrow Z$ is bijective by Theorem in section 7.3. Hence X and Z have the same cardinality.

example

Prove that the set of integers \mathbb{Z} and the set of even integer $2\mathbb{Z}$ have the same cardinality.

Solution: Let $f : \mathbb{Z} \rightarrow 2\mathbb{Z}$ be given by $f(n) = 2n$. It is easy to see that f is a bijection.

Let

$$\mathbb{Z}^+ = \{1, 2, 3, \dots\}$$

be the set of positive integers. Let X be a set. Suppose there is a bijection

$$f : \mathbb{Z}^+ \rightarrow X$$

Then by setting $x_n = f(n)$ for $n \in \mathbb{Z}^+$, the bijection gives a list

$$x_1, x_2, x_3 \dots$$

of all the elements of X , with each element of X appearing exactly once. So we have counted or enumerated the elements of X . This gives rise to the following often used terminology (next slide)

Countable

Definition

1. A set X is **countably infinite** if it has the same cardinality as \mathbb{Z}^+ . That means, there is a bijection

$$f : \mathbb{Z}^+ \rightarrow X$$

or equivalently there is a list

$$x_1, x_2, x_3 \dots$$

of all the elements of X , with each element of X appearing exactly once.

2. A set is **countable** if it is finite or countably infinite.
3. A set is **uncountable** if it is not countable. In other words, there is no bijective function $f : \mathbb{Z}^+ \rightarrow X$.

example

The set of integers \mathbb{Z} is countable.

Proof. We construct a bijection $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}$ (there are many). In other words, we have to list (or count off) the elements of \mathbb{Z} such that every integer appears exactly one. The trick is to start the list with (for example) with zero and alternate with positive and negative integers, gradually increasing in magnitude. The following picture from Epp. p.336 illustrates one way of doing so:

In other words, to define a bijection $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}$, we set

$f(1) = 0, f(2) = 1, f(3) = -1, f(4) = 2, \dots$. The point is that *all* integers will eventually appear in the list (once and only once).

example

Prove that the set of even integers is countable.

Proof We have seen earlier that \mathbb{Z} and $2\mathbb{Z}$ have the same cardinality ($n \mapsto 2n$ gives a bijection) and the previous example shows \mathbb{Z}^+ and \mathbb{Z} have the same cardinality. Hence (by a theorem we proved) \mathbb{Z}^+ and $2\mathbb{Z}$ have the same cardinality. So $2\mathbb{Z}$ is countable.

\mathbb{Q}^+ is countable

Theorem

The set \mathbb{Q}^+ of positive rational numbers is countable.

proof

The proof is quite ingenious. Make a 2-dimensional grid of the positive rational numbers with the fraction $\frac{m}{n}$ placed in row m and column n . Every rational number appears more than once (e.g $1 = \frac{1}{1} = \frac{2}{2}$), but we will deal with that.

Define a function $f : \mathbb{Z}^+ \rightarrow \mathbb{Q}^+$ by following the path indicated in the picture, where we skip a rational number that we've already seen before. So set $f(1) = \frac{1}{1}$, $f(2) = \frac{1}{2}$, $\frac{3}{2}, f(4) = 3$. Then skip $\frac{2}{2} = 1$ which was already counted before, and set $f(5) = \frac{1}{3}$. Continuing in this manner gives a function $f : \mathbb{Z}^+ \rightarrow \mathbb{Q}^+$ that is easily seen to be bijective.

The following is a famous result and its proof is very ingenious:

Theorem (Cantor)

The set of real numbers between 0 and 1 is uncountable.

