Harvard Math 101

Sets, Groups, and Topology Course Notes

Taught by Brooke Ullery

Notes by Reuben Stern

This version: September 21, 2017

Contents

0.1 Preliminaries . . . 2

1 Thursday, August 31 **3**
1.1 Sets . . . 3
1.2 Subsets . . . 3
1.3 Operations with Sets . . . 4
1.4 Basic Properties of Unions and Intersections . . . 6

2 Tuesday, September 5 **8**
2.1 Mathematical Statements and Basic Logic . . . 8
2.2 De Morgan's Laws . . . 9
2.3 Predicates . . . 11

3 Thursday, September 7 **12**
3.1 Logic, continued . . . 12
3.2 Proof Strategies . . . 13
3.3 Miscellaneous Set Operations (Needed for Homework) . . . 15

4 Tuesday, September 12 **16**
4.1 Proof strategies, continued . . . 16
4.2 More Set Operations . . . 17
4.3 Relations . . . 19

5 Thursday, September 14 **20**
5.1 Relations, continued . . . 20

6 Tuesday, September 19 **23**
6.1 Functions 23

7 Thursday, September 21 **26**
7.1 More about functions 26

A Collected Homework Problems **28**
A.1 Due Tuesday, September 12 28

0.1 Preliminaries

Welcome to Math 101, "Sets, Groups, and Topology"! This course is taught by Brooke Ullery, who can be reached at bullery@math.harvard.edu. We meet Tuesdays and Thursdays from 10–11:30, in Room 310 in the Science Center. The course website may be found at www.math.harvard.edu/bullery/math101. There are two course assistants for Math 101: Katie Fraser and Reuben Stern. Katie can be reached at kfraser@college.harvard.edu; Reuben at reuben_stern@college.harvard.edu. I'll be keeping these notes and other miscellaneous materials up on my website, https://scholar.harvard.edu/rastern/teaching.

The class will cover some subset of the following topics (and more may be added later): *Sets* – proof-writing, basic set theory, relations, functions, the Axiom of Choice, Zorn's Lemma; *Groups* – groups and subgroups, quotient groups, symmetry groups, cyclic groups, homomorphisms, group actions; *Topology* – topological spaces, finite spaces, topology of Euclidean space, closed sets and limit points, continuous functions, metric spaces.

Reuben's Aside 0.1. I will be "live-TEXing" notes for the course. Sometimes, I'll want to put in an aside, which I'll denote by the "Reuben's Aside" environment.

Brooke's office is Science Center 503, and her office hours are Monday and Thursday, 2-3. Problem sets will be due on Tuesdays. Reuben's office hours will be Thursdays from 3-4 pm in the Math department lounge and Saturdays from 1-3 at the Dunster dining hall. Katie's office hours will be Sunday 2-3 in the Adams dining hall and Monday 8-9 at Math Night (Leverett dining hall).

There will be three exams:

1. The first midterm is on **Thursday, October 5**.
2. The second midterm is on **Thursday, October 9**.
3. The take-home final is on **TBD**.

1 Thursday, August 31

Before we get into the nitty-gritty of proof-writing and logic, let's discuss math more broadly.

1.1 Sets

We'll not get into the axiomatic details of set theory, but rather take some properties on faith.

Definition 1.1. A SET is roughly an unordered collection of distinct elements. These can be anything we want: numbers, cats, vegetables, other sets, you name it! The most basic relation one can say about sets is that an element x is IN a set S: we write this as $x \in S$.

A set is determined by the elements that it has: if A and B are sets, then $A = B$ means that A and B have exactly the same elements.

Examples 1.2. The real numbers $\mathbb{R}$ form a set. Elements include π, 2, $\sqrt{51}$. Similarly, the integers $\mathbb{Z}$ are a set $(\ldots, -2, -1, 0, 1, 2, \cdots \in \mathbb{Z})$. For instance, $3 \in \mathbb{Z}$, but $\frac{-1}{2} \notin \mathbb{Z}$[1].

As a somewhat less "mathy" example, the set of U.S. states is the set

$$\text{U.S. States } = \{\text{Alabama, Alaska, } \ldots\}.$$

Note 1.3. The set $\{a, b, c\}$ is the same as the set $\{b, c, a\}$.

Examples 1.4. The rational numbers $\mathbb{Q}$ form a set. We can describe the rational numbers in terms of the integers $\mathbb{Z}$:

$$\mathbb{Q} := \left\{ \frac{a}{b} \in \mathbb{R} : b \neq 0 \text{ and } a, b \in \mathbb{Z} \right\}.$$

This notation is sometimes called "set builder notation"; we are specifying where our elements live on the left of the colon, and what relations they must satisfy on the right.

We can form a set S^1 of points on the unit circle. This can be written using set builder notation as

$$S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

Definition 1.5. The EMPTY SET, written $\varnothing$, is the set with no elements: $\varnothing = \{\}$. For instance, $\varnothing$ is the set of integers that are both odd and even.

Example 1.6. As mentioned, elements of a set can be whatever we want. So we can have a set $A = \{1, 3, \{7, 10\}\}$. There are only 3 elements in this set, $1, 3$, and the *set* $\{7, 10\}$. Note that $7 \notin A$, but $\{7, 10\} \in A$.

1.2 Subsets

Definition 1.7. The most natural relation between sets is to say that a set A is a SUBSET of a set B: this holds when every element of A is a subset of B. We write this $A \subseteq B$ (the notation $A \subset B$ is often reserved to mean "A is a subset of B and also A does not equal B", and is read "A is a *proper* subset of B).

[1] That "$\notin$" symbol means "not in".

Examples 1.8. The integers are a subset of the rationals, which are inside the reals, etc.: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. The set $\{b, a\} \subseteq \{a, b, c\}$. If S is any set, then $\varnothing \subseteq S$.

As a non-example, it is *not* true that $\{7, 10\} \subseteq \{1, 3, \{7, 10\}\}$. However, $\{\{7, 10\}\} \subseteq \{1, 3, \{7, 10\}\}$.

Because the empty set is a subset of every set, we have $\varnothing \subseteq \{\varnothing\}$. Nonetheless, $\varnothing \neq \{\varnothing\}$. This is because the right side has one element, while the left has none.

If S^1 is our set of points on the unit circle, $S^1 \subseteq \mathbb{R}^2$.

Note 1.9. Saying $\{a\} \subseteq A$ is *equivalent* to saying $a \in A$.

1.3 Operations with Sets

We can take multiple sets to create other sets!

Definition 1.10. Let A and B be sets. The UNION of A and B is the set

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

By "or" we mean A or B *or both*. For example, if $A = \{1, 2\}$ and $B = \{2, 3, 4\}$, then $A \cup B = \{1, 2, 3, 4\}$. Note that $A \cup B$ doesn't have multiple "2"s!

The INTERSECTION of A and B is the set

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

Our example with $A = \{1, 2\}$ and $B = \{2, 3, 4\}$ then has intersection $A \cap B = \{2\}$.

One thing we can see right away is that $A \cap B \subseteq A$ and $A \cap B \subseteq B$, while $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

Example 1.11. Let $A = \{a, b, \{c, d\}\}$ and $B = \{c, d\}$. Then $A \cap B = \varnothing$, while $A \cup B = \{a, b, c, d, \{c, d\}\}$. Consider now the intersection $\mathbb{Z} \cap \mathbb{R}_{>0}$, the positive real numbers. This intersection gives us the NATURAL NUMBERS $\mathbb{N} = \{x \in \mathbb{Z} : x \geq 0\}$. A funny example is

$$\{\varnothing\} \cup \varnothing = \{\varnothing\}, \text{ while } \{\varnothing\} \cap \varnothing = \varnothing.$$

Reuben's Aside 1.12. Someone in class mentioned that "union with the empty set" is kind of like adding zero. This can be made formal: the collection of sets with the operation of union $\cup$ forms an algebraic structure known as a COMMUTATIVE MONOID. You don't need to know that, though.

