Logic, Proof, and General Mathematics

Michael W. Dekker
David M. McClendon

Department of Mathematics
Ferris State University

Fall 2021 edition

Contents

Chapter 1

Set theory and logic

1.1 Propositions

Definition 1.1 *A* **proposition** *is a statement that has exactly one truth value. This truth value is either* **true** *(denoted by T) or* **false** *(denoted by F).*

Proposition or not a proposition?

PROP	NOT PROP	
□	□	Lansing is the capital of Michigan.
□	□	The moon is made of green cheese.
□	□	Sunsets are beautiful.
□	□	How much did your parking permit cost?
□	□	He is a professional basketball player.
□	□	LeBron James is a professional basketball player.
□	□	x is an even number.
□	□	This statement is false.

Definition 1.2 *A* **paradox** *is a statement which, based on reasonable premises and acceptable reasoning, seems to be contradictory.*

Definition 1.3 *A proposition is called* **atomic** *(a.k.a.* **simple***) if it is made up of only one basic idea.*

A proposition is called **compound** *if it is made up of multiple ideas connected by* **connectives** *(words like "and", "or", "if", "not", etc.).*

A compound proposition is also called a **propositional form***.*

EXERCISE

Consider the following two propositions:

G = The moon is made of green cheese.
E = I can eat the moon.

Decide whether you (and/or your group) think each compound proposition in the first column below is true or false, in each the situations indicated in the first row of the chart.

WARNING: your answers here may be wrong; we'll see the right answers later.

		What you are to assume			
		G and E are both true	G true, but E false	G false, but E true	G and E are both false
What you are to determine the truth value of	"G and E"				
	"G or E"				
	"not G"				
	"if G, then E"				
	"G implies E"				
	"G, if E"				
	"G, only if E"				
	"G, but not E"				
	"G if and only if E"				

Definition 1.4 *Let P and Q be two propositions.*

1. *The* **conjunction** *of P and Q, written “P and Q” or “$P \wedge Q$”, is the proposition which is true exactly when* <u>*both*</u> *P and Q are true.*

2. *The* **disjunction** *of P and Q, written “P or Q” or “$P \vee Q$”, is the proposition which is true exactly when* <u>*at least one*</u> *of P and Q is true.*

3. *The* **negation** *of P and Q, written “not P” or “$\sim P$” or “$\neg P$”, is the proposition which is true exactly when P is false.*

“or” in mathematics versus “or” in English

Consider the statement:

I will have pepperoni or mushroom on the next pizza I order.

Interpreting this “or” as an **exclusive or**, this means you will have pepperoni or mushroom but not both toppings. Interpreting it as an **inclusive or**, this means you will have pepperoni, mushroom, or both toppings on your next pizza.

In math, all “or”s are <u>inclusive</u>.

Math Joke 1 *A mathematician’s wife gives birth. The doctor hands the newborn to the father. His wife asks, “Honey, is it a boy or a girl?” The mathematician replies, “   ”.*

If you ever need a symbol for the exclusive or, it’s $\veebar$.

Order of operations with connectives

When writing propositional forms, use parentheses whenever possible for clarity. Avoid writing things like

$$P \vee Q \wedge R.$$

That said, there is a clearly defined order of operations with connectives:

1. First, do anything in parentheses.

2. Second, or in the absence of parenthesis, do things in the following order:

   1) negation(s)
   2) conjunction(s) (i.e. “and”)
   3) disjunction(s) (i.e. “or”)

Based on these order of operations, $P \vee Q \wedge {\sim} R \vee S$ technically means

In English, commas suggest where parentheses belong:

"the door is open, and Johnny is here or it is raining"
vs.
"the door is open and Johnny is here, or it is raining"

Another example re: commas: "Let's eat, Mom!" versus "Let's eat Mom!")

Truth tables

Definition 1.5 *Given a compound proposition, a* **truth table** *for that proposition is a list of truth values of the form, given all possible truth values of its components.*

Basic truth tables:

P	${\sim} P$

P	Q	$P \wedge Q$	$P \vee Q$

Example 1

Construct a truth table for ${\sim} (P \wedge Q) \wedge R$.

P	Q	R	

Example 2

Construct a truth table for $(P \wedge Q) \vee \sim Q$.

P	Q		$\sim Q$	
T	T			
T	F			
F	T			
F	F			

Example 3

Construct the truth table for $P \vee \sim P$:

P	$\sim P$	$P \vee \sim P$
T		
F		

Question

For a compound proposition with n atomic components, how many rows are needed in your truth table?

Definition 1.6 *A* **tautology** *is a proposition that is true no matter what truth values are assigned to its components.*

Prototype example of a tautology

$$P \vee \sim P$$

"Sherlock Holmes is fictional, or Sherlock Holmes is not fictional."

Math Joke 2 *The first rule of Tautology Club is the first rule of Tautology Club.*

Definition 1.7 *A* **contradiction** *is a proposition that is false no matter what truth values are assigned to its components.*

Prototype example of a contradiction

Math Joke 3 *The first rule of Contradiction Club is not the first rule of Contradiction Club.*

Remark: The negation of a tautology is a contradiction, and vice versa.

Definition 1.8 *Two propositional forms are called* **logically equivalent** *(or just* **equivalent***) if they have the same truth values, no matter what truth values are assigned to their components (i.e. they have the same truth tables).*

$\Leftrightarrow$ versus $=$

We use the symbol $\Leftrightarrow$ to represent logical equivalence.

The symbol $=$ is used to represent ________________ , which is something else.

The importance of "logical equivalence":

If you are asked to prove a statement, you can prove <u>any</u> logically equivalent statement instead.

EXAMPLE 4

Determine whether or not $\sim(P \vee Q)$ and $\sim P \wedge \sim Q$ are logically equivalent.

Definition 1.9 *A* **denial** *of proposition P is any proposition that is logically equivalent to $\sim P$.*

EXAMPLE 5

Write down some denials of “It is raining and it is cold.”

EXAMPLE 6

Write down a denial of “The dog barked or my car was not stolen.”

Theorem 1.10 (Common Logical Equivalences) *Let P, Q and R be propositions. Then the following logical equivalences hold:*

Double Negation Law: $\sim(\sim P) \Leftrightarrow P$.

Commutative Laws:

“and” is commutative: $P \wedge Q \Leftrightarrow Q \wedge P$;

“or” is commutative: $P \vee Q \Leftrightarrow Q \vee P$.

Associative Laws:

“and” is associative: $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$;

“or” is associative: $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$.

Distributive Laws:

“and” distributes across “or”: $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$;

“or” distributes across “and”: $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.

DeMorgan Laws:

“not of an or” is the “and of the nots”: $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$;

“not of an and” is the “or of the nots”: $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$.

PROOF To prove the DeMorgan Laws, we use the following truth table:

P	Q	$P \wedge Q$	$\sim (P \wedge Q)$	$P \vee Q$	$\sim (P \vee Q)$	$\sim P$	$\sim Q$	$\sim P \vee \sim Q$	$\sim P \wedge \sim Q$
T	T	T	F	T	F	F	F	F	F
T	F	F	T	T	F	F	T	T	F
F	T	F	T	T	F	T	F	T	F
F	F	F	T	F	T	T	T	T	T

Since the fourth and ninth columns are the same, we see

$$\sim (P \wedge Q) \Leftrightarrow \sim P \vee \sim Q.$$

Since the sixth and last columns are the same, we see

$$\sim (P \vee Q) \Leftrightarrow \sim P \wedge \sim Q.$$

The proofs of the other statements also use truth tables and are omitted. □

Comments on this proof:

1. The proof starts with the word PROOF. When written by hand, this word should be underlined: “Proof:” The word Proof may be abbreviated Pf:
2. The proof is written in complete sentences and written in second person, present tense (i.e. “we see; we find; we know; etc.”) The **we** refers to the writer(s) of the proof and the reader(s) of the proof.
3. The proof begins with a phrase or sentence that describes how the proof works.
4. The proof ends with a □ (this symbol lets the reader know when the proof ends; this has its origins in a picture of a tombstone, because it means the problem of proving a statement is “dead and buried” once the statement is proven). Other symbols/remarks that can be used to signal the end of a proof are “Proven.”; “Proof done.”; “Q.E.D.”; #; ■; //; ⋈; ✓; ☺; etc. Pick a symbol you like and stick with it.

Your proofs should always have these (and other) characteristics.

1.2 Conditionals and biconditionals

Biconditionals

In the last section, we saw three connectives for propositions: $\wedge$, $\vee$ and $\sim$. In this section, we discuss two more connectives:

Definition 1.11 *A compound proposition "if P, then Q", where P and Q are propositions, is called a* **conditional***.*

In this context, P is called the **antecedent** *(or* **hypothesis** *or* **if part***) and Q is called the* **consequent** *(or* **conclusion** *or* **then part***).*

A conditional is true if whenever P is true, Q is also true.

We denote "if P, then Q" symbolically by $P \Rightarrow Q$.

Different ways of writing $P \Rightarrow Q$ in English include:

- if P, then Q
- P implies Q
- Q, if P
- P, only if Q
- P, therefore Q

More on $=$ versus $\Leftrightarrow$ versus $\Rightarrow$

Symbol	Meaning	What the symbol goes between	What the symbol means	Example(s)
$=$	equality	Two mathematical quantities	That the quantities are equal	$25 = \sqrt{625}$ $5 = x + 3$ $f(x) = g(h(x))$ $\mathbf{v} = (3, -5, 2)$
$\Leftrightarrow$	logical equivalence (if and only if)	Two propositions	That the propositions are both true, or both false	$P \Leftrightarrow Q$ $x = 4 \Leftrightarrow x - 3 = 1$ x is even $\Leftrightarrow$ x is not odd
$\Rightarrow$				
$\rightarrow$				
$\equiv$	congruence	?	TBD	

EXAMPLE 7 (FROM MATH 220)

Find the equation of the tangent line to $f(x) = x^2$ when $x = 3$.

Solution of a student who doesn't know what $=$ *means:*

$$f(x) = x^2 = f'(x) = 2x = 6 = 9 = \boxed{y = 9 + 6(x - 3)}.$$

Solution of a student who doesn't know what $\rightarrow$ *means:*

$$x^2 \rightarrow 2x \rightarrow 6 \rightarrow \boxed{y = 9 + 6(x - 3)}.$$

Solution of a student who almost gets it fully:

$$f(x) = x^2 \Rightarrow f'(x) = 2x \Rightarrow f'(3) = 6 \Rightarrow f(3) = 9 \Rightarrow \boxed{y = 9 + 6(x - 3)}.$$

Solution of a student who actually understands these symbols:

$f(x) = x^2 \Rightarrow f'(x) = 2x \Rightarrow f'(3) = 6$. Also, $f(3) = 9$. Tangent line is $\boxed{y = 9 + 6(x - 3)}$.

Use $=$, $\Leftrightarrow$, $\Rightarrow$ and $\rightarrow$ correctly.

Misuse of any of these symbols will be penalized.

An equivalent form of a conditional

Lemma 1.12 (Disjunctive normal form) $(P \Rightarrow Q) \Leftrightarrow (\sim P \vee Q)$.

PROOF These propositional forms have the same truth tables:

P	Q	$P \Rightarrow Q$	$\sim P$	$\sim P \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Since they have the same truth tables, they are logically equivalent. □

NOTE: The conditional $P \Rightarrow Q$ is true whenever P is false (no matter what is going on with Q).

Definition 1.13 *We say that* $P \Rightarrow Q$ *is* **vacuously true** *whenever* P *is false.*

P.S. What is a lemma?

EXAMPLE 8

Classify these conditionals as true or false:

1. If the moon is made of green cheese, then I can eat the moon.
2. 3 being a prime number implies 7 is a prime number.
3. $\sqrt{16} = 5$ whenever $\sqrt{9} = 3$.

Biconditionals

Definition 1.14 *Any compound proposition of the form "P if and only if Q", where P and Q are propositions, is called a* **biconditional***.*

Biconditionals are denoted symbolically by writing $P \Leftrightarrow Q$.

A biconditional $P \Leftrightarrow Q$ is true exactly when both P and Q are true, or both P and Q are false (put another way, $P \Leftrightarrow Q$ is true if P and Q are logically equivalent).

Lemma 1.15 $(P \Leftrightarrow Q) \Leftrightarrow ((P \wedge Q) \vee (\sim P \wedge \sim Q))$.

PROOF This was essentially stated in the definition of biconditional. □

Equivalent ways of writing $P \Leftrightarrow Q$ in English:

- P if and only if Q
- P iff Q
- P is logically equivalent to Q
- P and Q are (logically) equivalent

Lemma 1.16 *$P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.*

PROOF HW

Updated order of operations for logical connectives:

1. Connectives in parentheses.
2. $\sim$, then $\wedge$, then $\vee$, then $\Rightarrow$, then $\Leftrightarrow$.

EXAMPLE 9

Classify the following propositions as true or false:

1. Daniel Craig has played the role of James Bond if and only if Sean Connery has played the role of James Bond.
2. $2 + 7 = 8$ iff $8 \times 6 = 32$.
3. The graph of $y = x^2$ is a parabola $\Leftrightarrow$ if 8 is a prime number.

Sometimes, "if" means "iff"

Consider the following statements:

- I will play golf if today is Friday.
- You may play video games if you finish your chores.
- **Definition:** A number is **positive** if it is greater than zero.

Applications in algebra

You have a lot of practice with conditionals and biconditionals (even if you don't realize it):

EXAMPLE 10

Solve for x, if $5(x - 2) + 7(2x + 1) = 54$.

What you really meant when you wrote the steps on the previous page was:

$$\begin{aligned} && 5(x-2)+7(2x+1) &= 54 \\ \Leftrightarrow && 5x-10+14x+7 &= 54 \\ \Leftrightarrow && 19x-3 &= 54 \\ \Leftrightarrow && 19x &= 57 \\ \Leftrightarrow && x &= 3. \end{aligned}$$

In other words, each equation is its own proposition[1], and these propositions are equivalent (based on the laws of algebra). This is essentially a proof of the statement "$5(x-2)+7(2x+1)=54 \;\Leftrightarrow\; x=3$". That is what is meant by *solving* an equation: to solve an equation means to find a set such that the original equation is logically equivalent to the variable(s) belonging to that set (in this example, the set is $\{3\}$).

Comments on this solution:

When doing algebra in a proof (or anywhere else), you don't have to write the ⇔. But if you do, they should be to the left as above.

Also, notice that my equals signs and ⇔ signs are in vertical columns, directly above one another. **Yours should be too, if at all possible.** The align* command in Overleaf allows you to do this, by lining up the symbols after the &'s in each line.

Example 11 (Be careful!)

Solve for x if $\log_2 x + \log_2(x+2) = 3$.

Proposed solution:

$$\begin{aligned} && \log_2 x + \log_2(x+2) &= 3 \\ \Leftrightarrow && \log_2[x(x+2)] &= 3 \\ \Leftrightarrow && x(x+2) &= 2^3 \\ \Leftrightarrow && x^2+2x &= 8 \\ \Leftrightarrow && x^2+2x-8 &= 0 \\ \Leftrightarrow && (x-2)(x+4) &= 0 \\ \Leftrightarrow && x-2=0 & \quad \text{or } x+4=0 \\ \Leftrightarrow && x=2 & \quad \text{or } x=-4. \end{aligned}$$

Problem:

[1] Of course, since there's a variable x in these statements, they technically aren't propositions. They are something called *open sentences*, which we will discuss in the next section.

Recall the exercise from page 5:

$G =$ The moon is made of green cheese.
$E =$ I can eat the moon.

Here is the way the chart on page 5 should be filled out:

	G and E are both true	G true, but E false	G false, but E true	G and E are both false
"G and E" a.k.a. $G \wedge E$	T	F	F	F
"G aor E" a.k.a. $G \vee E$	T	T	T	F
"not G" a.k.a. $\sim G$	F	F	T	T
"if G, then E" a.k.a. "G implies E" a.k.a. "G, only if E" a.k.a. $G \Rightarrow E$	T	F	T	T
"G, if E" a.k.a. $E \Rightarrow G$	T	T	F	T
"G, but not E" a.k.a. $G \wedge \sim E$	F	T	F	F
"G if and only if E" a.k.a. $G \Leftrightarrow E$	T	F	F	T

Converse, contrapositive and inverse

Definition 1.17 *Let $P \Rightarrow Q$ be a conditional.*

- *The* **converse** *of $P \Rightarrow Q$ is the conditional $Q \Rightarrow P$.*
- *The* **contrapositive** *of $P \Rightarrow Q$ is the conditional $\sim Q \Rightarrow \sim P$.*
- *The* **inverse** *of $P \Rightarrow Q$ is the conditional $\sim P \Rightarrow \sim Q$.*

EXAMPLE 12

Write the converse, contrapositive and inverse of each statement.

1. If the moon is made of green cheese, then I can eat the moon.

   Converse:

   Inverse:

   Contrapositive:

2. If x is a prime number and x is even, then $x = 2$.

   Converse: If $x = 2$, then x is a prime number and x is even.

   Inverse: If x is not prime or x is odd, then $x \neq 2$.

   Contrapositive: If $x \neq 2$, then x is not prime or x is odd.

3. If f is differentiable or g is not continuous, then h is concave up.

   Converse:

   Inverse:

   Contrapositive:

<u>Truth tables for these conditionals</u>:

				conditional	converse	contrapositive	inverse
P	Q	$\sim P$	$\sim Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$\sim Q \Rightarrow \sim P$	$\sim P \Rightarrow \sim Q$
T	T	F	F	T	T		
T	F	F	T	F	T		
F	T	T	F	T	F		
F	F	T	T	T	T		

We have proven the following important result:

Theorem 1.18 *A conditional is logically equivalent to its contrapositive, and the converse of a conditional is logically equivalent to its inverse.*

Application of Theorem 1.18 in proofs:

If asked to prove a conditional $P \Rightarrow Q$, sometimes it is easier to prove the contrapositive $\sim Q \Rightarrow \sim P$.

This is especially true if the Q part already has a "not" in it somewhere.

1.3 Open sentences and sets

Definition 1.19 *A* **open sentence** *(a.k.a.* **predicate***) is a sentence that contains a variable (or variables). In this case the sentence is denoted $P(x)$ (if x is the only variable) or $P(x,y)$, etc.*

EXAMPLES

$x \leq 9$.

$x + y$ is a prime number.

Given an open sentence, we need to distinguish the variables that make the sentence true from the variables that make the sentence false. This leads us to a discussion of *sets*:

What is a set?

Definition 1.20 *A* **set** *is a definable collection of objects.*

The objects which comprise a set are called the set's **elements***.*

If x is an element of set E, we write $x \in E$ (we can also write $E \ni x$, but this direction is to be avoided if possible).

If x is not an element of set E, we write $x \notin E$.

Sets are usually denoted by capital letters, but they can be denoted by all kinds of things.

How do we define/describe sets?

In words: describe the set in a complete sentence (or sentences).

Example: E is the set of real numbers which are greater than π.
Example: Let F be the set of students in this MATH 324 class.

By writing the set's *roster* (a list of things in the set): such a list should be surrounded by braces.

Example: $A = \{1, 5, 7, 15, 19\}$
Example: $B = \{1, 2, 4, 8, 16, 32, ..., 2^{20}\}$
Example: $\mathbb{N} = \{0, 1, 2, 3, ...\}$

Using set-builder notation: this means defining a set as the collection of values which make some open sentence true. (That open sentence is called the **open sentence associated to the set** and if we need notation for it, we call it $P_E(x)$ if the set is called E.)

Example: $C = \{x \in \mathbb{N} : x \text{ is prime and } x > 30\}$

Example: $B = \{2^n : n \in \mathbb{N} \text{ and } n \leq 20\}$

Example: $E = \{x \in \mathbb{R} : x > \pi\}$

Example: $7\mathbb{Z} = \{7n : n \in \mathbb{Z}\}$

Three abbreviations for the phrase "such that"

s.t. $\quad$: $\quad$ |

EXAMPLE 13

Complete this chart:

SET DESCRIPTION IN WORDS	LIST OF ELEMENTS	SET-BUILDER NOTATION
	$E = \{7, 8, 9, 10, 11\}$	
		$F = \{x \in \mathbb{Z} : x^2 < 20\}$
G is the set of vowels in the English alphabet.		

Venn diagrams

We use Venn diagrams to illustrate the relationships among sets. In a Venn diagram, sets are represented by circles (or other shapes). The elements of a set are the "points" inside the circle representing that set, and the non-elements of a set are thought of as"points" outside the circle.

EXAMPLE 14

$A = \{0, 1, 2, 3\}$; $B = \{2, 3, 4\}$; $C = \{3, 4, 5\}$

Interval notation

Certain sets of real numbers can be described with interval notation:

Definition 1.21 *Let $a, b \in \mathbb{R}$. Define the following sets:*

- $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
- $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$
- $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
- $[a, \infty) = \{x \in \mathbb{R} : a \leq x\}$
- $(a, \infty) = \{x \in \mathbb{R} : a < x\}$
- $(-\infty, a] = \{x \in \mathbb{R} : x \leq a\}$
- $(-\infty, a) = \{x \in \mathbb{R} : x < a\}$

Any set of these eight types is called an **interval**.

Remark: "$a \leq x \leq b$" is shorthand for "$a \leq x$ and $x \leq b$".

EXAMPLE 15

1. Sketch a picture of the set $(-3,6]$.
2. True or false: $7 \in [8,14]$.
3. True or false: $9 \in (-\infty, 9)$.
4. What is $[5,3]$?

The empty set

Definition 1.22 *The* **empty set***, denoted $\varnothing$, is the set with no elements.*

The empty set is also denoted $\{\,\}$.

Remark: The use of the word "the" (as opposed to "a") before "empty set" needs to be justified (might there be more than one empty set?) See Theorem 1.26 below.

Subsets

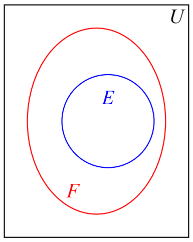
We say E is a subset of F if every element of E is an element of F:

Definition 1.23 *Let E and F be two sets. We say E is a* **subset** *of F, and write $E \subseteq F$, if $x \in E \Rightarrow x \in F$.*

If E is not a subset of F, we write $E \nsubseteq F$.

If $E \subseteq F$, we also write $F \supseteq E$ and say that F is a **superset** *of E.*

If $E \subseteq F$, then the corresponding Venn diagram of these two sets should look like this:



EXAMPLES

- If $A = \{1,2,3\}$ and $B = \{1,2,3,4,5\}$, then $A \subseteq B$.
- $[3,6] \subseteq [0,10]$.
- $[4,8] \nsubseteq [5,\infty)$.

EXERCISE

Let $A = \{1,2,3,4,5\}$ and $B = \{1,3,5\}$. Classify the following statements:

	VALID	VALID	
	NOTATION	NOTATION	
NONSENSE	BUT FALSE	AND TRUE	
□	□	□	$3 \in A$
□	□	□	$3 \subseteq A$
□	□	□	$3 \nsubseteq A$
□	□	□	$\{3\} \subseteq A$
□	□	□	$4 \notin A$
□	□	□	$4 \notin B$
□	□	□	$1,2,3 \in A$
□	□	□	$\{1,2,3\} \in A$
□	□	□	$0,1,2 \in A$
□	□	□	$\{0,1,2\} \subseteq A$
□	□	□	$\{1,2,3\} \subseteq A$
□	□	□	$B \subseteq A$
□	□	□	$A \subseteq B$
□	□	□	$A \nsubseteq B$

Lemma 1.24 *The empty set is a subset of every other set.*

PROOF Let E be a set. The statement "$\varnothing \subseteq E$" is equivalent to the conditional "if $x \in \varnothing$, then $x \in E$". But the hypothesis of this conditional is always false, so the conditional is vacuously true. □

Equality of sets

Two sets E and F are equal if they have exactly the same members. This means every element of E is an element of F (i.e. $E \subseteq F$) and every element of F is a subset of E (i.e. $F \subseteq E$):

Definition 1.25 *Let E and F be two sets. We say E and F are* **equal**, *and write $E = F$, if $E \subseteq F$ and $F \subseteq E$.*

If E and F are not equal, we write $E \neq F$.

We can now justify why we say "the empty set" rather than "an empty set":

Theorem 1.26 *There is only one empty set.*

PROOF Suppose A and B are both empty sets (i.e. they both have no elements). By Lemma 1.24 applied to the empty set A, $A \subseteq B$. By the same lemma applied to the empty set B, $B \subseteq A$. Thus $A = B$. □

Definition 1.27 *Let E and F be two sets. We say E is a* **proper subset** *of F if $E \subseteq F$ and $E \neq F$.*

Some authors use $\subseteq$ for subset and $\subset$ for proper subset, but others use $\subset$ for subset and $\subsetneq$ for proper subset. In this class we will use $\subseteq$ for subset and not use any symbol for proper subset.

Sets of sets

It is allowable for elements of sets to be themselves sets.

EXAMPLE 16

Suppose $A = \{0, 1, \{2, 3\}, \{4, 5, 6\}\}$. Classify the following statements as true or false:

1. $1 \in A$
2. $\{2, 3\} \in A$
3. $\{2, 3\} \subseteq A$
4. $\{\{2, 3\}\} \subseteq A$
5. $\{1, \{4, 5, 6\}\} \subseteq A$
6. $5 \in A$
7. $\{0, 1\} \in A$
8. $\{\{3, 4\}\} \subseteq A$

Definition 1.28 *Let E be a set. The* **power set** *of E, denoted 2^E or $\mathcal{P}(E)$, is the set of all subsets of E.*

EXAMPLE 17

Suppose $E = \{a, b, c\}$. List the elements of 2^E.

What isn't a set?

For a long time, mathematicians believed that any collection of objects constituted a set. This causes problems, however. Here is an example, called **Russell's paradox**:

Let X be the set consisting of all sets. Define a set $E \in X$ to be **ordinary** if it is not a subset of itself. In other words,

$$E \text{ is ordinary } \Leftrightarrow E \notin E.$$

Let O be the set of all ordinary sets. Is O ordinary?

To fix this paradox, mathematicians restrict the kinds of collections of objects that can be called a "set". These restrictions are called the Zermelo-Fraenkel (ZF) axioms (Google them if you want to read more about them); collections whose definitions obey these axioms are called **definable**; that's why we define a set to be a definable collection of objects.

That said, you shouldn't worry - you would never cook up an undefinable collection of objects unless you were specifically trying to do so.

Connecting sets with open sentences

Every every open sentence goes with a set, and every set translates to an open sentence, via the following correspondence:

Definition 1.29 *Given an open sentence $P(x)$, the set of all x for which $P(x)$ is true is called the* **truth set** *of $P(x)$.*

Lemma 1.30 *Given a set E, the open sentence $P_E(x)$ ="$x \in E$" is an open sentence whose truth set is E.*

Important Note: Exactly what the truth set is depends on what kinds of things we are thinking of as the variables in the open sentence. For example, consider the open sentence

He is a professional basketball player.