proof

1. Proof by contradiction. Assume the interval $(0, 1)$ (this is not the ordered pair set!) was countable.
2. So there is a bijection $f : \mathbb{Z}^+ \rightarrow (0, 1)$. Let $a_{i,j} \in \{0, 1, 2, \dots, 9\}$ represent the j th decimal digit of the number $f(i)$ so

$$f(i) = 0.a_{i,1}a_{i,2}a_{i,3}\dots a_{i,j}\dots$$

3. We list $f(i)$ is row i ; the assumption that f is a bijection means that every number in $(0, 1)$ appears somewhere in the list:

$$f(1) = 0.\boxed{a_{1,1}}a_{1,2}a_{1,3}\dots$$

$$f(2) = 0.a_{2,1}\boxed{a_{2,2}}a_{2,3}\dots$$

$$f(3) = 0.a_{3,1}a_{3,2}\boxed{a_{3,3}}\dots$$

4. Cantor's trick is the focus on the diagonal elements (boxed) to cook up a number d not in the list: let $d = 0.d_1d_2d_3\dots$ where d_i is any digit besides $a_{i,i}$. (We need to be a bit careful to avoid letting d end all 9's so for example, for each $i \geq 1$, set

$$d_i = \begin{cases} 1 & \text{if } a_{i,i} \neq 1 \\ 2 & \text{if } a_{i,i} = 1 \end{cases}$$

The choice of 1, 2 is not really important

5. The crucial point though is that $a_{i,i} \neq d_i$ for all i .
6. We claim that d is not in the image of f : i.e. there is no i for which $f(i) = d$, since the i th decimal digit of $f(i)$ is $a_{i,i}$ while that of d is d_i and was chosen to be different from $a_{i,i}$!
7. Hence f is not surjective, a contradiction to the assumption that f was bijective.

Cardinality of Power set

- ▶ Given a set A , recall that the power set $\mathcal{P}(A)$ of A is the set of all subsets of A (including the empty set).
- ▶ If A is a finite set with n elements, then $\mathcal{P}(A)$ has 2^n elements, so A and $\mathcal{P}(A)$ have different cardinalities when A is finite.
- ▶ For every set A there is an injective function $i : A \rightarrow \mathcal{P}(A)$ given by sending $a \in A$ to $\{a\} \in \mathcal{P}(A)$.
- ▶ The following theorem shows there is no surjective function $f : A \rightarrow \mathcal{P}$, and hence A and $\mathcal{P}(A)$ do not have the same cardinality; $\mathcal{P}(A)$ has a “larger” cardinality than A .

Power set is bigger

Theorem (Cantor)

Let A be any set. There is no surjective function $f : A \rightarrow \mathcal{P}(A)$ from A to the power set of A .

proof

1. Proof by contradiction. Suppose there was a surjective function $f : A \rightarrow P(A)$.
2. The trick is to define the set

$$T = \{x \in A \mid x \notin f(x)\}$$

3. The set T is a subset of A , and hence an element of the power set $P(A)$ of A .
4. Since f is surjective, there exists $a \in A$ such that $f(a) = T$.
5. The statement " $a \in T$ " is either true or false, and we'll see both cases lead to a contradiction:
6. If $a \in T$ is true, then $a \notin f(a)$ by definition of T , so $a \notin T$ (as $f(a) = T$) a contradiction.
7. So it must be the case that $a \notin T$, and so $a \notin f(a)$. But then $a \in T$ by definition of T , a contradiction.

As a result, we can create an infinite sequence of larger and larger infinities! For example, the cardinalities of the sets in the sequence

$$\mathbb{Z}, \mathcal{P}(\mathbb{Z}), \mathcal{P}(\mathcal{P}(\mathbb{Z})), \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{Z}))), \dots$$

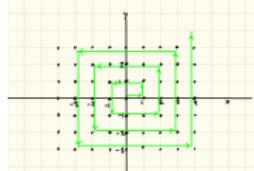
are strictly increasing.

Theorem

$\mathbb{Z} \times \mathbb{Z}$ is countably infinite.

proof

1. We have to construct a bijection $f : \mathbb{Z}^+ \rightarrow \mathbb{Z} \times \mathbb{Z}$, or equivalently a list x_1, x_2, \dots of the elements of $\mathbb{Z} \times \mathbb{Z}$ such that every element appears exactly once.
2. Plot the points of $\mathbb{Z} \times \mathbb{Z}$ in the xy-plane as usual.
3. We can then count/list the points of $\mathbb{Z} \times \mathbb{Z}$ by beginning at the origin $(0, 0)$ and spiraling out:



4. So our list is

$$(0, 0), (1, 0), (1, 1), (0, 1), (-1, 1), (-1, 0), (-1, -1), \dots$$

and from the spiral in the picture it is clear that every element of $\mathbb{Z} \times \mathbb{Z}$ will (eventually) appear in the list and it will never be repeated.