We can extend the notion of taking intersections and unions to arbitrarily many sets!

Definition 1.13 (Unions and intersections of collections of sets)**.** What we've been doing so far is taking a pair of sets, and considering their union and intersection. One thing we can do is consider these two sets as *elements of another set*. Let's generalize this: if $\mathscr{C}$ is a set of sets (a set for which every element is a set), then we define the UNION OF $\mathscr{C}$ as

$$\bigcup_{S \in \mathscr{C}} S = \{x : x \in S \text{ for any } S \in \mathscr{C}\}.$$

Similarly, we can define the INTERSECTION OF $\mathscr{C}$ as

$$\bigcap_{S\in\mathscr{C}} S = \{x : x \in S \text{ for every } S \in \mathscr{C}\}.$$

Examples 1.14. For each natural number $n \in \mathbb{N}$, define a set

$$S_n = \{0, 1, \dots, n\}$$[2]

Then define $\mathscr{C} = \{S_0, S_1, S_2, S_3, \dots\}$. By the "..." we mean that $\mathscr{C} = \{S_n : n \in \mathbb{N}\}$, i.e., that the list continues indefinitely.

We can see

$$\bigcap_{n\in\mathbb{N}} S_n = \{0\},$$

and that

$$\bigcup_{n\in\mathbb{N}} S_n = \mathbb{N}.$$

One thing to note from this example is that $S_i \subseteq S_j$ whenever $i \leq j$; this forms a "chain" of sets. Ignore me though. Also, even though every set in the union is finite, the union overall is infinite! This is cool and important.

Notation 1.15. Sometimes, people will write

$$\bigcap \mathscr{C}$$

to mean

$$\bigcap_{S\in\mathscr{C}} S.$$

Just be aware that this notation exists out in the aether, and do not be surprised if you encounter it.

Example 1.16. What if our collection $\mathscr{C}$ is

$$\mathscr{C} = \{\{\varnothing\}, \{\{\varnothing\}\}, \{\{\{\varnothing\}\}\}, \dots\}?$$

Then

$$\bigcap_{S\in\mathscr{C}} S = \varnothing,$$

because none of the sets share any elements. Similarly,

$$\bigcup_{S\in\mathscr{C}} S = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\{\{\varnothing\}\}\}, \dots\},$$

so we sort of just pulled off a bracket from each of the sets inside $\mathscr{C}$.

Example 1.17. For each prime number $p \in \mathbb{N}$, define

$$A_p = \{x \in \mathbb{N} : p \text{ divides } x\}.$$

[2] Brooke and I have different conventions for whether or not the natural numbers include zero. I want them to.

(We sometimes write $p|x$ for "p divides x".) For example,

$$A_2 = \{2, 4, 6, 8, \dots\}.$$

Now, let $\mathscr{C} = \{A_p : p \text{ is prime}\}$. Then

$$\bigcup_{p \text{ prime}} A_p = \{0, 2, 3, 4, 5, \dots\},$$

because every natural number has a (unique) prime factorization, and we left out 1 from the mix. Conversely,

$$\bigcap_{p \text{ prime}} A_p = \varnothing,$$

because no natural number is divisible by all primes (every natural number has a unique, *finite* prime factorization).

Reuben's Aside 1.18. Someone asked about the infinitude of the primes: there are indeed infinitely many primes. To see this, suppose to the contrary that there were only finitely many primes. Multiply them all together, and add one. This new number is either prime, in which case we are done, or composite. If it is composite, can it be divisible by any of our original primes? Well, no! To see this, consider a small example: is $2 \cdot 3 \cdot 5 + 1$ divisible by 2, 3, or 5? If it were, then 1 would be divisible by all of those, which is absurd.

Question 1.19. With $\mathscr{C}$ being the collection of A_p as before, suppose $\mathscr{C}' \subset \mathscr{C}$ is a finite subset. What is

$$\bigcap_{S \in \mathscr{C}'} S?$$

1.4 Basic Properties of Unions and Intersections

We know, for instance, how the empty set works with unions and intersections: $A \cup \varnothing = A$ and $A \cap \varnothing = \varnothing$. It's also clear that $A \cup B = B \cup A$, and $A \cap B = B \cap A$; that is, union and intersection are COMMUTATIVE operations.

Proposition 1.20. *If A, B, and C are sets, then*

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

and

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

This property is called ASSOCIATIVITY.

Proof. Let's show this for union: the set $A \cup (B \cup C)$ is the set of all elements x that are in A or in $B \cup C$, which is in turn the set of x that are in A or in B or in C. Similarly, the set $(A \cup B) \cup C$ is the set of elements x that are in $A \cup B$ or in C, which in turn is the set of x that are in A or in B or in C. Now it's clear that the two sets are equal. □

Now if $A \subseteq B$, then $A \cup B = B$ and $A \cap B = A$. We can also ask how union and intersection interact!

Proposition 1.21. *If A, B, and C are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. On the other hand, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. In this sense, union and intersection* distribute *over each other.*

Proof. Proof of $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$: we need to show that both sets contain exactly the same elements. That is to say, both sets are *subsets* of each other. Let's start by showing that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$: if $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$. Furthermore, if $x \in B \cup C$, then $x \in B$ or $x \in C$. Thus we have two possibilities: either $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$. These translate back into set notation to say $x \in (A \cap B)$ or $x \in (A \cap C)$, so $x \in (A \cap B) \cup (A \cap C)$!

Now, we want to show that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. If $x \in (A \cap B) \cup (A \cap C)$, then $x \in A \cap B$ or $x \in A \cap C$. These two conditions mean that either x is in A and B, or x is in A and C. Thus we know for sure that $x \in A$, and either $x \in B$ or $x \in C$. Translate back into set notation to see $x \in A \cap (B \cup C)$. We're done!

Proof of $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$: Try proving this one yourself! You may want to use set builder notation to help. Pictures can be helpful to gain intuition, but don't provide a solid proof. □

Note 1.22. More about proofs and proof strategies will be covered next week.

2 Tuesday, September 5

Day 2. There still are not enough seats for everyone in the class. Perhaps the powers that be want for us to get closer to each other...

Note 2.1. My (Reuben's) office hours will be Thursdays 4-5 in the 4th floor math lounge and Saturdays 2-4 in the Dunster d-hall. If you can't make either of these, let me know! My schedule is pretty full, but I can try to make time.

The first homework will be posted today. That is due in a week: Tuesday 9/12.

2.1 Mathematical Statements and Basic Logic

Definition 2.2. A STATEMENT is a sentence that is either true or false (but not both). That is, the sentence has a TRUTH VALUE.

Example 2.3. *"Today is September 5, 2017"* is a TRUE statement. The mathematical statement

$$\pi = \frac{22}{7}$$

is a FALSE statement. *"The sum of two odd integers is odd"* is a FALSE statement.

It is a perfectly reasonable thing to do to replace a statement with a letter, say P. For instance, we could have P represent the statement "the product of any two odd integers is odd". Then we say P has a truth value of TRUE. Don't get too afraid of all the variables!

Definition 2.4. Given a statement P, the NEGATION of P is the statement that is true whenever P is false, and false whenever P is true. We write this $\neg P$, and read it as "not P".

Examples 2.5. The negation of "today is September 5, 2017" is "today is *not* September 5, 2017". If P is the statement "7 is odd", then $\neg P$ is the statement "7 is even"

Reuben's Aside 2.6. That last example is a little bit hairy, because we really mean "7 is an odd integer", and then the negation would technically be "7 is not an odd integer". So for instance, 7 could be a basketball, or a quiche.

Examples 2.7. What if P is the statement "all integers are prime"? Then $\neg P$ is either "not all integers are prime" or, equivalently, "there is some integer that is not prime". Thus to prove $\neg P$, all we have to do is find *one example* of an integer that is not prime.