The things we are thinking of as "he" are human beings. We say the **universe of discourse** of this statement is the set of human beings; then the truth set is the set of (male) professional basketball players.

Typical universes of discourse in mathematics (for single variables):

$\mathbb{N}$	=	natural numbers	$= \{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	=	integers	$= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$n\mathbb{Z}$	=	multiples of n	$= \{\ldots, -2n, -n, 0, n, 2n, 3n, \ldots\}$
$\mathbb{Q}$	=	rational numbers	$= \{\frac{p}{q} : p, q \in \mathbb{Z}$ and $q \neq 0\}$
$\mathbb{R}$	=	real numbers	
$\mathbb{C}$	=	complex numbers	$= \{x + iy : x, y \in \mathbb{R}\}$
Ω	=	some probability space	(discussed in MATH 414)

More on these sets later in the course.

Definition 1.31 *Two open sentences $P(x)$ and $Q(x)$ are called* **(logically) equivalent in a given universe** *if they have the same truth set in that universe.*

Two open sentences are called **(logically) equivalent** *if they have the same truth set in any universe. In this setting, we can write $P(x) \Leftrightarrow Q(x)$.*

Theorem 1.32 *Two sets E and F are equal if and only if their corresponding open sentences $P_E(x)$ ="$x \in E$" and $P_F(x)$ ="$x \in F$" are logically equivalent.*

PROOF If $P_E(x) \Leftrightarrow P_F(x)$, then $x \in E$ implies $x \in F$ (meaning $E \subseteq F$) and vice versa (meaning $F \subseteq E$). Thus $E = F$ by definition of set equality.

Conversely, if $E = F$, then $E \subseteq F$ so by definition of subset $P_E(x) \Rightarrow P_F(x)$. Similarly, $F \subseteq E$, implying $P_F(x) \Rightarrow P_E(x)$. Since $P_E(x)$ and $P_F(x)$ both imply the other, we conclude they are logically equivalent (by definition of logical equivalence). □

EXAMPLE 18

Consider the open sentence $x^2 = 25$.

1. What is the truth set in $\mathbb{N}$? *Answer:* $\{5\}$.
2. What is the truth set in $\mathbb{Z}$? *Answer:* $\{-5, 5\}$.
3. What is the truth set in $\mathbb{R}$? *Answer:* $\{-5, 5\}$.
4. What is the truth set in the interval $[-3, 3]$?

EXAMPLE 19

Consider the open sentences

$$\log[x(x+9)] = 1 \text{ and } \log x + \log(x+9) = 1.$$

1. Are these equivalent in $\mathbb{N}$? *Answer:* Yes. Both have truth set $\{1\}$.
2. Are these equivalent in $\mathbb{R}$? *Answer:* No. The first has truth set $\{-10, 1\}$ but the second has truth set $\{1\}$.

1.4 Existential and universal quantifiers

Turning open sentences into propositions

Consider an open sentence like "x is a power of a prime number". Here are some ways to turn this open sentence into a proposition:

1. Choose a specific value for x, like 20511149. Then the corresponding proposition is

   "20511149 is a power of a prime number."

2. Add an "existential quantifier" in front of the open sentence, like so:

   " x is a power of a prime number."

3. Add a "universal quantifier" in front of the open sentence, like so:

   " x is a power of a prime number."

Existential quantifiers

Definition 1.33 *Let $P(x)$ be an open statement. The proposition*

"there exists an x such that $P(x)$ is true"

is denoted

$$(\exists x)P(x) \text{ or } \exists x\, P(x) \text{ or } \exists x : P(x) \text{ or } \exists x \,|\, P(x) \text{ or } \exists x \text{ s.t. } P(x).$$

This sentence is true if the truth set of $P(x)$ is nonempty.
The symbol $\exists$ is called an **existential quantifier**.

EXAMPLE 20

Consider the proposition $\exists x : x^2 + 1 = 0$.

1. Is this proposition true or false in $\mathbb{R}$?
2. Is this proposition true or false in $\mathbb{C}$?

To specify the universe of discourse as a set U, we would write an existential quantifier as $\exists x \in U : x^2 + 1 = 0$.

English phrases suggesting existential quantifiers: "for some"; "there is"; "there are"; "at least one"; etc.

Unique existential quantifiers

Definition 1.34 *Let $P(x)$ be an open statement. The proposition*

"there exists a unique x such that $P(x)$ is true"

is denoted

$$(\exists! x)P(x) \text{ or } \exists! x\, P(x) \text{ or } \exists! x : P(x) \text{ or } \exists! x \,|\, P(x) \text{ or } \exists! x \text{ s.t. } P(x).$$

This sentence is true if the truth set of $P(x)$ has exactly one member.
The symbol $\exists!$ is called a **unique existential quantifier**.

EXAMPLE 21

Consider the proposition $\exists! x : x^2 = 16$.

1. Is this proposition true or false in $\mathbb{N}$?
2. Is this proposition true or false in $\mathbb{Z}$?

English phrases suggesting unique existential quantifiers: “one and only one”; “exactly one”; etc.

Universal quantifiers

Definition 1.35 *Let $P(x)$ be an open statement. The proposition “for every x in the universe, $P(x)$ is true” is denoted*

$$(\forall x)P(x) \text{ or } \forall x\, P(x) \text{ or } \forall x, P(x) \text{ or } \forall x \in U, P(x).$$

This sentence is true if the truth set of $P(x)$ is the entire universe U. The symbol $\forall$ is called a **universal quantifier***.*

Example 22

Consider the proposition $\forall x$, $x \geq 0$.

1. Is this proposition true or false in $\mathbb{N}$?
2. Is this proposition true or false in $\mathbb{R}$?

English phrases suggesting universal quantifiers: “all”; “every”; “each”; etc.

Implied universal quantifiers:

We often write statements in mathematics like

$$(x \text{ is prime and } x \neq 2) \Rightarrow x \text{ is odd.}$$

What we really mean by a statement like this is

$$\forall x, [(x \text{ is prime and } x \neq 2) \Rightarrow x \text{ is odd}].$$

In other words, in a (bi)conditional involving open sentences, the universal quantifier is implied but not always stated.

Negations and denials of quantified statements

Consider the proposition “all swans are white”. The negation of this is technically

“It is not the case that all swans are white.”

What is a more useful way of expressing this negation (i.e. what is a more useful denial)?

Lemma 1.36 (Denial of a universal quantifier) *For any open sentence $P(x)$,*

$$\exists x :\sim P(x) \text{ is a denial of } \forall x, P(x).$$

PROOF In any universe:

$$\begin{aligned} \sim \forall x, P(x) \text{ is true } &\Leftrightarrow \forall x, P(x) \text{ is false} \\ &\Leftrightarrow \text{the truth set of } P(x) \text{ is not the entire universe} \\ &\Leftrightarrow \text{the truth set of } \sim P(x) \text{ is not empty} \\ &\Leftrightarrow \exists x :\sim P(x) \text{ is true. } \square \end{aligned}$$

Now consider the proposition “there is a dog which can speak English”. Its negation is

“It is not the case that there is a dog which can speak English.”

A more useful denial is

Lemma 1.37 (Denial of a existential quantifier) *For any open sentence $P(x)$,*

$$\forall x, \sim P(x) \text{ is a denial of } \exists x, P(x).$$

PROOF In any universe:

$$\begin{aligned} \sim \exists x : P(x) \text{ is true } &\Leftrightarrow \exists x : P(x) \text{ is false} \\ &\Leftrightarrow \text{the truth set of } P(x) \text{ is empty} \\ &\Leftrightarrow \text{the truth set of } \sim P(x) \text{ is the whole universe} \\ &\Leftrightarrow \forall x, \sim P(x) \text{ is true. } \square \end{aligned}$$

EXAMPLE 23

Construct useful denials of the following propositions:

1. $\forall x\, \exists y\, \exists z\, \forall u\, \exists v : x + y + z > 2u + v$

2. Every positive real number has a multiplicative inverse.

1.5 Operations on sets

The big picture

In the last section, we saw that there is a correspondence between sets and open sentences.

$$\text{set } E \rightsquigarrow \text{ open sentence } P_E(x) = \text{“}x \in E\text{”}$$
$$\text{open sentence } P(x) \rightsquigarrow \text{ truth set } E_{P(x)} \text{ of } P(x)$$

Earlier in the course, we learned a series of connectives which can be used to make complicated propositions/open sentences out of simpler ones. These connectives include:

In this section, we discuss operations on sets which are analogues of these connectives.

The big picture is that sets, together with the operations on sets presented in this section, provide a formal mathematical language for doing logical thinking. This explains why sets are a key building block of mathematics.

Union

The union of two (or more) sets is the set of objects which belong to at least one of the sets:

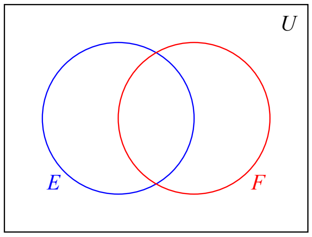
Definition 1.38 *Let E and F be sets. The* **union** *of E and F, denoted $E \cup F$, is defined as follows:*

$$E \cup F = \{x : x \in E \text{ or } x \in F\}.$$

Equivalently, if E and F are associated to open sentences are $P_E(x)$ and $P_F(x)$, respectively, then $E \cup F$ is the truth set of $P_E(x) \vee P_F(x)$.

Concept: $\cup$ is set language for “or”.

Venn diagram:



Basic example: If $E = \{1,2\}$ and $F = \{2,3\}$, then $E \cup F = \{1,2,3\}$.

Definition 1.39 *Let Δ be a nonempty set, so that for each $\alpha \in \Delta$ there is a corresponding set E_α.*

The collection of sets $\{E_\alpha : \alpha \in \Delta\}$ is called an **indexed family** *of sets (this family is denoted by $\{E_\alpha\}_{\alpha\in\Delta}$).*

The **index** *of the set is α and the* **index set** *of the family is Δ.*

We often use letters from the middle of the alphabet (i through n) for the index, but the use of these letters strongly implies that the index set is $\mathbb{N}$ or $\mathbb{Z}$, or a subset of $\mathbb{N}$ or $\mathbb{Z}$.

Definition 1.40 *Let $\{E_\alpha\}_{\alpha\in\Delta}$ be an indexed family of sets. The* **union** *of these sets, denoted $\bigcup_\alpha E_\alpha$ or $\bigcup\limits_{\alpha\in\Delta} E_\alpha$, is defined as follows:*

$$\bigcup_\alpha E_\alpha = \{x : \exists \alpha \in \Delta \text{ s.t. } x \in E_\alpha\}$$

So $\bigcup_\alpha E_\alpha$ is the set of things belonging to <u>at least one</u> of the E_α.

EXAMPLE 24

$\Delta = \mathbb{N}$; $E_n = \{1,2,3,...,n\}$. What is $\bigcup\limits_{n\in\mathbb{N}} E_n$? What about $\bigcup\limits_{n=1}^{8} E_n$?

Intersection

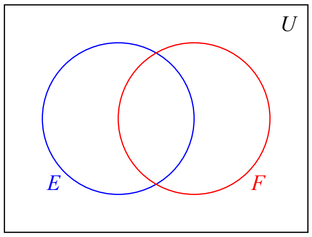
Definition 1.41 *Let E and F be sets. The* **intersection** *of E and F, denoted $E \cap F$, is defined as follows:*

$$E \cap F = \{x : x \in E \text{ and } x \in F\}.$$

Equivalently, if E and F are associated to open sentences are $P_E(x)$ and $P_F(x)$, respectively, then $E \cup F$ is the truth set of $P_E(x) \wedge P_F(x)$.

Concept: $\cap$ is set language for "and".

Venn diagram:



Basic example: If $E = \{1, 2\}$ and $F = \{2, 3\}$, then $E \cap F = \{2\}$.

Definition 1.42 *Let $\{E_\alpha\}_{\alpha \in \Delta}$ be an indexed family of sets. The* **intersection** *of these sets, denoted $\bigcap_\alpha E_\alpha$ or $\bigcap_{\alpha \in \Delta} E_\alpha$, is defined as follows:*

$$\bigcap_\alpha E_\alpha = \{x : \forall \alpha \in \Delta, x \in E_\alpha\}$$

So $\bigcap_\alpha E_\alpha$ is the set of things belonging to all of the E_α.

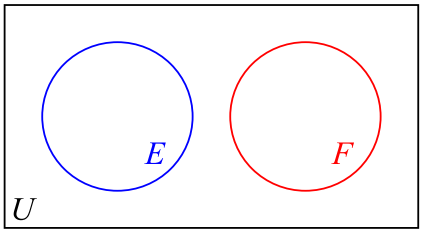
EXAMPLE 25

$\Delta = [0, \infty)$; $E_\alpha = [\alpha, \infty)$. What is $\bigcap\limits_{\alpha \in \mathbb{R}} E_\alpha$? What about $\bigcap\limits_{n=2}^{5} E_\alpha$?

Disjointness

Sets which have no elements in common are called disjoint:

Definition 1.43 *Let E and F be sets. We say E and F are* **disjoint** *(a.k.a.* **mutually exclusive***) if $E \cap F = \varnothing$. Equivalently, this means the open sentence $P_E(x) \wedge P_F(x)$ is a contradiction.*



Definition 1.44 *Let $\{E_\alpha\}_{\alpha \in I}$ be a collection of sets indexed by α. We say the E_α are* **pairwise disjoint** *if for every $\alpha, \beta \in I$, if $\alpha \neq \beta$ then $E_\alpha \cap E_\beta = \varnothing$.*

Some authors use notation like

$$X = E \mathbin{\dot{\bigcup}} F \qquad \text{or} \qquad X = E \bigsqcup F.$$

These two statements mean the same thing: that X is the **disjoint union** of E and F, i.e. that

1. $X = E \cup F$; and
2. E and F are disjoint.

Complement

The complement of a set is the set of things not in the set:

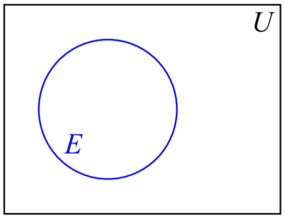
Definition 1.45 *Let E be a set. The* **complement** *of E, denoted E^C, is the set*

$$E^C = \{x : x \notin E\}.$$

Equivalently, if E is associated to open sentence $P_E(x)$, then E^C is the truth set of $\sim P_E(x)$.

Concept: complement is set language for “not”.

Venn diagram:



Other notation: E^C is also denoted $\sim E$, $\widetilde{E}$, $\overline{E}$, E^c, $\neg E$, $-E$, and lots of other things as well.

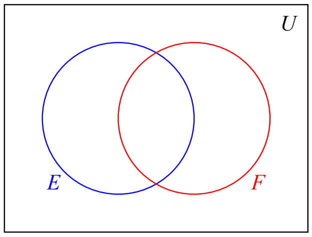
NOTE: The complement has to be taken with respect to a universe of discourse U, which is usually understood without being stated.

Difference and symmetric difference

Definition 1.46 *Let E and F be sets. The* **difference** *of E and F, denoted $E - F$ and read "E minus F", is the set $E - F = E \cap F^C$.*

Concept: start with the set of things in E, then "take away" the things in F to get $E - F$.

Venn diagram:

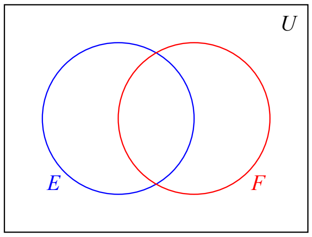


Other notation: $E - F$ is also denoted $E \backslash F$ and $E \sim F$.

Definition 1.47 *Let E and F be sets. The* **symmetric difference** *of E and F, denoted $E \bigtriangleup F$, is the set $E \bigtriangleup F = (E - F) \cup (F - E)$. Equivalently, if E and F are associated to open sentences are $P_E(x)$ and $P_F(x)$, respectively, then $E \cup F$ is the truth set of $P_E(x) \veebar P_F(x)$.*

Concept: $\bigtriangleup$ is set language for the exclusive or.

Venn diagram:



Cartesian product

The Cartesian product of two sets is the set of ordered pairs, where the first element comes from the first set and the second element comes from the second set.

Definition 1.48 *Let E and F be sets. The* **(Cartesian) product** *of E and F, denoted $E \times F$ and read "E cross F", is the set*

$$E \times F = \{(x, y) : x \in E \text{ and } y \in F\}.$$

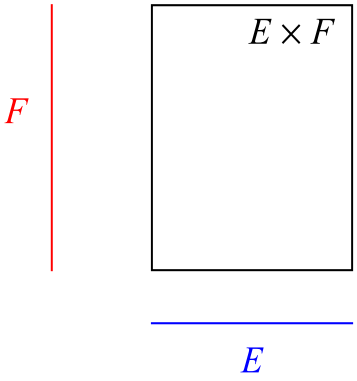
The elements of a Cartesian product are called **ordered pairs***.*

We denote $E \times E$ by E^2.

Equivalently, if E and F are associated to open sentences are $P_E(x)$ and $P_F(y)$, respectively, then $E \cup F$ is the truth set of $P_E(x) \wedge P_F(y)$ (this is a set of ordered pairs (x, y)).

Concept: Cartesian product is set language for "and", where the two open sentences being conjoined have different variables.

Venn diagram:



Definition 1.49 (Equality in Cartesian product) *Let (a, b) and (x, y) be ordered pairs. To say $(a, b) = (x, y)$ means $a = x$ and $b = y$.*

This means in particular that (unless $a = b$), $(a, b) \neq (b, a)$.

Similarly, unless $E = F$, $E \times F$ is not equal to $F \times E$.

Most common example: $\mathbb{R}^2$ is the set of ordered pairs (x, y) of real numbers.

Note: (a, b), $\{a, b\}$, and $[a, b]$ are all different:

$$\begin{aligned} [a,b] &= \text{ the interval of real numbers } [a,b] = \{x \in \mathbb{R} : a \leq x \leq b\} \\ \{a,b\} &= \text{ the set with two elements } a \text{ and } b \\ (a,b) &= \begin{cases} \text{the interval of real numbers } (a,b) = \{x \in \mathbb{R} : a < x < b\} \\ \quad \textit{OR} \\ \text{the ordered pair } (a,b) \in \text{ some Cartesian product} \end{cases} \end{aligned}$$

Definition 1.50 *Let E be a set and let n be a positive integer. The n^{th}* **Cartesian power** *of E, denoted E^n, is the set of* **ordered n-tuples** *of elements from E:*

$$E^n = \{(x_1, x_2, ..., x_n) : \forall j, x_j \in E\}.$$

Two ordered n-tuples $(x_1, ..., x_n)$ and $(y_1, ..., y_n)$ are equal if $x_j = y_j$ for all j.

Order of operations with set notation:

1. Anything in parentheses
2. Complements
3. Intersections
4. Unions
5. Cartesian products

That said, it is best to always write set expressions with parentheses to avoid confusion.

EXAMPLE 26

Let $A = \{2,3,5,7\}$, $B = \{1,3,5,7,9\}$ and $C = \{2,4\}$ (consider these to be in the universe $U = \{1,2,3,4,5,6,7,8,9,10\}$). Give lists of each set:

1. $A \cup B$

2. $A \cap B$

3. $C \cup (B \cap A)$

4. $(C \cup B) \cap A$

   Note: the answers to # 3 and # 4 are not the same. This means that you should avoid writing things like $C \cup B \cap A$ (even though technically this means what is written in # 3).

5. $A - B$

6. $B - A$

7. A^C

8. $A \bigtriangleup B$

9. $A \bigtriangleup A$

10. $A \times C$

11. C^2

12. $(A \cap C)^2$

Translation between set operations and logic

- Given a set E, think of the open sentence $P_E(x) =$ "$x \in E$".
- Given an open sentence $P(x)$, let E be its truth set.

LOGICAL CONSTRUCT		CORRESPONDING SET CONSTRUCT	
open sentence	$P_E(x)$	set	E
or	$P_E(x) \vee P_F(x)$	union	$E \cup F$
and (same variables in both sentences)	$P_E(x) \wedge P_F(x)$	intersection	$E \cap F$
and (different variables in each sentence)	$P_E(x) \wedge P_F(y)$	Cartesian product	$E \times F$
negation	$\sim P_E(x)$	complement	E^C
exclusive or	$P_E(x) \veebar P_F(x)$	symmetric difference	$E \vartriangle F$
implication	$P_E(x) \Rightarrow P_F(x)$	subset	$E \subseteq F$
logical equivalence	$P_E(x) \Leftrightarrow P_F(x)$	set equality	$E = F$
tautology	T	universe of discourse	U
contradiction	F	empty set	$\varnothing$

Here's a shorthand version of the same chart:

SET CONSTRUCT	E	$\cup$	$\cap$	^{C}	$\vartriangle$	$\subseteq$	$=$	U	$\varnothing$
LOGICAL CONSTRUCT	$P_E(x)$	$\vee$	$\wedge$	$\sim$	$\veebar$	$\Rightarrow$	$\Leftrightarrow$	T	F

In Theorem 1.10, we learned these common logical equivalences (proved by showing they have the same truth tables):

Double Negation Law: $\sim(\sim P) \Leftrightarrow P$.
Commutative Laws:
"and" is commutative: $P \wedge Q \Leftrightarrow Q \wedge P$;
"or" is commutative: $P \vee Q \Leftrightarrow Q \vee P$.
Associative Laws:
"and" is associative: $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$;
"or" is associative: $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$.
Distributive Laws:
"and" distributes across "or": $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$;
"or" distributes across "and": $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$.
DeMorgan Laws:
"not of an or" is the "and of the nots": $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$;
"not of an and" is the "or of the nots": $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$.

Each of these common logical equivalences translates directly into a corresponding property about sets:

Theorem 1.51 (Basic Properties of Set Operations) *Let E, F, G be sets. Then:*

Double complement law: $(E^C)^C = E$.

Commutative laws:
$\cup$ *is commutative:* $E \cup F = F \cup E$;
$\cap$ *is commutative:* $E \cap F = F \cap E$.

Associative laws:
$\cup$ *is associative:* $(E \cup F) \cup G = E \cup (F \cup G)$;
$\cap$ *is associative:* $(E \cap F) \cap G = E \cap (F \cap G)$.

Distributive laws:
$\cap$ *distributes across* $\cup$: $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$;
$\cup$ *distributes across* $\cap$: $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$.

DeMorgan laws:
complement of a union is the intersection of the complements:

$$(E \cup F)^C = E^C \cap F^C;$$

complement of an intersection is the union of the complements:

$$(E \cap F)^C = E^C \cup F^C.$$

PROOF Throughout this proof, for any set S we let $P_S(x)$ be the open sentence "$x \in S$". Recall from Theorem 1.32 that two sets are equal if and only if their corresponding open sentences are logically equivalent.

To prove the Double Complement Law, note that the open sentence associated to $(E^C)^C$ satisfies

$$P_{(E^C)^C}(x) \Leftrightarrow \sim P_{E^C}(x) \Leftrightarrow \sim (\sim P_E(x)) \Leftrightarrow P_E(x).$$

Since $P_{(E^C)^C}(x) \Leftrightarrow P_E(x)$, we can conclude $(E^C)^C = E$ by Theorem 1.32.

To prove the first DeMorgan Law, note that the open sentence associate to $(E \cup F)^C$ satisfies

$$P_{(E\cup F)^C}(x) \Leftrightarrow \sim P_{E\cup F}(x) \Leftrightarrow \sim [P_E(x) \vee P_F(x)].$$

By DeMorgan's Law for logical operations, this last statement is equivalent to

$$\sim P_E(x) \wedge \sim P_F(x) \Leftrightarrow P_{E^C}(x) \wedge P_{F^C}(x) \Leftrightarrow P_{E^C \cap F^C}(x).$$

Since $P_{(E\cup F)^C}(x) \Leftrightarrow P_{E^C \cap F^C}(x)$, we can conclude $(E \cup F)^C = E^C \cap F^C$ by Theorem 1.32.

The other proofs are similar and omitted (although I may ask you to prove some as homework). □

1.6 Rules of inference

Definition 1.52 *A* **rule of inference** *is a conditional which is a tautology.*

Some initial comments:

Recall that a **conditional** is an "if, then" statement, and a **tautology** is something that is always true.

Rules of inference are used commonly in proofs.

You don't *memorize* rules of inference; rather, you *internalize* them.

Every rule of inference has a natural interpretation in terms of sets. *Throughout this section, think of P, Q and R as the open sentences corresponding to sets E, F and G.*

Modus ponens

Theorem 1.53 (Modus ponens) *Let P and Q be propositions.*

$$[(P \Rightarrow Q) \wedge P] \Rightarrow Q.$$

PROOF All rules of inference can be proven by truth tables:

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge P$	$[(P \Rightarrow Q) \wedge P] \Rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

From the above, modus ponens is a tautology. □

Corollary 1.54 (Set version of modus ponens) *Let E and F be sets. If $E \subseteq F$ and $x \in E$, then $x \in F$.*

Modus ponens is the most important and most commonly used tool in logical reasoning:

EXAMPLES OF MODUS PONENS

1. *Assumptions:* If today is Friday, I will buy a beer. Today is Friday.

   Conclusion: I will buy a beer.

2. *Assumptions:* All animals that quack are ducks. Tom is an animal that quacks.

   Conclusion: Tom is a duck.

3. *Assumptions:* All differentiable functions are continuous.
   $f(x) = 2x^2 \sin x$ is differentiable.

   Conclusion: f is a continuous function.

4. *Assumption:* $x \in \mathbb{Z}$.

   Conclusion: $x \in \mathbb{R}$.

Disjunctive syllogism

Theorem 1.55 (Disjunctive syllogism) *Let P and Q be propositions.*

$$[(P \vee Q) \wedge \sim P] \Rightarrow Q.$$

PROOF Use truth tables:

P	Q	$P \vee Q$	$\sim P$	$(P \vee Q) \wedge \sim P$	$[(P \vee Q) \wedge \sim P] \Rightarrow Q$
T	T	T	F	F	
T	F	T	F	F	
F	T	T	T	T	
F	F	F	T	F	

From the above, disjunctive syllogism is a tautology. □

Corollary 1.56 (Set version of disjunctive syllogism) *Let E and F be sets. If $x \in E \cup F$ and $x \notin E$, then $x \in F$.*

EXAMPLES OF DISJUNCTIVE SYLLOGISM

1. *Assumptions:* I will eat a sandwich for lunch, or my car is green.
   I eat (only) soup for lunch.