Theorem

$\mathbb{Z}^+ \times \mathbb{Z}^+$ is countably infinite.

The proof is a similar “proof by picture” to the previous proof:
plot the points of $\mathbb{Z}^+ \times \mathbb{Z}^+$ in the xy-plane and then (for example)
by zig-zag along the diagonals.

Corollary

If X and Y are countably infinite sets, then $X \times Y$ is countable infinite.

Proof

1. Assume X and Y are countably infinite, so there exists bijections $f : \mathbb{Z}^+ \rightarrow X$ and $g : \mathbb{Z}^+ \rightarrow Y$.
2. The map $f \times g : \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow X \times Y$ defined by $(f \times g)(m, n) = (f(m), g(n))$ is a bijection (proof omitted).
3. Since $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countably infinite, there exists a bijection $h : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \times \mathbb{Z}^+$
4. Then the composition

$$\mathbb{Z}^+ \xrightarrow{h} \mathbb{Z}^+ \times \mathbb{Z}^+ \xrightarrow{f \times g} X \times Y$$

is a composition of bijective functions and is therefore (by a theorem in section 7.3) is bijective.

Chapter 8: Relations

Recall from the previous chapter:

Given two sets X, Y recall that the (Cartesian) product $X \times Y$ is the set of ordered pairs

$$X \times Y := \{(x, y) \mid x \in X, y \in Y\}$$

Relations

Definition

Let X, Y be two sets. A (binary) **relation** R from X to Y is simply a subset of $X \times Y$:

$$R \subseteq X \times Y$$

We define

$$x R y \text{ to mean } (x, y) \in R$$

So $x R y$ is true if $(x, y) \in R$ is true, and $x R y$ is false if $(x, y) \notin R$ is true.

Equivalently, we can define a relation from X to Y to be a predicate $R(x, y)$ (which we instead will usually write $x R y$) with domain $X \times Y$. This is usually how we will work and think of relations: given $x \in X, y \in Y$, then $x R y$ is either true or false (but not both), depending on x and y .

In this chapter we will mostly deal with relations on a single set:

Definition

A **relation** R on a single set X is a relation from X to X , i.e. simply a subset $R \subseteq X \times X$. Instead of working with the underlying set R , we usually work with the true or false statement/predicate $x_1 R x_2$ (where $x_1, x_2 \in X$).

example: mod 5

Define a relation M_5 (for mod 5) on the set \mathbb{Z} of integers by, for $x, y \in \mathbb{Z}$,

$$x M_5 y \iff 5 \mid (x - y) \iff \frac{x - y}{5} \in \mathbb{Z}$$

(i.e. $x M_5 y$ is true if 5 divides $x - y$, false otherwise). So for example $1 M_5 6$ is true, but $1 M_5 5$ is false. Note that M_5 is the mod5 relation:

$$x M_5 y \iff 5 \mid (x - y) \iff x \equiv y \pmod{5}$$

example: less than

Define a relation L on the set \mathbb{R} for $x, y \in \mathbb{R}$,

$$x L y \iff x < y$$

So for example, $1 L 2$ is true, but $2 L 1$ is false.

Section 8.2: Reflexive, symmetric, transitive relations

Of particular interest are three properties that a relation may or may not have: reflexivity, symmetry, and transitivity (all defined below). Relations that have all three are called equivalence relations, and behave a bit like “equals”, and come up often in math.

Definition

Let R be a relation on a set X . We say

- ▶ R is **reflexive** if the following statement is true:

$$\forall x \in X, x R x$$

- ▶ R is **symmetric** if the following statement is true:

$$\forall x, y \in X, x R y \rightarrow y R x$$

(In words, for all $x, y \in X$, if $x R y$ then $y R x$.)

- ▶ R is **transitive** if the following statement is true:

$$\forall x, y, z \in X (x R y) \wedge (y R z) \rightarrow (x R z)$$

In words, for all $x, y, z \in X$, if $x R y$ and $y R z$ then $x R z$.

example

Define a relation L on the set \mathbb{R} for $x, y \in \mathbb{R}$,

$$x L y \iff x < y$$

Then L is not reflexive (since $x < x$ is false), L not symmetric, but L is transitive (since if $x < y$ and $y < z$ then $x < z$).