Now let P be "some dogs are brown". Then $\neg P$ would be "no dogs are brown". It is *not* the statement "some dogs are not brown".

Definition 2.8. A TRUTH TABLE shows the possible truth values of a logical operation (based on the possible truth values of its constituent parts). For instance, here is the truth table for the $\neg P$ construction:

P	$\neg P$
T	F
F	T

Definition 2.9. Given two statements P and Q, we say that P and Q are EQUIVALENT if they never have different truth values. For instance, for any $x \in \mathbb{R}$, the statements "$x^2 > 0$" and $x \neq 0$ are equivalent. Similarly, "not all dogs are brown" is equivalent to "there exists a dog that is not brown".

If P is equivalent to Q, we write $P \Leftrightarrow Q$; this is read as "P if and only if Q", which is sometimes abbreviated as "P iff Q". Mathematicians are lazy.

Here is the following truth table for equivalence:

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Definition 2.10. Given two statements P and Q, the statement $P \wedge Q$ (read "P and Q) is true precisely when both P and Q are true, and false otherwise. The truth table for the LOGICAL AND operator is

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

The LOGICAL OR operation, forming $P \vee Q$, is true if P is true, Q is true, *or both*. That is to say, it is an *inclusive or*. Here is the truth table for "or":

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Note 2.11. If P is a statement, $P \vee (\neg P)$ is always true. Similarly, $P \wedge (\neg P)$ is always false.

2.2 De Morgan's Laws

How does negation play across the "and" and "or" operators? To get a feel for this, let's look at an English language example:

Example 2.12. Let P be the statement "I bought carrots" and Q be "I bought lettuce. Then "I bought carrots and lettuce" is the statement $P \wedge Q$. To negate this in English, you'd say something like "Either I didn't buy carrots or I didn't buy lettuce". This suggests that $\neg(P \wedge Q)$ is the same thing as the statement $(\neg P) \vee (\neg Q)$.

Proposition 2.13 (De Morgan #1)**.** *There is an equivalence of statements* $\neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$.

Proof. We can see this with a truth table:

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

You can (and should!) try to work this out "in English", to get a better feel for how the logic works. □

We can do a similar thing for the "or" construction: what is $\neg(P \vee Q)$? For instance, "you can't rent this apartment if you have a cat or a dog". Let P be "you can rent this apartment", Q be "you have a cat", and R be "you have a dog". Then the statement is "if $Q \vee R$, then $\neg P$. Then $\neg(Q \vee R)$ means "you have neither a cat nor a dog", i.e., $(\neg Q) \wedge (\neg R)$. Note that even in English, negating $Q \vee R$ needs a double negative ("neither–nor"). This is the second De Morgan Law:

Proposition 2.14 (De Morgan #2)**.** *There is an equivalence of statements*

$$\neg(Q \vee R) \iff (\neg Q) \wedge (\neg R).$$

Proof. On your homework. □

Now, the previous paragraph had a sort of "if–then" statement in it; how can we formalize that logically? Given two statements P and Q, we can form the IMPLICATION $P \Rightarrow Q$ (read this as "if P, then Q" or "P implies Q"). To understand the possible truth values of this implication, let's consider an example:

Example 2.15. Consider the statement "if it is raining tomorrow, then I won't ride my bike". If P is "it's raining tomorrow" and Q is "I won't ride my bike", then the original statement is $P \Rightarrow Q$. Note that even if P is false, Q could logically be true: if it isn't raining, I still might not ride my bike. We thus have the following truth table:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

You can remember this by thinking "false implies anything".

Reuben's Aside 2.16. There's a rule of logic known as *modus ponens*, "the method of crossing the bridge". It says if P is true, and if $P \Rightarrow Q$ is true, then Q is true. Try working this out with a truth table! Hint: the statement you want to show is $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$.

Certain weird examples of implications come up in math: if you start with a false mathematical statement, you can conclude anything. For instance, if $0 = 1$, then $7 > 9$ is a *true statement*. This suggests a possible proof strategy: if you start with a statement that you don't know the truth value of, and manage to conclude something that you know to be false, then the original statement must have been false to begin with.

Example 2.17. Let's negate an implication: what is $\neg(P \Rightarrow Q)$? We'll check with a truth table that it is $P \wedge (\neg Q)$:

P	Q	$\neg(P \Rightarrow Q)$	$P \wedge (\neg Q)$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	F	F

Note 2.18. An equivalence of statements $P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. That is to say, if both statements imply each other, then they are equivalent. Use a truth table to see why this is true.

2.3 Predicates

Often in math, we are interested in statements that are true or false depending on some input, or variable. This leads us to talking about PREDICATES. For instance, "$x^2 < 2$" doesn't have a truth value until we know what x is. That is to say, the predicate $P(x) = (x^2 < 2)$ evaluates to "true" or "false" depending on the input x. Note that $P(x)$ is a predicate, while $P(0)$ is a statement.

The negation of $P(x)$ will be $\neg(P(x)) = (x^2 \geq 2)$, *another predicate*. Next time, we will talk about how to take predicates and turn them into statements using *quantifiers*, such as "for all" and "there exists".

3 Thursday, September 7

Day 3: The class is still full. Someone suggests to make the problem sets harder. Brooke laughs, cool and remote, as if a mountain were to laugh.

3.1 Logic, continued

Recall that a *predicate* is like a statement, but it doesn't have a truth value until an input is given. One way to build statements out of predicates is using *quantifiers*:

Definition 3.1. A QUANTIFIER is a symbol meaning "for all" (written $\forall$) or "there exists" (written $\exists$). For example, "there exists $x \in \mathbb{Z}$ such that $x^2 < 2$". In this statement, $x^2 < 2$ is a predicate, but adding "there exists $x \in \mathbb{Z}$ such that" makes it a statement with truth value true. In shorthand, we can write this as

$$\exists\, x \in \mathbb{Z}(x^2 < 2).$$

We can negate this as a statement: the negation would be something like "for all $x \in \mathbb{Z}$, $x^2 \geq 2$". Thus, we can remember this negation as "$\neg\exists = \forall\neg$".

Example 3.2. "Every rational number is a real number" is a statement with quantifier; this can be rewritten as

$$\forall\, x \in \mathbb{Q}(x \in \mathbb{R}).$$

Note that "$x \in \mathbb{R}$" is a *predicate* without a truth value, that *becomes* a statement when we've added a quantifier. The negation of this is "there exists $x \in \mathbb{Q}$ such that $x \notin \mathbb{R}$", or

$$\exists\, x \in \mathbb{Q}(x \notin \mathbb{R}).$$

We can remember this by "$\neg\forall = \exists\neg$".

"Every real number has a real number smaller than it" can be written as

$$\forall\, x \in \mathbb{R}, \exists\, y \in \mathbb{R}(y < x).$$

The negation of this statement would be

$$\exists\, x \in \mathbb{R}(\forall\, y \in \mathbb{R}(y \geq x)).$$

Note 3.3. You may see that negation changes $\forall$ to $\exists$ and vice versa; this is a general trend: if $P(x)$ is a predicate, then there are equivalences of statements

$$\exists\, x(P(x)) \Leftrightarrow \neg\forall\, x(\neg P(x))$$

and

$$\forall\, x(P(x)) \Leftrightarrow \neg\exists\, x(\neg P(x)).$$

3.2 Proof Strategies

Goal 3.4. The goal when writing a proof is to prove that a statement is true (or maybe false). A proof should have/be:

- A beginning: introduce your list of assumptions, what you are trying to prove, and potentially how you will go about proving something (the proof strategy).
- Clear, logical arguments and deductions.
- Grammatically correct English or mathematical sentences.
- Precise: leave no room for doubt. A proof is trying to convince the reader without any shadow of a doubt that something is true.
- A conclusion: ultimately, state what you've just proved.
- Readable, even if the reader doesn't know what you were trying to show. That is, there should be enough details for the careful reader to intuit what's going on from context.

Warning 3.5. A proof should *not* have/be:

- Long-winded (you don't need to state *every* single detail)[3].
- A "proof by example": just giving one or more examples does not constitute a proof that something holds. For instance, you can't prove that the sum of two odd numbers is even by showing, e.g., $3 + 5 = 8$. Of course, you can prove existence statements by exhibiting examples! Just not "for all" statements.
- Variables you haven't defined. For instance, you could say "let A and B be finite sets..." or "let $x \in \mathbb{R}$..."
- Start with what you are trying to prove. This seems silly, but don't do it! Avoid circular arguments at all costs.
- (more generally) Incorrect logic. Be careful, for instance, negating incorrectly, or proving $Q \Rightarrow P$ instead of $P \Rightarrow Q$, etc.

Note 3.6. Proofs are meant to be read! When you are writing a proof, focus on making them as readable as possible. Whenever possible, write things out in English rather than symbols.

Now that you may or may not have an idea for what proofs should be, let's talk about general *types* or proofs (i.e., plans of attack to have in your arsenal).

Definition 3.7. A DIRECT PROOF is the most basic type of proof. Let's discuss this by means of an example: suppose we want to show $P \Rightarrow Q$. The shape of a direct proof may go along the lines of: assume P. Then $P \Rightarrow P_1$, $P_1 \Rightarrow P_2$, $P_2 \Rightarrow Q$. Therefore Q.

Example 3.8. Show that if $A \subseteq B$, then $A \cap B = A$.

[3] This takes practice! You'll eventually have to use your judgment.

Proof. Let A and B be sets such that $A \subseteq B$. We know by definition that $A \cap B \subseteq A$. In the other direction, let $x \in A$. Since $A \subseteq B$, we also know that $x \in B$. As x is in both A and B, $x \in A \cap B$. Thus $A \cap B \supseteq A$, from which we can conclude that $A \cap B = A$. □

Aside 3.9. That little "□" symbol at the end of a proof is called a "tombstone". It stands in for the Latin phrase *quod erat demonstrandum*, "that which was to be demonstrated", often abbreviated "Q.E.D.". (In French proofs, people sometimes write "cqfd", standing for "*ce qu'il fallait démontrer*").

Definition 3.10. The next proof strategy is proof of the CONTRAPOSITIVE: the contrapositive of an implication $P \Rightarrow Q$ is the statement "$\neg Q \Rightarrow \neg P$". We can see by a truth table that these two statements are equivalent:

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Reuben's Aside 3.11. Note that neither an implication nor its contrapositive is equivalent to $\neg P \Rightarrow \neg Q$! This is a pitfall to avoid at all costs.

Example 3.12. Show by contrapositive that if $A \subseteq B$, then $A \cap B = A$.

Proof. Let A and B be sets, and suppose to the contrary that $A \cap B \neq A$. Since $A \cap B \subseteq A$, there must be some $x \in A$ that is not also in $A \cap B$. By definition, this means that $x \notin B$ (because $x \in A$ by assumption), so it follows that $A \not\subseteq B$. Therefore, if $A \subseteq B$, then $A \cap B = A$. □

Definition 3.13. The next strategy is PROOF BY CONTRADICTION: the idea is that you assume that what you're trying to prove is *false*, and then derive a known contradiction (*reductio ad absurdum*). You then know that the assumption you started with was false, so what you were trying to prove true all along *is* actually true.

Reuben's Aside 3.14. Note the difference between this and proving the contrapositive: proof by contrapositive is a strategy for proving an implication $P \Rightarrow Q$. Proof by contradiction is a strategy for proving any statement P, by assuming $\neg P$. (recall that the contrapositive is not the negation of an implication; it is equivalent!)

Example 3.15. Show that there are infinitely many prime numbers.

Proof. Suppose to the contrary that there were only finitely many primes, say $\{p_1, \ldots, p_n\}$. Consider the integer $q = p_1 \cdot p_2 \cdots p_n + 1$: is q prime? We know that $q > p_i$ for all $i \in \{1, \ldots, n\}$, so in particular $q \neq p_i$ for any i. Thus q is not prime itself, and it is also divisible by p_j for some j. We know that $p_1 \cdots p_n$ is divisible by p_j, but 1 is not. Thus q is not divisible by p_j; a contradiction. □

Now we want to say a few words about induction, but won't get too much into the details. Induction is one of the most important and powerful proof strategies out there, but also one of the most confusing to first-time proof-writers.

Definition 3.16. A proof by INDUCTION can help you prove that a statement P_i is true for all $i \in \mathbb{N}$. We do this as follows: prove that P_1 is true; this is known as the "base case". Then prove that for all i, $P_i \Rightarrow P_{i+1}$. Note the recursive nature of this proof strategy: it's like recursion in programming, but in reverse!

3.3 Miscellaneous Set Operations (Needed for Homework)

Definition 3.17. If A and B are sets, then the DIFFERENCE between A and B (written $A \setminus B$ or $A - B$) is the set

$$A - B := \{x \in A : x \notin B\}.$$

Definition 3.18. Fix a set B, and let $A \subseteq B$ be a subset[4]. The COMPLEMENT of A (in B) is the set A' or A^c or $\overline{A}$ defined by

$$A' := \{x \in B : x \notin A\} = B - A.$$

[4]Sometimes, we don't make explicit what the ambient set is. This can be confusing, but it is the unfortunate truth about lazy mathematicians. I am one of these, unfortunately.

4 Tuesday, September 12

Stand straight with feet about one meter apart, hands on hips. Bend at the waist, knees straight, and touch left foot with right hand. Straighten. Bend again and touch right foot with left hand. Straighten. Repeat 15 times.

Exercise VIII.8.3 of Sarason's *Notes on Complex Function Theory*

Note 4.1. The next homework will be posted later today (before 3 pm).

4.1 Proof strategies, continued

What kinds of statements do we prove in mathematics? How might we approach these kinds of statements?

Examples 4.2. Perhaps we want to prove $x = y$, where x and y are some sort of mathematical structure. The proof of this statement depends on what x and y are: if x and y are real numbers (i.e., valued in $\mathbb{R}$), we might show $x \leq y$ and $y \leq x$. If x and y are sets, we might show $x \subseteq y$ and $y \subseteq x$. Perhaps we might show $x = y_1$, $y_1 = y_2$, and so on, until $y_n = y$.

Commonly, we'll want to show $P \implies Q$ for some statements P and Q. Also commonly, we'll want to show $P \iff Q$. To prove this, you can show $P \implies Q$ and $Q \implies P$; alternatively, you could prove $P \implies Q$ and $\neg P \implies \neg Q$. Sometimes, and you have to be careful about this, you can show

$$P \iff Q_1 \iff Q_2 \iff \cdots \iff Q.$$

You may also want to show $\forall\, x\, (P(x))$. To do this, you will have to work with arbitrary x; we then show that $P(x)$ holds.

Example 4.3. Show that any rational number can be expressed as $\frac{m}{n}$, where m and n are not both even.

Proof. Let $x \in \mathbb{Q}$, and suppose x can be represented as $\frac{p}{q}$. If p or q are not even, then we are done. If on the other hand p and q are both even, then write $p = 2^a \cdot p'$ and $q = 2^b \cdot q'$, where p' and q' are products of odd primes. Suppose without loss of generality that $a \geq c$; it is then clear that $x = \frac{2^{a-c}p'}{q'}$, and q' is not even. □

Note that existence statements can be shown by example; however, this isn't the *only* way to prove existence statements!

Example 4.4. One can also have statements such as $\forall\, x\, \exists\, y\, (P(x, y))$. For instance, show that for all $x \in \mathbb{Q}$ such that $x > 0$, there exists $y \in \mathbb{Q}$ such that $0 < y < x$.

Proof. Let $x \in \mathbb{Q}$ be greater than zero. Then $x/2$ is also in $\mathbb{Q}$, and $0 < x/2 < x$.[5] □

[5] Depending on context, you may need more details.

Another super common statement to prove is of the form "suppose A, B, and C. Show D." The shape of a proof could go something like this: $A \implies D_1 \implies D_2$, $(B \wedge C) \implies D_3$, and $(D_2 \wedge D_3) \implies D$. You'll very likely need to use all the assumptions.

Aside 4.5 (Getting started on a proof)**.** If you don't know where to start, on scratch paper:

- Write out all the assumptions and definitions you might need to use.
- Break down the statement you're trying to prove into a more basic form (something like "$P \implies (Q \wedge S)$" or "$\forall\, x \in \mathbb{Q}(P(x))$").
- Write out desired conclusion.
- Work at it from both ends, if need be: what can you conclude from the assumptions? What *must* you need to show in order to conclude the result? What might imply it nicely?
- Sketch an outline of the proof, before writing your final version.

4.2 More Set Operations

We talked last time about set complements and set differences (A^c and $A - B$).

Proposition 4.6. *Let A be a set (perhaps sitting inside some ambient set B).*

1. $(A^c)^c = A$.
2. $\varnothing^c = B$.
3. $A \cap A^c = \varnothing$. *We say that A and A^c are* DISJOINT SUBSETS.
4. $A \cup A^c = B$.
5. $A \subset C$ *if and only if* $C^c \subseteq A^c$.
6. *De Morgan's Laws:* $(A \cup C)^c = A^c \cap C^c$ *and* $(A \cap C)^c = A^c \cup C^c$.

Definition 4.7. Let A and B be sets. The SYMMETRIC DIFFERENCE of A and B, written $A + B$, is the set

$$A + B := (A - B) \cup (B - A) = \{x \in A \cup B : x \notin A \cap B\}.$$

Definition 4.8. Let A be a set. The POWER SET of A is the set $\mathscr{P}(A)$ of all subsets of A:

$$\mathscr{P}(A) := \{B : B \subseteq A\}.$$

Examples 4.9.

- $\mathscr{P}(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$.
- $\mathscr{P}(\varnothing) = \{\varnothing\} \neq \varnothing$. $\mathscr{P}(\mathscr{P}(\varnothing)) = \{\varnothing, \{\varnothing\}\}$.

Reuben's Aside 4.10. When set theorists are formalizing the natural numbers $\mathbb{N}$ in set theory, they define 0 to be the empty set. Then $1 := \mathscr{P}(\varnothing)$, $2 := \mathscr{P}(1)$, and so on: $n := \mathscr{P}(n-1)$.

In general, if X is a finite set with n elements, then $\mathscr{P}(X)$ has 2^n elements. How do we see this? If $X = \{a_1, \ldots, a_n\}$, then a subset is just saying if each element a_i is in the subset or not: this is two choices for each element of the set, giving 2^n.[6] We can thus imagine that a subset $A \subset X$ gives us a function from X into the set $\{0, 1\}$, where $x \in X$ evaluates to 1 if $x \in A$, and 0 otherwise.

What happens to the power set of an infinite set? In a sense that will be made precise later, if X is any (possibly infinite) set, then $\mathscr{P}(X)$ is "bigger" than X. You may have heard the terms "countably infinite" and "uncountably infinite": these correspond to the size of $\mathbb{Z}$ and the size of $\mathscr{P}(\mathbb{Z})$ (which is the same size as $\mathbb{R}$).[7]

Proposition 4.11. *If E and F are sets, then*

1. $\mathscr{P}(E) \cap \mathscr{P}(F) = \mathscr{P}(E \cap F)$.
2. $\mathscr{P}(E) \cup \mathscr{P}(F) \subseteq \mathscr{P}(E \cup F)$ *(in general, equality will not hold here).*

Proof. 1. We'll show this by two mutual inclusions. First, let $A \in \mathscr{P}(E) \cap \mathscr{P}(F)$. Then $A \subseteq E$ and $A \subseteq F$, so $A \subseteq E \cap F$. Thus $A \in \mathscr{P}(E \cap F)$, so $\mathscr{P}(E) \cap \mathscr{P}(F) \subseteq \mathscr{P}(E \cap F)$. In the other direction, let $B \in \mathscr{P}(E \cap F)$. Then $B \subseteq E \cap F$, so in particular, $B \subseteq E$ and $B \subseteq F$. It follows by definition that $B \in \mathscr{P}(E)$ and $B \in \mathscr{P}(F)$, so $B \in \mathscr{P}(E) \cap \mathscr{P}(F)$. Thus $\mathscr{P}(E \cap F) \subseteq \mathscr{P}(E) \cap \mathscr{P}(F)$, and we are done[8].

2. See homework for a generalization.

□

Fact 4.12. More facts about power sets!

- If $E \subseteq F$, then $\mathscr{P}(E) \subseteq \mathscr{P}(F)$.
- $\displaystyle\bigcap_{X \in \mathscr{P}(E)} X = \varnothing$.
- $\displaystyle\bigcup_{X \in \mathscr{P}(E)} X = E$.

Definition 4.13. Let A and B be sets. Then the CARTESIAN PRODUCT of A and B, written $A \times B$, is the set of *ordered pairs* of elements in A and B:

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

Examples 4.14. 1. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the "xy-plane".

2. $\{x, y\} \times \{x, z\} = \{(x, x), (x, z), (y, x), (y, z)\}$.

[6] For this reason, esoteric set theorists sometimes write $\mathscr{P}(X)$ by 2^X, denoting "functions from the set X into the set 2".

[7] I've been a little imprecise with my wording here: "uncountably infinite" refers to any size larger than "countably infinite"; in particular, there are infinitely many sizes of uncountable infinity!

[8] It is possible here to forgo the "two mutual inclusions" reasoning, and just do things via "if and only if" statements. A proof could go something like "$A \in \mathscr{P}(E) \cap \mathscr{P}(F)$ if and only if $A \subseteq E$ and $A \subseteq F$. This holds if and only if $A \subseteq E \cap F$, which holds if and only if $A \in \mathscr{P}(E \cap F)$. It is nonetheless clearer to go both ways, and usually it is not this easy.

3. If A is any set, $A \times \varnothing = \varnothing$.

Reuben's Aside 4.15. The cartesian product satisfies a ton of nice properties! In high-falutin' language, the category of sets Set with cartesian product and the empty set $\varnothing$ is *closed symmetric monoidal*. Sigh, I'm a hopeless category theorist.

Reuben's Aside 4.16. Please ignore the previous aside.

4.3 Relations

Let's get a sense of relations by a few examples.

Examples 4.17.

- "Being a sibling of" is a relation.
- "$<$" is a relation between real numbers: for any two $x, y \in \mathbb{R}$, either $x < y$ or $x \not< y$. In particular, we can tell if an ordered pair of numbers satisfies this relation.
- "Having a higher frequency" is a relation between pitches.

The idea here is that we're taking an *ordered pair*, and asking whether that pair satisfies our relation. Precisely, we have the following definition:

Definition 4.18. Let X be a set. A RELATION R on X is a subset of the cartesian product $R \subseteq X \times X$. If the ordered pair (x, y) is in the subset R, then we write $x\,R\,y$, meaning "x is related to y".

Examples 4.19. Let $P = \{\text{people in the world}\}$. Define the following relations:

$$D = \{(x, y) \in P^2 : x \text{ is a descendant of } y\}$$
$$B = \{(x, y) \in P^2 : x \text{ and } y \text{ have a common ancestor}\}$$
$$S = \{(x, y) \in P^2 : x \text{ and } y \text{ have the same parents}\}$$

One property that B has that D doesn't have is that if $(x, y) \in B$, then $(y, x) \in B$: if x and y have a common ancestor, then y and x have a common ancestor. On the other hand, if x is a descendant of y, then it is (hopefully) not the case that y is a descendant of x. This says that B is a SYMMETRIC relation.

We can think of the "less than" relation as a subset of $\mathbb{R}^2$: $(2, 3) \in <$ if $2 < 3$.

Definition 4.20. Let A be a set. An EQUIVALENCE RELATION on A is a relation $R \subseteq A \times A$ satisfying the following properties:

1. (Reflexivity) If $x \in A$, then $x\,R\,x$.
2. (Symmetry) If $x\,R\,y$, then $y\,R\,x$.
3. (Transitivity) If $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$.

5 Thursday, September 14

5.1 Relations, continued

> *[T]he cohomology of proofs is an amazing device for detecting holes in your proofs. And it will detect a hole of any dimension!*
>
> Adams and Krantz, *The Cohomology of Proofs*

Let's recall the definition of a relation from last time:

Definition 5.1. Let A be a set. A RELATION *on* A is a subset $R \subseteq A \times A$. A relation *between* sets A and B is a subset $S \subseteq A \times B$.

Definition 5.2. We say that a relation C on A is an EQUIVALENCE RELATION if

1. (Reflexivity) $x \, C \, x$ for all $x \in A$.
2. (Symmetry) If $x \, C \, y$, then $y \, C \, x$.
3. (Transitivity) if $x \, C \, y$ and $y \, C \, z$, then $x \, C \, z$.

We will frequently use a tilde "$\sim$" to denote an equivalence relation.

Definition 5.3. Let $\sim$ be an equivalence relation on a set A. The EQUIVALENCE CLASS associated to an element $x \in A$ is the set

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

Example 5.4. One of the most basic equivalence relations is equality: say that $x \sim y$ if and only if $x = y$. In this case, $[x]$ is just the one-element set $\{x\}$.

Note that a relation doesn't have to be given by a fun rule; it can just be any subset of $A \times A$. Thus:

Example 5.5. The set $A \times A$ itself is an equivalence relation on A. It is given by the rule $x \sim y$ for all $x, y \in A$.

What are the equivalence classes for this relation? Well, if $x \in A$, then $y \sim x$ for all $y \in A$, so $[x] = A$.

Reuben's Aside 5.6. There's been a little bit of confusion around equivalence relations, in particular with the last example. This one is *a specific example*, rather than something that holds for all equivalence relations. In some sense, there's a scale of equivalence relations, where "equality" is the finest and "everything is equivalent" is the coarsest. Let the relation "=" be represented by the set $E \subseteq A \times A$, and the everything is equivalent relation be represented by $A \times A$ itself. Then trivially

$$E \subseteq A \times A.$$

It turns out that for *any* equivalence relation $\sim$, defined by a subset $F \subseteq A \times A$, then

$$E \subseteq F \subseteq A \times A.$$

Notation 5.7. Sometimes, when we are considering multiple equivalence relations on a set A (say $\sim$ and $\simeq$), we'll denote equivalence classes by brackets with a subscript of the equivalence relation: e.g., $[x]_\sim$ and $[x]_\simeq$.

Proposition 5.8. *Let $\sim$ be an equivalence relation on some set A. Two equivalence classes E and F are either disjoint ($E \cap F = \varnothing$) or equal.*

Proof. Let's recall that equivalence classes are subsets of A. Suppose E is determined by x, that is, $E = [x]$, and F is determined by y. Assume that E and F are not disjoint. Then there is some $a \in E \cap F$ that is equivalent both to x and to y. That is to say, $x \sim a$ and $y \sim a$. By symmetry, we know that $a \sim y$. By transitivity, it follows that $x \sim y$. Thus $y \in [x]$, and by transitivity again (with possible applications of symmetry here and there), any $b \in [y]$ is also equivalent to x, and thus in $[x]$. It follows that $F \subseteq E$; we can use the same argument focused on F to show that $E \subseteq F$, and thus $E = F$. □

Why is this a valid proof? That is, how does the logic work? We've started trying to prove $P \vee Q$ for some statements P and Q. By a truth table, we can check that $(\neg P) \Rightarrow Q$ is an equivalent statement to $P \vee Q$:

P	Q	$P \vee Q$	$(\neg P) \Rightarrow Q$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

Definition 5.9. If $\sim$ is an equivalence relation on A, let $A/\sim$ denote the set of equivalence classes of A with respect to $\sim$. We read this as "A mod $\sim$".

Let $\mathscr{E} = A/\sim$. Then the distinct elements of $\mathscr{E}$ are disjoint subsets of A, and we know that

$$\bigcup_{S \in \mathscr{E}} S = A.$$

This is because every element $x \in A$ is contained in the equivalence class $[x]_\sim$.

Definition 5.10. Let A be a set. If $\mathscr{E}$ is a set of pairwise-disjoint[9], nonempty subsets of A such that

$$\bigcup_{S \in \mathscr{E}} S = A,$$

then we say that $\mathscr{E}$ is a PARTITION of A.

It turns out that there's an intimate relation between partitions and equivalence relations:

Proposition 5.11. *Let $\mathscr{C}$ be a partition of A. Then there is a unique equivalence relation $\sim_{\mathscr{C}}$ on A such that $A/\sim_{\mathscr{C}} = \mathscr{C}$.*

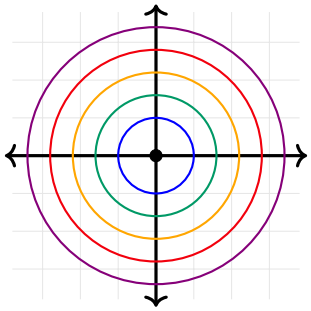
Proof. We can define the relation $\sim_{\mathscr{C}}$ by saying that $x \sim y$ if and only if both x and y are in X for some $X \in \mathscr{C}$. Let's check that this is an equivalence relation: $x \sim_{\mathscr{C}} x$ trivially, since if $x \in X \in \mathscr{C}$ then $x \in X \in \mathscr{C}$. If $x \sim_{\mathscr{C}} y$, then both x and $y \in X$ for some $X \in \mathscr{C}$, so clearly y and x are in X,

[9] By "pairwise-disjoint" I mean that for any $S, T \in \mathscr{E}$, we have $S \cap T = \varnothing$.

and thus $y \sim_{\mathscr{C}} x$. Finally, if x and y are contained in the same set $X \in \mathscr{C}$ and y and z are also contained in the same set $Y \in \mathscr{C}$, pairwise-disjointness of $\mathscr{C}$ implies that $X = Y$, so $x \sim_{\mathscr{C}} z$.

Now we show uniqueness: suppose that both $\sim_{\mathscr{C}}$ and $\sim'$ are equivalence relations on A such that $A/\sim_{\mathscr{C}} = A/\sim' = \mathscr{C}$. If $x \sim_{\mathscr{C}} y$, then there is a set $X \in \mathscr{C}$ such that $x, y \in X$. Because $A/\sim' = \mathscr{C}$, then x and y are in the same equivalence class with respect to $\sim'$, so $x \sim' y$. Working backwards, we can see that $x \sim' y$ implies $x \sim_{\mathscr{C}} y$, so the two equivalence relations are the same. □

Example 5.12. Define $P, Q \in \mathbb{R}^2$ to be equivalent if they are the same distance from the origin. The set $\mathbb{R}^2/\sim$ is the set of circles centered at the origin and the point at the origin:



With a relation more generally, we won't necessarily get this breakup into neat equivalence classes.

Definition 5.13. If R is any relation (a subset of $A \times B$), the DOMAIN of R is the set $\operatorname{dom} R = \{x \in A : x\, R\, y \text{ for some } y \in B\}$. The RANGE of R is the set $\operatorname{ran} R = \{y \in B : x\, R\, y \text{ for some } x \in A\}$. Note that the domain of any equivalence relation is the whole set on which it is defined; the same holds for its range.

6 Tuesday, September 19

The pigeon-hole principle states that if you have n pigeons and $n+1$ holes, there will be at least one pigeon with more than one hole in it. Most pigeons will be dead.

6.1 Functions

When we've been talking about relations, usually we've restricted ourselves to talking about a relation on a single set, i.e., a subset of $A \times A$. But we mentioned that it's possible to consider a relation *between* sets A and B. A *function* is such a relation:

Definition 6.1. If X and Y are sets, a FUNCTION f from X to Y is a relation f on $X \times Y$ such that $\operatorname{dom} f = X$ and for all $x \in X$, there exists a *unique* $y \in Y$ such that $(x, y) \in f$. We write this unique y as $f(x)$. It is called the VALUE of f at x.

Heuristically, this definition is saying we assign one and only one element of Y to every element of X. We will write $f : X \to Y$ to mean "f is a function from X to Y". The set X is called the "domain" or "source" of f, and Y is the "codomain" or "target"[10].

Examples 6.2. The relation $\{(x, x^3 - 1) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$ is a relation on $\mathbb{R}$ is the function $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = x^3 - 1$.

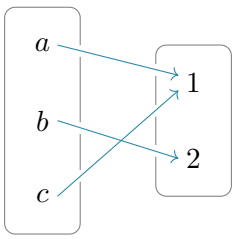
There is a function $f : \{\text{set of people}\} \to \{\text{set of addresses}\}$ given by $f(x) = \text{address of } x$.

Example 6.3. Here's a slightly trickier one: let f be a function

$$f(x) = \frac{x^2 - 1}{x}.$$

What is the domain of this function? Well, since we can't divide by zero, we get a function $f : \mathbb{R} - \{0\} \to \mathbb{R}$.

Example 6.4. There is a function $f : \{a, b, c\} \to \{1, 2\}$ defined by $f(a) = 1$, $f(b) = 2$, and $f(c) = 1$. Pictorially, this looks like



[10] The term "range" is often ambiguous; don't use it.

Definition 6.5. Let $f : A \to B$ be a function, and suppose that $A_0 \subseteq A$ is a subset. Then the IMAGE of A_0 under f is the set

$$f(A_0) := \{b \in B : \text{ there exists some } a \in A_0 \text{ for which } f(a) = b\}.$$

The set $f(A)$ is sometimes called the "image of f".

Definition 6.6. If $f : A \to B$ is a function, and $f(A) = B$, then we say that f is SURJECTIVE: everything in B is "hit" by something in A under f. We sometimes also say that f is ONTO.

Definition 6.7. If $f : A \to B$ is a function and $A_0 \subseteq A$ is a subset, then the RESTRICTION of f to A_0 is the function $f|_{A_0} : A_0 \to B$ defined by $f|_{A_0}(a) = f(a)$ for $a \in A_0$.

Definition 6.8. If $f : A \to B$ and $g : B \to C$ are functions, then the COMPOSITE $(g \circ f) : A \to C$ is the function defined by $(g \circ f)(a) = g(f(a))$. Formally, $g \circ f = \{(a, c) \in A \times C : f(a) = b \text{ and } g(b) = c \text{ for some } b \in B\}$.

Example 6.9. Let $f(x) = x^3$, and $g(x) = \frac{1}{x^2+1}$. Then

$$(g \circ f)(x) = g(x^3) = \frac{1}{x^6 + 1}$$

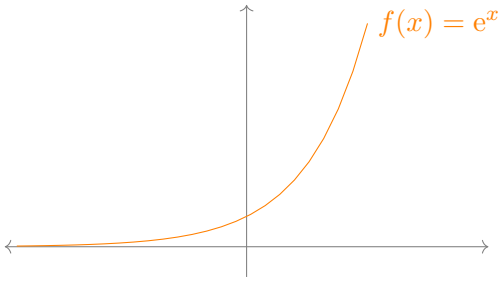
and

$$(f \circ g)(x) = f\left(\frac{1}{x^2 + 1}\right) = \frac{1}{(x^2 + 1)^3}.$$

Definition 6.10. A function $f : A \to B$ is said to be INJECTIVE or ONE-TO-ONE if $f(a) = f(b)$ implies $a = b$. Equivalently, if $a \neq b$, then $f(a) \neq f(b)$.

Reuben's Aside 6.11. Really, a better name for injective would be "two-to-two": two distinct elements of A will map to distinct elements of B. Alas, the name "one-to-one" has stuck. Silly mathematicians.

Examples 6.12. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$ is injective, but it is not surjective: for no $x \in \mathbb{R}$ will e^x be negative:



Our function $f : \{a, b, c\} \to \{1, 2\}$ from Example 6.4 is surjective but not injective: both a and c map to 1.

Reuben's Aside 6.13. Let A be a finite set with n elements and B a finite set with m elements, where n is strictly greater than m. The fact that *no function* $f : A \to B$ can be injective is called the PIGEON-HOLE PRINCIPLE. This is equivalent logically to the principle of mathematical induction, and the well-ordering principle. We'll talk about these in due time.

If $A_0 \subseteq A$ is a subset, then the function $i : A_0 \to A$ given by $i(a) = a$ is called the INCLUSION or EMBEDDING of A_0 into A. This is always injective, by definition. A combination of the subset symbol "$\subset$" and the function arrow "$\to$" gives us a standard notation for injective functions:

$$f : X \hookrightarrow Y.$$

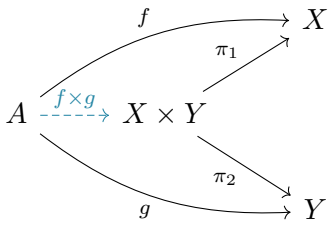
The map $\mathbb{1}_A : A \to A$ given by $\mathbb{1}_A(a) = a$ is the IDENTITY MAP on A; it is both injective and surjective.

Definition 6.14. Let X and Y be nonempty sets; define a function

$$f : X \times Y \to X$$

by $f(x, y) = x$. This is called the PROJECTION onto X, and it is clearly surjective. It is only injective if Y has exactly one element. We write the projection onto the first coordinate as $\pi_1 : X \times Y \to X$, and onto the second coordinate as $\pi_2 : X \times Y \to Y$.

Reuben's Aside 6.15. Let $f : A \to X$ and $g : A \to Y$ be any functions, where A, X, and Y are nonempty sets. Then there is a unique function $f \times g : A \to X \times Y$ such that $\pi_1 \circ (f \times g) = f$ and $\pi_2 \circ (f \times g) = g$. This function is defined by $(f \times g)(a) = (f(a), g(a))$. All this information can be summed up by saying that the following diagram is *commutative*:



One can check that $f \times g$ as we have defined it is the *only* function $A \to X \times Y$ that makes this diagram commute; we thus say that $X \times Y$ is the *categorical product* of X and Y[11].

Definition 6.16. Let $\sim$ be an equivalence relation on A. Define the CANONICAL MAP $f : A \to A/\sim$ by $f(a) = [a]_\sim$. This map is clearly surjective, but it is only injective if $\sim$ is the trivial relation ($a \sim b$ if and only if $a = b$).

Example 6.17. Let $x, y \in \mathbb{Z}$. We say that x and y have the same PARITY if $x - y$ is even. Define an equivalence relation $\sim$ to be $x \sim y$ if and only if x and y have the same parity. What is the set $\mathbb{Z}/\sim$ of equivalence classes? Well, there are only two equivalence classes: the set of even numbers and the set of even numbers! The canonical map

$$c : \mathbb{Z} \to \mathbb{Z}/\sim$$

is defined by $c(2n + 1) = [1]$ and $c(2n) = [0]$, for all $n \in \mathbb{Z}$.

Definition 6.18. A function $f : A \to B$ is BIJECTIVE if it is both injective *and* surjective.

Example 6.19. The function given by $f(x) = x + 1$ is a bijection from the set of odd integers to the set of even integers.

[11] I like category theory[a lot].

7 Thursday, September 21

> "*Mathematics is a collection of cheap tricks and dirty jokes.*"
>
> Lipman Bers

7.1 More about functions

If $f : X \to Y$ is an arbitrary function, we can define an equivalence relation on X by saying $x \sim x'$ if and only if $f(x) = f(x')$. This is certainly reflexive and symmetric, and transitivity holds because equality in Y is transitive. Assume now that f is surjective; define a new function $g : Y \to X/\sim$ by setting $g(y) = \{x \in X : f(x) = y\}$. Check that this is well-defined! This function is in fact a bijection:

Proof. First, let's check injectivity. Suppose y_1 and y_2 are distinct elements of Y. We can thus find some x_1 that maps to y_1 and x_2 that maps to y_2 by surjectivity of f. Thus $f(x_1) \neq f(x_2)$, so $x_1 \not\sim x_2$. Therefore $g(y_1) \neq g(y_2)$, as we know $x_1 \in g(y_1)$ and $x_2 \in g(y_2)$.

Now, we check surjectivity. Let $\overline{x} \in X/\sim$. Consider $g(f(x))$: by first applying $f(x)$, we get an element $y \in Y$. Then $g(y) = \{a \in X : f(a) = y = f(x)\}$. But this is just the same as $\overline{x}$! So $g(f(x)) = \overline{x}$, and g is surjective. □

Lemma 7.1. *Let $f : A \to B$ and $g : B \to C$ be functions. Then*

1. *if f and g are surjective, then so is $g \circ f : A \to C$;*
2. *if f and g are injective, then so is $g \circ f$.*

Proof.

1. Let c be an element of C; we'll find an element of A that maps to c under $g \circ f$. Because g is surjective, we can find some $b \in B$ such that $g(b) = c$. Because f is surjective, we can find some $a \in A$ such that $f(a) = b$. Then $(g \circ f)(a) = g(f(a)) = g(b) = c$.
2. On homework.

□

A diagrammatic depiction of the proof of part 1 is illustrated in this diagram: make diagram
Note that this lemma implies the composition of two bijections is a bijection.

Reuben's Aside 7.2. A *lemma* is a small rodent that jumps off cliffs. Oh wait, that's a lem*ming*...

Definition 7.3. If $f : A \to B$ is bijective, then there exists a function $f^{-1} : B \to A$, called the INVERSE of f, such that $(f \circ f^{-1})(b) = b$ and $(f^{-1} \circ f)(a) = a$ for all $a \in A$ and $b \in B$. This is defined by $f^{-1}(b)$ be the unique element $a \in A$ such that $f(a) = b$. (Note that we can say "the" and "unique" because of injectivity, and this exists by surjectivity.)

Example 7.4. Let $f : X \to Y$ be a function, and $A \subseteq Y$. The INVERSE IMAGE or PREIMAGE of A is defined to be the set

$$f^{-1}(A) = \{x \in X : f(x) \in A\}.$$

As a caution, f doesn't need to be bijective to define the inverse image.

Proposition 7.5. *Let $f : X \to Y$ be a function, and $A \subseteq X$ and $B \subseteq Y$ be subsets. Then*

1. *$f\left(f^{-1}(B)\right) \subseteq B$ and*
2. *$A \subseteq f^{-1}(f(A))$.*

Proof. 1. If $b \in f\left(f^{-1}(B)\right)$, then $b = f(a)$ for some $a \in f^{-1}(B)$. That means that $f(a) \in B$, so $b \in B$.

2. Let $a \in A$. Then $f(a) \in f(A)$ by definition, so $a \in \{x \in X : f(x) \in f(A)\}$, which is precisely the definition of the inverse image $f^{-1}(f(A))$.

□

Proposition 7.6. *The inverse image preserves unions, intersections, and inclusions.*

A Collected Homework Problems

A.1 Due Tuesday, September 12

Problem 1. Write the negation of the following statements and predicates. Assume that x is a real number.

(a) All cows are brown.

(b) $x \leq 2$.

(c) All cows are brown and eat grass.

(d) x is a prime number greater than 12.

(e) There exists a cow that is black and doesn't eat grass.

(f) Every square is a rectangle.

(g) If x is not an integer, then x is negative.

(h) Every nonzero integer is either negative or positive.

(i) If x is an odd integer, then x^2 will be a positive odd integer.

(j) If it is cold or raining, I am wearing long sleeves or a jacket.

Problem 2. (a) Come up with two statements P and Q such that $P \Rightarrow Q$ is true but $Q \Rightarrow P$ is false.

(b) Using your statements from (a), write out "if $\neg Q$, then $\neg P$." ("if $\neg Q$, then $\neg P$" is called the CONTRAPOSITIVE of "if P, then Q." Notice that these two statements are equivalent!)

Problem 3. (a) Prove De Morgan's second law:

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

You can use either the method we used in class and show that if the left side is true then the right side is true and if the left side is false then the right side is false (why is this sufficient?) or use the fact that the two statements are equivalent if and only if they imply each other.

(b) Using a truth table, verify both of De Morgan's laws. Recall that the first law claims

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

Problem 4. List all of the subsets of the following sets:

(a) $\varnothing$

(b) $\{1, 2, 3\}$

(c) $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$

Problem 5. Let A, B, and C be sets. Prove that $(A \cap B) \cup C = A \cap (B \cup C)$ if and only if $C \subseteq A$.

Problem 6. Let $\mathscr{C}$ be a collection of sets.

(a) Prove

$$A \cup \left(\bigcap_{S \in \mathscr{C}} S \right) = \bigcap_{S \in \mathscr{C}} (A \cup S).$$

(b) Give a similar formula for

$$A \cap \left(\bigcup_{S \in \mathscr{C}} S \right),$$

and prove that your formula is correct.

Problem 7. For each collection of sets $\mathscr{C}$ below, calculate $\bigcap_{S \in \mathscr{C}} S$ and $\bigcup_{S \in \mathscr{C}} S$.

(a) A_1 is the set of odd integers, A_2 is the set of positive integers, A_3 is the set of integers divisible by 3, and $\mathscr{C} = \{A_1, A_2, A_3\}$.

(b) For each $i \in \mathbb{N}$, $S_i = \{x \in \mathbb{N} : x \geq i\}$, and $\mathscr{C} = \{S_i : i \in \mathbb{N}\}$.

(c) For every $n \in \mathbb{Z}$, $T_n = \mathbb{Z} - \{n\}$, i.e., the set of integers other than n, and $\mathscr{C} = \{T_n : n \in \mathbb{Z}\}$.

(d) T_n is defined as in part (c) and $\mathscr{C} = \{S_n : n \text{ is a prime number}\}$.

Problem 8. Prove De Morgan's laws for sets: $(A \cap B)' = A' \cup B'$ and $(A \cup B)' = A' \cap B'$.

Problem 9. Choose one of De Morgan's laws from 8 and formulate and prove it for arbitrary unions or intersections (i.e., instead of for a pair of sets, formulate it in terms of an arbitrary collection of sets $\mathscr{C}$).

Index

associativity, 6

bijective, 25

canonical map, 25
cartesian product, 18
commutative, 6
commutative monoid, 4
complement, 15
composite, 24
contrapositive, 14, 27

difference, 15
direct proof, 13
disjoint subsets, 17
domain, 22

embedding, 25
empty set, 3
equivalence class, 20
equivalence relation, 19, 20
equivalent, 9

function, 23

identity map, 25
image, 24
implication, 10
in, 3
inclusion, 25
induction, 15
injective, 24
intersection, 4
intersection of $\mathscr{C}$, 5

logical and, 9
logical or, 9

natural numbers, 4
negation, 8

one-to-one, 24
onto, 24

parity, 25
partition, 21
pigeon-hole principle, 24
power set, 17
predicates, 11
projection, 25
proof by contradiction, 14

quantifier, 12

range, 22
relation, 19, 20
restriction, 24

set, 3
statement, 8
subset, 3
surjective, 24
symmetric, 19
symmetric difference, 17

truth table, 8
truth value, 8

union, 4
union of $\mathscr{C}$, 4

value, 23