   Conclusion:

2. *Assumptions:* $x \in \{1, 2, 3, 4, 5\}$, but $x \notin \{1, 2, 3\}$.

   Conclusion:

Reductio ad absurdum

Theorem 1.57 (Reductio ad absurdum) *Let P and Q be propositions.*

$$[\sim P \Rightarrow (Q \wedge \sim Q)] \Rightarrow P.$$

PROOF HW

Sherlock Holmes is famous for applying reductio ad absurdum: "When you have eliminated the impossible, what remains, however improbable, must be the truth."

Corollary 1.58 (Set version of reductio ad absurdum) *Let E and F be sets. If $E^C \subseteq (F \cap F^C)$, then E is the universal set.*

Remark: This set version of reductio ad absurdum isn't that useful, because it is really just saying $E^C \subseteq \varnothing$, which implies $E^C = \varnothing$, meaning E is universal.

EXAMPLES OF REDUCTIO AD ABSURDUM 1.

Assumption: If it doesn't rain tomorrow, then I will both drink tea and not drink tea tomorrow.

Conclusion: It will rain tomorrow.

2. *Assumption:* If $z > 0$, then x is even and x is not even.

Conclusion:

Modus tollens

Theorem 1.59 (Modus tollens) *Let P and Q be propositions.*

$$[(P \Rightarrow Q) \wedge \sim Q] \Rightarrow \sim P.$$

PROOF Use truth tables (details omitted).

Corollary 1.60 (Modus tollens, set version) *Let E and F be sets.*

If , *then* .

EXAMPLES OF MODUS TOLLENS

1. *Assumptions:* If the moon is made of green cheese, then I can eat it.
I cannot eat the moon.

Conclusion:

2. *Assumptions:* If P is a probability measure, then $\sum_x P(x) = 1$. $\sum_x P(x) = 2$.

Conclusion: P is not a probability measure.

3. *Assumptions:* If A is not invertible, then the determinant of A is zero.
The determinant of A is 5.

Conclusion: A is invertible.

Conjunction elimination

Theorem 1.61 (Conjunction elimination) *Let P and Q be propositions.*

$$(P \wedge Q) \Rightarrow P.$$

Corollary 1.62 (Conjunction elimination, set version) *Let E and F be sets. If $x \in E \cap F$, then $x \in E$.*

Example of conjunction elimination

Assumption: Granny Smith apples are green and it is snowing.

Conclusion: Granny Smith apples are green.
Conclusion # 2: It is snowing.

Disjunction introduction

Theorem 1.63 (Disjunction introduction) *Let P and Q be propositions.*

$$P \Rightarrow (P \vee Q).$$

Corollary 1.64 (Disjunction introduction, set version) *Let E and F be sets. If $x \in E$, then $x \in E \cup F$.*

Example of disjunction introduction

Assumption: The distance from Chicago to Detroit is less than 1000 miles.

Conclusion: The distance from Chicago to Detroit is less than 1000 miles, or $3 < 2$.

Case analysis

Theorem 1.65 (Case analysis) *Let P, Q and R be propositions.*

$$[(P \Rightarrow R) \wedge (Q \Rightarrow R)] \Rightarrow [(P \vee Q) \Rightarrow R].$$

Corollary 1.66 (Case analysis, set version) *Let E, F and G be sets.*

If , *then* .

Example of case analysis

Assumption: Every positive real number is surd. Every negative real number is surd.

Conclusion:

Disjunctive normal form

Theorem 1.67 (Disjunctive normal form) *Let P and Q be propositions.*

$$(P \Rightarrow Q) \Leftrightarrow (\sim P \vee Q).$$

(This is a restatement of Lemma 1.12 from earlier.)

Corollary 1.68 (Disjunctive normal form, set version) *Let E and F be sets. Then*

$$E \subseteq F \text{ if and only if } F^C \subseteq E^C.$$

EXAMPLES APPLYING DISJUNCTIVE NORMAL FORM

1. *Assumption:* If a polynomial is a cubic, then it has exactly three roots.

   Equivalent formulation:

2. *Assumption:* Either a polygon has exactly three sides, or it is not a triangle.

   Equivalent formulation: If a polygon is a triangle, then it has exactly three sides.

   Not an equivalent formulation: If a polygon has exactly three sides, it is a triangle.

Double negation

Theorem 1.69 (Double negation) *Let P be a proposition.*

$$\sim (\sim P) \Leftrightarrow P.$$

(This is a restatement of part of Theorem 1.10 from earlier.)

Corollary 1.70 (Double complement) *Let E be a set. Then $(E^C)^C = E$.*

EXAMPLE OF DOUBLE NEGATION

Assumption: Ferris' football team did not not win the GLIAC in 2016.

Conclusion: Ferris' football team won the GLIAC in 2016.

Chapter 2

Introduction to proof

2.1 Getting started with proofs

Definition 2.1 *In mathematics, a* **theorem** *is a statement that has been (or can be) proved on the basis of previously established statements.*

A **lemma** *is a theorem used in the proof of more substantial theorems.*

A **corollary** *is a theorem which is a consequence of a more substantial theorem.*

Definition 2.2 *A* **proof** *of a theorem is an argument which convinces Dr. McClendon of two things:*

1. *that the theorem is true, and*
2. *that the author of the proof completely understands why the theorem is true.*

Typically, such a proof is an inferential argument which explains how the theorem can be deduced from previously established statements and rules of inference.

Why do we need proofs?

1. A proof provide us with answers to the question "why is this true?"

2. A proof provides us with certainty as to the truth or falsehood of a statement.

Math Joke 4 *A mathematician believes nothing until it is proven.*

A physicist believes everything until it is proven wrong.

A chemist doesn't care.

A biologist doesn't understand the question.

3. A proof establishes the permanence and universality of a statement.

   “Physicists defer only to mathematicians. Mathematicians defer only to God.”

4. A proof provides evidence the author knows what he/she is doing.

5. Proofs are templates for well-written computer programs.

6. A proof often gives us greater insight into the result being proved, and suggests further things to study.

   “Mathematics is a game with rules, but no objectives.”

7. Proofs prevent us from claiming things that aren’t true (for example, consider the activity we will do on how the chords of a circle divide the circle into regions).

We can’t prove mathematical results without assuming something (although we’d like to assume as little as possible). The things we assume in mathematics without proof are called **axioms** (or **postulates**).

There is no complete list of rules for writing proofs. Proving a theorem is more like art than science (actually, its kind of like playing a game like chess or bridge well). That being said, here are some “laws” for writing proofs I believe in. Let’s call them...

McClendon's Laws of writing proofs

THE FIRST LAW: Work on scratch paper before writing the proof.

THE SECOND LAW: When in doubt, start by breaking down the logical structure of the statement to be proved.

This means identifying quantifiers, variables, conditionals, etc. The logical structure of the statement often suggests what your proof should "look like".

THE THIRD LAW: Keep in mind what you are always allowed to do in a proof.

- At any time, you can always:
  - state a hypothesis of the result you are to prove;
  - state or use any axiom;
  - state or apply any definition; and/or
  - state or apply a previously proved result.
- At any time, you can state any sentence whose symbolic translation is a tautology.
- At any time, you can apply any rule of inference.
  - Most importantly, you can apply modus ponens. If you know P is true and you know $P \Rightarrow Q$, then you can state Q is true.
- At any time, you can change a statement into any logically equivalent form (like disjunctive normal form or contrapositive).

THE FOURTH LAW: Be willing to try something, even if you aren't sure it will work.

If you go through a line of reasoning that doesn't end where you want, that doesn't mean you are dumb. Try something else, and learn from what didn't work.

Topics for proofs

To learn how to write proofs, we need to practice writing proofs.

Those proofs have to be about something.

Here, I present some basic number theory. This material will serve as one of our "somethings" to write proofs about.

Definition 2.3 (Even and odd numbers) *Let $n \in \mathbb{Z}$.*

n is called **even** *if n is a multiple of 2, i.e. $\exists\, k \in \mathbb{Z} : n = 2k$.*
Equivalently, n is even if $n \in 2\mathbb{Z}$.

n is called **odd** *if $\exists k \in \mathbb{Z} : n = 2k + 1$.*

EXAMPLES

28 is even because $28 = 2 \cdot 14$ and $14 \in \mathbb{Z}$.

-7 is odd because $-7 = 2(-4) + 1$ and $-4 \in \mathbb{Z}$.

Lemma 2.4 *Every integer is either even or odd, and no integer is both even and odd.*

PROOF ? (Try this as HW)

Definition 2.5 *Let $a, b \in \mathbb{Z}$ with $a \neq 0$.*

We say a **divides** *b, and write $a \mid b$, if $\exists\, k \in \mathbb{Z} : b = ak$.*
Equivalently, to say $a \mid b$ means $b \in a\mathbb{Z}$.

If it is not the case that a divides b, we write $a \nmid b$.

EXAMPLES

$6 \mid 42$ because $42 = 6 \cdot 7$.

$7 \nmid 17$. (How would you prove this? It's not clear.)

Definition 2.6 *A natural number n is called* **prime** *if for any $a \in \mathbb{N}$ such that $a \mid n$, either $a = 1$ or $a = n$.*

A natural number n is called **composite** *if it is not prime.*

EXAMPLES

14 is composite because $14 = 2 \mid 14$.

37 is prime (but how exactly do you prove this? It's not clear.)

MATH 324 POLICIES

1. You may assume Lemma 2.3 without proof, i.e. assert that every integer is either even or odd, but not both. (We'll get around to proving this result later.)
2. You may assert whether or not one integer divides another without proof.
3. You may assert whether or not a number is prime without proof.
4. You may assert that the square of any real number is ≥ 0.
5. You may assert that the sum/difference/product of integers is an integer.
6. You may assert that a positive number times a negative number is negative, etc.
7. You may assert other facts about $<, >, \leq, \geq, =$ that are "obvious".

This brings us to the first result we we will prove in class:

Proposition 2.7 *Every prime number other than* 2 *is odd.*

SCRATCH WORK FOR PROOF:

After all that scratch work, here's what you'd actually write:

Claim: Every prime number other than 2 is odd.

PROOF Suppose n is a prime number which is even.

Then, by definition of even number, we can write $n = 2k$ for some $k \in \mathbb{Z}$.

But then by the definition of divides, $2 \mid n$.

Since n is prime, this means $n = 2$, as desired. □

A person who wants to write things in paragraph form might write format their proof (which has identical text to what's written above) this way:

Claim: Every prime number other than 2 is odd.

PROOF Suppose n is a prime number which is even. Then, by definition of even number, we can write $n = 2k$ for some $k \in \mathbb{Z}$. But then by the definition of divides, $2 \mid n$. Since n is prime, this means $n = 2$, as desired. □

Some comments on this proof:

1. It starts with PROOF and ends with a □.
2. The proof doesn't really "look" like the scratch work.
3. Every letter used in this proof that wasn't explicitly stated in the claim (i.e. n and k) was described the first time it was used.
4. The proof is written in complete sentences and in second person, present tense ("we say", "we conclude", "we can write", etc.)
5. Each step in the proof is justified by appealing to a definition (in other cases, you might appeal to a theorem or an axiom).
6. Any rules of inference used weren't stated by name.

Another remark: exactly what needs to be written in a proof depends on the reputation of the author and the audience of the proof. Here are some various proofs of the theorem we just established, written by various people for their peers:

Claim: Every prime number other than 2 is odd.

PROOF (BY A STUDENT WHO HAS FINISHED THIS COURSE) Suppose n is an even prime. Then $n = 2k$ for $k \in \mathbb{Z}$, so $2 \mid n$ and since n is prime, n must be 2. □

PROOF (WHEN DISCUSSING WITH PEOPLE IN THE MATH CLUB WHO LIKE TO TALK ABOUT MATH A LOT) If n is even, then $2 \mid n$. □

PROOF (BY A GRAD STUDENT) Duh. □

(Of course, it would be expected that as a graduate student, you could reproduce the earlier versions of this proof if someone asked.)

Proposition 2.8 *Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.*

SCRATCH WORK FOR PROOF:

2.2 Direct proofs and subset proofs

Most theorems that you are to prove are conditionals (i.e. "if [hypothesis], then [conclusion]"). The first approach one usually tries to prove such a statement is called a **direct proof**. Such a proof has the following structure:

DIRECT PROOF of $P \Rightarrow Q$:

Assume P.
....
(some logical argument which typically uses modus ponens several times)
....
Therefore, Q. □

The proof of Proposition 2.8 on the previous page is a direct proof. Now, let's do some other direct proofs:

Proposition 2.9 *Let $x \in \mathbb{Z}$. If x is odd, then $x + 1$ is even.*

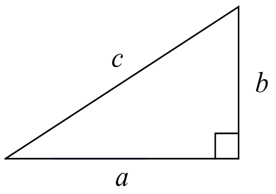
Working backwards

Sometimes, to figure out how a direct proof should work, you can perform scratch work which will try to recover the hypothesis from the conclusion. Before you write the proof down however, you should check that your scratch work is reversible, and when you write the proof, you reverse your scratch work (putting the logic back in the right order).

Proposition 2.10 *Let $x \in \mathbb{R}$. If $x^2 \leq 4$, then $x^2 + 2x < 15$.*

SCRATCH WORK FOR PROOF:

Another example: In ancient Babylon, it was believed that the three sides of a right triangle satisfied the equation $c = a + \frac{b^2}{2a}$:



(Of course we know by the Pythagorean Theorem that $c = \sqrt{a^2 + b^2}$).)

Proposition 2.11 *The Babylonian formula always overestimates the length of the hypotenuse of a right triangle, i.e.*

SCRATCH WORK:

Sometimes, you need to discover a pattern in your scratch work:

Proposition 2.12 *Suppose that $4 \mid x$. Then x is the difference of two perfect squares (a* **perfect square** *is any number of the form k^2, where k is an integer).*

SCRATCH:

Sometimes, a direct proof is simply a verification of an equation:

Proposition 2.13 *For any two natural numbers n and k with $k \leq n$, define*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

(The number $\binom{n}{k}$, pronounced "n choose k", is important in probability: it is the number of ways to choose a set of size k from a set of size n.) Prove that for any n and $k \leq n$,

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}.$$

SCRATCH:

Subset proofs

Recall that the subset relationship $E \subseteq F$ can be restated as a conditional:

This suggests a direct method for proving one set is a subset of another, called a **generic particular argument**:

GENERIC PARTICULAR ARGUMENT to prove $E \subseteq F$:

Assume $x \in E$.
....
(some logical argument)
....
Therefore, $x \in F$. □

The x we use in such a proof is called a "generic and particular" element of E. What makes it "particular" is that we have given it a name: "x". What makes it "generic" is that x isn't assumed to have any properties other than being in E, so the argument applies no matter the value of x.

Proposition 2.14 $6\mathbb{Z} \subseteq 2\mathbb{Z}$.

2.3 Cases

Sometimes a statement that you want to prove is of the form $(P_1 \vee P_2) \Rightarrow Q$ (or is equivalent to this form). To do this, we use the following rule of inference (called "proof by cases" in the previous chapter):

$$[(P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)] \Rightarrow (P_1 \vee P_2) \Rightarrow Q.$$

A proof that uses this rule of inference is called a **proof by exhaustion** or a **proof by cases**:

PROOF BY EXHAUSTION of $P \Rightarrow Q$:

We consider n cases:

Case 1: Assume P_1.
....
(some logical argument)
....
Therefore, Q.

Case 2: Assume P_2.
....
(some logical argument)
....
Therefore, Q.

(more cases if necessary)

Case n: Assume P_n.
....
(some logical argument)
....
Therefore, Q.

In all cases, Q. □

Important note: In order for such a proof to be valid, it must be the case that the hypothesis P implies that at least one of the cases P_j are true.

This bit of logic (that P implies at least one of the P_j) is usually not stated in a proof, but you have to keep it in mind:

Example of a bad proof by exhaustion

Claim: For every real number x, $x^2 > 0$.

Alleged Proof We consider two cases:

Case 1: Assume $x > 0$. Then $x^2 = x(x) > 0$ as desired.

Case 2: Assume $x < 0$. Then $x^2 = x(x) > 0$ as desired.

In both cases, $x^2 > 0$. □

Remarks on how a proof by exhaustion should look:

1. For now, I want you to start such a proof with the statement "We consider ___ cases:" and end such a proof with "In all cases, "___." I'll relax this requirement after a while.
2. The cases should be numbered, starting with 1. When you start working on a case, label the work "*Case* #:" (and underline or boldface or italicize the "Case 1", etc.) and immediately state what is being assumed in that particular case.
3. Based on how you use paragraphs, spacing, italics, underlining, etc., it should be very easy to tell where your cases begin and end, just by glancing at the proof.

Proposition 2.15 *Let $n \in \mathbb{Z}$. Then $n^2 + n + 7$ is odd.*

SCRATCH:

Proposition 2.16 *Let $m, n \in \mathbb{Z}$. If mn is even, then m is even or n is even.*

SCRATCH:

Here is a differently phrased proof of the same result:

Proposition 2.17 *Let $m, n \in \mathbb{Z}$. If mn is even, then m is even or n is even.*

PROOF Assume that mn is even; that means $mn = 2k$ for some $k \in \mathbb{Z}$.

Next, WLOG assume m is odd. Then $m = 2l + 1$ for some $l \in \mathbb{Z}$. That means

$$2k = mn = (2l+1)n = 2ln + n$$

so

$$n = 2k - 2ln = 2(k - ln)$$

and therefore n is even. □

WLOG

The WLOG in this proof stands for **without loss of generality**. This phrase is used when you are doing a proof by cases, and all the cases have basically the same proof. What "WLOG" signals is that you are going to prove one of several possible cases, and the other cases are identical (or their structure can be easily discerned from the proof of the case you give). For its use to be appropriate, either

(a) it must be totally obvious that the argument you give can be applied to any other cases; or

(b) any other cases should have some other totally obvious proof; or

(c) directions must be given to "reduce" other cases to the case you prove.

A typical application is when proving results about two integers (or real numbers) a and b. Assuming the roles of a and b are the same in the statement to be proven, you can assume WLOG that $a \leq b$.

EXAMPLES

- To prove $(2a+b)(a+2b)$ is something or other...

  it is OK to assume WLOG that $a \leq b$.

- To prove $(a+b)(a-b)$ is something or other...

  it is NOT OK to assume WLOG that $a \leq b$.

Do not overuse the phrase WLOG. It is not a "catch-all" that allows you to assume anything under the sun.

Proposition 2.18 *If E, F and G are sets such that $E \subseteq F$, then $E \cup G \subseteq F \cup G$.*

Situations where you might want to consider splitting a proof into cases:

1. Suppose that you discover that you have to divide by some quantity q at some point in your proof. Then you probably need two cases: one case is $q \neq 0$ (where you are allowed divide by q) and the other case is $q = 0$ (where the result usually simplifies into something obvious).

2. Suppose you have to prove a statement about an integer or rational number n. You can always think of using two cases: n even, and n odd.

3. More generally, if you have to prove a statement about an integer or rational number n, you can always try using d cases, depending on the remainder you get when n is divided by d (which must be one of $0, 1, 2, ..., d - 1$).

4. At some point, you come up with some variable x that belongs to the union of two sets $E \cup F$. You can proceed with two cases: $x \in E$, and $x \in F$.

This generalizes: if $x \in \bigcup_j E_j$, you can work out the proof with a separate case for each E_α, or sometimes assume WLOG that $x \in E_\alpha$ for some generic, particular α and go from there.)

5. You have to prove a statement about an integer, rational number or real number x. There are three natural cases here: $x > 0$, $x < 0$ and $x = 0$ (sometimes you can get away with $x < 0$ and $x \geq 0$).

   More generally, if there are two variables x and y in the statement, you may want to use the cases $x < y$ and $x \geq y$ (or $x < y$, $x = y$ and $x > y$).

6. (MATH 322) You have to prove a statement about a vector space V. Two natural cases are $\dim V < \infty$ and $\dim V = \infty$ (two other natural cases might be $V = \{\mathbf{0}\}$ and $V \neq \{\mathbf{0}\}$).

7. You have to prove something about a function $f : \mathbb{R} \to \mathbb{R}$. Often, such a proof starts with the case that $\forall x, f(x) \geq 0$, then builds up from there. Alternatively, you might start with a case that f has a particular formula, then work from there. (This is common in a grad school analysis class; if you are interested in grad school in mathematics, stop by my office - I'll have more to say about this.)

8. You are proving something about sets A and B. One case might be that A and B are disjoint, i.e. $A \cap B = \varnothing$; the other case would be $A \cap B \neq \varnothing$.

9. (MATH 414) There are two types of random variables: discrete and continuous. This means that most proofs about random variables have two cases: discrete and continuous.

10. If you discover in your scratch work that if you were just able to assume something extra, you could prove the result, then try this: *Case 1*: assume that something extra. *Case 2:* assume the something extra is false.

Anecdote: A famous theorem called the **Four Color Theorem** says that if you take a plane and divvy it up into regions (the way a map divides the earth into countries), then no matter how this is done, there is a way to color the regions with four colors so that no two regions of the same color share a common boundary. The original proof of this theorem consists of reducing the problem to 1,879 cases, and checking each of those cases.

2.4 Proof by contraposition

Recall that the conditional $P \Rightarrow Q$ is logically equivalent to its contrapositive $\sim Q \Rightarrow \sim P$. This means that we can prove conditional statements by giving a direct proof of their contrapositive:

PROOF BY CONTRAPOSITION of $P \Rightarrow Q$:

We prove the contrapositive. Assume $\sim Q$.
....
(some logical argument)
....
Therefore, $\sim P$.

By contraposition, we are done. □

Proof by contraposition is a natural technique when the statement itself (especially the conclusion of the statement) contains negations.

For example, if the statement you are to prove is stated $P \Rightarrow \sim Q$, then it may be easier to prove $Q \Rightarrow \sim P$.

Do not overuse proof by contraposition.

Proposition 2.19 *Let n be a natural number. If $3 \nmid n$, then $9 \nmid n$.*

Proposition 2.20 *Let $m \in \mathbb{Z}$. If m^2 is even, then m is even.*

Proposition 2.21 *Let $m \in \mathbb{Z}$. If m^2 is odd, then m is odd.*

PROOF Suppose that m is even. Then $m = 2k$ for some $k \in \mathbb{Z}$. Therefore

$$m^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

so m^2 is even. By contraposition, we are done. □

2.5 Proof by contradiction

Recall the rule of inference **reductio ad absurdum**, which says

$$[\sim P \Rightarrow (Q \wedge \sim Q)] \Rightarrow P.$$

A proof of statement P that applies this rule of inference is called a **proof by contradiction**:

PROOF BY CONTRADICTION of P:

Suppose not. (This is "math lingo" for "Assume $\sim P$".)
....
(some logical argument)
....
Therefore, Q.
....
(some more logical argument)
....
Therefore, $\sim Q$.
Contradiction! Therefore, P. □

PROOF BY CONTRADICTION of $P \Rightarrow Q$:

Assume $P \wedge \sim Q$.)
....
(some logical argument)
....
Therefore, R.
....
(some more logical argument)
....
Therefore, $\sim R$.
Contradiction! Therefore, $P \Rightarrow Q$. □

Sometimes, the contradiction needs to be explained (if it's not clear what the contradiction is).

Proposition 2.22 *For every* $x \in [0, \pi/2]$, $\sin x + \cos x \geq 1$.

PROOF

Proposition 2.23 *There is no greatest even integer.*

PROOF Suppose not, i.e. there is a greatest even integer. Call that integer n. Since n is even, $n = 2k$ for some $k \in \mathbb{Z}$.

One typical use of proof by contradiction is to prove that a set is empty.

PROOF BY CONTRADICTION that $E = \varnothing$:

Suppose not, i.e $E \neq \varnothing$. Then, we can let $x \in E$.
....
(some logical argument)
....
Contradiction! Therefore, $E = \varnothing$. □

Applying this argument where $E = A \cap B$ proves that sets A and B are disjoint.

2.6 Proofs of biconditionals

Recall that a biconditional is a statement of the form "$P \Leftrightarrow Q$", i.e. "P if and only if Q".

To prove a biconditional, there are two methods. The standard method is to rely on the fact that $P \Leftrightarrow Q$ is logically equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$:

BICONDITIONAL PROOF of $P \Leftrightarrow Q$:

($\Rightarrow$) Assume P.

....
(some logical argument)
....
Therefore, Q.

($\Leftarrow$) Assume Q.

....
(another logical argument)
....
Therefore, P. □

Remarks:

1. The two parts of this proof ($(P \Rightarrow Q)$ and $(Q \Rightarrow P)$) are called the two **directions** of the proof.

2. Use the notation ($\Rightarrow$) to indicate the start of the direction $P \Rightarrow Q$; use the notation ($\Leftarrow$) to indicate the start of the direction $Q \Rightarrow P$. Skip a line in your proof after you finish the first direction.

3. The ($\Leftarrow$) part can be done before the ($\Rightarrow$) part.

Definition 2.24 *Two integers m and n are said to have the same* **parity** *if they are both odd, or they are both even. Otherwise, they are said to have different parity.*

Proposition 2.25 *Let $m, n \in \mathbb{Z}$. m and n have the same parity if and only if $m^2 + n^2$ is even.*

PROOF

Proposition 2.26 *Let $x \in \mathbb{R}$. $x^2 < x$ if and only if $x \in (0,1)$.*

PROOF

Shortcut biconditional proofs

Sometimes you don't actually have to prove each direction of a biconditional.

SHORTCUT BICONDITIONAL PROOF of $P \Leftrightarrow Q$:

P iff ....
iff ....
iff ....
iff ....
iff ....
iff Q. □

Note: Be careful with proofs like this, that all the "iff"s are actually "iff" and not "if" or "only if". Often, a shortcut proof like this is not doable, so I suggest proceeding with this type of proof *only if you can see how all the steps would work in advance*.

Proposition 2.27 *Let $x \in \mathbb{R}$. $5(x+3)+2 = 3(2x-1)+13$ if and only if $x = 7$.*

2.7 Set equality proofs

Recall: that two sets E and F are equal iff

This means that proving two sets are equal is essentially a biconditional proof. Given sets E and F, to prove $E = F$ you perform the generic particular argument twice, once to prove $E \subseteq F$ and again to prove $F \subseteq E$. The parts of the proof are labelled ($\subseteq$) and ($\supseteq$):

SET EQUALITY PROOF of $E = F$:

($\subseteq$) Assume $x \in E$.

....

(some logical argument)

....

Therefore, $x \in F$.

($\supseteq$) Assume $x \in F$.

....

(another logical argument)

....