Section 8.3 Equivalence relations

Definition

An **equivalence relation** R on a set X is a relation that is reflexive, symmetric, and transitive.

example

Prove that the mod 5 relation M_5 on \mathbb{Z} is an equivalence relation.

Recall

$$x \ M_5 \ y \iff 5 \mid (x - y) \iff \frac{x - y}{5} \in \mathbb{Z}$$

Proof:

1. We have to show M_5 is reflexive, symmetric, and transitive.
2. **To show M_5 is reflexive**, we have to show $\forall x \in \mathbb{Z}, x \ M_5 \ x$.
3. Let $x \in \mathbb{Z}$ be arbitrary.. Then $x \ M_5 \ x$ is logically equivalent to $5 \mid (x - x)$, i.e $5 \mid 0$, which is true since $\frac{0}{5} = 0 \in \mathbb{Z}$. So $x \ M_5 \ x$ is true, and M_5 is reflexive.
4. **To show M_5 is symmetric**, we have to show

$$\forall x, y \in \mathbb{Z}, (x \ M_5 \ y) \rightarrow (y \ M_5 \ x)$$

5. Let $x, y \in \mathbb{Z}$ be arbitrary. Assume $x \ M_5 \ y$, and we have to show $y \ M_5 \ x$.
6. $x \ M_5 \ y$ means $\frac{x-y}{5} \in \mathbb{Z}$. Then multiplying the integer $\frac{x-y}{5}$ by -1 gives $\frac{y-x}{5}$, and will also be an integer. Hence $y \ M_5 \ x$.

7. To show M_5 is transitive, we have to show

$$\forall x, y, z \in \mathbb{Z} (x M_5 y) \wedge (y M_5 z) \rightarrow (x M_5 z)$$

8. Let $x, y, z \in \mathbb{Z}$ be arbitrary. Assume $(x M_5 y)$ and $(y M_5 z)$ are true. We have to show $(x M_5 z)$ is true.
9. We have $\frac{x-y}{5} \in \mathbb{Z}$ and $\frac{y-z}{5} \in \mathbb{Z}$. Adding two integers gives an integer and hence

$$\frac{x-y}{5} + \frac{y-z}{5} = \frac{x-z}{5}$$

is an integer, and so $x M_5 z$ is true.

example

Let $X = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ be the set of ordered pairs of integers (a, b) with $b \neq 0$. Define a relation Q on X by

$$(a, b) Q (c, d) \iff ad = bc \quad \text{where } (a, b), (c, d) \in X$$

(Note that $ad = bc$ implies that $\frac{a}{b} = \frac{c}{d}$ as numbers in \mathbb{Q} since $b, d \neq 0$.) Show that Q is an equivalence relation

proof

1. Q is reflexive: if $(a, b) \in X$ then
 $(a, b) Q (a, b) \iff ab = ba$, and $ab = ba$ is true since $a, b \in \mathbb{Z}$.
2. Q is symmetric: assume $(a, b) Q (c, d)$, we want to show $(c, d) Q (a, b)$. So $ad = bc$, and hence $cb = da$, which means $(c, d) Q (a, b)$.
3. Q is transitive: assume $(a, b) Q (c, d)$ and $(c, d) Q (e, f)$. We want to show $(a, b) Q (e, f)$.
4. Our assumptions translate to $ad = bc$ and $cf = de$. We want to show $af \stackrel{?}{=} be$.
5. Multiplying both sides of $ad = bc$ by f we get $adf = bcf$.
6. Since $cf = de$, we get $adf = b(cf) = bde$.
7. So $adf = bde$. Dividing both sides by $d \neq 0$, we get $af = be$.