Therefore, $x \in E$. □

As with biconditionals, there is a shortcut which is sometimes available:

SHORTCUT SET EQUALITY PROOF of $E = F$:

$x \in E$ iff ....
iff ....
iff ....
iff ....
iff ....
iff $x \in F$. □

ALTERNATIVE SHORTCUT SET EQUALITY PROOF of $E = F$:

E = ...
= ....
= ....
= ....
= F. □

Proposition 2.28 $18\mathbb{Z} = 6\mathbb{Z} \cap 9\mathbb{Z}$.

Proposition 2.29 *Let* $A = 8\mathbb{Z}$ *and let* $B = 8\mathbb{Z} + 4 = \{x + 4 : x \in 8\mathbb{Z}\}$. *Then* $A \cup B = 4\mathbb{Z}$.

2.8 Properties of set operations

Here are some lists of properties of set operations, many of which we encountered during earlier in-class activities. Some of these are proven here; some were proven earlier; others are homework problems; others we won't bother proving (but you should be able to prove any of them on an exam). These are properties which you should *understand* rather than memorize; they can be used in proofs henceforth in the course.

Note: Usually one does not cite any of these properties by name, because they are so "basic".

In light of the fact that all set operations can be translated into logical connectives (by the chart at the end of Section 3.2), you should understand many of these statements simply as restatements of logical equivalences, etc. proven in Chapter 1. See, for example, Theorem 1.10.

Theorem 2.30 (Properties of set operations) *Let E, F and G be sets. Then:*

Nested subset property: *If $E \subseteq F$ and $F \subseteq G$, then $E \subseteq G$.*

Taking a union makes a set bigger: $E \subseteq E \cup F$.

Intersecting a set makes it smaller: $E \cap F \subseteq E$.

Union and intersection with empty set: $E \cup \varnothing = E$ *and* $E \cap \varnothing = \varnothing$.

Union and intersection of set with itself: $E \cup E = E$ *and* $E \cap E = E$.

Commutative Laws:
$\cup$ *is commutative:* $E \cup F = F \cup E$;
$\cap$ *is commutative:* $E \cap F = F \cap E$.

Associative Laws:
$\cup$ *is associative:* $(E \cup F) \cup G = E \cup (F \cup G)$;
$\cap$ *is associative:* $(E \cap F) \cap G = E \cap (F \cap G)$.

Distributive Laws:
$\cap$ *distributes across* $\cup$: $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$;
$\cup$ *distributes across* $\cap$: $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$.

Union and intersection with a third set preserve subset relationship:
If $E \subseteq F$, then $E \cup G \subseteq F \cup G$;
If $E \subseteq F$, then $E \cap G \subseteq F \cap G$.

Theorem 2.31 (Equivalent properties to subset relationship:) *Let E and F be sets. TFAE:*

1. $E \subseteq F$;
2. $E \cup F = F$;
3. $E \cap F = E$;
4. $F^C \subseteq E^C$.

Theorem 2.32 (Properties of complements) *Let E and F be sets in universe of discourse U. Then:*

Double complement law: $(E^C)^C = E$.

Unions and intersections with complements:
$E \cup E^C = U$;
$E \cap E^C = \varnothing$.

DeMorgan laws:
complement of a union is the intersection of the complements:

$$(E \cup F)^C = E^C \cap F^C;$$

complement of an intersection is the union of the complements:

$$(E \cap F)^C = E^C \cup F^C.$$

Equivalent property to disjointness: *E and F are disjoint if and only if $E \subseteq F^C$.*

Self-symmetric difference is empty: $E \bigtriangleup E = \varnothing$.

Theorem 2.33 (Properties of Cartesian products) *Let E, F, G and H be sets. Then:*

Distributive laws:
× distributes across ∪: $E \times (F \cup G) = (E \times F) \cup (E \times G)$;
× distributes across ∪: $E \times (F \cap G) = (E \times F) \cap (E \times G)$.

Product with empty set is empty: $E \times \varnothing = \varnothing$.

Interchange of product with intersection:
$(E \times F) \cap (G \times H) = (E \cap G) \times (F \cap H)$.

Interchange of product with union:
$(E \times F) \cup (G \times H) \subseteq (E \cup G) \times (F \bigcup H)$.

PROOFS OF SELECTED STATEMENTS FROM THESE THEOREMS These statements are all proven with subset or set equality arguments. I'll give some here; you should be able to prove any of the others on an exam.

Proof of nested subset property: Let $x \in E$. Since $E \subseteq F$, $x \in F$. Since $F \subseteq G$, that means $x \in G$ as wanted. □

Proof that taking a union makes a set bigger: Let $x \in E$. By disjunction introduction, $x \in E$ or $x \in F$, i.e. $x \in E \cup F$. □

Proof that intersecting a set makes it smaller: HW

Proof of $E \bigcup \varnothing = E$:

(⊆) Let $x \in E \bigcup \varnothing$.

Case 1: $x \in E$. Then we are done.

Case 2: $x \in \varnothing$. This is impossible, as $\varnothing$ has no elements.

(⊇) This is obvious, because taking unions makes sets bigger. □

Proof of commutative laws: This was done in Theorem 1.51.

Proof of associative laws: This was done in Theorem 1.51.

Proof of distributive laws: This was done in Theorem 1.51.

Proof that union with a third set preserves subset relationship: This was Proposition 2.18.

Proof that intersection with a third set preserves subset relationship: HW

Proof of equivalent properties to subset relationship:

(1 ⇒ 2): Suppose $E \subseteq F$. We need to prove $E \cup F = F$:

(⊆): Suppose $x \in E \cup F$.

Case 1: $x \in E$. Since $E \subseteq F$, this means $x \in F$ as desired.

Case 2: $x \in F$. Then we are done.

(⊇): obvious (taking a union makes a set bigger)

(2 ⇒ 3): Suppose $E \cup F = F$. Now we prove that $E \cap F = E$:

(⊆): obvious (intersecting a set makes it smaller)

(⊇): Suppose $x \in E$. Then $x \in E \cup F$ so by hypothesis, $x \in F$.

Since $x \in E$ and $x \in F$, $x \in E \cap F$.

(3 ⇒ 4): Assume $E \cap F = E$. Now, let $x \in F^C$. This means $x \notin F$.

Suppose not, i.e. $x \notin E^C$. This means $x \in E$ and since we assume $E \cap F = E$, this means $x \in F$. Contradiction!

Therefore $x \in E^C$ so $F^C \subseteq E^C$ as desired.

(4 ⇒ 1): Assume $F^C \subseteq E^C$. Since we have already proven (1 ⇒ 2), (2 ⇒ 3) and (3 ⇒ 4), we know (1 ⇒ 4).

By the (1 ⇒ 4) case applied to the sets F^C and E^C, $(E^C)^C \subseteq (F^C)^C$.

In other words, $E \subseteq F$ as desired. □

Proof that $E \cap \varnothing = \varnothing$: HW

Proof that $E \cup E = E$: HW

Proof that $E \cap E = E$: HW

Proof of double complement law: This was done in Theorem 1.51.

Proof of union with complement: HW

Proof of intersection with complement: The truth set of $E \cap E^C$ is the truth set of $P(x)$ = "$x \in E$ and $x \notin E$". Since $P(x)$ is a contradiction, its truth set is $\varnothing$, meaning $E \cap E^C = \varnothing$ as wanted. □

Proof of DeMorgan laws: This was done in Theorem 1.51.

Proof of equivalent property to disjointness:

Proof that self-symmetric difference is empty: HW

Proof that products distribute over unions: ($\subseteq$) Let $x \in E \times (F \cup G)$. Then $x = (a, b)$ where $a \in E$ and $b \in F \cup G$.

Case 1: $b \in F$. Then $x = (a, b) \in E \times F \subseteq (E \times F) \cup (E \times G)$.

Case 2: $b \in G$. Then $x = (a, b) \in E \times G \subseteq (E \times F) \cup (E \times G)$.

($\supseteq$) Let $x \in (E \times F) \cup (E \times G)$. WLOG $x \in E \times F$. Therefore $x = (a, b)$ where $a \in E$ and $b \in F$. Thus $b \in F \cup G$, so $x = (a, b) \in E \times (F \cup G)$. □

Proof that products distribute over intersections: HW

Proof of product with empty set is empty: HW

Interchange of product with intersection: HW

Proof of interchange of product with union:

Suppose $x \in (E \times F) \cup (G \times H)$. WLOG $x \in E \times F$. Then $x = (a, b)$ where $a \in E$ and $b \in F$. Then $a \in E \cup G$ and $b \in F \cup H$ (since unions make sets bigger) so $x \in (E \cup G) \times (F \cup H)$ as desired. □

TFAE propositions

The acronym **TFAE** stands for "the following are (logically) equivalent". When you see a proposition of the form

TFAE:
1. something
2. something else
3. another something else
4. one last thing

that is the same thing as the proposition $1 \Leftrightarrow 2 \Leftrightarrow 3 \Leftrightarrow 4$. To prove such a proposition, you need to prove a "circle" of conditionals. For example, to prove

$$1 \Leftrightarrow 2 \Leftrightarrow 3 \Leftrightarrow 4,$$

it is sufficient to prove $1 \Rightarrow 2$, $2 \Rightarrow 3$, $3 \Rightarrow 4$ and $4 \Rightarrow 1$. This is a "circle" of equivalences because we can think of the picture

Sometimes you can't prove a circle like this, and you actually have to prove a bunch of biconditional statements like $1 \Leftrightarrow 2$, $2 \Leftrightarrow 3$, and $3 \Leftrightarrow 4$ (or any equivalent combination of statements).

Here is an example which shows the structure and syntax of a proof of a TFAE proposition:

Proposition 2.34 *Let $x \in \mathbb{Z}$: TFAE:*

1. *x is even;*
2. *$x + 1$ is odd;*
3. *$x + 2$ is even.*

PROOF $(1 \Rightarrow 2)$ Assume x is even. That means $x = 2n$ where $n \in \mathbb{Z}$. Then $x+1 = 2n+1$ so by definition of odd number, $x + 1$ is odd.

$(2 \Rightarrow 3)$ Assume $x + 1$ is odd. That means $x + 1 = 2n + 1$ where $n \in \mathbb{Z}$. Then

$$x + 2 = (x + 1) + 1 = (2n + 1) + 1 = 2n + 2 = 2(n + 1)$$

so x is even by definition of even number.

$(3 \Rightarrow 1)$ Assume $x + 2$ is even. That means $x + 2 = 2n$ for $n \in \mathbb{Z}$. Then

$$x = (x + 2) - 2 = 2n - 2 = 2(n - 1)$$

so x is even by definition of even number. □

2.9 Proofs involving universal quantifiers

Many definitions of mathematical terms involve universal quantifiers. Here are some examples you may have seen:

Definition 2.35 (Math 220) *A function f is* **continuous** *if for every number a,*

$$\lim_{x \to a} f(x) = f(a).$$

Definition 2.36 (Math 322) *A subset W of a vector space V is called a* **subspace** *if:*

1. *W contains the zero vector, i.e. $\mathbf{0} \in W$;*
2. *W is closed under addition, i.e. for every $\mathbf{v}, \mathbf{w} \in W$, $\mathbf{v} + \mathbf{w} \in W$; and*
3. *W is closed under scalar multiplication, i.e. for every $r \in \mathbb{R}$ and $\mathbf{w} \in W$, $r\mathbf{w} \in W$.*

To gain understanding of terms like "continuous" or "subspace", you often are asked questions like:

(Math 220) Is the function f defined by $f(x) = \begin{cases} 2x+1 & \text{if } x \neq 3 \\ 5 & \text{if } x = 3 \end{cases}$ continuous? Why or why not?

(Math 322) Let $V = \mathbb{R}^4$ and let W be the set of vectors of the form $(a+2b, -a, 3b, 0)$. Is W a subspace? Why or why not?

To have confidence in your answer to a question like this, you should have some idea about how to prove that your answer is correct. A proof of a "yes" answer is essentially verifying that a definition involving a universal quantifier holds for a specific example. To do this, use the following type of argument:

Verifying $\forall x \in E, P(x)$ via **GENERIC PARTICULAR ARGUMENT**:

Let $x \in E$.
....
(some logical argument)
....
Therefore, $P(x)$. □

As in a subset proof, this x is generic and particular.

Proposition 2.37 *Define a function $f : \mathbb{R} \to \mathbb{R}$ to be* **additive** *if for any x and y, $f(x+y) = f(x) + f(y)$. Given this definition, the function $f(x) = 3x$ is additive.*

INVALID PROOF Let $x = 3$ and $y = 4$. $f(x+y) = f(3+4) = f(7) = 3(7) = 21$ and $f(x) + f(y) = 3(3) + 3(4) = 9 + 12 = 21$. Since $f(x+y) = f(x) + f(y)$, f is additive. □

CORRECT PROOF

Proposition 2.38 *A function $f : \mathbb{R} \to \mathbb{R}$ is called* **increasing** *if $x \leq y$ implies $f(x) \leq f(y)$ (i.e. the function preserves inequality signs). Given this definition, the function $f(x) = x^3 + 5x + 1$ is increasing.*

If you don't want to prove a universally quantified statement with the generic particular argument, you can try a proof by contradiction (remember that a denial of $\forall x, P(x)$ is $\exists x : \sim P(x)$):

Proposition 2.39 *For every $x \in \mathbb{R}$, $x^2 + 5 > 0$.*

2.10 Counterexamples and disproof

To **disprove** a proposition means proving the negation of that proposition (just as well, proving any denial of the proposition).

The most frequent types of disproofs we need to give in mathematics are those which disprove universally quantified statements. To do this, we use the fact that a useful denial of $\forall x, P(x)$ is

Disproving $\forall x \in E, P(x)$ via **COUNTEREXAMPLE**:

Let $x =$ something.
....
(some logical argument, if necessary)
....
Therefore, $x \in E$.
....
(some logical argument)
....
Therefore, $\sim P(x)$. □

Proposition 2.40 *Recall that a function f is called* **increasing** *if $x \leq y$ implies $f(x) \leq f(y)$. Prove that the function $f(x) = e^{-x}$ is not increasing (i.e. disprove the claim that $f(x) = e^{-x}$ is increasing).*

PROOF

EXERCISE

Prove or disprove the assertion "if x is prime, then $x + 5$ is composite."

SOLUTION This assertion is false. Let $x = 2$. Then $x + 5 = 7$ which is prime. □

EXERCISE

Prove or disprove the assertion that the function $f(x) = x^2$ is additive.

SOLUTION This assertion is false. Let $x = y = 1$. Then $f(x+y) = f(1+1) = 2^2 = 4$ but $f(x) + f(y) = 1^2 + 1^2 = 2$. Since $f(x+y) \neq f(x) + f(y)$, f is not additive. □

2.11 Existence results and their proofs

Math Joke 5 *An engineer, a physicist and a mathematician are staying in a hotel. The engineer wakes up and smells smoke. He goes out into the hallway and sees a fire, so he fills a trash can from his room with water and douses the fire. Then, he goes back to bed.*

Later, the physicist wakes up and smells smoke. She opens her door and sees a fire in the hallway. She walks down the hall to a fire hose and after calculating the flame velocity, distance, water pressure, trajectory, etc. extinguishes the fire with the minimum amount of water and energy needed. Then, she goes back to bed.

Later, the mathematician wakes up and smells smoke. She goes to the hall, sees the fire and then the fire hose. After thinking for a moment, she exclaims, "Aha! A solution exists!" She then goes back to bed.

Suppose we are tasked with proving a proposition whose conclusion is of the form $\exists x : P(x)$ (such a result is called an **existence theorem** or **existence result**. To prove a result, there are two common methods: *constructive proofs* and *non-constructive proofs*.

Constructive proofs

CONSTRUCTIVE PROOF of $\exists x \in E : P(x)$:

Let x = something.
....
(some logical argument, if necessary)
....
Therefore, $x \in E$.
....
(some logical argument)
....
Therefore, $P(x)$. □

Proposition 2.41 *There is a prime number between* 30 *and* 40.

PROOF 31 is a prime number between 30 and 40. □

Proposition 2.42 *There is a function whose derivative is* $3x$.

PROOF

Proposition 2.43 *If $b^2 - 4ac \geq 0$, then there is a real number x which is a solution of $ax^2 + bx + c = 0$.*

PROOF Let $x = \frac{-b+\sqrt{b^2-4ac}}{2a}$. This x exists because of the hypothesis $b^2 - 4ac \geq 0$. Now, by plugging this x in the equation, we have

$$
\begin{aligned}
ax^2 + bx + c &= a\left(\frac{-b+\sqrt{b^2-4ac}}{2a}\right)^2 + b\left(\frac{-b+\sqrt{b^2-4ac}}{2a}\right) + c \\
&= a\left(\frac{b^2 - 2b\sqrt{b^2-4ac} + b^2 - 4ac}{4a^2}\right) + \frac{-b^2 + b\sqrt{b^2-4ac}}{2a} + c \\
&= \left(\frac{b^2 - 2b\sqrt{b^2-4ac} + b^2 - 4ac}{4a}\right) + \frac{-2b^2 + 2b\sqrt{b^2-4ac}}{4a} + \frac{4ac}{4a} \\
&= \frac{2b^2 - 2b\sqrt{b^2-4ac} - 4ac - 2b^2 + 2b\sqrt{b^2-4ac} + 4ac}{4a} \\
&= \frac{0}{4a} \\
&= 0.
\end{aligned}
$$

Therefore this x is a solution of $ax^2 + bx + c$. □

Non-constructive proofs

NON-CONSTRUCTIVE PROOF of $\exists x \in E : P(x)$:

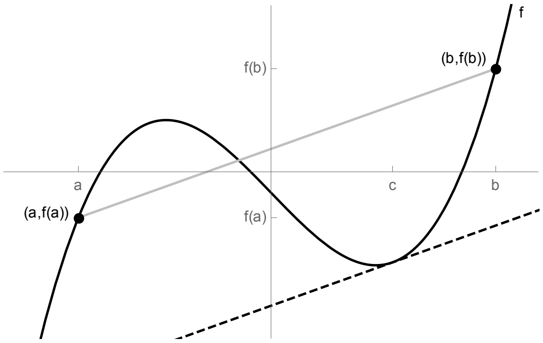
Start with the assumptions of the result you want to prove.
....
(some logical argument, if necessary)
(usually, somewhere in here you appeal to some other existence theorem that you've already learned)
....
Therefore, $\exists x \in E$ with some property
....
(some more logical argument)
....
Therefore, $P(x)$. □

What existence theorem(s) might you appeal to? The ones you know mostly come from calculus:

Theorem 2.44 (Mean Value Theorem (MVT)) *Let f be a continuous function on $[a,b]$ and suppose that f is differentiable on (a,b). Then there is a number $c \in [a,b]$ such that*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

A picture to explain:

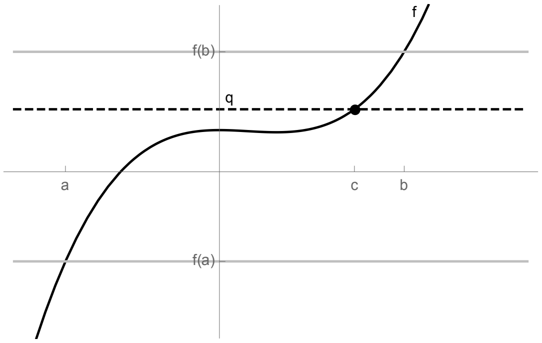


PROOF Requires a lot of machinery from advanced mathematics. Take MATH 430 if you want to see this.

Here is another significant existence theorem which, like the MVT, has a difficult non-constructive proof (also done in MATH 430).

Theorem 2.45 (Intermediate Value Theorem (IVT)) *Let f be a continuous function on $[a,b]$. If q is between $f(a)$ and $f(b)$, then there is a $c \in [a,b]$ such that $f(c) = q$.*

A picture to explain:



The IVT is used to give non-constructive proofs establishing the existence of solutions to certain kinds of equations.

Proposition 2.46 *There is a real number x such that $2x^5 - 7x^3 + 3x + 1 = 0$.*

Proof

Anecdote: There are mathematicians who do not believe that non-constructive proofs are valid. They believe that the only way to prove an existence statement is to provide a constructive proof. These nutjobs are called **constructionists**. Here is a theorem that they do not believe (because the only known proofs are non-constructive), which has wide application in physics and economics (you can read the Wikipedia article on this theorem for more on this):

Theorem 2.47 (Brouwer Fixed Point Theorem) *Let D be the set of points (x, y) such that $x^2 + y^2 \leq 1$ (i.e. D is a disk of radius 1). Let f be a continuous function from D to D. Then f has a fixed point, i.e. there exists a point (x_0, y_0) in D such that $f(x_0, y_0) = (x_0, y_0)$.*

Interestingly, Brouwer (who is famous for giving the first proof of this theorem) became a constructionist later in his life and disavowed his own result!

2.12 Existence / uniqueness proofs

Suppose we are tasked with proving a proposition whose conclusion is of the form $\exists! x : P(x)$ (such a proposition is called an **existence/uniqueness theorem** or **existence/uniqueness result**. Based on the definition of the unique existential quantifier, this means we need to show two things:

1. there is at least one x such that $P(x)$ is true; and
2.

Proving the first statement is an existence proof, as described in the previous section. To establish the second statement, the standard method is to prove it by contradiction.

EXISTENCE/UNIQUENESS PROOF of $\exists! x \in E : P(x)$:

First, we prove existence.
(Then prove $\exists x \in E : P(x)$, as in the previous section.)

Next, we prove uniqueness. Suppose $P(x)$ and $P(y)$ are true.
....
(logical argument)
....
Therefore, $x = y$. □

Proposition 2.48 *Every nonzero real number has a unique multiplicative inverse (a* **multiplicative inverse** *of $x \in \mathbb{R}$ to be another real number y such that $xy = 1$).*

Disproving an existence result

To disprove an existentially quantified sentence like $\exists x : P(x)$, there are two usual methods.

1. First, you can prove the denial $\forall x, \sim P(x)$ (usually by generic particular argument).

2. Disprove the statement by contradiction (see below):

DISPROVING $\exists x \in E : P(x)$:

Suppose not, i.e. $\exists\, x \in E : P(x)$.
....
Contradiction! Therefore $\forall\, x \in E, \sim P(x)$. □

For an example of this type of proof, look back at Proposition 2.23, where we disproved the statement

"There exists a number which is the greatest even integer."

2.13 Summary of basic proof techniques

First, identify the logical structure of the result to be proved. Here are some general techniques for each type of logical structure:

- To prove "If P, then Q":

  Direct proof: Suppose P. ... ... Therefore Q. □
  Proof by contraposition: Suppose $\sim Q$. ... ... Therefore $\sim P$. □
  Proof by contradiction: Suppose $P \wedge \sim Q$. ... ... Therefore R. ... ... Therefore $\sim R$. Contradiction! □
  Proof by cases: Suppose P. *Case 1:* ... ... Therefore Q. *Case 2:* ... ... Therefore Q. ... ... In all cases, Q. □

- To prove $E \subseteq F$:

  Subset proof (generic particular argument): Let $x \in E$. ... ... $x \in F$. □

- To prove "P if and only if Q":

  Biconditional proof: ($\Rightarrow$) Suppose P. ... ... Therefore Q.
  ($\Leftarrow$) Suppose Q. ... ... Therefore P. □
  Shortcut biconditional proof: P iff ... iff ... iff ... ... iff Q. □.

- To prove $E = F$:

  Set equality proof (generic particular argument): ($\subseteq$) Let $x \in E$. ... ... $x \in F$.
  ($\supseteq$) Let $x \in F$. ... ... $x \in E$. □
  Shortcut set equality proof: $x \in E$ iff ... iff ... iff ... iff $x \in F$.
  Shortcut set equality proof: $E = ... = ... = ... = F$.

- To prove $E = \varnothing$,

  Proof by contradiction: Suppose $E \neq \varnothing$. Then we can let $x \in E$. ... ... Contradiction! Thus $E = \varnothing$. □

- To prove sets E and F are disjoint:

  Use equivalent property of disjointness: Let $x \in E$. ... ... $x \neq F$. □
  Proof by contradiction: Suppose $E \cap F \neq \varnothing$. Then we can let $x \in E \cap F$. ... ... Contradiction! Thus $E \cap F = \varnothing$. □

- To prove "TFAE: 1; 2; 3; ..."

  Circle of implications proof: Prove ($1 \Rightarrow 2$), then ($2 \Rightarrow 3$), then ($3 \Rightarrow 1$), etc.

- To prove "$\forall x \in E, P(x)$":

  Generic particular argument: Let $x \in E$. ... ... Therefore $P(x)$. □

- To disprove "$\forall x \in E, P(x)$":

  Disproof by counterexample: Let $x =$. ... ... Therefore $\sim P(x)$. □

- To prove "$\exists x \in E : P(x)$":

  Constructive proof: Let $x =$. ... ... Therefore $P(x)$. □
  Non-constructive proof: ... ... Therefore x exists by (some theorem). ... ... Therefore $P(x)$. □

- To disprove "$\exists x \in E, P(x)$", prove the denial "$\forall x \in E, \sim P(x)$".

- To prove "$\exists! x \in E : P(x)$".

  Existence/uniqueness proof: First, prove $\exists x \in E : P(x)$.
  Then, suppose $P(x)$ and $P(y)$. ... ... Therefore $x = y$. □

- To disprove "$\exists! x \in E : P(x)$", do one of two things:

  1. Disprove "$\exists x \in E, P(x)$" by proving the denial "$\forall x \in E, \sim P(x)$", or
  2. Disprove uniqueness by writing down specific x and y in E (with $x \neq y$) such that $P(x) \wedge P(y)$.

Chapter 3

Equivalence relations

3.1 Relations

A *relation* is a subset of a Cartesian product space:

Definition 3.1 *Let A and B be sets.*

A **relation from** *A* **to** *B is a subset R of $A \times B$.*

If $(x, y) \in A \times B$ satisfies $(x, y) \in R$, we write $x\,R\,y$ and say "x is related to y".

If $(x, y) \notin R$, we write $x \not R\, y$.

When $A = B$, then we say the relation is a **relation on** *A.*

Definition 3.2 *Let R be a relation from A to B.*

The **domain** *of R, denoted $Dom(R)$, is the subset of A defined by*

$$Dom(R) = \{x \in A : \exists\, y \in B \text{ s.t. } x\,R\,y\}.$$

The **range** *of R, a.k.a. the* **image** *of R, denoted $Range(R)$ or $Im(R)$, is the subset of B defined by*

$$Range(R) = Im(R) = \{y \in B : \exists\, x \in A \text{ s.t. } x\,R\,y\}$$

Relations are very general objects (since any subset of $A \times B$ is a relation)! The next few pages give several examples:

Examples of relations

EXAMPLE 1

Let $A = \{\triangle, \bigtriangledown, \square, \heartsuit\}$ and $B = \{\star, \blacksquare, \blacktriangle\}$;

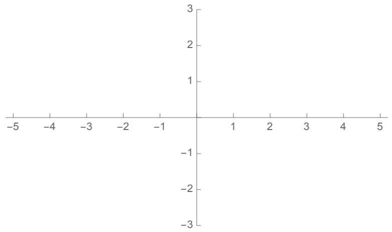
$$R = \{(\triangle, \star), (\triangle, \blacksquare), (\square, \blacksquare), (\heartsuit, \star), (\heartsuit, \blacksquare)\}.$$

EXAMPLE 2

Let R be the relation from $E = \{-5, -4, ..., 4, 5\}$ to $F = \{-3, -2, .., 2, 3\}$ defined by $R = \{(x, y) \in E \times F : y = x + 3\}$.

A list of the elements of R:

A picture of R:



True statements:

False statements:

Various different ways that the relation of Example 2 could be defined:

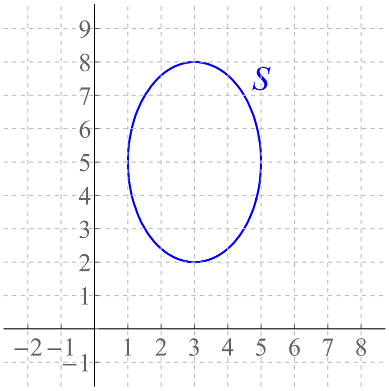
- **As a list:** $R = \{(-5,-2),(-4,-1),(-3,0),(-2,1),(-1,2),(0,3)\}$.
- **With set-builder notation:** $R = \{(x,y) \in E \times F : y = x + 3\}$.
- **As a biconditional:** $xRy \Leftrightarrow y = x + 3$.
- **In words:** Define R to be the set of elements in $E \times F$ where the second coordinate is three more than the first.

NOTE: E and F have to be defined first for a relation from E to F to make sense.

Example 3

Let S be the relation on $\mathbb{R}$ defined by

$$S = \left\{(x,y) \in \mathbb{R}^2 : \frac{(x-3)^2}{4} + \frac{(y-5)^2}{9} = 1\right\}.$$



Relations are often denoted by symbols like $\sim$, $\approx$, $\equiv$, $<$, $>$, $\leq$, $\prec$, $\ll$, $\parallel$, $\asymp$, $\lhd$, $\bowtie$, etc.

Example 4 (the keyboard example)

Let $\mathcal{A}$ be the set of letters in the English alphabet: $\mathcal{A} = \{A, B, ..., Z\}$. Then define $\bowtie$ to be the set of pairs of letters which appear on the same row of a standard keyboard.

Example 5

Let $E = \{1,2,3,4,5\}$. Define $\asymp$ to be the relation on 2^E defined by

$$A \asymp B \Leftrightarrow A \text{ has the same number of elements as } B.$$

In this situation, $\{1,2\} \asymp \{1,3\}$, $\{1,2,4\} \not\asymp \{3,5\}$, etc.

Three relations you have encountered before

EXAMPLE 6: EQUALITY

Definition 3.3 *Let E be any set. The* **identity relation** *on E, a.k.a. the* **equality relation** *on E, is the relation*

$$I_E = \{(x,x) : x \in E\}.$$

Of course, we also denote the identity relation by =, so formally, to say $x = y$ means $(x,y) \in I_E$. (Among other things, this means x and y have to be members of the same set in order to be equal, so $3 \neq (3,0)$, or example.)

EXAMPLE 7: SUBSET

Let U be some collection of definable sets. Then $\subseteq$ is a relation on U.

EXAMPLE 8: ORDER

Less than or equal to, a.k.a. $\leq$ (more on this in Chapter 4)

3.2 Equivalence relations

Definition 3.4 *Let R be a relation on E.*

- *R is called* **reflexive** *if $\forall x \in E$, $x\,R\,x$.*
- *R is called* **symmetric** *if $\forall x, y \in E$, $x\,R\,y$ implies $y\,R\,x$.*
- *R is called* **transitive** *if $\forall x, y, z \in E$, $x\,R\,y$ and $y\,R\,z$ implies $x\,R\,z$.*

If R is reflexive, symmetric and transitive, then R is called an **equivalence relation (on E)**.

If R is an equivalence relation on R and $x\,R\,y$, we say x and y are **equivalent (or congruent) modulo R ("mod R" for short)** *and we write $x \equiv y \mod R$.*

Note: The definitions of reflexive/symmetric/transitive have universal quantifiers in them. So to prove a relation is an equivalence relation, you verify each part of the definition with a generic particular argument, and to prove a relation is not an equivalence relation, you find an explicit counterexample disproving (at least) one of reflexivity/symmetry/transitivity.

EXAMPLE 9 (A VARIANT OF EXAMPLE 2)

Let $R = \{(x,y) \in \mathbb{R}^2 : y = x + 3\}$.

- *Is R reflexive?*
- *Is R an equivalence relation?*

EXAMPLE 7 (SUBSET)

- *Is $\subseteq$ reflexive?*
- *Is $\subseteq$ symmetric?*
- *Is $\subseteq$ an equivalence relation?*

EXAMPLE 10 (NEW)

$T = \{(x,y) \in \mathbb{R}^2 : |x - y| \leq 1\}$.

- *Is T reflexive?*
- *Is T symmetric?*
- *Is T transitive?*
- *Is T an equivalence relation?*

EXAMPLE 4 (THE KEYBOARD EXAMPLE)

Define two English letters to be related if they appear on the same row of a standard keyboard.

- *Is $\bowtie$ reflexive?*
- *Is $\bowtie$ symmetric?*
- *Is $\bowtie$ transitive?*
- *Is $\bowtie$ an equivalence relation?*

Here is a fundamental axiom of mathematics (recall that an axiom is a statement that we accept without proof):

Axiom 3.5 (Axiom of equality) *Let E be any set. Then the equality relation I_E on E is an equivalence relation.*

(There are whack jobs who do not accept or believe this axiom. They do not believe, for example, that if $x = y$ and $y = z$, then it is necessarily the case that $x = z$. Don't be one of these people.)

3.3 Equivalence classes and partitions

Equivalence classes

Concept: Every equivalence relation on E *partitions* E into disjoint subsets called *equivalence classes*, where whether or not two elements get put in the same subset depends on whether the elements are congruent or not.

Definition 3.6 *Suppose R is an equivalence relation on E. For each $x \in E$, define the set*

$$[x] = [x]_R = \{y \in E : x \, R \, y\}.$$

*This set is called the R-**equivalence class** of x (or just the **equivalence class** of x, or the **congruence class** of x, or just the **class** of x).*

*Any subset of E which is of the form $[x]_R$ for some $x \in E$ is called an **equivalence class of** R.*

$[x]_R$ is also written "$x \mod R$".

EXAMPLE 6 (EQUALITY)

In this case, the equivalence classes consist of single elements.

$$[x]_= = \{x\}$$

EXAMPLE 4 (THE KEYBOARD EXAMPLE)

Here are the equivalence classes:

$$[Q]_{\bowtie} = \{Q, W, E, R, T, Y, U, I, O, P\}$$
$$[A]_{\bowtie} = \{A, S, D, F, G, H, J, K, L\}$$
$$[Z]_{\bowtie} = \{Z, X, C, V, B, N, M\}$$

Observations:

1. $[A]_{\bowtie} = [F]_{\bowtie} = [J]_{\bowtie}$; $[Q]_{\bowtie} = [I]_{\bowtie}$; etc.

   Conjecture A: If R is *any equivalence relation* on *any set* E and __________,

   then ____________________.

2. $[Q]_{\bowtie} \cap [S]_{\bowtie} = \varnothing$; $[A]_{\bowtie} \cap [X]_{\bowtie} = \varnothing$; etc.

   Conjecture B: If R is *any equivalence relation* on *any set* E, then any two

   R-equivalence classes are either ________________ or ____________________.

3. $[Q]_{\bowtie} \cup [A]_{\bowtie} \cup [Z]_{\bowtie} = \mathcal{A}$.

Conjecture C: If R is *any equivalence relation* on *any set* E, then

______________________________ .

Notice that conjectures B and C collectively imply that if R is an equivalence relation on E, then every element of E belongs to one and only one R-equivalence class.

In fact, Conjectures A, B and C are all true; we formulate Conjecture B now:

Lemma 3.7 *Let R be an equivalence relation on set E.*

1. *If $x \, R \, y$, then $[x]_R = [y]_R$.*
2. *If $x \not R \, y$, then $[x]_R \cap [y]_R = \varnothing$.*

PROOF HW

EXAMPLE 11 (NEW)

Let V be the relation on $\mathbb{R}^2$ defined by

$$((x_1, y_1), (x_2, y_2)) \in V \Leftrightarrow x_1 = x_2.$$

Prove V is an equivalence relation, and describe the equivalence classes of V.

PROOF

Reflexivity:

Symmetry:

Transitivity:

Equivalence classes:

Partitions

Definition 3.8 *Let E be a set.*

A **partition** *of E is a collection $\mathcal{P}$ of subsets of E which are pairwise disjoint, and whose union is E.*

The sets which comprise $\mathcal{P}$ are called the **atoms** *of $\mathcal{P}$.*

Generic picture:

EXAMPLE 12

For each $n \in \mathbb{Z}$, let $I_n = [n, n+1) \subseteq \mathbb{R}$.

Then $\mathcal{P} = \{I_n\}_{n\in\mathbb{Z}}$ is a partition of $\mathbb{R}$ (the atoms are the intervals I_n).

EXAMPLE 13

For each $c \in \mathbb{R}$, let $E_c = \{(x, y) \in \mathbb{R}^2 : y = x + c\}$.

Prove $\mathcal{P} = \{E_c\}_{c\in\mathbb{R}}$ is a partition of $\mathbb{R}^2$, and describe its atoms.

Partitions and equivalence relations correspond with one another completely:

Theorem 3.9 (Correspondence theorem) *Let E be a set.*

1. *Every equivalence relation R on a set E produces a partition $\mathcal{P}_R$ of E into its R-equivalence classes; and*
2. *every partition $\mathcal{P}$ of E defines an equivalence relation $\equiv_{\mathcal{P}}$ on E where $x \equiv_{\mathcal{P}} y$ if and only if x and y belong to the same atom of $\mathcal{P}$.*

Proof We begin with statement (1). Let $\mathcal{P}_R$ be the collection of the R-equivalence classes, i.e. $\mathcal{P}_R = \{[x]_R : x \in E\}$. We need to prove $\mathcal{P}_R$ is a partition of E.

First, we will prove $\bigcup_{x \in E} [x]_R = X$ by a set equality argument.
(This is Conjecture C from earlier.)

($\subseteq$) Let $y \in \bigcup_{x \in E} [x]_R$.
This means $y \in [x]_R$ for some x.
Since $[x]_R \subseteq E$, $y \in E$ as desired.

($\supseteq$) Let $y \in E$.
By reflexivity of R $y\,R\,y$, meaning $y \in [y]_R$.
It follows that $y \in \bigcup_{x \in E} [x]_R$, as wanted.

Second, we apply Lemma 3.7, which tells us that different equivalence classes are pairwise disjoint. *(This is Conjecture B from earlier.)*

Since the different equivalence classes are pairwise disjoint and their union is all of E, they form a partition.

Now for statement (2). Let $\equiv_{\mathcal{P}}$ be as in the statement of the theorem; we need to prove this is an equivalence relation.

Reflexivity: clearly x and x lie in the same atom of $\mathcal{P}$, so $\equiv_{\mathcal{P}}$ is reflexive.

Symmetry: if $x \equiv_{\mathcal{P}} y$, then x and y lie in the same atom of $\mathcal{P}$.
Clearly that implies y and x lie in the same atom of $\mathcal{P}$, so $y \equiv_{\mathcal{P}} x$.
Thus $\equiv_{\mathcal{P}}$ is symmetric.

Transitivity: suppose $x \equiv_{\mathcal{P}} y$ and $y \equiv_{\mathcal{P}} z$.
Then x and y lie in the same atom of $\mathcal{P}$.
Also, y and z lie in the same atom of $\mathcal{P}$.
Therefore x and z lie in the same atom of $\mathcal{P}$, so $x \equiv_{\mathcal{P}} z$, i.e. R is transitive. □

3.4 Congruence mod m

EXAMPLE 14 (CONGRUENCE MODULO m)

Definition 3.10 *Let m be a positive integer. $\equiv_m$ is the relation on $\mathbb{Z}$ defined by*

$$x \equiv_m y \iff m \mid (x - y).$$

We call this relation on $\mathbb{Z}$ **congruence mod(ulo)** *m.*
In this context, we write "$x \equiv y \mod m$" as shorthand for "$x \equiv y \mod \equiv_m$".

Observe that each integer $m > 0$ gives rise to a different relation of this type.

If it is clear what m is, you can write $\overline{x}$ for the equivalence class $[x]_m = x \mod m$.

True statements:

(Essentially, to say $x \equiv y \mod m$ means x and y have the same "remainder" when divided by m.)

False statements:

Theorem 3.11 *Congruence modulo m is an equivalence relation on $\mathbb{Z}$.*

PROOF

Reflexivity: Let $x \in \mathbb{Z}$.
$0 = 0m$, so $m \mid 0$, so $m \mid (x - x)$.
Therefore $(x, x) \in R_m$.

Symmetry: Suppose $(x, y) \in R_m$.
This means $m \mid (x - y)$, so there is a $k \in \mathbb{Z}$ such that $km = x - y$.
Therefore $(-k)m = -(x - y) = y - x$.
So $m \mid (y - x)$, which means $(y, x) \in R_m$.
Thus R_m is symmetric.

Transitivity: Suppose $(x, y) \in R_m$ and $(y, z) \in R_m$.
This means $m \mid (y - x)$ and $m \mid (z - y)$.
That means there are $k_1, k_2 \in \mathbb{Z}$ such that $k_1 m = y - x$ and $k_2 m = z - y$.
Adding these two equations, we get

$$(k_1 + k_2)m = k_1 m + k_2 m = (y - x) + (z - y) = z - x.$$

Therefore $m \mid (z - x)$ so $(z, x) \in R_m$.
Since R_m was already proved symmetric, $(x, z) \in R_m$ so R_m is transitive.

Since R_m is reflexive, symmetric and transitive, it is an equivalence relation. □

Question: Given the relation R_m, how many equivalence classes are there?

Other equivalence relations

Generally speaking, any relation of a set defined by some notion of equality or in terms of a shared trait is an equivalence relation.

- equality of numbers; equality of functions; equality of matrices; equality of vectors; equality of sets; etc.
- congruence of geometric shapes; similarity of geometric shapes; etc.
- a relation on the set of people defined by "living in the same country" or "having the same birthday"; etc.
- the relation on integers defined by "having the same remainder when divided by m" (this is congruence modulo m);
- the relation on angles defined by "the angles are coterminal" (i.e. they end in the same place when drawn in standard position);
- isomorphism of groups, rings, or fields (MATH 420);
- the relation on real vector spaces defined by "having the same dimension" (MATH 322);
- relations on square matrices defined by "having the same trace" or "having the same determinant" or "being row equivalent";
- relations on functions defined by "having the same derivative" or "having the same limit as $x \to a$" or "having the same integral from a to b" or "having the same value at x_0";
- etc.

3.5 Quotient spaces

Definition 3.12 *Let R be an equivalence relation on set E. Define the* **quotient space of E by** R*, denoted E/R and pronounced "E mod R", to be the set of R-equivalence classes.*

Example 4 (the keyboard example)

$\mathcal{A}/\bowtie$ =

Example 6 (equality)

The elements of $E/=$, i.e. the equivalence classes, are

Therefore "$E/=$" =

Example 11

Recall V is the equivalence relation on $\mathbb{R}^2$ defined by

$$(x_1, y_1) \equiv (x_2, y_2) \mod V \Leftrightarrow x_1 = x_2.$$

Describe $\mathbb{R}^2/V$.

EXAMPLE 14 (CONGRUENCE MOD m)

The quotient space of the equivalence relation $\equiv_m$ on $\mathbb{Z}$ defined by

$$x \equiv_m y \Leftrightarrow m|(x-y).$$

is usually[1] denoted $\mathbb{Z}/m\mathbb{Z}$. Describe $\mathbb{Z}/m\mathbb{Z}$.

[1] Sometimes this quotient space is denoted by $\mathbb{Z}_m$, but this is bad notation that should be used for something else.

3.6 Integers, rationals and real numbers

Question: what exactly is an integer?

Usually when you first learn about integers, you are just given a list of them:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

or you are told they are the union of the natural numbers and the opposites of the natural numbers. Both these definitions are problematic.

Fortunately, we've now done enough so that I can tell you what an integer really is. To define the integers, let's suppose for now that we are familiar with the set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, ...\}$ (I'll define this set formally in the next chapter), the addition operation on $\mathbb{N}$, and the $\leq$ relation on $\mathbb{N}$.

Math Joke 6 *A boy is watching a building that is originally empty. He then sees two people enter the building (through the only entrance), and later he sees three people leave the building. No one else enters or leaves. Being confused by what he sees, the boy seeks an explanation of this phenomenon from a group of experts consisting of an engineer, a biologist and a mathematician.*

The engineer says, "Obviously, you must have been wrong when you assumed the building was originally empty."

The biologist says, "Obviously, one of the people who entered the building was pregnant, and she gave birth while she was inside."

The mathematician says, "Obviously, if one more person enters the building, then it will again be empty."

There is real meaning behind this joke. It explains exactly what an integer is (sort of).

Definition 3.13 *Let $R_{\mathbb{Z}}$ be the relation on $\mathbb{N}^2$ defined by*

$$(a, b)\, R_{\mathbb{Z}}\, (c, d) \Leftrightarrow a + d = b + c.$$

An **integer** *is an $R_{\mathbb{Z}}$-equivalence class.*

The quotient space of this relation is called the **the set of integers** *and is denoted $\mathbb{Z}$.*

In particular, given $n \in \mathbb{N}$, the integer n is the equivalence class $[(n, 0)]_{R_{\mathbb{Z}}}$, and the integer $-n$ is the equivalence class $[(0, n)]_{R_{\mathbb{Z}}}$.

Think of the equivalence class of (a, b) as the number of people in the building if the building starts out empty, and a people go in and b people come out (no births or deaths inside).

Examples

$$[(28,23)] = [(7,2)] = [(858,853)] = [(5,0)]$$

$$[(14,23)] = [(0,9)] = [(100,109)]$$

Put another way , the equivalence class of (a,b) is the integer $a - b$ you know and love.

Thus we recover the familiar representation of the integers as

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

There is a lot of stuff that has to be proven for this to be sound:

1. We have have to prove that $R_{\mathbb{Z}}$ is an equivalence relation.

2. We have to prove that if $m \neq n \in \mathbb{N}$, then $(0,m)$ and $(0,n)$ are not in the same $R_{\mathbb{Z}}$–equivalence class (ensuring different natural numbers are actually different integers);

3. We have to prove that if $m \neq n \in \mathbb{N}$, then $(m,0)$ and $(n,0)$ are not in the same $R_{\mathbb{Z}}$–equivalence class (so the opposites of different natural numbers are different integers);

4. We have to prove that there are no other equivalence classes other than the classes of each $(n,0)$ and $(0,n)$ for $n \in \mathbb{N}$. (ensuring that all the integers are natural numbers and their opposites).

These are all HW exercises. Statement (1) can be proven directly; statements (2) and (3) have simple contrapositive proofs. To prove statement (4) is trickier; that requires cases depending on whether $a \geq b$ or $a < b$.

Punchline: Now, I've told you what an integer actually is.

Next question: what exactly is a rational number?

The rational numbers are built from the integers in much the same way that the integers are built from the natural numbers:

Definition 3.14 *Let $R_{\mathbb{Q}}$ be the equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ defined by*

$$(a, b)\, R_{\mathbb{Q}}\, (c, d) \Leftrightarrow ad = bc.$$

A **rational number** *is an $R_{\mathbb{Q}}$-equivalence class.*

We denote the equivalence class of (a, b) by $\frac{a}{b}$.

The set of rational numbers is denoted $\mathbb{Q}$.

Given integer $n \in \mathbb{Z}$, the rational number n is the equivalence class $\frac{n}{1}$.

Example

$\frac{6}{21} = \frac{8}{28}$ because

In general, you think of the equivalence class $[(a, b)]_{R_{\mathbb{Q}}} = \frac{a}{b}$ as the size of a quantity where you start with 1, multiply by a and then divide by b.

The fact that $R_{\mathbb{Q}}$ is an equivalence relation needs a proof (HW).

Question

We've defined a *rational number* as an equivalence class of pairs of integers.

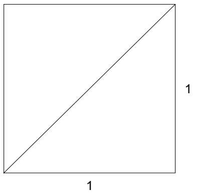
Two pages ago, we defined an *integer* as an equivalence class of pairs of natural numbers.

But how do we define a *natural number*?

What about *real numbers*?

A quantity which is irrational

The ancient Greeks (at least some of them) believed that all numbers were rational. This is in part because they thought of numbers as ratios between lengths. They ran into a problem when they tried to find the length of a diagonal of a square of length 1:



A Greek mathematician named Hippasus discovered the following theorem:

Theorem 3.15 (Hippasus' Theorem) *There is no rational number x such that $x^2 = 2$.*

PROOF Suppose not, i.e. that $x \in \mathbb{Q}$ is such that $x^2 = 2$. Write $x = \frac{a}{b}$ in lowest terms. Since this fraction is in lowest terms, this means that either a or b must be odd (otherwise, 2 divides both the numerator and denominator so the fraction isn't in lowest terms). Then

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

Therefore a^2 is even, so a is even, so we can write $a = 2k$ where $k \in \mathbb{Z}$. Then

Therefore b^2 is even, so b is even. This is a contradiction (earlier we noted that either a or b must be odd). This proves the theorem. □

Hippasus showed this proof to his Greek mathematician friends onboard a ship. His friends were so upset at him for proving this that they threw him overboard (he drowned).

Notice the way the preceding theorem was phrased. Suppose you rephrased Hippasus' Theorem as

$$\sqrt{2} \text{ is not a rational number.}$$

What is wrong with this phrasing?

This leads to a question: is there such a thing as $\sqrt{2}$? What about $\sqrt{-1}$?

More generally, what exactly is a real number? Why is $\sqrt{2}$ real, but $\sqrt{-1}$ isn't?

A short discussion of what a real number is

The set $\mathbb{N}$ of natural numbers has a "problem" that makes it insufficient for dealing with math problems:

Expanding the natural numbers to create the integers "fixes" this problem, but $\mathbb{Z}$ has another problem:

Expanding to the rational numbers fixes this problem. But is $\mathbb{Q}$ problem-free?

The problem with rational numbers has to do with *limits*: if you take sequences of them that "should" have a limit, they don't necessarily have a limit that is a rational number.

For example, consider this sequence:

$$\{1, 1.4, 1.41, 1.414, 1.4142, 1.41421, 1.414213, 1.4142135, ...\}$$

This is a sequence of rational numbers which are getting "closer and closer" together as you go further and further out in the sequence.

(More precisely, the sequence is something called a **Cauchy sequence**).

Since the terms of this sequence are getting closer and closer together, the sequence "should" have a limit.

But if the limit of this sequence is x, then $x^2 = 2$, so this x cannot be rational.

To construct the real numbers, you consider the set of objects(*) which are "limits" of sequences like the one I wrote above.

(*) Technically speaking, these objects are equivalence classes of sequences like the one I wrote above, because if two sequences have the same "limit", they should represent the same real number.

For example, the equivalence class of the sequence described above is the real number we denote as $\sqrt{2}$).

The set you get by doing this is called $\mathbb{R}$, and its elements are called **real numbers**. This set has all the usual properties of real numbers that you know and love.

Formally, $\sqrt{-1}$ isn't a real number because you can't get $\sqrt{-1}$ as the limit of a sequence of rational numbers (the way you prove this, though, is by showing that for any real number x, $x^2 \geq 0$).

For more on this, take MATH 430 and/or ask me.

Last question: is $\mathbb{R}$ problem-free?

Chapter 4

Functions

4.1 Definition of a function

Sets are the first building block of mathematical reasoning. Functions are the second building block; they make formal the idea of a *procedure*, and allow us to make associations between different sets.

Definition 4.1 *Let A and B be sets.*

A **function**, *a.k.a.* **map**, *a.k.a.* **mapping** *f from A to B is a relation from A to B with the following property:*

$$\text{if } (x, y) \in f \text{ and } (x, z) \in f, \text{ then } y = z.$$

If $x \in A$ is such that $\exists y \in B$ with $(x, y) \in f$, then by the above hypothesis, this is the only y such that $(x, y) \in f$.

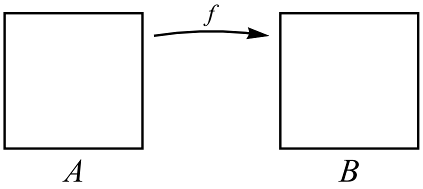
In this situation, we write $y = f(x)$ (or just $y = f\,x$) and we say that y is the **value of** *f* **at** *x, or the* **image of** *f* **at** *x.*

The notation $f : A \to B$ means that f is a function from A to B.

The line of the definition set off in the middle of the box above should remind you of the Vertical Line Test, which any function $f : \mathbb{R} \to \mathbb{R}$ must pass.

If $y = f(x)$, we think of x as being an input and y the corresponding output of the function, and f being a "procedure" that produces the y from the x. Thus if $f : A \to B$, A is the set of possible inputs to f, and B is the set of possible outputs to f. Values of a function are actual outputs of the function.

To help us think logically about functions, we draw pictures like these, called **mapping diagrams**:



That said, technically a function is a relation, meaning that it is just a set of ordered pairs (i.e. a subset of $A \times B$).

Functions are named by pretty much anything: lowercase English letters, uppercase English letters, Greek letters, Hebrew letters, letters with subscripts or superscripts, cursive capital letters, phrases like $\sin$ or $\log$ or $\arg$ or $\arctan$, etc. Sometimes functions are named by symbols (like $\sqrt{\ }$).

Remark: If $f : A \to B$, then "f" and "$f(x)$" are not synonyms:

Definition 4.2 *Let $f : A \to B$.*

- *The* **domain** *of f, defined $Dom(f)$, is the set of inputs at which f has a value:*

$$Dom(f) = \{x \in A : \exists y \in B \text{ s.t. } (x, y) \in f\}.$$

- *The* **codomain** *of f is B.*
- *The* **range** *of f, a.k.a.* **image** *of f, denoted $Range(f)$ or $Im(f)$, is the set of the function's values:*

$$Range(f) = Im(f) = \{y \in B : \exists x \in A \text{ s.t. } f(x) = y\}.$$

- *A* **rule** *for f is a procedure or a formula which specifies how to determine $f(x)$ from each $x \in Dom(f)$.*

A function can have many codomains, since any superset of the range can be considered a codomain of the function. Usually, but not always, $A = Dom(f)$ (otherwise we could replace A with $Dom(f)$).

Are these functions?

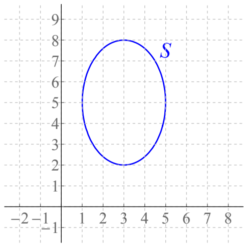
Example 1

The relation R from $E = \{-5, -4, ..., 4, 5\}$ to $F = \{-3, -2, ..., 2, 3\}$, defined by $R = \{(x, y) \in E \times F : y = x + 3\}$.

Example 2

Let S be the relation on $\mathbb{R}$, defined by

$$S = \left\{(x, y) \in \mathbb{R}^2 : \frac{(x-3)^2}{4} + \frac{(y-5)^2}{9} = 1\right\}.$$



Example 3

Let $\bowtie$ be the "same row of a keyboard" relation on the set $\mathcal{A}$ of English letters.

EXAMPLE 4

Let C be the relation from $\mathcal{A}$ to $\mathbb{N}$, where $(x, y) \in C$ if and only if the letter x appears y times in the phrase

```
bibbidi bobbidi boo
```

EXAMPLE 5

Let tr be the relation from the set of 2×2 matrices with real entries to $\mathbb{R}$, defined by $(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, y) \in tr \Leftrightarrow a + d = y$.

Ways to define a function

1. **As a list of ordered pairs:**

   Example: $f = \{(3,2),(4,8),(5,0),(6,2),(7,3)\}$.

2. **Using set-builder notation:**

   Example: $g = \{(x,y) \in \mathbb{R} \times \mathbb{R} : y = x^3 + 2\}$

3. **By describing the rule in words:**

   Example: $g : \mathbb{R} \to \mathbb{R}$ takes its input, cubes it, and then adds 2 to produce output.

   Example: $\sqrt{} : \mathbb{R} \to \mathbb{R}$ takes the (nonnegative) square root of the input.

4. **By describing how to produce the output from each input in words:**

   Example: given $\theta \in \mathbb{R}$, draw an angle of measure θ radians in standard position. Then, define $\sin\theta$ to be the y-coordinate of the point where the terminal side of this angle intersects the unit circle. *(This defines a function* $\sin : \mathbb{R} \to \mathbb{R}$*.)*

   WARNING: In order for the procedure to describe a function, you should not be making any kind of choice in the procedure that leads to different outputs. Such a procedure is called **ill-defined** and is not a description of a function.

   Example of an ill-defined function: given $x \in \mathbb{R}$, let $m(x)$ be a real number y such that $y^4 = x$.

   (more on ill-definedness later)

5. **By describing the rule using a formula with a generic particular input:**

   Example: $g : \mathbb{R} \to \mathbb{R}$ is defined by $g(x) = x^3 + 2$.

   Example: Let $h : \mathbb{R}^2 \to \mathbb{R}$ be $h(x,y) = x^2 \sin(x - y)$.

   Example: Let $k : \mathbb{R}^2 \to \mathbb{R}^3$ be $h(x,y) = \begin{cases} (x+y, 2, 3) & \text{if } x < y \\ (x^2, 2y^3, y - x) & \text{if } x \geq y \end{cases}$.

6. **By defining the function in terms of other previously defined functions:**

   Example: Let $g = h \circ (f + F)$.

   Example: Let $g(x) = h|_A((f_1 \otimes f_2)(x,x))$.

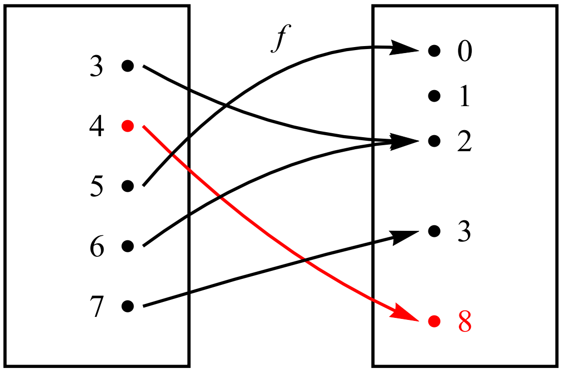
   (more on this later)

Ways to think about/visualize a function

1. **Use its definition:** this can be any of the ideas outlined above

2. **Draw a mapping diagram:**

   Example: for $f = \{(3,2),(4,8),(5,0),(6,2),(7,3)\}$, we might draw this:



   NOTE: We don't use the same dot for the input 3 and the output 3.

   Example: For the function $\sqrt{\ }$, we might draw a partial mapping diagram:

3. **Use a table:**

   Example: for the function f given above, a table of values is

x	3	4	5	6	7
$f(x)$	2	8	0	2	3

   Example: for the function $\sin$, we might consider a partial table of values:

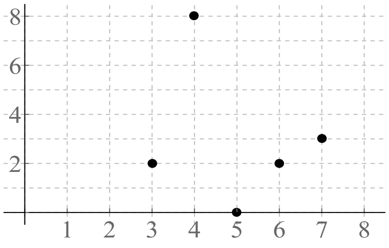
x	0	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π	$\frac{-3\pi}{4}$	$\cdots$
$\sin x$	0	$\frac{\sqrt{3}}{2}$	1	0	$\frac{-\sqrt{2}}{2}$	$\cdots$

   Example: $\mathbf{x} : \mathbb{R} \to \mathbb{R}^2$ defined by $\mathbf{x}(t) = (2\cos t, 2\sin t)$:

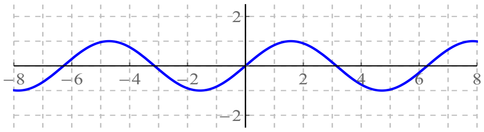
t	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{2}$	π	$\cdots$
$\mathbf{x}(t)$	$(2,0)$	$\left(\sqrt{3},1\right)$	$\left(\sqrt{2},\sqrt{2}\right)$	$(0,2)$	$(-2,0)$	$\cdots$

4. **Sketch a graph or other picture:**

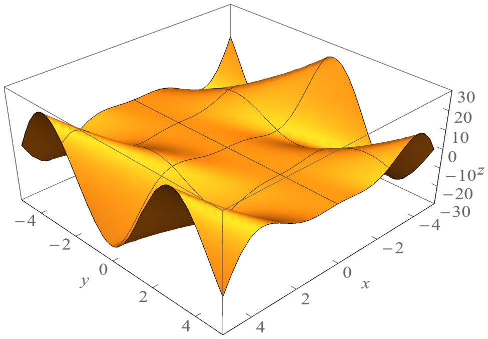
   Example: for the function f, its graph is



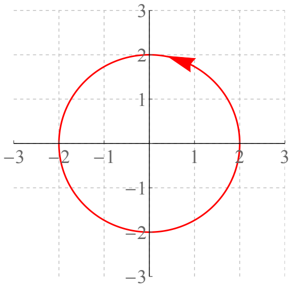
   Example: the graph of $\sin : \mathbb{R} \to \mathbb{R}$ is



   Example: the graph of $h(x, y) = x^2 \sin(x - y)$ is



   Example: the "graph" of $\mathbf{x} : \mathbb{R} \to \mathbb{R}^2$ defined by $\mathbf{x}(t) = (2 \cos t, 2 \sin t)$ is



Well-definedness

Suppose R is an equivalence relation on E; then the quotient space E/R is the set of equivalence classes. Often we want to define functions whose domain is a quotient space. But this can be tricky:

Example 6

Consider these two "functions":

- $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $f(x \mod 6) = x \mod 2$; and
- $g : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ defined by $g(x \mod 2) = 6 \mod 2$.

Which of f and/or g (or neither or both) are actually functions? (Firstly, what might not make them functions?)

Definition 4.3 *An operation or function on a quotient space is* **well-defined** *if the output of the operation or function is unchanged when different inputs from the same equivalence class are used. (The opposite of well-defined is* **ill-defined***.)*

In Example 6 above, f is well-defined, but g is not.

Note: Don't use the phrase "ill-defined function". Things that are "ill-defined" aren't "ill-defined [blanks]", they are just plain "ill-defined".

PROVING WELL-DEFINEDNESS
of a function f defined on a quotient space E/R.:

Suppose $x, y \in E$ are such that $x\,R\,y$.
....
Therefore $f(x) = f(y)$. Thus f is well-defined. □

PROVING ILL-DEFINEDNESS
of a function f defined on a quotient space E/R.:

Define specific $x, y \in E$.

.... Therefore $x\,R\,y$.

.... Therefore $f(x) \neq f(y)$.

Thus f is ill-defined. □

EXAMPLE 7

Determine whether $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(\frac{p}{q}) = p$ is well-defined.

EXAMPLE 8

Determine whether $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ defined by $f(\frac{a}{b}, \frac{p}{q}) = \frac{aq+bp}{bq}$ is well-defined.

4.2 Equality of functions

Recall that functions are a specific kind of relations, and relations are a specific kind of set. Thus functions are sets, so to say two functions are equal technically means that they are equal as sets (each is a subset of the other). Here is an equivalent formulation of this notion of equality that is more useful:

Definition 4.4 (Equality of functions) *To say two functions $f : A \to B$ and $g : C \to D$ are* **equal** *(denoted $f = g$) means that $Dom(f) = Dom(g)$ and for all $x \in Dom(f)$, $f(x) = g(x)$.*

TO PROVE TWO FUNCTIONS ARE EQUAL:
(say $f : A \to B$ and $g : C \to D$):

First, prove $Dom(f) = Dom(g)$ (by a set equality argument).

Then, let $x \in Dom(f)$.
....
(calculate $f(x)$)
....
(calculate $g(x)$)

Therefore $f(x) = g(x)$. □

EXAMPLE 9

Let $f : \{2,3\} \to \mathbb{Z}$ be defined by $f(x) = x^2$ and let $g : \{2,3\} \to \mathbb{R}$ be defined by $g(x) = 5x - 6$. Are f and g the same function?

EXAMPLE 10

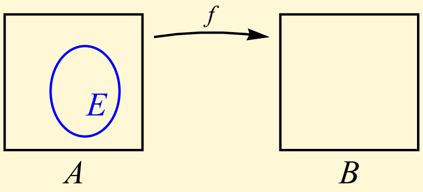
Let $f, g : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \frac{x^2-9}{x-3}$ and $g(x) = x + 3$. Are f and g the same function?

4.3 Images and preimages

Definition 4.5 *Let $f : A \to B$.*

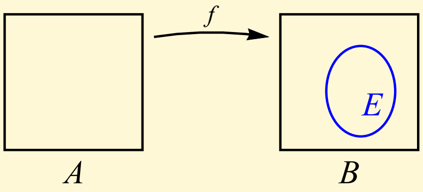
- *Given $E \subseteq A$, the* **image of E under f**, *denoted $f(E)$, is the set*

$$f(E) = \{y \in B : \exists x \in E \text{ s.t. } y = f(x).\}$$



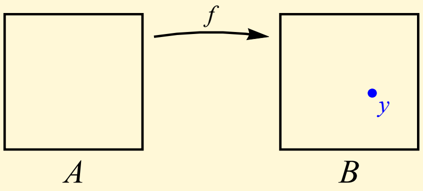
- *Given $E \subseteq B$, the* **preimage (of E under f)**, *also called the* **inverse image (of E under f)**, *denoted $f^{-1}(E)$, is the set*

$$f^{-1}(E) = \{x \in A : f(x) \in E\}.$$



- *Given $y \in B$, the* **preimage (of y under f)**, *also called the* **inverse image (of y under f)**, *denoted $f^{-1}(y)$, is the set defined by*

$$f^{-1}(y) = f^{-1}(\{y\}) = \{x \in A : f(x) = y\}.$$

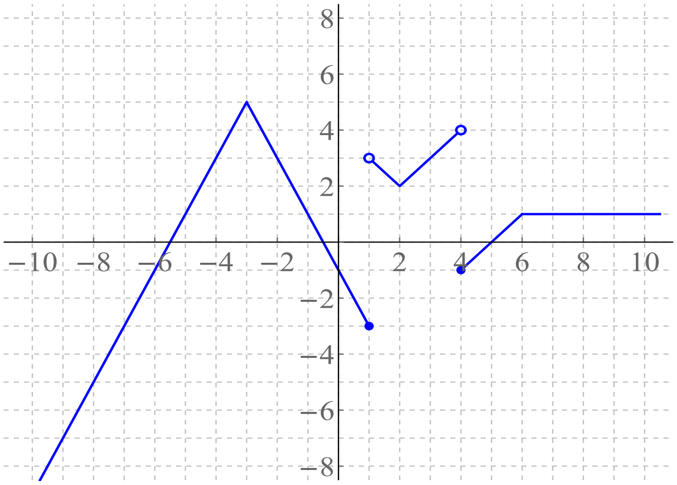


IMPORTANT: Note the difference between the phrases *image of a set* and *image of the function*.

In particular, given $f : A \to B$, the image $Im(f)$ of the function is the image $f(A)$.

EXAMPLE 11

Let $g : \mathbb{R} \to \mathbb{R}$ be the function with this graph:



Describe each of the following sets:

1. $g(6)$

2. $g^{-1}(3)$

3. $g^{-1}(1)$

4. $g([0, 2])$

5. $g^{-1}([2, 3])$

6. $g^{-1}(g(-8))$

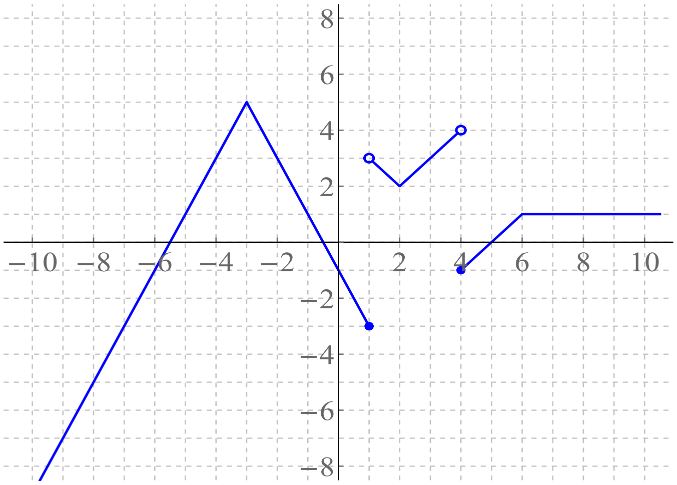
7. $g^{-1}(g(1))$

8. $g(g^{-1}(2))$

9. $g(g^{-1}(6))$

Example 11, continued

Here again is the graph of g:



In each column of this chart, you are given two sets E and F. In each row, you are given a red set and a blue set. In the remaining boxes:

- write = if the red set = the blue set;
- write ⊆ if the red set ⊆ the blue set (but they aren't equal);
- write ⊇ if the red set ⊇ the blue set (but they aren't equal).
- Write "NR" if none of the above hold.

	$E = \{3\}$ $F = \{5\}$	$E = \{6\}$ $F = [4, 7]$	$E = [-9, -7]$ $F = [-8, -4]$	$E = [3, 5]$ $F = [5, 7]$
E and $g^{-1}(g(E))$				
E and $g(g^{-1}(E))$				
$g(E^C)$ and $g(E)^C$ (assume the universal set is $\mathbb{R}$)				
$g^{-1}(E^C)$ and $[g^{-1}(E)]^C$ (assume the universal set is $\mathbb{R}$)				
$g(E \cup F)$ and $g(E) \cup g(F)$				
$g(E \cap F)$ and $g(E) \cap g(F)$				
$g^{-1}(E \cup F)$ and $g^{-1}(E) \cup g^{-1}(F)$				
$g^{-1}(E \cap F)$ and $g^{-1}(E) \cap g^{-1}(F)$				

Properties of images and preimages

What we saw in Example 11 generalizes:

Theorem 4.6 (Properties of images) *Let $f : A \to B$ be a function, and let $E, F \subseteq A$. Then:*

Functions preserve unions: $f(E \cup F) = f(E) \cup f(F)$.

Image of intersection is contained in intersection of image:

$$f(E \cap F) \subseteq f(E) \cap f(F).$$

PROOF We begin with the first statement:

($\subseteq$) Let $y \in f(E \cup F)$. That means ____________________________________.

Case 1: ______________. That means $y = f(x) \in f(E) \subseteq f(E) \cup f(F)$.

Case 2: ______________. That means $y = f(x) \in f(F) \subseteq f(E) \cup f(F)$.

Either way, $y \in f(E) \cup f(F)$.

($\supseteq$) Let $y \in f(E) \cup f(F)$.

Case 1: $y \in f(E)$. This means $y = f(x)$ where $x \in E \subseteq E \cup F$.

Case 2: $y \in f(F)$. This means $y = f(x)$ where $x \in F \subseteq E \cup F$.

Either way, $y = f(x)$ for $x \in E \cup F$, so $y \in f(E \cup F)$.

The second statement is a HW problem (use a set inclusion argument). □

Theorem 4.7 (Properties of preimages) *Let $f : A \to B$ be a function, and let $E, F \subseteq B$. Then:*

Preimages preserve complements: $f^{-1}(E^C) = [f^{-1}(E)]^C$.

Preimages preserve unions: $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$.

Preimages preserve intersections: $f^{-1}(E \cap F) \subseteq f^{-1}(E) \cap f^{-1}(F)$

PROOF We prove the first statement here, and leave the other two as HW. This one we will do with a shortcut set equality proof:

$$\begin{aligned} x \in f^{-1}(E^C) &\Leftrightarrow f(x) \in E^C \\ &\Leftrightarrow f(x) \notin E \\ &\Leftrightarrow x \notin f^{-1}(E) \\ &\Leftrightarrow x \in [f^{-1}(E)]^C. \ \square \end{aligned}$$

Theorem 4.8 (Composing f and f^{-1}:) *Let $f : A \to B$ be a function. Then:*

f, then f^{-1} makes a set bigger: *For any $E \subseteq A$, $E \subseteq f^{-1}(f(E))$.*

f^{-1}, then f makes a set smaller: *For any set $E \subseteq B$, $f(f^{-1}(E)) = E \cap Im(f)$.*

f^{-1}, then f keeps a subset of the image the same: *If $E \subseteq Im(f)$, then*

$$f(f^{-1}(E)) = E.$$

PROOF The third statement follows immediately from the second. The first two statements are HW (these are set inclusion / set equality arguments)

4.4 Elementary functions

Here are some functions that are used often in mathematics. I mention these in part because we will use them later in MATH 324, and also so that if you see this notation somewhere else and it isn't explained to you at the time, you aren't totally lost (if you remember the language):

More complicated functions are often built from these in the way that compounds are built from *elements* in chemistry, so we call these *elementary* functions.

Identity functions

Definition 4.9 *Let E be any set. The* **identity function** *on E, denoted I_E, or I or 1_E or 1, is the function $I_E : E \to E$ defined by the rule $I_E(x) = x$.*

(Put another way, the identity function is just the equality relation on E. It sends every input to itself.)

The notation here is inherited from linear algebra (MATH 322), where you learn that the identity function $\mathbb{R}^n \to \mathbb{R}^n$ is matrix multiplication by the identity matrix, which is called I.

Inclusion maps

Definition 4.10 *Let $A \subseteq B$. The* **inclusion map** *from A to B, denoted i, is the function $i : A \to B$ defined by the rule $i(x) = x$.*

Constant functions

Definition 4.11 *A function $f : A \to B$ is called a* **constant function** *if $\exists b \in B$ s.t. $\forall x \in Dom(f), f(x) = b$.*

To write "$f \equiv b$" means that $\forall x \in Dom(f)$, $f(x) = b$.

(Put another way, a constant function is one that sends every input to the same output.)

Characteristic functions

Definition 4.12 *Let $E \subseteq A$. The* **characteristic function** *of E, a.k.a. the* **indicator function** *of E, is the function $\mathbb{1}_E : A \to \{0,1\}$ defined by*

$$\mathbb{1}_E(x) = \begin{cases} 1 & \text{if } x \in E \\ 0 & \text{if } x \notin E \end{cases}$$

$\mathbb{1}_E$ is also denoted χ_E.

(Put another way, a characteristic function indicates whether or not you are in E.)

Examples

1. Let $A = \mathbb{R}$. Then $\mathbb{1}_{\mathbb{Z}}(3) = 1$ and $\mathbb{1}_{[-5,5]}(2) = 1$ but $\mathbb{1}_{[-15,15]}(23) = 0$.

2. Let $A = \mathbb{R}$. Then $\mathbb{1}_{[2,5)}$ has graph

Note: For any characteristic function, $\mathbb{1}_E^{-1}(1) = E$ and $\mathbb{1}_E^{-1}(0) = E^C$.

Characteristic functions give you a way to turn set operations into arithmetic. For example, here are some cool facts about characteristic functions (you might be asked to prove some of these in the HW):

$$\begin{array}{cc} \mathbb{1}_{E\cap F} = \mathbb{1}_E \mathbb{1}_F & \mathbb{1}_{E\cup F} = \max\{\mathbb{1}_E, \mathbb{1}_F\} \\ \mathbb{1}_{E^C} = 1 - \mathbb{1}_E & \mathbb{1}_E + \mathbb{1}_F = \mathbb{1}_{E\cup F} + \mathbb{1}_{E\cap F} \\ E \subseteq F \Leftrightarrow \forall x, \mathbb{1}_E(x) \le \mathbb{1}_F(x) & E = F \Leftrightarrow \mathbb{1}_E = \mathbb{1}_F \end{array}$$

Kronecker delta functions

Definition 4.13 *Let E be a set. The* **Kronecker delta function** *is the function $\delta : E \times E \to \{0,1\}$ defined by*

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

(A Kronecker delta function tells you whether the two components of the input are equal or not.)

Examples

$\delta_{3,5} = 0$ and $\delta_{4,4} = 1$.

$\delta_{(1,2),(2,1)} = 0$.

Coordinate maps

Definition 4.14 *Let E and F be sets. The* **projection(s)** *of $E \times F$ onto E and F, denoted π_1 and π_2 respectively, are the functions $\pi_1 : E \times F \to E$ and $\pi_2 : E \times F \to F$ defined by*

$$\pi_1(x,y) = x \quad \text{and} \quad \pi_2(x,y) = y.$$

(Projections give you a way of extracting each coordinate from an ordered pair: π_1 gives you the first coordinate, and π_2 gives you the second coordinate. Because of this, projections are also called **coordinate maps**.)

NOTE: The word "projection" is being used here to mean something different than what it does in MATH 322 (where you are talking about "projection" onto a line or plane or other subspace). You can reconcile these two notions of "projection" with a little more linear algebra machinery that I don't teach in MATH 322.

Examples

$\pi_1(3,6) = 3$ and $\pi_2(A,C) = C$.

This notation extends to ordered n-tuples: unless you are told π_5 means something else, you would, for example, assume that

$$\pi_5(1,8,5,-3,2,7,8,3) =$$

Quotient maps

Definition 4.15 *Let E be a set and let R be an equivalence relation on E. The map $\pi_R : E \to E/R$ defined by $\pi_R(x) = [x]_R$ is called the* **quotient map** *or* **canonical map** *for R.*

Note that each input of a canonical map is a single element of E, but each output is a set.

EXAMPLE

Let R_7 be congruence modulo 7. Then $\pi_{R_7}(26) =$

4.5 Constructing more complicated functions

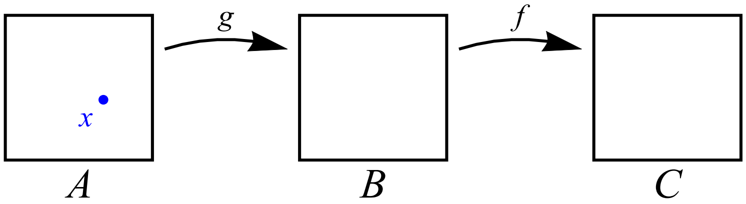
Earlier, we said that one way to define a function is to build it out of previously defined functions. This section runs through many different ways to do this. We begin with the most important construction:

Composition

Definition 4.16 *Let $g : A \to B$ and let $f : B \to C$. Define the* **composition** *of f with g, denoted $f \circ g$, to be the function from A to C defined by the rule*

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

Mapping diagram:



Theorem 4.17 (Properties of compositions) *Let $h : A \to B$, $g : B \to C$ and $f : C \to D$. Then:*

1. **Domain of a composition:** $Dom(f \circ g) = g^{-1}(Dom(f))$;
2. **Preimages under composition:** *for any* $E \subseteq D$, $(f \circ g)^{-1}(E) = g^{-1}(f^{-1}(E))$.
3. **Composition is associative:** $(f \circ g) \circ h = f \circ (g \circ h)$.
4. **Composition with identity function:** $f \circ I_C = f$ *and* $I_D \circ f = f$.

PROOF We prove the first statement with a shortcut set equality proof:

$$\begin{aligned} x \in Dom(f \circ g) &\Leftrightarrow \exists\, y \in D \text{ s.t. } (f \circ g)(x) = y \\ &\Leftrightarrow \exists\, y \in D \text{ s.t. } f(g(x)) = y \\ &\Leftrightarrow g(x) \in Dom(f) \\ &\Leftrightarrow x \in g^{-1}(Dom(f)). \end{aligned}$$

We prove the second statement with a shortcut set equality proof. Let $E \subseteq D$.

$$\begin{aligned} x \in (f \circ g)^{-1}(E) &\Leftrightarrow (f \circ g)(x) \in E \\ &\Leftrightarrow f(g(x)) \in E \\ &\Leftrightarrow g(x) \in f^{-1}(E) \\ &\Leftrightarrow x \in g^{-1}(f^{-1}(E)). \end{aligned}$$

To prove the third statement, we prove that $(f \circ g) \circ h$ and $f \circ (g \circ h)$ have the same domain by a shortcut set equality proof:

$$\begin{aligned} Dom((f \circ g) \circ h) &= h^{-1}(Dom(f \circ g)) \quad \text{(by property 1)} \\ &= h^{-1}(g^{-1}(Dom(f)) \quad \text{(by property 1 again)} \\ &= (g \circ h)^{-1}(Dom(f)) \quad \text{(by property 2)} \\ &= Dom(f \circ (g \circ h)) \quad \text{(by property 1).} \end{aligned}$$

It is left to show the functions have the same rule. But

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

so the functions have the same rule. Thus $(f \circ g) \circ h = f \circ (g \circ h)$.

For the last statement, observe that $Dom(I_C) = C$ and $Dom(I_D) = D$. So

$$Dom(f \circ I_C) = I_C^{-1}(Dom(f)) = Dom(f) \quad \text{and} \quad Dom(I_D \circ f) = f^{-1}(D) = Dom(f)$$

so the functions have the same domain. They also have the same rule, because

$$f \circ I_C(x) = f(I_C(x)) = f(x) \quad \text{and } I_D \circ f(x) = I_D(f(x)) = f(x). \square$$

NOTE: In general, composition is not commutative:

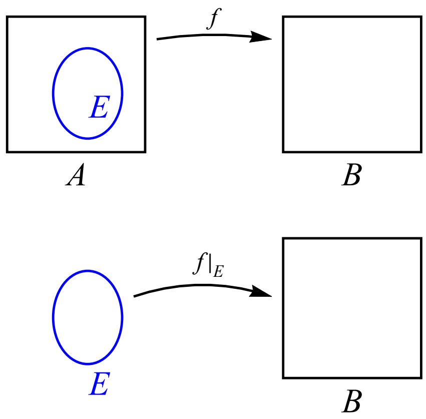
Restriction

To *restrict* a function means to use the same rule, but to "restrict" the domain, i.e. shrink the set of the things that are allowed to be considered inputs:

Definition 4.18 *Let $f : A \to B$ and let $E \subseteq A$. Define the* **restriction** *of f to E, denoted $f|_E$, to be the function from E to B defined by the rule*

$$f|_E(x) = f(x) \text{ for all } x \in E.$$

Mapping diagram:



EXAMPLE

Let $f : \mathbb{R} \to \mathbb{R}$ be the absolute value function $f(x) = |x|$.

Then $f|_{[0,\infty)}$ is the identity function on $[0, \infty)$.

Extension

To *extend* a function means to make its domain larger without changing its rule on the previous domain:

Definition 4.19 *Let $f : A \to B$ and let $E \supseteq A$. An* **extension** *of f to E is any function $g : E \to B$ where $g|_A = f$.*

With extensions, we often abuse notation and call the extension the same letter as the original function.

EXAMPLE

$f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x|$ is an extension of the identity function on $[0, \infty)$.

Union

If we have two functions with the same codomain which coincide on the intersection of their domains, we can make a function which extends both of them called their *union*:

Definition 4.20 *Let $f_1 : A_1 \to B$ and $f_2 : A_2 \to B$ where either*

$$A_1 \cap A_2 = \varnothing \text{ or } f_1|_{A_1 \cap A_2} = f_2|_{A_1 \cap A_2}.$$

Define the **union** *of f_1 and f_2 to be the function $f_1 \cup f_2 : (A_1 \cup A_2) \to B$ by*

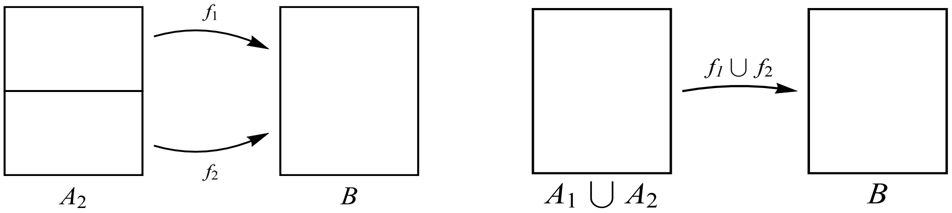
$$(f_1 \cup f_2)(x) = \begin{cases} f_1(x) \text{ if } x \in A_1 \\ f_2(x) \text{ if } x \in A_2 \end{cases}$$

If $f_1|_{A_1 \cap A_2} \neq f_2|_{A_1 \cap A_2}$, then $f_1 \cup f_2$ is not well-defined.

The reason we use the $\cup$ symbol is that if we think of the function as subsets of $(A_1 \cup A_2) \times B$, the function $f_1 \cup f_2$ is literally the union of these two subsets. The union of two functions is sometimes denoted $f_1 \oplus f_2$.

It is clear that $f_1 \cup f_2 = f_2 \cup f_1$, since these functions have the same domain and same rule.

Mapping diagrams (where $A_1 \cap A_2 = \varnothing$)



Example 12

Let $f : [0, \infty) \to \mathbb{R}$ be defined by $f(x) = |x| + 1$ and let $g : (-\infty, 2] \to \mathbb{R}$ be defined by $g(x) = 1 - x$. Describe $f \cup g$, if this function is defined.

Direct product

Definition 4.21 *Let $f_1 : A_1 \to B_1$ and $f_2 : A_2 \to B_2$. The* **direct product** *of f_1 and f_2, denoted $f_1 \otimes f_2$, is the function $f_1 \otimes f_2 : A_1 \times A_2 \to B_1 \times B_2$ defined by*

$$f_1 \otimes f_2(a_1, a_2) = (f_1(a_1), f_2(a_2)).$$

Direct product is also denoted $f_1 \times f_2$.

4.6 Surjectivity and injectivity

Surjectivity

Definition 4.22 *A function $f : A \to B$ is called* **surjective***, a.k.a.* **onto***, if $f(A) = B$. If f is surjective, we can write $f : A \twoheadrightarrow B$.*

The noun form of "surjective" is **surjection**.

Typing tip: To get the $\twoheadrightarrow$ in Overleaf, type \twoheadrightarrow while in math mode. If you use my template, you can type \onto as a shortcut.

Equivalent characterizations of surjectivity:

1. $f(A) = B$.

   This is the definition of surjectivity.

2. $Im(f) = B$.

   Reason: We showed earlier $f(A) = Im(f)$.

3. The codomain of f equals its range.

   Reason: B is the codomain; $Im(f)$ is the range.

4. Every potential output of f is an actual output.

   Reason: potential outputs form the codomain; actual outputs form the range.

5. For every $y \in B$, there is an $x \in A$ such that $f(x) = y$.

   Reason: This is a more formal statement of (1) above.

Remark: if the function f has some additional algebraic structure (i.e. f is a linear transformation or group homomorphism), then there are other characterizations of surjectivity which can be useful. But those don't hold for arbitrary functions.

Characterization (5) above gives you a standard way to prove whether or not a function is surjective:

PROVING that $f : A \to B$ is surjective:

Let $y \in B$.
Write down a formula for some $x \in A$ (that comes from some scratch work).
Show that for the x you wrote down, $f(x) = y$.
Conclude that f is onto. □

DISPROVING that $f : A \to B$ is surjective:

Write down a specific $y \in B$.
Prove that $\sim \exists\, x \in A$ s.t. $f(x) = y$.
(Usually you suppose $f(x) = y$ and derive a contradiction.)
Conclude that f is not onto. □

Example 13

Determine, with proof, whether or not each function is surjective:

1. $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = x^2$:

2. $G : \mathbb{R} \to \mathbb{R}$ defined by $G(x) = x + 4$:

3. $H : \mathbb{R}^2 \to \mathbb{R}$ defined by $H(x, y) = xy$:

4. $J : 2\mathbb{Z} \to (2\mathbb{Z} + 1)$ defined by $J(x) = 2x + 7$:

Properties of surjections

Here is a laundry list of functions which are always surjections:

Theorem 4.23 *All of the following functions are onto:*

- *the identity function on any set;*
- *any projection map;*
- *any quotient map;*
- *the composition of any two surjections;*
- *the extension of any surjection;*
- *the union of two surjections;*
- *the direct product of two surjections.*

PROOF Here is the proof that any quotient map is onto.

Let E be a set and R be an equivalence relation on E; let $\pi_R : E \to E/R$ denote the quotient map.

Let $A \in E/R$. That means A is an R-equivalence class, i.e. $A = [x]_R$ for some $x \in E$.
For this x, $\pi_R(x) = A$. Therefore π_R is onto.

The rest of these proofs are left as HW. □

NOTE: the only method of constructing a new function from two old ones that not on this laundry list is *restriction*. The restriction of a surjection may not be onto.

Surjections have the following nice property: if you take a subset of the codomain, "pull it back" by f^{-1}, then "push it back forward" by f, then if f is onto you get exactly the subset you started with. Recall that this isn't true for general functions.

Theorem 4.24 *If $f : A \twoheadrightarrow B$ is onto, then for any $E \subseteq B$, $f(f^{-1}(E)) = E$.*

PROOF HW

Hint: We proved the $(\supseteq)$ direction for all functions earlier; here you have to prove the $(\subseteq)$ direction.

Last, the composition of two surjections is always a surjection:

Theorem 4.25 (Composition of surjections is onto) *If $g : A \twoheadrightarrow B$ and $f : B \twoheadrightarrow C$ are both onto, then $f \circ g$ is onto.*

PROOF HW

Injectivity

Definition 4.26 *A function $f : A \to B$ is called* **injective**, *a.k.a.* **one-to-one**, *a.k.a.* $1 - 1$, *if for every $x, y \in A$, $f(x) = f(y)$ implies $x = y$.*

If $f : A \to B$ is injective, we write $f : A \hookrightarrow B$.

The noun form of "injective" is **injection**.

Typing tip: To get the $\hookrightarrow$ in Overleaf, type \hookrightarrow while in math mode. If you use my template, you can type \into as a shortcut.

Equivalent characterizations of injectivity:

1. $f(x) = f(y)$ implies $x = y$.

   This is the definition.

2. $x \neq y$ implies $f(x) \neq f(y)$.

   Reason: This is the contrapositive of the definition.

3. Different inputs go to different outputs.

   Reason: This is a restatement of (2) above.

Remark: if the function f has some additional algebraic structure (i.e. f is a linear transformation or group homomorphism), then there is an additional characterization of injectivity which is very useful: $ker(f) = \{0\}$. But this doesn't make sense for arbitrary functions.

You usually prove a function is injective by the first characterization above.

PROVING that $f : A \to B$ is injective:

Suppose $x, y \in A$ are such that $f(x) = f(y)$.
....
Therefore, $x = y$.
Conclude that f is $1 - 1$. □

DISPROVING that $f : A \to B$ is injective:

Write down two specific $x, y \in A$.
....
Therefore, $f(x) = f(y)$.
Conclude that f is not $1 - 1$. □

Example 13, continued

Determine, with proof, whether or not each function is injective:

1. $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = x^2$:

2. $G : \mathbb{R} \to \mathbb{R}$ defined by $G(x) = x + 4$:

3. $H : \mathbb{R}^2 \to \mathbb{R}$ defined by $H(x, y) = xy$:

4. $J : 2\mathbb{Z} \to (2\mathbb{Z} + 1)$ defined by $J(x) = 2x + 7$:

Properties of injections

Here is a laundry list of functions which are always injections:

Theorem 4.27 *All of the following functions are* $1-1$*:*

- *the identity function on any set;*
- *any inclusion map;*
- *the composition of any two injections;*
- *the restriction of any injection;*
- *the union of two injections whose ranges are disjoint;*
- *the direct product of two injections.*

PROOF Here is the proof that the restriction of any injection is $1-1$:

Let $f : A \to B$ be $1-1$ and let $E \subseteq A$.

Suppose $f|_E(x) = f|_E(y)$ for $x, y \in E$.
That means, by definition of restriction, that $f(x) = f(y)$.
But since f is $1-1$, that means $x = y$.
Therefore $f|_E$ is $1-1$.

The rest of these proofs are left as HW. □

NOTE: the only method of constructing a new function from two old ones that not on this laundry list is *extension*. An extension of an injection may not be $1-1$.

Careful: the union of two injections whose ranges overlap need not be $1-1$.

Injections have the following nice property: if you take a subset of the domain, "push it forward" by f, then "pull it back" by f^{-1}, you get exactly the subset you started with. Recall that this isn't true for general functions.

Theorem 4.28 *If* $f : A \hookrightarrow B$ *is* $1-1$*, then for any* $E \subseteq Dom(f)$, $f^{-1}(f(E)) = E$.

PROOF HW

Theorem 4.29 (Composition of injections is 1 – 1) *If* $g : A \hookrightarrow B$ *and* $f : B \hookrightarrow C$ *are both* $1-1$*, then so is* $f \circ g$.

PROOF HW

4.7 Inverse functions

Bijectivity

Definition 4.30 *A function $f : A \to B$ is called* **bijective**, *a.k.a. a* $1-1$ **correspondence**, *if f is both surjective and injective.*

In this situation, you can write $f : A \leftrightarrow B$, but keep in mind that this notation means that f is a bijective function from the left-hand set to the right-hand set.

NOTE: "$1-1$ correspondence" and "$1-1$" are not synonyms. "$1-1$" means *injection*; "$1-1$ correspondence" means *bijection*.

The noun form of "bijective" is **bijection**.

Typing tip: To get the ↔ in Overleaf, type \leftrightarrow while in math mode. If you use my template, you can type \lra as a shortcut.

Equivalent characterizations of bijectivity:

1. f is both surjective and injective.

   This is the definition.

2. For every $y \in B$, there is one and only one $x \in A$ such that $f(x) = y$.

   Reason: there is at least one x because of surjectivity, and at most x because of injectivity.

3. Every point in the codomain has a unique preimage.

   Reason: this is a restatement of (2).

PROVING that $f : A \to B$ is bijective:

Prove f is surjective.
Prove f is injective.
Conclude that f is bijective. □

DISPROVING that $f : A \to B$ is bijective:

Either prove f is not surjective, or prove that f is not injective.
Conclude that f is not bijective. □

EXAMPLE 13, CONTINUED

Determine whether or not each function is bijective:

1. $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = x^2$:

   Answer: **NO** (neither surjective nor injective)

2. $G : \mathbb{R} \to \mathbb{R}$ defined by $G(x) = x + 4$:

   Answer: **YES** (surjective and injective)

3. $H : \mathbb{R}^2 \to \mathbb{R}$ defined by $H(x, y) = xy$:

   Answer: **NO** (not injective)

4. $J : 2\mathbb{Z} \to (2\mathbb{Z} + 1)$ defined by $J(x) = 2x + 7$:

   Answer: **NO** (not surjective)

Laundry list of bijections

Theorem 4.31 *All of the following functions are bijections:*

- *the identity function on any set;*
- *the composition of any two bijections;*
- *the union of two bijections whose ranges are disjoint;*
- *the direct product of two bijections.*

PROOF This follows directly from Theorems 4.27 and 4.23. □

Invertibility

Question: When can you "undo" a function by another function?

Definition 4.32 *Let $f : A \to B$ be a function (with $Dom(f) = A$). If there is another function $f^{-1} : B \to A$ (with $Dom(f^{-1}) = B$) such that*

$$f^{-1} \circ f = I_A \quad \textit{and} \quad f \circ f^{-1} = I_B,$$

then we say f is **invertible** *and that f^{-1} is an* **inverse (function)** *of f.*

The equations in the definition above can be restated as

$$\forall x \in A, f^{-1}(f(x)) = x \quad \text{and} \quad \forall y \in B, f(f^{-1}(y)) = y.$$

EXAMPLE 14

Let $A = \mathbb{R}$ and $B = (0, \infty)$. Let $f : A \to B$ be defined by $f(x) = e^x$ and $f^{-1} : B \to A$ be defined by $f^{-1}(y) = \ln y$. Prove that f and f^{-1} are inverses.

Theorem 4.33 *Let $f : A \to B$. f is invertible if and only if f is bijective.*

PROOF (⇒) Suppose f is invertible; let the inverse of f be denoted f^{-1}.

First, we prove f is onto. To do this, let $y \in B$.
Then we can set $x = f^{-1}(y)$. Notice $x \in A$.
Notice also that $f(x) = f(f^{-1}(y)) = y$, so f is onto.

Next, we prove that f is $1-1$. To do this, suppose $f(x) = f(y)$.
Apply f^{-1} to both sides to get $f^{-1}(f(x)) = f^{-1}(f(y))$.
Restated, this is $(f \circ f^{-1})(x) = (f \circ f^{-1})(y)$.
Since f and f^{-1} are inverses, this can be rewritten as $x = y$.
Therefore f is $1-1$, hence bijective.

(⇐) Suppose f is bijective. Let $y \in B$.
Because f is bijective, there is a unique $x \in A$ such that $f(x) = y$.
Define $f^{-1}(y)$ to be this x; this defines a function $f^{-1} : B \to A$.
By definition, $f \circ f^{-1}(y) = f(x) = y$ and $f^{-1} \circ f(x) = f^{-1}(y) = x$.
Thus f^{-1} is an inverse function of f, so f is invertible. □

PROVING that $f : A \to B$ is bijective
(by constructing an inverse function of f):

Write down a formula for $f^{-1} : B \to A$.
Show that for any $x \in A$, $f^{-1}(f(x)) = x$.
Show that for any $y \in B$, $f(f^{-1}(y)) = y$.
Conclude that f is invertible, hence bijective. □

Computing the inverse of a function

Example 15

Let $f : (\mathbb{R} - \{-2\}) \to (\mathbb{R} - \{1\})$ be defined by $f(x) = \frac{x-4}{x+2}$. Prove f is bijective by finding a rule for f^{-1}, and proving that the rule you define gives an inverse of f.

Properties of inverses

Question: Might the function f in Example 15 above have an inverse function other than the one you found? The following theorem guarantees that the answer to this question is **NO**.

Consequence: we can say "THE inverse of f", rather than "AN inverse of f".

Theorem 4.34 (Uniqueness of inverse functions) *Let $f : A \leftrightarrow B$ be an invertible function. Then f has only one inverse function.*

Proof Suppose $g : B \to A$ and $h : B \to A$ are both inverses of f.
Clearly g and h have the same domain (namely, B).
Let $x \in B$. Then $f(g(x)) = x = f(h(x))$.
Since f is invertible, it is injective, so $g(x) = h(x)$.
Since x is arbitrary, $g = h$. □

Theorem 4.35 (Inverse of an inverse) *Let f be invertible. Then f^{-1} is invertible, and $(f^{-1})^{-1} = f$.*

PROOF This follows from the definition of inverse function. □

Theorem 4.36 (Inverse of a composition) *Suppose f and g are invertible. Then $f \circ g$ is invertible, and $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.*

PROOF Since bijective and invertible are synonyms, the fact that $f \circ g$ is invertible follows from Theorem 4.31. The inverse formula follows from applying Property 2 of Theorem 4.17 to sets of the form $E = \{y\}$. □

WARNING on the notation "f^{-1}": the symbol f^{-1} is used for two different things: *preimage* and *inverse function*:

Permutations

Definition 4.37 *Let E be a set. A bijection $f : E \leftrightarrow E$ is called a* **permutation** *of E. The set of permutations of a set is called the* **symmetric group on** *E and is denoted $Sym(E)$ (or S_n if E has exactly n elements).*

$Sym(E)$ is the prototypical example of a mathematical object called a *group*[1]; groups are studied extensively in MATH 420.

[1] The group operation of $Sym(E)$ is composition of functions; I_E is the identity element of this group.

Chapter 5

Mathematical induction

5.1 Order relations

In Chapter 3 we introduced the idea of a *relation*, and spent a lot of time on the most important class of relations: *equivalence relations*. These generalize the properties you know about equality.

A second important class of relations are *order relations*. These generalize the concept of "less than or equal to". In MATH 324, all you need to know about order relations is contained in two prototypical examples that we'll introduce shortly.

Partial orderings

Definition 5.1 *Let R be a relation on a set E.*
We say R is a **partial order** *on E if R has the following three properties:*

Reflexivity: *for all $x \in E$, $(x,x) \in R$.*

Antisymmetry: *if $x, y \in E$ are such that $(x,y) \in R$ and $(y,x) \in R$, then $x = y$.*

Transitivity: *if $x, y \in E$ are such that $(x,y) \in R$ and $(y,z) \in R$, then $(x,z) \in R$.*

A pair (E,R), where R is a partial order on E, is called a **partially ordered set**, *or* **poset** *for short.*

Now for the two main examples you need to understand:

PROTOTYPE EXAMPLE 1

$\leq$ is a partial order on $\mathbb{R}$ (also on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, but not on $\mathbb{C}$).

- *Reflexivity:* $x \leq x$
- *Antisymmetry:* if $x \leq y$ and $y \leq x$, then $x = y$.
- *Transitivity:* if $x \leq y$ and $y \leq z$, then $x \leq z$.

PROTOTYPE EXAMPLE 2

Let E be any set. Then $\subseteq$ is a partial order on 2^E.

- *Reflexivity:* $A \subseteq A$
- *Antisymmetry:* if $A \subseteq B$ and $B \subseteq A$, then $A = B$.
- *Transitivity:* if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Total orderings

Definition 5.2 *Let R be a partial ordering on set E.*

We say $x, y \in E$ are **comparable** *if either xRy or yRx.*

A partial ordering R on set E is called a **total ordering***, a.k.a.* **linear ordering***, if every pair of elements in E is comparable.*

PROTOTYPE EXAMPLE 1

$\leq$ is a total order on $\mathbb{R}$ (also on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$).

Reason:

- $\leq$ is a partial ordering (earlier);
- if $x, y \in \mathbb{R}$, either $x \leq y$ or $y \leq x$ (i.e. any two real numbers are comparable).

PROTOTYPE EXAMPLE 2

$\subseteq$ is **not** a total order on 2^E.

Reason:

- $\subseteq$ is a partial ordering (earlier); but
- suppose $E = \{1, 2\}$. Let $A = \{1\}$ and $B = \{2\}$.
  $A \nsubseteq B$ and $B \nsubseteq A$ (i.e. A and B are not comparable).

Well orderings

Definition 5.3 *Let R be a total ordering on E. We say R is a* **well ordering** *(or that E is* **well ordered** *(by R)) if every nonempty subset $A \subseteq E$ contains a smallest element, i.e.*

$$\exists\, x \in A \text{ s.t. } (y \in A \Rightarrow x\, R\, y)$$

PROTOTYPE EXAMPLE 1

$\leq$ is **<u>not</u>** a well ordering of $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$.
Reason:

- $\leq$ is a total ordering (earlier); but
- Let $A = \{..., -5, -4, -3, -2, -1, 0\}$ be the set of negative integers. A is a nonempty subset which does not have a smallest element under $\leq$.

PROTOTYPE EXAMPLE 1 (DIFFERENT CONTEXT)

$\leq$ appears to be a well ordering of $\mathbb{N}$.
Reason:

- $\leq$ is a total ordering (earlier); and
- it seems like if A is a nonempty set of natural numbers, then A has a least element. But how do you prove this?

PROTOTYPE EXAMPLE 2

$\subseteq$ is **<u>not</u>** a total ordering on 2^E, so it can't be a well ordering.

Here is a somewhat controversial axiom about well orderings:

Axiom 5.4 (Well ordering axiom) *Let E be a set. Then there is a relation on E which is a well ordering.*

Why mathematicians like/accept this axiom:

Assuming this axiom is true allows us to prove lots of things that "should be" true (Google the **axiom of choice** for more on this). One example (from MATH 322) is a theorem which says that every vector space has a basis.

Why physicists do not like/accept this axiom:

Among other things, using this axiom you can prove that it is possible to something seemingly impossible: in particular, you can

1. take a sphere of radius 1 unit,
2. cut it into finitely many pieces,
3. shift and rotate the pieces around without stretching or shrinking them,
4. then put them back together so that they exactly occupy two disjoint spheres, each of which has radius 1.

This phenomenon is called the **Banach-Tarski paradox**, but it's only a paradox to physicists (mathematicians have pretty much resolved the issues).

5.2 What are the natural numbers?

Natural numbers are used for counting things, and ordering things. It is very hard (but doable) to rigorously construct the natural numbers from (almost) nothing,[1] so we'll just accept five axioms about the natural numbers:

Axiom 5.5 (Peano's axioms) *The set of natural numbers is denoted $\mathbb{N}$. This is a set which satisfies five axioms, four of which are given here and one which is given later:*

Peano's first axiom: 0 *is a natural number.*

Peano's second axiom: *Every natural number n has a* **successor** $s(n)$ *which is a natural number.*

Peano's third axiom: 0 *is not the successor of any natural number.*

Peano's fourth axiom: *The successor function $s : \mathbb{N} \to \mathbb{N}$ is injective.*

The successor of a natural number is the "next" natural number, i.e.

$$s(0) = 1 \qquad s(14) = 15 \qquad s(2282350) = 2282351 \qquad \text{etc.}$$

[1] Google "Frege's Theorem" for more on this.

We therefore obtain the natural numbers

$$\begin{aligned}\mathbb{N} &= \{0, s(0), s(s(0)), s(s(s(0))), \ldots, (s \circ s \circ s \circ \cdots \circ s)(0), \ldots\}\\ &= \{0, 1, 2, 3, 4, 5, 6, \ldots, n, \ldots\}\end{aligned}$$

and by the third and fourth Peano axioms, all these numbers are different. In particular, the natural number n is

$$n = (s \circ s \circ s \circ s \circ \cdots \circ s)(0).$$

Addition

Addition of natural numbers can be defined by repeated iteration of the successor function s:

Definition 5.6 *Let $a, b \in \mathbb{N}$. We define the* **sum** *$a + b$ as follows:*

$$a + 0 = a \tag{5.1}$$

$$a + s(b) = s(a + b) \tag{5.2}$$

Computing $b + a$ from a and b is called **adding** *b and a.*

EXAMPLE

Suppose you want to add $6+3$. Here's how the two rules described in the definition are sufficient to do this:

$$\begin{aligned}6 + 3 &= 6 + s(2) && \text{since } s(2) = 3\\ &= s(6 + 2) && \text{by (5.2) with } b = 2\\ &= s(6 + s(1)) && \text{since } s(1) = 2\\ &= s(s(6 + 1)) && \text{by (5.2) with } b = 3\\ &= s(s(6 + s(0))) && \text{since } s(0) = 1\\ &= s(s(s(6 + 0))) && \text{by (5.2) with } b = 0\\ &= s(s(s(6))) && \text{by (5.1) with } a = 6\\ &= s(s(7)) && \text{since } s(6) = 7\\ &= s(8) && \text{since } s(7) = 8\\ &= 9 && \text{since } s(8) = 9\end{aligned}$$

The next lemma explains the connection between the successor function s and addition:

Lemma 5.7 *For any $n \in \mathbb{N}$, $s(n) = n + 1$ (where $1 = s(0)$).*

PROOF This is a simplified version of what we just did in the preceding example:

$$\begin{aligned} s(n) &= s(n+0) && \text{(by (5.1))} \\ &= n + s(0) && \text{(by (5.2))} \\ &= n + 1. \ \square \end{aligned}$$

Ordering the natural numbers

Addition can then be used to define an ordering on $\mathbb{N}$:

Definition 5.8 *We define the relation $\leq$ on $\mathbb{N}$ by*

$$a \leq b \Leftrightarrow \exists\, c \in \mathbb{N} \ s.t. \ a + c = b.$$

This relation leads to one more axiom that the natural numbers should satisfy:

Axiom 5.9 (Peano's fifth axiom (my version)) *The natural numbers are well ordered by $\leq$.*

This axiom is called the **well ordering property of** $\mathbb{N}$ or **WOP** (its not as controversial as the well ordering *axiom*, which has to do with arbitrary sets).

The WOP ensures that every nonempty subset of $\mathbb{N}$ has a least element, and is therefore useful for proving existence results about the natural numbers. Here is an example:

Theorem 5.10 (Euclid's Lemma) *Given any natural number $n \geq 2$, there is a prime number p such that $p \mid n$.*

PROOF Let $E = \{k \in \mathbb{N} : k \geq 1 \text{ and } k \mid n\}$.

Since $n \mid n$, $n \in E$, so E is nonempty.

Therefore, by the WOP, E has a least element, which we call p.

By definition of p, $p \mid n$.

To show p is prime,

Math Joke 7

Theorem: *All natural numbers are interesting.*

PROOF Let I be the set of interesting natural numbers.

Suppose not, this means $I^C \neq \varnothing$.
By the WOP, I^C has a least element, say n.
That means n is the least natural number which is not interesting.
But that makes n interesting!

Contradiction!

Therefore our supposition that $I^C \neq \varnothing$ is false, so $I = \mathbb{N}$.
Thus all natural numbers are interesting. □

Theorem 5.11 (Fundamental Theorem of Arithmetic) *Given any natural number $n \geq 2$, n can be written as a product of prime numbers.*

PROOF Let $E = \{n \in \mathbb{N} : n$ cannot be written as a product of primes$\}$.
Suppose not, i.e. $E \neq \varnothing$. By the WOP, E has a least element, which we call p.

Case 1: p is prime. Then, since $p = p$, p is a product of one prime (itself), so $p \in E^C$. Contradiction!

Case 2: p is composite. Then

WOP PROOF of $\forall n \in \mathbb{N}, P(n)$:

Let $E = \{n \in \mathbb{N} : \sim P(n)\}$ be the truth set of $\sim P(n)$ in $\mathbb{N}$.
Suppose not (i.e. $E = \varnothing$. By the WOP, E has a least element, say x.
....
(some logical argument)
....
Contradiction! Therefore $E = \varnothing$, so $\forall n \in \mathbb{N}, P(n)$. □

5.3 Well-ordering and mathematical induction

The original version of Peano's fifth axiom looks a little different, but it is extraordinarily useful for proving theorems:

Axiom 5.12 (Principle of Mathematical Induction (PMI)) *Suppose $E \subseteq \mathbb{N}$ is a set with two properties:*

1. *$0 \in E$; and*
2. *if $n \in E$, then $n+1 \in E$.*

Then $E = \mathbb{N}$.

Theorem 5.13 *The following are equivalent:*

1. *The Well Ordering Property of $\mathbb{N}$ (Axiom 5.9).*
2. *The Principle of Mathematical Induction (Axiom 5.12).*

Proof $(1 \Rightarrow 2)$ Assume the WOP.

Let $E \subseteq \mathbb{N}$ be a set such that $0 \in E$ and $n \in E \Rightarrow n+1 \in E$.

To verify the PMI we need to show that $E = \mathbb{N}$.

Suppose not; then E^C is nonempty and by the WOP, E^C has a least element p.

Since $0 \in E$ and $p \in E^C$, $p \geq 1$ so $p-1 \in \mathbb{N}$.

Since $p-1 < p$, $p-1 \notin E^C$, i.e. $p-1 \in E$.

But by the second hypothesis about E, this means $(p-1)+1 = p \in E$.

This is a contradiction, so $E = \mathbb{N}$ as wanted.

$(2 \Rightarrow 1)$ Assume the PMI. Let $E \subseteq \mathbb{N}$ be nonempty.

To verify the WOP we need to show E has a least element.

Suppose not, i.e. E has no least element.

We will apply the PMI to E^C.

First, $0 \notin E$ (otherwise 0 would be the least element), so $0 \in E^C$.

Second, suppose $n \in E^C$, i.e. $n \notin E$.

This means $\{0, 1, \ldots, n\} \cap E = \varnothing$ (otherwise, the smallest of these would be the least element in E).

Also, $n+1 \in E^C$ (otherwise, $n+1$ would be the least element of E).

Therefore the PMI applies to E^C, so $E^C = \mathbb{N}$, implying $E = \varnothing$.

This contradicts the assumption that E has no least element. □

Significance: Suppose you want to prove a statement of the form $\forall n \in \mathbb{N}, P(n)$. If you can show

1.

2.

then you have proven the statement. This is called a **proof by induction**.

Theorem 5.14 (Equivalent formulation of PMI)

$$[P(0) \wedge (\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1))] \Rightarrow \forall n \in \mathbb{N}, P(n).$$

To visualize how the logic of the PMI works, consider a row of dominos lined up (the row has a left-most domino, but goes forever to the right). Think of the the n^{th} domino as the open sentence $P(n)$, and envision a domino as being "knocked over" if $P(n)$ is true. In this analogy:

$P(0)$ means

$\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$ means

I hope you agree that if you know these two statements are true, then all the dominoes get knocked over.

Proofs by induction

Given the discussion above, we now have a framework for proving statements which are universally quantified over the natural numbers:

PROOF BY INDUCTION of $\forall n \in \mathbb{N}$, $P(n)$:

We proceed by induction (on n).

Base case: Verify $P(0)$.

Inductive step: Assume $P(k)$.
....
(some logical argument)
....
Therefore, $P(k+1)$.

By induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Remarks:

1. When writing an induction proof, always start by announcing that you are writing an induction proof.
2. Make sure the base case and inductive step are easy to find (and labelled).
3. The thing you assume in the inductive step, i.e. $P(k)$, is called the **inductive hypothesis**, or **IH**. Make sure you always indicate the place(s) in the inductive step where you use the IH.

   If you aren't using the IH in your inductive step, alarm bells should be going off in your head; your proof is either wrong, or not actually a proof by induction.
4. You may need scratch work to figure out how to get from $P(k)$ to $P(k+1)$.

Proposition 5.15 *Let $r \in \mathbb{R}$ such that $r \neq 1$. Then for any $n \in \mathbb{N}$,*

$$\sum_{j=0}^{n} r^j = \frac{1 - r^{n+1}}{1 - r}.$$

PROOF

Proposition 5.16 *For $n \in \mathbb{N}$, define the n^{th}* **triangular number** *to be*

$$t_n = 0 + 1 + 2 + \ldots + n.$$

Then

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

PROOF

This proof illustrates two major drawbacks of induction proofs:

1.

2.

Here's another proof of the same proposition, which explains why we call t_n a *triangular number*:

Proposition 5.17 *For all $n \in \mathbb{N}$, $6 \mid (7^n - 1)$.*

PROOF

Recall: what constitutes a proof depends on the author, and the reader. Here's how this manifests itself in the context of induction proofs:

Claim: For all $n \in \mathbb{N}$, $6 \mid (7^n - 1)$.

OUR PROOF (PREVIOUS PAGE) We proceed by induction on n.

Base case: When $n = 0$, $7^0 - 1 = 1 - 1 = 0$. $6 \mid 0$ as desired.

Inductive step: Let $k \in \mathbb{N}$; assume that $6 \mid (7^k - 1)$. That means there exists $m \in \mathbb{N}$ such that $6m = 7^k - 1$. Now

$$\begin{aligned} 7^{k+1} - 1 = 7 \cdot 7^k - 1 = 7(7^k - 1 + 1) - 1 &= 7[6m + 1] - 1 \\ &= 42m + 7 - 1 \\ &= 42m + 6 \\ &= 6(7m + 1). \end{aligned}$$

Therefore $6 \mid 7^{k+1} - 1$.

By the PMI, $6 \mid (7^n - 1)$ for all $n \in \mathbb{N}$. □

PROOF BY A MORE ADVANCED STUDENT Induction on n:

Base case: $6 \mid (7^0 - 1)$.

Inductive step: Suppose $6 \mid (7^k - 1)$. Then $\exists\, m \in \mathbb{N}$ s.t. $6m = 7^k - 1$. Thus

$$7^{k+1} - 1 = 7(7^k - 1 + 1) - 1 = 7[6m + 1] - 1 = 6(7m + 1)$$

so $6 \mid (7^{k+1} - 1)$. □

PROOF BY A BEGINNING GRADUATE STUDENT Suppose $6 \mid (7^n - 1)$. Then $\exists\, m \in \mathbb{N}$ s.t. $6m = 7^n - 1$. Then we can write $7^{n+1} - 1 = 6(7m + 1)$, so by induction, we are done. □

PROOF BY A MORE ADVANCED GRADUATE STUDENT Induction on n. □

PROOF BY DR. MCCLENDON Duh. □

You can also do induction proofs where the base case isn't $n = 0$, but then you would conclude the result is true only for natural numbers at least as large as the one you used in the base case:

Theorem 5.18 (Generalized PMI) *Suppose $E \subseteq \mathbb{N}$ is such that*

1. *$b \in E$, and*
2. *$k \in E$ implies $k + 1 \in E$.*

Then $E \supseteq \{b, b+1, b+2, \ldots\}$.

PROOF Given E as in the theorem, let $F = E - b = \{x - b : x \in E\} \cap \mathbb{N}$.

Since $b \in E$, $b - b = 0 \in F$.

If $x \in F$, then

$$x + b \in E \Rightarrow x + b + 1 \in E \Rightarrow (x + b + 1) - b = x + 1 \in F.$$

So by the usual PMI, $F = \mathbb{N}$.

Therefore $(E - b) \cap \mathbb{N} = \mathbb{N}$ which means $E \supseteq b + \mathbb{N} = \{b, b+1, b+2, \ldots\}$. □

The generalized PMI is used for proving results that don't start at $n = 0$, but that start at $n = b$.

Proposition 5.19 *For all natural numbers $n \geq 5$, $2^n > n^2$.*

PROOF

Recall this result, which was proven by cases in an earlier in-class activity:

Theorem 5.20 (Triangle inequality for $\mathbb{R}$) *Let $x, y \in \mathbb{R}$. Then $|x+y| \le |x| + |y|$.*

The following proof illustrates how the PMI can be used to extend known results about two objects (i.e. the x and y above) to any finite number of objects. This is a very common use of induction proofs.

Proposition 5.21 (Generalized triangle inequality for $\mathbb{R}$) *Let $x_1, x_2, \dots, x_n \in \mathbb{R}$. Then*

$$\left|\sum_{j=1}^{n} x_j\right| \le \sum_{j=1}^{n} |x_j|.$$

PROOF We proceed by induction on n.

Base case: Let $n = 1$. Then $\left|\sum_{j=1}^{1} x_j\right| = |x_1| = \sum_{j=1}^{1} |x_j|$.

Inductive step: Suppose that for any $x_1, \dots, x_k \in \mathbb{R}$, $\left|\sum_{j=1}^{k} x_j\right| \le \sum_{j=1}^{k} |x_j|$.

Now, let $x_1, \dots, x_{k+1} \in \mathbb{R}$. We have

Remark: One thing this proof does **not** show is

$$\left|\sum_{j=1}^{\infty} x_j\right| \le \sum_{j=1}^{\infty} |x_j|.$$

This is because ∞ is not a natural number. (That inequality is true, however, so long as $\sum x_j$ absolutely converges... you just need a different proof)

Proposition 5.22 *Let $n \in \mathbb{N}$ and suppose E is a set with n elements. Then E has exactly subsets.*

PROOF Induction on n.

Base case: Suppose $n = 0$. Then $E = \varnothing$, and E has only 1 subset (namely, itself).

Inductive step: Suppose the result is true for any set of k elements.

Suppose E is a set with $k + 1$ elements.

Proposition 5.23 *For any natural number $n \geq 1$,*

$$\frac{d}{dx}(x^n) = nx^{n-1}.$$

(You may assume the Product Rule in this proof.)

PROOF Induction on n.

Base case: Let $f(x) = x^1 = x$. Then

$$f'(x) = \lim_{h\to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h\to 0} \frac{(x+h) - x}{h} = \lim_{h\to 0} \frac{h}{h} = \lim_{h\to 0} 1 = 1.$$

Inductive step: Assume $\frac{d}{dx}(x^k) = kx^{k-1}$. Then

$$\begin{aligned}\frac{d}{dx}(x^{k+1}) = \frac{d}{dx}(x^k \cdot x) &= \frac{d}{dx}(x^k) \cdot x + x^k \cdot \frac{d}{dx}(x) \quad \text{(by the Product Rule)}\\ &= kx^{k-1} \cdot x + x^k \cdot 1 \quad \text{(by the IH and base case)}\\ &= kx^k + x^k\\ &= (k+1)x^k.\end{aligned}$$

By induction, we are done. □

The pie fight problem

Suppose n people each have a cream pie. They each throw their pie at the person who is standing closest to them (assume there are no ties among the distances between the people).

Proposition 5.24 *If n is odd, then there is someone who does not get hit by a pie.*

PROOF

5.4 Proofs of basic algebraic results

Alternate title of this section: "Messy induction proofs of obvious facts"

Properties of addition

Earlier, we defined addition by the following two rules:

$$a + 0 = a \tag{5.3}$$

$$a + s(b) = s(a + b) \tag{5.4}$$

Since $s(n) = n+1$, (5.4) can be restated as $a+(b+1) = (a+b)+1$. Using induction, we can give (horrible) proofs three important (and somewhat "obvious") properties of addition:

Theorem 5.25 (Properties of +) *Let $a, b, c \in \mathbb{N}$. Then:*

0 **is an identity element for** $+$**:** $a + 0 = a$ *and* $0 + a = a$.

$+$ **is associative:** $(a + b) + c = a + (b + c)$.

$+$ **is commutative:** $a + b = b + a$.

PROOF The first part of the first statement is (5.3). We prove the second part of the first statement by induction on a.

Base case: $0 + 0 = 0$ by (5.3).

Inductive step: Assume $0 + k = k$. Then

$$\begin{aligned} 0 + (k + 1) &= 0 + s(k) \\ &= s(0 + k) && \text{by (5.4)} \\ &= s(k) && \text{by the IH} \\ &= k + 1. \end{aligned}$$

By induction, the first statement is true.

Now, for the second statement. Let $a, b \in \mathbb{N}$; we proceed by induction on c.

Base case: By the first statement of this theorem,

$$\begin{aligned} (a + b) + 0 &= a + b && \text{by first statement applied to } a + b \\ &= a + (b + 0) && \text{by the first statement applied to } b \end{aligned}$$

Inductive step: Assume $(a + b) + k = a + (b + k)$. Then

$$\begin{aligned}
(a+b)+(k+1) &= (a+b)+s(k) && \\
&= s((a+b)+k) && \text{by (5.4)}\\
&= s(a+(b+k)) && \text{by the IH}\\
&= a+s(b+k) && \text{by (5.4)}\\
&= a+(b+s(k)) && \text{by (5.4) again}\\
&= a+(b+(k+1)).
\end{aligned}$$

By induction, + is associative.

Finally, we prove commutativity.

Claim 1: For all $a \in \mathbb{N}$, $a+1=1+a$.

Proof of Claim 1: Induction on a.

Base case: $0+1=1=1+0$ by the first statement of this theorem.

Inductive step: Assume $k+1=1+k$. Then

$$\begin{aligned}
(k+1)+1 &= k+1+s(0) && \\
&= s((k+1)+0) && \text{by (5.4)}\\
&= s(k+1) && \text{by the first statement of this theorem}\\
&= s(1+k) && \text{by the IH}\\
&= (1+k)+1.
\end{aligned}$$

By induction, Claim 1 is true.

Last, fix $a \in \mathbb{N}$. We prove commutativity by induction on b.

Base case: $a+0=a=0+a$ by the first statement of this theorem.

Inductive step: Assume $a+k=k+a$. Then

$$\begin{aligned}
a+(k+1) &= a+s(k) && \\
&= s(a+k) && \text{by (5.4)}\\
&= s(k+a) && \text{by the IH}\\
&= k+s(a) && \text{by (5.4)}\\
&= k+(a+1) && \\
&= k+(1+a) && \text{by Claim 1}\\
&= (k+1)+a && \text{by associativity.}
\end{aligned}$$

By induction, + is commutative. □

Multiplication

Definition 5.26 *Let $a, b \in \mathbb{N}$. The* **product** *of a and b, denoted ab, $a(b)$, $(a)b$ or $a \cdot b$, is defined by the following rules:*

$$a \cdot 0 = 0 \tag{5.5}$$

$$a \cdot s(b) = a \cdot b + a \tag{5.6}$$

Computing the product of a and b is called **multiplying** *a and b.*

Theorem 5.27 (Properties of multiplication) *Let $a, b, c \in \mathbb{N}$. Then:*

Product with 0 is 0: $0a = 0$ *and* $a0 = 0$.

1 **is an identity element for $\cdot$:** $1a = a$ *and* $a1 = a$.

$\cdot$ **is associative:** $(ab)c = a(bc)$.

$\cdot$ **is commutative:** $ab = ba$.

$\cdot$ **distributes over $+$:** $a(b + c) = ab + ac$.

PROOF These are horrible induction proofs, similar to the proofs of the properties of $+$. I'm not doing them, but may assign one or more of them as HW. □

The division theorem

One of the things you learn as a kid is how to divide one whole number by another, leaving a remainder. The following theorem guarantees that you can always do this and get a standard type of answer:

Theorem 5.28 (Division Theorem) *Let $a, b \in \mathbb{N}$ with $a \neq 0$. There exists $q \in \mathbb{N}$ and $r \in \{0, 1, 2, ..., a - 1\}$ such that*

$$b = aq + r.$$

Furthermore, the choices of a and r are unique.

EXAMPLES

1. Suppose $a = 11$ and $b = 37$.

2. Suppose $a = 12$ and $b = 385$.

PROOF Let $a \in \mathbb{N}$ be an arbitrary nonzero natural number.

To establish the existence of q and r, we proceed by induction on b:

Base case: When $b = 0$, $0 = a0 + 0$.

Therefore we can choose $q = 0$ and $r = 0$ to satisfy the theorem.

Inductive step: Suppose the result is true when $b = k$. That means

$$k = aq + r$$

where $q \in \mathbb{N}$ and $r \in \{0, 1, 2, ..., a - 1\}$. There are two cases:

Case 1: $r = a - 1$. In this case, we have $k = aq + a - 1$. Then

$$k + 1 = [aq + a - 1] + 1 = aq + a = a(q + 1) = a(q + 1) + 0$$

so by choosing "q"= $q + 1$ and $r = 0$, the result is true when $b = k + 1$.

Case 2: $r \in \{0, 1, 2, ..., a - 2\}$.

In this case, we have $k = aq + r$ so $k + 1 = aq + (r + 1)$.

By choosing the same q and "r"= $r + 1$ (which is in the set $\{1, 2, ..., a - 1\}$ since $0 \le r \le a - 2$), the result is true when $b = k + 1$.

So the existence has been proven by induction. Now for the uniqueness; suppose

$$b = aq_1 + r_1 = aq_2 + r_2$$

where $q_1, q_2 \in \mathbb{N}$ and $r_1, r_2 \in \{0, 1, ..., a - 1\}$.

WLOG $r_2 \ge r_1$; therefore $0 \le r_1 \le r_2 \le a - 1$ which means $0 \le r_2 - r_1 \le a - 1 < a$.

At the same time,

$$r_2 - r_1 = aq_1 - aq_2 = a(q_1 - q_2) \text{ so } a \mid (r_2 - r_1)$$

Since a divides a nonnegative number smaller than a, it must be the case that $r_2 - r_1 = 0$, so $r_1 = r_2$. Now we have

$$b = aq_1 + r_1 = aq_2 + r_1$$

so $aq_1 = aq_2$; since $a \ne 0$, we have $q_1 = q_2$. □

Theorem 5.29 (Division Theorem for $\mathbb{Z}$) *Let $a, b \in \mathbb{Z}$ with $a > 0$. There exists $q \in \mathbb{N}$ and $r \in \{0, 1, 2, \dots, a-1\}$ such that*

$$b = aq + r.$$

Furthermore, the choices of a and r are unique.

Proof If $b \geq 0$, this is the previous theorem.

If $b < 0$, apply the previous theorem to $-b$ to get

$$-b = aq + r$$

where $q \in \mathbb{N}$ and $r \in \{0, 1, \dots, a-1\}$. Multiply through by -1 to get

$$b = a(-q) - r.$$

Case 1: $r = 0$. In this case, $b = a(-q) + 0$ so we are done.

Case 2: $r \in \{1, \dots, a-1\}$. In this case,

$$b = a(-q) - r = a(-q) - a + a - r = a(-q-1) + [a - r]$$

so by choosing "q"$= -q - 1$ and "r"$= a - r$ (which is in $\{1, \dots, a-1\}$ since the old r is in $\{1, \dots, a-1\}$), we get the result of the theorem. □

Corollary 5.30 *Let m be a positive integer. Define, as before, the equivalence relation R_m on $\mathbb{Z}$ by $(x, y) \in R_m$ if and only if $m \mid (y - x)$. Then there are exactly m equivalence classes under this relation, and these classes are*

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}.$$

Proof First, we show that every integer belongs to one of these m classes.

By the Division Theorem, any integer x can be written as $x = qm + r$ where $r \in \{0, \dots, m-1\}$.

Thus $qm = x - r$ so $m \mid x - r$ so $x \equiv r \mod m$ (i.e. $[x] = [r]$).

Second, we show that all these equivalence classes are different.

Suppose $[i] = [j]$ where $i, j \in \{0, \dots, m-1\}$.

WLOG $i \geq j$; then $0 \leq j - i \leq m - 1$. Since $[i] = [j]$, $m \mid j - i$ but since $0 \leq j - i < m$, $j - i = 0$, i.e. $i = j$. □

Corollary 5.31 *Every integer is either even or odd, but not both.*

PROOF The even and odd integers are, respectively, the equivalence classes of 0 and 1 under the equivalence relation R_2. □

5.5 Strong induction

Imagine, as before, a row of dominos lined up (the row has a left-most domino, but goes forever to the right), where the the n^{th} domino is the open sentence $P(n)$, and a domino is "knocked over" if $P(n)$ is true.

Suppose you didn't know that each domino could knock over the next one *by itself*. But instead, you knew that if all the dominos to the left of domino $k+1$ fell over, their combined weight would knock over the $(k{+}1)^{st}$ domino. This is also sufficient to knock all the dominos over (if you know the left-most one gets knocked over). Here are some theorems that formalize this idea:

Theorem 5.32 (Strong form of PMI) *Suppose $E \subseteq \mathbb{N}$ is a set with two properties:*

1. *$0 \in E$; and*
2. *if $\{0, 1, ..., n\} \subseteq E$, then $n+1 \in E$.*

Then $E = \mathbb{N}$.

PROOF We prove $E = \mathbb{N}$ by a set equality argument.

($\subseteq$) is given as a hypothesis.

($\supseteq$) Suppose not; then $E^C \neq \varnothing$.

By the WOP, E^C has a least element, say x.

$0 \in E$ by hypothesis (1), so $x \geq 1$.

But then $\{0, ..., x-1\} \subseteq E$, so by hypothesis (2), $x \in E$.

This is a contradiction. □

Theorem 5.33 (Equivalent formulation of the strong form of PMI)

$$\left[P(0) \wedge \left(\forall k \in \mathbb{N}, \bigwedge_{j=0}^{k} P(j) \Rightarrow P(k+1)\right)\right] \Rightarrow \forall n \in \mathbb{N}, P(n).$$

Theorem 5.34 (Generalized strong form of PMI) *Suppose $E \subseteq \mathbb{N}$ is such that:*

1. *$b \in E$; and*
2. *for all $k \geq b$, $\{b, b+1, .., k\} \subseteq E$ implies $k+1 \in E$.*

Then $E \supseteq \{b, b+1, b+2, ...\}$.

PROOF HW

The reason this is called *strong induction* is that the inductive hypothesis that can be made in this type of argument is much stronger than what can be made when using regular induction:

PROOF BY STRONG INDUCTION of $\forall n \in \mathbb{N}$, $P(n)$:

We proceed by induction (on n).

Base case(s): Verify $P(0)$ (sometimes it is necessary to also verify $P(1)$ or $P(2)$ (maybe more), depending on how the inductive step works).

Inductive step: Assume that for all $j \leq k$, $P(j)$.
....
(some logical argument)
....
Therefore, $P(k+1)$.

By strong induction, $P(n)$ is true for all $n \in \mathbb{N}$. □

Definition 5.35 *The n^{th}* **Fibonacci number***, denoted F_n, is obtained by the following procedure: define $F_0 = 0$ and $F_1 = 1$, and for all $n \geq 2$, set*

$$F_n = F_{n-1} + F_{n-2}.$$

Thus $\{F_n\} = \{0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...\}$.

Note: The equation $F_n = F_{n-1} + F_{n-2}$ can be rewritten as:

$F_{n+2} = F_{n+1} + F_n$ (by replacing each n with $n + 2$), or
$F_{n+1} = F_n + F_{n-1}$ (by replacing each n with $n + 1$), etc.

Proposition 5.36 *If F_n is the n^{th} Fibonacci number, then $F_n < 2^n$.*

PROOF

When induction goes horribly wrong

Can you spot what is wrong with the following argument?

Proposition 5.37 *For all natural numbers n, $9^n = 1$.*

ALLEGED PROOF We proceed by induction on n.

Base case: $9^0 = 1$.

Inductive step: Assume that $9^n = 1$ for all $n \leq k$. Now,

$$\begin{aligned} 9^{k+1} = 9^{2k-(k-1)} = 9^{k+k-(k-1)} = \frac{9^k \cdot 9^k}{9^{k-1}} &= \frac{1 \cdot 1}{1} \text{ (by the IH)} \\ &= 1. \end{aligned}$$

By strong induction, $9^n = 1$ for all $n \in \mathbb{N}$. □

Another bad "proof"

Proposition 5.38 *All horses are the same color.*

ALLEGED PROOF We proceed by induction on n, the number of horses.

Base case: $n = 1$. In this case, there is only one horse, so clearly all horses must be colored the same.

Inductive step: Assume that for any set of k horses, all horses are the same color.

Suppose there are $k + 1$ horses, say $\{h_1, \dots, h_{k+1}\}$. Therefore:

$A = \{h_1, \dots, h_k\}$ is a set of k horses, which have the same color by the IH, and

$B = \{h_2, \dots, h_{k+1}\}$ is a set of k horses, which have the same color by the IH.

But since A and B overlap, that means all the horses in $A \cup B = \{h_1, \dots, h_{k+1}\}$ are of the same color.

By induction, all horses are of the same color. □

Proposition 5.39 *Suppose that an ATM machine has an unlimited supply of \$2 and \$5 bills (but no other money). Then, this ATM can distribute any whole number amount of money greater than \$3.*

PROOF

Index