Definition

Let R be an equivalence relation on a set X . Given $x \in X$, the **equivalence class** of x is the set $[x]$ consisting of all elements of X that are related by R to x :

$$[x] := \{y \in X \mid x R y\}$$

Since R is symmetric, we may also write $[x]$ as

$$[x] = \{y \in X \mid y R x\}$$

example

In the mod 5 equivalence relation M_5 on \mathbb{Z} , we have

$$[0] = \{\dots, -5, 0, 5, 10, \dots\} = \{5k \mid k \in \mathbb{Z}\}$$

$$[1] = \{\dots, -4, 1, 6, 11, \dots\} = \{5k + 1 \mid k \in \mathbb{Z}\}$$

$$[2] = \{\dots, -3, 0, 7, 12, \dots\} = \{5k + 2 \mid k \in \mathbb{Z}\}$$

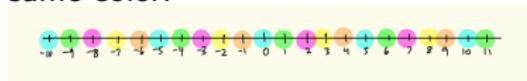
$$[3] = \{\dots, -2, 0, 8, 13, \dots\} = \{5k + 3 \mid k \in \mathbb{Z}\}$$

$$[4] = \{\dots, -1, 0, 9, 14, \dots\} = \{5k + 4 \mid k \in \mathbb{Z}\}$$

$$[5] = \{\dots, -5, 0, 5, 10, \dots\} = \{5k + 5 \mid k \in \mathbb{Z}\} = \{5\ell \mid \ell \in \mathbb{Z}\} = [0]$$

$$[0] = [5] = [10], \quad [-4] = [1] = [6]$$

In the diagram below I've colored numbers equivalent to each other mod 5 the same color:



We see that there are a total of 5 different equivalence classes. Furthermore, two different equivalence classes are disjoint (i.e. have no number in common), and every integer appears in exactly one of the five different equivalence classes.

Partitions

In the previous example, we saw that the mod 5 equivalence relation gives rise to equivalence classes which partition the set of integers:

Definition

Gives a set X , a **partition** P of X is a set $P = \{X_i \mid i \in I\}$ (for some index set I) of subsets X_i of X such that

1. $X = \bigcup_{i \in I} X_i$
2. for all $i, j \in I$, if $X_i \neq X_j$ then $X_i \cap X_j = \emptyset$

We will see that a partition of X and an equivalence relation on X are equivalent ideas.

example

Consider the equivalence relation M_5 on \mathbb{Z} . Let $I = \{0, 1, 2, 3, 4\}$ and let $X_i = [i]$. Then

$P = \{X_0, X_1, X_2, X_3, X_4\} = \{[0], [1], [2], [3], [4]\}$ is a partition of \mathbb{Z}
- every integer is in exactly one element of P .

In the previous example we saw that for example $1 \sim_5 6$ and $[1] = [6]$, i.e. equivalent elements (such as 1 and 6) give rise to the same equivalence class. This holds in general:

Lemma

If R is an equivalence relation on a set X , and $x, y \in X$ are such that $x R y$, then $[x] = [y]$.

proof

1. Let $x, y \in X$ with $x R y$, and hence $y R x$ since R is symmetric.
2. $[x]$ and $[y]$ are sets, and to show they are equal, we show $[x] \subseteq [y]$ and $[y] \subseteq [x]$.
3. To show $[x] \subseteq [y]$, let $z \in [x]$ be arbitrary. We have to show $z \in [y]$.
4. $z \in [x]$ means $x R z$.
5. Since $y R x$ and $x R z$ it follows that $y R z$ since R is transitive. Hence $z \in [y]$, and so $[x] \subseteq [y]$.
6. The proof that $[y] \subseteq [x]$ is similar.

The following theorem shows how an equivalence relation gives rise to a partition:

Theorem

Let R be an equivalence relation on a set X . The set of distinct equivalence classes for R form a partition P of X :

$$P = \{[x] \mid x \in X\}$$

proof

1. According to the definition of partition, we have to show
 - a) $X = \bigcup_{x \in X} [x]$
 - b) for all $x, y \in X$, if $[x] \neq [y]$ then $[x] \cap [y] = \emptyset$
2. To show part (a) we have to show $X \subseteq \bigcup_{x \in X} [x]$ and $\bigcup_{x \in X} [x] \subseteq X$
3. First we show $X \subseteq \bigcup_{x \in X} [x]$. Let $x_0 \in X$ be arbitrary. Since $x_0 R x_0$ (since R is an equivalence relation) so $x_0 \in [x_0]$ and hence we have $x_0 \in \bigcup_{x \in X} [x]$.
4. The inclusion $\bigcup_{x \in X} [x] \subseteq X$ follows from $[x] \subseteq X$. Hence we have established part (a).

5. To show part (b), we prove the contrapositive, namely
“For all $x, y \in X$, if $[x] \cap [y] \neq \emptyset$ then $[x] = [y]$.
6. Let $x, y \in X$ be arbitrary, and assume $[x] \cap [y] \neq \emptyset$. So there exists $z \in X$ such that $z \in [x]$ and $z \in [y]$. We have to show $[x] = [y]$
7. Our assumptions give $x R z$ and $y R z$.
8. Hence $y R x$ by symmetry and transitivity.
9. Hence by the lemma, $[x] = [y]$.

Conversely, the following theorem shows how given a partition P of a set X , we can define an equivalence relation on X :

Theorem

Let X be a set and $P = \{X_i \mid i \in I\}$ a partition of X . Define a relation R on X by $x R y$ if there exists $i \in I$ such that $x, y \in X_i$. Then R is an equivalence relation. Also, the partition associated to R by the previous theorem is P .

proof

1. To show R is an equivalence relation, we have to show it is reflexive, symmetric, and transitive.
2. R is reflexive: Let $x \in X$. Then since P is a partition, $X = \bigcup_{i \in I} X_i$, and therefore there exists $i \in I$ such that $x \in X_i$. Hence $x R x$ since $x, x \in X_i$.
3. R is symmetric: Let $x, y \in X$ with $x R y$. Then there exists $i \in I$ such that $x, y \in X_i$. Therefore $y R x$.
4. R is transitive: Let $x, y, z \in X$ with $x R y$ and $y R z$. Then there exists $i \in I$ such that $x, y \in X_i$ and there exists $j \in I$ such that $y, z \in X_j$. Since $X_i \cap X_j$ contains the element y , it is non-empty, and hence we have $X_i = X_j$ (by condition (2) in the definition of partition). Hence $x, y, z \in X_i$ and in particular $x R z$.
5. The partition associated (in the previous theorem) to an equivalence relation is given by the set of equivalence classes. For $x \in X$, if $i \in I$ is such that $x \in X_i$, then $[x] = X_i$ since both sets are $\{y \in X \mid x R y\}$.

Definition

Given a set X and an equivalence relation R on X , we define X/R , read “ X mod R ” to be the set of equivalence classes:

$$X/R = \{[x] \mid x \in X\}$$

If $S \in X/R$ is an equivalence class, we define a **a representative** of S to be an element $x \in X$ such that $S = [x]$.

So the elements of X/R are sets - they are subsets of X - but in X/R we think of each equivalence class as a single object. This can be a bit mentally taxing at first. This construction comes up all the time in number theory and abstract algebra.

example

The relation mod 5 relation M_5 on \mathbb{Z} yields a set \mathbb{Z}/M_5 with 5 elements:

$$\mathbb{Z}/M_5 = \{[0], [1], [2], [3], [4]\} = \{[5], [6], [2], [3], [4]\}$$

Note that $[0] = [5]$, $[1] = [6] = [11]$ and so on in \mathbb{Z}/M_5 .
Mathematicians usually denoted \mathbb{Z}/M_5 by $\mathbb{Z}/5\mathbb{Z}$, our book denotes it by \mathbb{Z}_5 . Let $S = [1]$. Then representatives of S are
 $1, 6, 11, 16, -4, -9, \dots$

You all (probably unknowingly) learned the following example in elementary school, when you accepted that $\frac{1}{2} = \frac{2}{4}$ and so on:

Recall we defined an equivalence relation Q on the set $X = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ of ordered pairs of integers (a, b) with $b \neq 0$ by

$$(a, b) Q (c, d) \iff ad = bc \quad \text{where } (a, b), (c, d) \in X,$$

(Note that $ad = bc$ implies that $\frac{a}{b} = \frac{c}{d}$ as numbers in \mathbb{Q} since $b, d \neq 0$.) Then I claim that the function

$$f : X/Q \rightarrow \mathbb{Q}$$

given by

$$f([(a, b)]) = \frac{a}{b}$$

is a well-defined function, and it is a bijection.

proof

- To show f is well defined, I have to show that if $[(a, b)] = [(c, d)]$ in X/Q , where $a, b, c, d \in \mathbb{Z}$ and $b, d \neq 0$, then $f([(a, b)]) \stackrel{?}{=} f([(c, d)])$. The condition $[(a, b)] = [(c, d)]$ means $ad = bc$, and hence that $\frac{a}{b} = \frac{c}{d}$ as numbers in \mathbb{Q} since $b, d \neq 0$. Hence

$$f([(a, b)]) = \frac{a}{b} = \frac{c}{d} = f([(c, d)])$$

so f is well-defined.

- The function f is clearly surjective - given $\frac{a}{b} \in \mathbb{Q}$, we have $f([(a, b)]) = \frac{a}{b}$.
- To show f is injective, suppose $f([(a, b)]) = f([(c, d)])$ where $a, b, c, d \in \mathbb{Z}$ and $b, d \neq 0$. Then $\frac{a}{b} = \frac{c}{d}$, and by definition of Q , this means $(a, b) \sim (c, d)$, i.e. $[(a, b)] = [(c, d)]$ and hence are the same element of X/Q !

Mod n, $\mathbb{Z}/n\mathbb{Z}$

There is nothing special about 5 in the example M_5 , we can replace 5 with any positive integer n :

Theorem

Let n be a positive integer. Let M_n denote the relation on \mathbb{Z} given by

$$x M_n y \iff x \equiv y \pmod{n}$$

Then M_n is an equivalence relation. The set \mathbb{Z}/M_n of equivalence classes has n elements and is denoted $\mathbb{Z}/n\mathbb{Z}$ (or Z_n in our book):

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$$

where for any $a \in \mathbb{Z}$,

$$[a] = \{a + nk \mid k \in \mathbb{Z}\} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$$

and any number $a + nk$ is a representative for $[a]$.

Recall the modular arithmetic theorem from Chapter 4, which states that mod respects the basic operations of arithmetic (except for division):

Theorem (Modular arithmetic)

Suppose $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then

1. $a + b \equiv a' + b' \pmod{n}$
2. $a - b \equiv a' - b' \pmod{n}$
3. $ab \equiv a'b' \pmod{n}$
4. $a^k \equiv (a')^k \pmod{n}$ for any positive integer k .

One consequence of the modular arithmetic theorem is that we can define addition and multiplication on $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$:

Theorem

Let n be a positive integer. The following binary operations $+$ and \cdot on $\mathbb{Z}/n\mathbb{Z}$ are well defined:

$$[a] + [b] = [a + b]$$

$$[a] \cdot [b] = [ab]$$

See p.383 of Epp for a more detailed discussion of what well-defined means; essentially if we have two $a, a' \in \mathbb{Z}$ such that $[a] = [a']$, then $[a] + [b]$ and $[a'] + [b]$, which by definition are $[a + b]$ and $[a' + b]$, are in fact equal. (This is basically the content of the modular arithmetic theorem).

Commutative Rings

Definition

Given a set A , a **binary operation** \star on A is a function $A \times A \rightarrow A$.

A **commutative ring** is a set A with two binary operations

$+ : A \times A \rightarrow A$ and $\star : A \times A \rightarrow A$, such that for all $a, b, c \in A$,

1. **commutative properties** $a + b = b + a$ and $a \cdot b = b \cdot a$
2. **associative properties** $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. **distributive property** $a(b + c) = a \cdot b + a \cdot c$.
4. A contains two distinct elements, which we will denote here by 0 and 1 such that $a + 0 = a$ and $a \cdot 1 = a$. So 0 is the additive identity and 1 is the multiplicative identity.
5. For all elements $a \in A$, there exists an element $a' \in A$ such that $a + a' = 0$. The element a' is called the additive inverse of a and is usually denoted $-a$.

Theorem

With the binary operations $+$ and \cdot defined on $\mathbb{Z}/n\mathbb{Z}$ by

$$[a] + [b] = [a + b]$$

$$[a] \cdot [b] = [ab]$$

the set $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring.