Contents

1 Logic and proofs 1
1.1 Propositions and Connectives 1
1.2 Conditionals and Biconditionals 2
1.3 Quantifiers 5
1.4 Proof Methods 7
1.5 Proofs Involving Quantifiers 10
1.6 How to prove it 11
1.7 Examples involving divisibility 12

2 Set theory 15
2.1 Basic concepts 15
2.2 Set operations 16
2.3 Indexed families of sets 19
2.4 Mathematical Induction 20
2.5 Well-Ordering and Strong Induction 21
2.6 Principles of counting 22

3 Relations and partitions 25
3.1 Relations 25
3.2 Equivalence relations 26
3.3 Order relations 29
3.4 Graphs 30

4 Functions 31
4.1 Functions as relations 31
4.2 Injective, surjective and bijective functions 32

5 Homework 37
5.1 Intro 37
5.2 Homework, 2/22/18 37
5.3 Test corrections, due Tuesday, 02/27/2018 37
5.4 Homework, due Tuesday 02/27/2018 38
5.5 Homework, due Tuesday 03/01/2018 38
5.6 Practice problems 1 38
5.7 Exam 1 Review 44
5.8 Exam 2 Review 48
5.9 Function Review 64
5.10 Comprehensive Final Exam Review 67

6 List of Definitions 73

A Prerequisites **75**
A.1 Number classes 75

B Notation **77**

Index **79**

Chapter 1

Logic and proofs

1.1 Propositions and Connectives

In this chapter we introduce classical logic which has two **truth values**, `True` and `False`. Every *proposition* takes on a single truth value.

Definition 1.1.1 (Proposition)**.** A **proposition** is a sentence that is either true or false.

Definition 1.1.2 (Conjunction, Disjunction, Negation)**.** Given propositions P and Q, the

conjunction of P and Q, denoted $P \wedge Q$, is the proposition "P and Q." $P \wedge Q$ is true exactly when *both* P and Q are true.

disjunction of P and Q, denoted $P \vee Q$, is the proposition "P or Q." $P \vee Q$ is true exactly when *at least one* P or Q is true.

negation of P, denoted $\neg P$, is the proposition "not P." $\neg P$ is true exactly when P is false.

Note that although the disjunction $P \vee Q$ is translated into English as "P or Q", it means something slightly different than the way we use "or" in everyday speech. In particular, disjunction is *inclusive*, which means that it is true whenever *at least one* of P or Q is true. On the other hand, in English, "or" is often *exclusive*, which means that it is true whenever *exactly one* of the alternatives is true. For example, if I said "today, I will either go to the park or to the pool," it would generally be understood that I will do one or the other, but not both. However, if P is the proposition "I will go to the park" and Q is the proposition, "I will go to the pool", then $P \vee Q$ means "I will go to the park or to the pool *or both*." Throughout the remainder of this course, whenever we say "or", we mean the inclusive version corresponding to disjunction.

Definition 1.1.3 (Well-formed formula)**.** A **well-formed formula** is an expression involving finitely many logical connective symbols and letters representing propositions which is *syntactically* (i.e., grammatically) correct.

For example, $\neg(P \vee Q)$ is a well-formed formula, but $\vee PQ$ is not.

Definition 1.1.4 (Equivalent forms)**.** Two well-formed formulas are **equivalent** if and only if they have the same truth tables.

From the defintion, we can see that $P \vee Q$ and $Q \vee P$ are equivalent forms. Similarly, $P \wedge Q$ and $Q \wedge P$ are equivalent forms. However, there are less obvious examples such as $\neg((P \vee Q) \wedge R)$ and $((\neg P) \vee (\neg R)) \wedge ((\neg Q) \vee (\neg R))$.

Definition 1.1.5 (Tautology)**.** A **tautology** is a well-formed formula that is true for every assignment of truth values to its components.

For example, the **Law of Excluded Middle** which states that, for any proposition P, the disjunction $P \vee (\neg P)$ is a tautology. The name refers to the fact that every proposition is either true or false, there are no possibilities in-between, i.e., the middle is excluded.

P	$\neg P$	$P \vee (\neg P)$
True	False	True
False	True	True

Table 1.1.6

Definition 1.1.7 (Contradiction)**.** A **contradiction** is a well-formed formula that is false for every assignment of truth values to its components.

For example, for any proposition P, the conjunction $P \wedge (\neg P)$ is a contradiction.

P	$\neg P$	$P \wedge (\neg P)$
True	False	False
False	True	False

Table 1.1.8

Definition 1.1.9 (Denial)**.** A **denial** of a proposition P is any proposition equivalent to $\neg P$.

For example, for any propositions P and Q, the statement

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

is a denial of P.

Exercise 1.1.10. Make a truth table for each of the following propositions, and determine whether any of them are contradictions or tautologies.

$$(P \vee (\neg Q)) \wedge (\neg R),$$
$$((\neg P) \vee (\neg Q)) \wedge ((\neg P) \vee Q),$$
$$(P \wedge Q) \vee (P \wedge (\neg Q)) \vee ((\neg P) \wedge Q) \vee ((\neg P) \wedge (\neg Q)),$$
$$(P \vee Q) \wedge (P \vee (\neg Q)) \wedge ((\neg P) \vee Q) \wedge ((\neg P) \vee (\neg Q)).$$

1.2 Conditionals and Biconditionals

Definition 1.2.1 (Conditional, Antecedent, Consequent)**.** For propositions P and Q, the **conditional sentence** $P \implies Q$ is the proposition "If P, then Q." The proposition P is called the **antecedent**, Q the **consequent**. The conditional sentence $P \implies Q$ is true if and only if P is false or Q is true. In other words, $P \implies Q$ is equivalent to $(\neg P) \vee Q$.

A conditional is meant to make precise the standard language construct "If ..., then ...", but it is has some seemingly counterintuitive properties. For example, do you think the statement "if the moon is made of green cheese, then it is tasty," is true or false? What about the statement, "if the moon is made of green cheese, then the Red Sox will win the world series," is it true or false? In fact, both statement are true because the *antecedent*, "the moon is made of green cheese", is false. Note, in each case, we are not asking about the truth of the atomic propositions, but rather the statement as a whole. Moreover, there is no reason the antecedent and consequent need to be logically connected, which violates our intuition.

Exercise 1.2.2. Suppose you are a waiter in a restaurant and you want to make sure that everyone at the table is obeying the law: the drinking age is 21. You know some information about who ordered what to drink and their ages which is indicated in the table below. What is the minimal additional information you need to determine if the law is obeyed?

Person	Age	Drink
A	33	—
B	—	Beer
C	15	—
D	—	Coke

Table 1.2.3

Solution. B's age and C's drink. You can think of obeying the law as making "If under 21, then no alcohol," a true statement. Then the statement is true whenever each person is either 21 and up or did not order alcohol. A is above 21, so he is obeying the law no matter what he ordered. B ordered alcohol, so we must check how old he is to determine if the law is obeyed. C is under 21, so we must check what he ordered to determine if the law is obeyed. D order coke, so he is obeying the law regardless of his age.

Definition 1.2.4 (Converse, Contrapositive)**.** Let P and Q be propositions and consider the conditional $P \implies Q$. Then the

converse is $Q \implies P$.

contrapositive is $(\neg Q) \implies (\neg P)$.

Theorem 1.2.5 (Contrapositive Equivalence)**.**

1. *A conditional sentence and its contrapositive are equivalent.*

2. *A conditional sentence and its converse are not equivalent.*

Proof. Make the truth table. □

Definition 1.2.6 (Biconditional)**.** For propositions P and Q, the **biconditional sentence** $P \iff Q$ is the proposition "P if and only if Q." $P \iff Q$ is true exactly when P and Q have the same truth value.

Theorem 1.2.7 (De Morgan's Laws)**.** *For propositions P and Q,*

1. $\neg(P \wedge Q)$ *is equivalent to* $(\neg P) \vee (\neg Q)$*;*

2. $\neg(P \vee Q)$ *is equivalent to* $(\neg P) \wedge (\neg Q)$*.*

These can be read in English as "the negation of a conjunction is the disjunction of the negations," and "the negation of a disjunction is the conjunction of the negations."

Proof. Make a truth table. □

Theorem 1.2.8 (Commutativity of Conjunction and Disjunction)**.** *For propositions P and Q,*

1. *$P \wedge Q$ is equivalent to $Q \wedge P$;*
2. *$P \vee Q$ is equivalent to $Q \vee P$.*

So there is no ambiguity when we say "the conjunction of P and Q," or "the disjunction of P and Q,"

Proof. Make a truth table. □

Theorem 1.2.9 (Associativity of Conjunction and Disjunction)**.** *For propositions P, Q and R,*

1. *$P \wedge (Q \wedge R)$ is equivalent to $(P \wedge Q) \wedge R$;*
2. *$P \vee (Q \vee R)$ is equivalent to $(P \vee Q) \vee R$.*

So there is no ambiguity in the propositions $P \wedge Q \wedge R$ or $P \vee Q \vee R$.

Proof. Make a truth table. □

Theorem 1.2.10 (Distributivity of Conjunction and Disjunction)**.** *For propositions P, Q and R,*

1. *$P \wedge (Q \vee R)$ is equivalent to $(P \wedge Q) \vee (P \wedge R)$;*
2. *$P \vee (Q \wedge R)$ is equivalent to $(P \vee Q) \wedge (P \vee R)$.*

You should interpret this as indicating that conjunction and disjunction distribute over each other.

Proof. Make a truth table. □

Theorem 1.2.11 (Conditional Equivalences)**.** *For propositions P and Q,*

1. *$P \implies Q$ is equivalent to $(\neg P) \vee Q$;*
2. *$\neg(P \implies Q)$ is equivalent to $P \wedge (\neg Q)$;*
3. *$P \iff Q$ is equivalent to $(P \implies Q) \wedge (Q \implies P)$.*

Proof. Make a truth table. □

Remark 1.2.12 (Dictionary of implication)**.** The logical conditional $P \implies Q$ has several translations into English which include:

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

Similarly, the biconditional $P \iff Q$ translates into a few of English phrases including:

- P if and only if Q.
- P is equivalent to Q.
- P is necessary and sufficient for Q.

1.3 Quantifiers

Remember that the sentence "x is an American," is *not* a proposition. This is because the truth of the statement changes based on different values for x. Such a sentence is called an **open sentence** or **predicate**. However, it is quite useful to include variables in our statements, so our logic should be able to accommodate that. To this end we introduce **quantifiers**. A quantifier is a symbol which states *how many* instances of the variable satisfy the sentence.

Definition 1.3.1 (Quantifiers)**.** For an open setence $P(x)$, we have the propositions

$(\exists x)P(x)$ which is true when *there exists at least one* x for which $P(x)$ is true. The symbol $\exists$ is called the **existential quantifier**.

$(\forall x)P(x)$ which is true when $P(x)$ is true *for every* x. The symbol $\forall$ is called the **universal quantifier**.

Remark 1.3.2 (Dictionary of quantification)**.** The existential statement $(\exists x)P(x)$ may be read as:

- "There exists x such that $P(x)$."
- "There exists x for which $P(x)$."
- "For some x, $P(x)$."

The symbol $\exists$ was chosen as a backwards E for "exists."

Similarly, the universal statement $(\forall x)P(x)$ may be read as:

- "For all x, $P(x)$."
- "For every x, $P(x)$."
- "For each x, $P(x)$."

The symbol $\forall$ was chosen as an inverted A for "all."

Perhaps you think quantifiers are now obvious, and if so, what is the truth value of the proposition $(\exists x)(x^2 = 2)$? The answer is, "it depends!" In particular, it depends on the **universe** of discourse; that is, what is the set of x's over which we are quantifying? This universe needs to be specified beforehand in order to make sense of the proposition and determine its truth value. For example, the existential statement above is false if the universe is the set of natural numbers, $\mathbb{N}$, but it is true if the universe is the set of real number, $\mathbb{R}$.

If the context does not make clear the universe over which we are quantifying, we may specify it explicitly by using the **set membership** symbol $\in$, which may be read "is an element of." For example, we read $x \in \mathbb{R}$ as any of:

- "x is an element of the set of real numbers."
- "x is a real number."
- "x is in the set of real numbers."

When we are feeling lazy, we omit "the set of." Now, we may rewrite our statement with respect to different universes as

$$(\exists x \in \mathbb{N})(x^2 = 2),$$
$$(\exists x \in \mathbb{R})(x^2 = 2).$$

Now, the first statement is false, and the second statement is true, so the universe of dicourse matters.

Does it surprise you that we only have two quantifiers? At first it might seem strange but what are the other possibilities? In general, it is not very useful to embed the idea "there are 5 x satisfying $P(x)$," directly into our logic. This is for a variety of reasons including

- we don't want to have too many symbols;
- we don't know how many elements each universe may have.

In addition, it can be difficult to make statements like "most sheep are white," precise. However, there is *another* quantifier that we find useful.

Definition 1.3.3 (Uniqueness quantifier)**.** For an open sentence $P(x)$, the proposition $(\exists! x)P(x)$ is true when there is *exactly one* x making $P(x)$ true. We read this proposition in English as "there exists a unique x such that $P(x)$." The symbol $\exists!$ is called the **unique existential quantifier**.

Remark 1.3.4. The proposition $(\exists! x)P(x)$ is just an abbreviation for

$$\Big((\exists x)P(x)\Big) \land \Big((\forall y)(\forall z)(P(y) \land P(z)) \implies (y = z)\Big).$$

You should interpret this as saying, "there is some x satisfying $P(x)$, and whenever any two elements y, z both satisfy this open sentence, then they are actually the same element."

The next theorem explains why we chose the universal $\forall$ and existential $\exists$ quantifiers as the *de facto* standard of quantification: they play nice with negation.

Theorem 1.3.5 (Quantifier negation)**.** *Negation interacts with the existential and universal quantifiers in the following ways.*

$$\neg((\exists x)P(x)) \iff (\forall x)(\neg P(x));$$
$$\neg((\forall x)P(x)) \iff (\exists x)(\neg P(x)).$$

Exercise 1.3.6 (Quantifier order)**.** Translate the following quantified sentences into English.

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

What is the difference between these two sentences? Do they have the same truth value, or different truth values?

Solution. The first statement may be translated as "for every natural number x, there exists a natural number y such that x is less than y." The second statement may be traslated as "there exists a natural number y such that for every natural number x, x is less than y."

The key difference between these two sentences is the following: in the first sentence, y can depend on x because x came first; in the second sentence, y must be independent of x. From here, we can recast our translations as: "for every natural number, there is some other natural number bigger than it," and "there is some natural number which is simultaneously bigger than every natural number (including itself!)."

Now, it should be clear that the first statement is true (if $x \in \mathbb{N}$, choose $y = x + 1 \in \mathbb{N}$), but the second statement is false (because we've just shown there is no biggest natural number).

This issue with the order of quantifiers only comes into play among *different* quantifiers. In particular, the order of *consecutive universal* quantifiers may be changed at will and yield an equivalent proposition. Similarly, the order of *consecutive existential* quantifiers may be changed at will and yield an equivalent proposition.

1.4 Proof Methods

A **proof** is just a convincing argument. However, mathematicians tend to have extraordinarily high standards for what convincing means. For example, consider the **Goldbach conjecture** which states that “every even number greater than 2 is the sum of two primes.” This conjecture has been verified for even numbers up to 10^{18} as of the time of this writing. The layman may say, “surely, this prove the result!” but the mathematician is not convinced because he (or she) requires a deductive argument, not an extrapolation based on observation. Before we begin, we need to define a few terms.

Definition 1.4.1 (Definition, Axiom, Theorem)**.** A **definition** is simply an abbreviation for a proposition or object. Definitions are *created* by mathematicians in order to more succinctly express ideas and relationships. An **axiom** is a proposition that we *assume to be true* without any justification (other than, perhaps, because our intution says so). Because axioms are *unjustified propositions* we try to avoid creating too many of them. A **theorem** is a proposition which we justify by means of a proof.

Remark 1.4.2. So, what are the rules of a proof from the mathematicians points of view? They can be encompassed in essentially four primary rules.

prior results It is always valid to state an assumption, axiom, or prior result.

replacement rule It is always valid to state a sentence equivalent to a sentence occurring earlier in the proof.

tautalogy rule It is always valid to state a tautology, e.g., the Law of Excluded Middle.

modus ponens After stating P and $P \implies Q$, one may state Q.

The *prior results rule* is vital and it is part of what makes mathematics so powerful. Instead of reproving the same result over and over, we can prove it once and for all, and then use it wherever we choose. For those of you with a background in software development, this is essentially what happens when you abstract and modularirze a piece of code into a function for reuse in other places. For this reason, you generally don’t want to prove monolithic theorems. Instead, if your theorem has a lot of different pieces, break them up into smaller pieces. Alternatively, if there are a lot of steps in your proof, you can often split the proof into smaller pieces called **lemmas**.

The *replacement rule* is often useful for substituting a term (e.g., even number) with its definition ($2k$ for some integer $k \in \mathbb{Z}$).

The *modus ponens* rule is based on the fact that $\big(P \wedge (P \implies Q)\big) \implies Q$ is a tautology. This is probably not immediately obvious to you, so you should make a truth table to justify it to yourself.

Probably the most common kind of proof is the **direct proof**, which has the following structure.

Theorem 1.4.3 (Direct proof of $P \implies Q$)**.** *If P, then Q.*

Proof. Assume P.
(apply rules of proofs judiciously)
Therefore, Q.
Thus, $P \implies Q$. □

As an example, we will prove the following proposition using a direct proof.

Proposition 1.4.4. *Let x be an integer. If x is odd, then $x+1$ is even.*

Proof. Let x be an odd integer. By Definition A.1.3, $x = 2k+1$ for some integer $k \in \mathbb{Z}$. Then $x+1 = 2k+2 = 2(k+1)$. Since the sum of two integers is an integer, $k+1 \in \mathbb{Z}$, and therefore, by Definition A.1.2, $x+1 = 2(k+1)$ is even. Hence, if x is odd, then $x+1$ is even. □

Remark 1.4.5. In the statement of the previous theorem occurred the sentence, "let x be an odd integer." This is not the antecedent of the implication (which is "if x is an odd integer"), but is rather something called a **hypothesis**, which provides the context in which the theorem takes place. In this case, we would be unable to say that x is odd (or even, for that matter) unless x is an integer.

The careful reader may have noticed that the statement we proved was not exactly a proposition in our strict sense: it is instead an open sentence because we did not pick a specific value of x. The resolution to this problem will be addressed in the next section. However, notice that our proof would have worked equally well *no matter which* odd integer we chose.

Theorem 1.4.6 (Proof by cases of $(P \vee Q) \implies R$)**.** *If either P or Q, then R.*

Proof. *Case 1.* Assume P, ..., therefore R. Hence $P \implies R$
Case 2. Assume Q, ..., therefore R. Hence $Q \implies R$. □

In the proof by cases above, we did not actually prove $(P \vee Q) \implies R$ directly. That is, we did not start by assuming $P \vee Q$. Instead, we prove *two* implications, namely, $P \implies R$ and $Q \implies R$. This is acceptable because of the equivalence

$$\big((P \vee Q) \implies R\big) \iff \big((P \implies R) \wedge (Q \implies R)\big)$$

Remark 1.4.7. We may implement a proof by cases *even when the antecedent does not include a disjunction.* This can be achieved by inserting the Law of Excluded Middle tautology for some appropriate proposition.

Proposition 1.4.8. *Suppose n is an odd integer. Then $n = 4j+1$ for some integer j, or $n = 4i-1$ for some integer i.*

Proof. Suppose $n \in \mathbb{Z}$ is odd. Then $n = 2k+1$ for some integer k. The integer k is either odd or even by Parity.

Case 1: k is even. Since k is even, $k = 2j$ for some integer j. Thus

$$n = 2k+1 = 2(2j)+1 = 4j+1.$$

Case 2: k is odd. Since k is odd, $k = 2i+1$ for some integer i. Thus

$$n = 2k+1 = 2(2i+1)+1 = 4i+3 = 4(i+1)-1.$$

Since $i+1$ is an integer, we have proven the desired result. □

Recall that Theorem 1.2.5 guarantees the conditional statement $P \implies Q$ is equivalent to its contrapositive, namely, $(\neg Q) \implies (\neg P)$. This leads to a new proof technique called **proof by contrapositiion**. In this proof technique, instead of proving the implication directly, we instead prove its contrapositive directly, and then use the stated equivalence.

Theorem 1.4.9 (Proof by contraposition of $P \implies Q$.)**.** *If P, then Q.*

Proof. Assume $\neg Q$, . . . , therefore $\neg P$. Hence, $(\neg Q) \implies (\neg P)$. Therefore $P \implies Q$. □

Proposition 1.4.10. *Let $x \in \mathbb{Z}$. If x^2 is even, then x is even.*

Proof. Suppose x is not even. By Parity x is odd. Thus $x = 2k + 1$ for some integer k. Hence

$$x^2 = (2k + 1)^2 = (2k)^2 + 2(2k) + 1 = 2(2k^2 + 2k) + 1.$$

Since the integers are closed under addition and multiplication, $2k^2 + 2k \in \mathbb{Z}$. Then by the definition of odd, x^2 is odd. Again, by Parity, x^2 is not even. Therefore, if x is not even, then x^2 is not even. Hence, by contraposition, we have proven the result. □

The next proof technique is often regarded as completely strange when first encountered, but you will become used to it after a while. This proof technique essentially relies on two facts.

- If you assume something is true (say R) and then reach a contradiction, the thing you assumed must have been false ($\neg R$).
- For any proposition, $(\neg\neg R)$ is equivalent to R.

Theorem 1.4.11 (Proof of P by contradiction)**.** *P is true.*

Proof. Suppose $\neg P$, . . . , therefore Q, . . . , therefore $\neg Q$. Hence $Q \wedge (\neg Q)$, a contradiction. Thus, $\neg\neg P$. Therefore, P. □

At this point, you should try to avoid proofs by contradiction. There are three reasons for this. First, they are conceptually harder to grasp than other proofs, both for you and for the reader. Second, many people prove things by contradiction when they really meant to use the contrapositive. Third, if you make any error in your reasoning during the proof, it can look like you've reached a contradiction and have thus proven your result, when really it was just an error.

Up until this point, we haven't mentioned how to prove a biconditional statement. However, Theorem 1.2.11 guarantees that we can just prove both directions, which we encapsulate in the following technique.

Theorem 1.4.12 (Two-part proof of $P \iff Q$)**.** *P if and only if Q.*

Proof. Prove $P \implies Q$ by any method. Prove $Q \implies P$ by any method. Therefore, $(P \implies Q) \wedge (Q \implies P)$, and hence $P \iff Q$. □

Proposition 1.4.13. *Let x be an integer. Then x is even if and only if x^2 is even.*

Proof. Let $x \in \mathbb{Z}$.

if x is even, then x^2 is even.. Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Thus $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Therefore x^2 is even by definition.

if x^2 is even, then x is even.. This was proven in Proposition 1.4.10 using contraposition.Thus, x is even if and only if x^2 is even. □

There is another way to prove "if and only if" (i.e. biconditional) statements, which is just to use a series of equivalent statements. Note, we use the useful abbreviation "iff" for "if and only if."

Theorem 1.4.14 (Biconditional proof of $P \iff Q$)**.** *P if and only if Q.*

Proof. P iff R_1 iff R_2 ... iff R_n iff Q. □

Remark 1.4.15. Before we prove the next proposition, it will be helpful to notice that biconditional equivalence has a nice property, namely,

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

Proposition 1.4.16. *Let x be an integer. Then x is odd if and only if x^2 is odd.*

Proof. Suppose x is an integer. Then x is odd if and only if x is not even (by Parity) if and only if x^2 is not even (by Proposition 1.4.13) if and only if x^2 is odd. □

1.5 Proofs Involving Quantifiers

Recall that many of the statements we proved before weren't exactly propositions because they had a variable, like x. See Proposition 1.4.4 for an example. We mentioned the strangeness at the time, but now we will confront it. In an example like Proposition 1.4.4, we see that it really *is* a proposition because it should be interpreted as a statement with a universal quantifier. So, that means we need to figure out what a proof of such a statement looks like.

Let's think about this. If I want to show a statement is true for *every* positive integer, it seems hopeless because I would need to prove infinitely many statements, one for each positive integer. Since I cannot ever prove infinitely many statements, all is lost. Well, not quite. What if I came up with a proof of my statement for the number one, but then I realized that my proof would work just as well for two? or three? or for any positive integer? In that case, I could work through my proof working with any positive integer, and then when I get to the end, I've proved it for any (i.e., *all*) positive integer.

Theorem 1.5.1 (Direct proof of $(\forall x)P(x)$)**.** *For every x, $P(x)$.*

Proof. Let x be an arbitrary object of the universe of discourse.

...

Hence $P(x)$ is true.

Since x is arbitrary, $(\forall x)P(x)$ is true. □

Now, having dealt with universal quantifiers, we also need to see how to deal with existential quantifiers. The most natural way to prove an existential statement $(\exists x)P(x)$ is to produce a *specific* a and show that $P(a)$ is true for your choice. This requires that we somehow figure out which x will work.

Theorem 1.5.2 (Direct proof of $(\exists x)P(x)$)**.** *There exists an x for which $P(x)$.*

Proof. Pick a to be a specific object in the universe of discourse.

...

Hence $P(a)$ is true.

Therefore, $(\exists x)P(x)$ is true. □

Of course, proof techniques can be mixed and matched at will, at least as long as they fit the required form. For example, you could prove an existential statement by contradiction. An interesting thing about a proof of that form is that when you finish, you have proven something exists without actually knowing what it is.

Remark 1.5.3. The natural number **1729** is called the the **Hardy–Ramanujan number** after a famous anecdote of the British mathematician G. H. Hardy regarding a visit to the hospital to see the Indian mathematician Srinivasa Ramanujan.

> I remember once going to see him when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways."
>
> —G. H. Hardy

Proposition 1.5.4 (Hardy–Ramanujan number)**.** *There exists a positive integer m which can be expressed as the sum of two cubes in two different ways.*

Proof. Consider $m = 1729$. Note that

$$1^3 + 12^3 = 1 + 1728 = 1729 = 1000 + 729 = 10^3 + 9^3. \qquad \square$$

In the following proof technique, we will show how to prove a unique existential statement. For this, it is important to remember that $(\exists! x)P(x)$ is just an abbreviation by Remark 1.3.4.

Theorem 1.5.5 (Proof of $(\exists! x)P(x)$)**.** *There exists a unique x for which $P(x)$.*

Proof. Prove $(\exists x)P(x)$.

Suppose y and z are two elements of the universe for which $P(y)$ and $P(z)$ are true.

...

Thus, $y = z$.

Therefore, $(\exists! x)P(x)$. □

1.6 How to prove it

Below is a list of suggestions to consider when writing proofs.

1. *Figure out what you are trying to prove.* This starts by determining the logical structure of the statement. From there, you can set up the basic structure of your proof. Part of this is also determining the assumptions (or hypotheses and antecedents) and the conclusions (or consequents).

2. *Fill in the boilerplate material.* For those of you who may be unfamiliar with this term, material is said to be **boilerplate** if it is standard regardless of context. Boilerplate material consists of that material which provides the basic structure to your proof (e.g., "assume P," in a direct proof of $P \implies Q$), as well as the insertion of definitions (e.g., inserting "$m = 2k$, for some $k \in \mathbb{Z}$," after the statement "m is even."). It is also recommended that you fill in the boilerplate material that goes at the *end* of the proof because this will show you what is your ultimate goal.

3. *Play around.* Once you've filled in the boilerplate and gotten down to the meat of the proof, just try things. That is, combine equations, look at a few examples, try and understand the concepts. It's this stage, before you've found the whole proof, where true understanding and insight can occur. We saw this in the proof of Proposition 1.4.8 during class where we tried a few examples before we understood the key idea. Once you think you understand *why* the result is true, try and turn that into a proof.

Now, different logical forms lend themselves to different methods of proof, which we review below.

1. $P \implies Q$. Try a direct proof first. If you try it for a while and get nowhere, consider trying to prove the contrapositive. As an absolute last resort (rarely necessary), consider a proof by contradiction. Such a proof would start "assume $\neg(P \implies Q)$," which is equivalent to "assume $P \wedge (\neg Q)$."

2. $(P \vee Q) \implies R$. Use a proof by cases, where in the first case you assume P and in the second case you assume Q.

3. $P \iff Q$. Start with a two-part proof (where you prove $P \implies Q$ and $Q \implies P$ separately) and then see if each step is reversible. If it is, turn the proof into a concise if-and-only-if proof.

4. $(\forall x)P(x)$. Generally the best way is to prove these by starting with an arbitrary element. Proofs by contradiction should be avoided.

5. $(\exists x)P(x)$. Most often you will want to play around or guess until you find an object satisfying $P(x)$. Then, just write down a proof which highlights that object and shows it has the specified property. However, if that doesn't work, you might try showing the object exists indirectly (i.e., without constructing it) by contrdiction. This is one of the places where a proof by contradiction can really shine. In this case, you would start by assuming $\neg(\exists x)P(x)$, which is equivalent to $(\forall x)\neg P(x)$ and then proceed to derive a contradiction.

1.7 Examples involving divisibility

Theorem 1.7.1 (Division Algorithm)**.** *For any integers a, b with $a \neq 0$, there exists unique integers q and r for which*

$$b = aq + r, \quad 0 \leq r < |a| .$$

The intger b is called the ***dividend****, a the* ***divisor****, q the* ***quotient****, and r the* ***remainder****.*

Proof. Saved for a later chapter. □

Definition 1.7.2 (Greatest Common Divisor)**.** Let $a, b, c \in \mathbb{Z}$ be nonzero. We say c is a **common divisor** of a and b if and only if c divides a and c divides b. The **greatest common divisor** of a, b is denoted $\gcd(a, b)$, and is the common divisor of a, b which is greater than every other common divisor.

Theorem 1.7.3. *For any $a, b, x, y \in \mathbb{Z}$, any divisor of a, b also divides $ax + by$. $ax + by$ is called a* ***linear combination*** *of a, b.*

Proof. Let $a, b, x, y \in \mathbb{Z}$ be arbitrary. Let c be any divisor of a and b so there exist integers r, s so that

$$a = rc, \quad b = sc.$$

Thus

$$ax + by = (rc)x + (sc)y = c(rx + sy).$$

Since $rx + sy \in \mathbb{Z}$, we have shown c divides $ax + by$. □

The following lemma is the first proof we encounter where the key idea to get started is not obvious, even after a bit of playing around. At this point in the course, you would not be expected to come up with a proof like this, although later in the course you would.

Lemma 1.7.4. *For any nonzero $a, b \in \mathbb{Z}$, the smallest positive linear combination of a, b is a common divisor.*

Proof. Let a, b be arbitrary nonzero integers. Assume $x, y \in \mathbb{Z}$ so that $s := ax + by$ is positive, but as small as possible (i.e., it is the smallest positive linear combination of a, b).

By Division Algorithm, we may write $a = sq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < |s| = s$. Now

$$r = a - sq = a - (ax + by)q = a(1 - xq) + b(yq)$$

is another (nonnegative) linear combination of a, b. But we know r cannot be positive, otherwise it would violate the minimality of s. Therefore, $r = 0$ and hence $a = sq$. Thus s divides a. A nearly identical argument shows s divides b, and so s is a common divisor. □

Theorem 1.7.5. *For any nonzero integers a, b, their greatest common divisor is their smallest linear combination.*

Proof. Let a, b be arbitrary nonzero integers and let s denote their smallest positive linear combination. By Lemma 1.7.4 s is a common divisor of a, b. Let x be any other positive common divisor of a, b. By Theorem 1.7.3, we know t divides s, and so there is some (positive) integer k for which $s = tk$. Since $k \in \mathbb{N}$, we have $k \geq 1$ and so $s = tk \geq t$. Therefore s is greater than any other common divisor and hence $s = \gcd(a, b)$. □

Definition 1.7.6 (Relatively Prime, Coprime)**.** We say nonzero integers a, b are **relatively prime**, or **coprime**, if $\gcd(a, b) = 1$.

Theorem 1.7.7. *For any relatively prime $a, b \in \mathbb{Z}$ (necessarily nonzero) and for any $c \in \mathbb{Z}$ there exist $x, y \in \mathbb{Z}$ so that $ax + by = c$.*

Proof. Suppose $a, b \in \mathbb{Z}$ are relatively prime. By Theorem 1.7.5 there exist r, s so that $ar + bs = 1$. Then

$$a(rc) + b(sc) = (ar + bs)c = c.$$

Setting $x = rc, y = sc \in \mathbb{Z}$ proves the result. □

Lemma 1.7.8 (Euclid's Lemma)**.** *Let $a, b, p \in \mathbb{Z}$ with p prime. If p divides ab, then either p divides a or p divides b.*

Proof. Let $a, b, p \in \mathbb{Z}$ with p prime and suppose p divides ab. Thus $ab = pk$ for some integer k. Note that $\gcd(a, p)$ can be only either 1 or p since p has no other divisors.

Case 1: $\gcd(a, p) = p$. Then p divides a and we are finished.

Case 2: $\gcd(a, p) = 1$. By Theorem 1.7.5 there exist $x, y \in \mathbb{Z}$ so that $ax + py = 1$. Multiplying both sides by b, we obtain

$$b = (ax + py)b = abx + pyb = pkx + pyb = p(kx + yb).$$

Therefore p divides b. □

Chapter 2

Set theory

2.1 Basic concepts

During the 19th century, mathematicians became increasingly concerned with the foundations of mathematics and formalizing logic. Late in that century, Georg Cantor started considering sets and their properties. We have the following *informal* definition of a set.

Definition 2.1.1 (Set)**.** A **set** is an *unordered* collection of objects.

Because a set is unordered, it does not make any sense to say that an element of a set occurs twice. We generally denote finite sets with curly braces, such as

$$\{1, 2, 3, 4, 5\}.$$

For large or infinite sets, it helps to use set builder notation. For example, the even integers can be expressed as

$$\{x \mid x = 2k, k \in \mathbb{Z}\}.$$

This should be read as "the set of all x such that $x = 2k$ for some integer k." It is the vertical bar | that is interpreted as "such that," but it may also be read as "with the property," or "satisfying," or "for which," and probably even others. Note that some authors (including those of your textbook, prefer to use a colon : instead of a vertical bar; you should get comfortable with both notations. We can simplify with shorthand the form of the set of even integers we wrote above as

$$\{2k \mid k \in \mathbb{Z}\}.$$

Also, whenever the elements of your collection lie in some larger set, you should specify this in the set builder notation. For example, our description of the even integers really should have specified that x itself is an integer, as in

$$\{x \in \mathbb{Z} \mid x = 2k, k \in \mathbb{Z}\}.$$

Set can contain just about anything, including other sets! For example, the set $A = \{0, \{1, 2\}, 3\}$ has as its elements the integers, $0, 3$ as well as the set $\{1, 2\}$. The set A has three elements.

Definition 2.1.2 (Empty Set)**.** The **empty set** is the set with no elements. In particular, the empty set is the unique set for which the statement $(\forall x, x \notin \varnothing)$ is true.

Definition 2.1.3 (Subset)**.** A set A is said to be a **subset** of B, denoted $A \subseteq B$, if every element of A is an element of B. Logically, this means

$$A \subseteq B \iff (\forall x)(x \in A \implies x \in B).$$

We also say that A is *contained* in B, or B *contains* A.

The logical form of $A \subseteq B$ tells us how to prove it. This statement is a universally quantified implication (conditional), so to prove it, we pick any element x of the set A and prove that it is also an element of B.

Theorem 2.1.4. *For any sets, A, B, C,*

1. $\varnothing \subseteq A$.
2. $A \subseteq A$.
3. *If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Definition 2.1.5 (Set equality)**.** Two sets A, B are **equal** if they have exactly the same elements. Logically, this means

$$A = B \iff (\forall x)(x \in A \iff x \in B).$$

Since a biconditional is equivalent to the conditional in both directions, this means

$$A = B \iff (A \subseteq B \wedge B \subseteq A).$$

The above definition tells us we may prove set equality two ways. Either, we may prove both subset relations, or wee may string together a bunch of if and only if statements.

Definition 2.1.6 (Power set)**.** Given a set A, we form form the **power set** of A, denoted $\mathscr{P}(A)$, which is the set containing all subsets of A. In set builder notation this is:

$$\mathscr{P}(A) = \{X \mid X \subseteq A\}.$$

Example 2.1.7. Suppose $A = \{1, 2, 3\}$, then the power set is:

$$\mathscr{P}(A) = \big\{\varnothing, \{1\}, \{2\}.\{3\}.\{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\big\},$$

which has 8 elements. We will prove later that if a finite set has n elements, then its power set has 2^n elements.

Remark 2.1.8. By Theorem 2.1.4, we can see that for any set A, the power set $\mathscr{P}(A)$ always contains $\varnothing$ and A. Note also that $X \in \mathscr{P}(A)$ if and only if $X \subseteq A$. You will have to be careful not to confuse *subsets* with *elements*; the notions are different.

2.2 Set operations

Now that we have defined sets, let's remind ourselves that we already know of a few: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, the natural numbers, integers, rational numbers, real numbers and complex numbers. Having defined sets, we also want to know how we can combine them to form new sets, which is the purpose of this section.

Definition 2.2.1 (Union, intersection, difference)**.** Given two sets A, B there are three basic binary operations we can perform.

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

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

difference $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$

It is straightforward to see that union and intersection are each commutative and associative since disjunction ($\vee$) and conjunction ($\wedge$) are. Moreover, they distribute over each other for the same reason. In addition, you can think of set difference as being analogous to negation ($\neg$), a point which will be made clearer later. These facts are encapsulated in the following theorem which I encourage you to prove for yourself using if-and-only-if proofs for set equality.

Theorem 2.2.2. *The binary operations union and intersection are commutative, associative and distribute over each other. That is,*

$$\begin{aligned} A \cup B = B \cup A \quad &\textit{and} \quad A \cap B = B \cap A, \\ (A \cup B) \cup C = A \cup (B \cup C) \quad &\textit{and} \quad (A \cap B) \cap C = A \cap (B \cap C), \\ (A \cup B) \cap C = (A \cap C) \cup (B \cap C) \quad &\textit{and} \quad (A \cap B) \cup C = (A \cup C) \cap (B \cup C). \end{aligned}$$

Moreover, with the difference they satisfy a sort of De Morgan's Laws:

$$\begin{aligned} A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C), \\ A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C). \end{aligned}$$

In addition, the set difference satisfies a sort of double negation elimination, namely,

$$A \setminus \big(A \setminus (A \setminus B)\big) = A \setminus B.$$

Definition 2.2.3 (Disjoint)**.** Sets A, B are said to be **disjoint** if their intersection is empty, i.e., $A \cap B = \varnothing$.

Definition 2.2.4 (Set complement)**.** If there is a universe of discourse U which is specified, and a set A of elements from this universe, we can talk about the **complement** of A, denoted A^c, which is defined as $U \setminus A$.

The complement satisfies a few nice properties, and it *really* acts like negation. So, for example, $(A^c)^c = A$ and it satisfies De Morgan's Laws by virtue of Theorem 2.2.2, namely,

$$\begin{aligned} (A \cup B)^c &= A^c \cap B^c, \\ (A \cap B)^c &= A^c \cup B^c. \end{aligned}$$

In the theorem below we collect a few more facts about set operations, particularly how they interact with the subset relation.

Theorem 2.2.5. *For any sets A, B,*

- $A \subseteq A \cup B$
- $A \cap B \subseteq A$
- $A \cap \varnothing = \varnothing$
- $A \cup \varnothing = A$
- *if $A \subseteq B$, then $B^c \subseteq A^c$*
- $A \cap A^c = \varnothing$

- $A \cup A^c = U$

One other way to make new sets is to make *ordered tuples*. Remember, sets are unordered, but it is very useful to have objects with order to them. For example, when we considered points in the plane in algebra and calculus, we used to represent them by a *pair* of real numbers, like (a, b) where a is the horizontal offset from the origin, and b is the vertical offset. It is clear that $(0, 1) \neq (1, 0)$, so *order matters*.

Definition 2.2.6 (Cartesian product)**.** For sets A, B we can form their **Cartesian product** (or just **product**) which consists of all ordered pairs where the first component is an element of A and the second component is an element of B. Symbollically,

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

Note that your book calls the Cartesian product the "cross product." This is simply incorrect; no one refers to it this way. Cross products are either the operation on three (or seven) dimensional vectors you learned in Calculus, or they are much more complicated objects that involve group actions (you are not supposed to know what a group action is). Just never use the term cross product in place of Cartesian product.

Of course, we can form multiple Cartesian products to get order triples, or more generally, order n-tuples. For example,

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

When we take the Cartesian product of a set with itself, we use exponential notation for convenience, i.e.,

$$\underbrace{A \times A \times \cdots \times A}_{n} = A^n.$$

This is precisely why we use the notation $\mathbb{R}^n$ in linear algebra to denote collection of vectors (they are ordered n-tuples of real numbers).

To maintain a grasp of Cartesian products, you should keep in mind the analogy of rectangles. Consider the open intervals $A = (2, 3)$ and $B = (4, 7)$. Then since $A, B \subseteq \mathbb{R}$, we see that $A \times B \subseteq \mathbb{R}^2$, that is, it lies in the plane, so we can visualize it! In particular, $A \times B$ is the (open) rectangle in the plane whose x-values are between 2 and 3 and whose y-values are between 6 and 7. So, when you have some property about Cartesian products and you want to see if and/or why it is true, imagine first that your Cartesian products are rectangles in the plane. Hopefully this helps your intuition for the following theorem.

Theorem 2.2.7. *Suppose A, B, C, D are sets. Then*

- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$
- $A \times \varnothing = \varnothing$
- $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
- $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

2.3 Indexed families of sets

Finite operations are useful, but only so far. Of course, restricting attention to finite operations may be useful when you want to do computation, but often it is more useful to use more general operations to prove theorems, and only later come back to find an efficient way to compute.

Definition 2.3.1 (Family, collection)**.** A set whose elements are themselves sets is often called a **family** or **collection** of sets. Technically, we could just call this a set, but we often use one of these terms in order to aid our intuition and memory. Generally, we will use *script letters*, such as $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ to denote families of sets. Again, this is not necessary, merely a helpful practice.

Definition 2.3.2 (Arbitrary union)**.** If $\mathcal{A}$ is a family of sets, the **union over** $\mathcal{A}$ is the set whose elements are in at least one of the sets in $\mathcal{A}$. Logically, this means

$$x \in \bigcup_{A \in \mathcal{A}} A \iff (\exists A \in \mathcal{A})(x \in A).$$

Definition 2.3.3 (Arbitrary intersection)**.** If $\mathcal{A}$ is a family of sets, the **intersection over** $\mathcal{A}$ is the set whose elements are in all of the sets in $\mathcal{A}$. Logically, this means

$$x \in \bigcap_{A \in \mathcal{A}} A \iff (\forall A \in \mathcal{A})(x \in A).$$

Note that if $B \in \mathcal{A}$, then

$$\bigcap_{A \in \mathcal{A}} A \subseteq B \subseteq \bigcup_{A \in \mathcal{A}} A.$$

Example 2.3.4. Let $\mathcal{A}$ be the collection $\{A_n \mid n \in \mathbb{N}\}$ where $A_n := \{1, 2, \ldots, n\}$. Then

$$\bigcap_{A \in \mathcal{A}} A = \{1\} \qquad \bigcup_{A \in \mathcal{A}} A = \mathbb{N}.$$

In the above example, notice how we used $\mathbb{N}$ as a tool to specify our collection $\mathcal{A}$ using set builder notation. This is a common phenomenon and we give it a name. We call a set an **index set** if it plays a role similar to that of $\mathbb{N}$ in the previous example. Moreover, we say that it **indexes** the family $\mathcal{A}$, and we call $\mathcal{A}$ an **indexed family**. This is because we can access (or lookup) any set in the family $\mathcal{A}$ using an element of the index set. We call an elemenet of the index set an **index** (the plural of this is **indices**).

With this concept, we can rewrite the union and intersection with slightly different notation, which is often more useful:

$$\bigcup_{n \in \mathbb{N}} A_n := \bigcup_{A \in \mathcal{A}} A \qquad \bigcap_{n \in \mathbb{N}} A_n := \bigcap_{A \in \mathcal{A}} A$$

In fact, when the index set is $\mathbb{N}$ or some contiguous string of integers, we often write the union and intersection with notation similar to summation notation from Calculus. That is,

$$\bigcup_{n=1}^{\infty} A_n := \bigcup_{n \in \mathbb{N}} A_n,$$

and similarly,

$$\bigcup_{n=1}^{k} A_n := A_1 \cup A_2 \cup \cdots \cup A_k.$$

And similarly for intersections.

Definition 2.3.5 (Pairwise disjoint)**.** An indexed family $\mathcal{A} = \{A_\alpha \mid \alpha \in I\}$ of sets is said to be **pairwise disjoint** if for any $\alpha, \beta \in I$ with $\alpha \neq \beta$, $A_\alpha \cap A_\beta = \varnothing$, i.e., sets corresponding to different indices are disjoint.

2.4 Mathematical Induction

"Wait, induction? I thought math was *deductive*?" Well, yes, math *is* deductive and, in fact, mathematical induction is actually a deductive form of reasoning; if that doesn't make your brain hurt, it should. So, actually, mathematical *induction* seems like a misnomer, but really we give it that name because it *reminds us of inductive reasoning in science*.

I like to think of mathematical induction via an analogy. How can I convince you that I can climb a ladder? Well, first I show you that I can climb onto the first rung, which is obviously important. Then I convince you that for any rung, *if* I can get to that rung, *then* I can get to the next one.

Are you convinced? Well, let's see. I showed you I can get to the first rung, and then, by the second property, since I can get to the first rung, I can get to the second. Then, since I can get to the second rung, by the second property, I can get to the third, and so on and so forth. Thus I can get to any rung.

Theorem 2.4.1 (Principle of Mathematical Induction (PMI))**.** *If $S \subseteq \mathbb{N}$ with the properties:*

1. $1 \in S$,
2. *for all $n \in \mathbb{N}$, if $n \in S$, then $n + 1 \in S$,*

then $S = \mathbb{N}$. A subset of $\mathbb{N}$ is called ***inductive*** *if it has the second property listed above. An inductive set is some tail of the set of natural numbers (i.e. it is the natural numbers less some initial segment)*

If you are wondering about a proof of this theorem, then stop. We should actually call it a theorem, but instead, the definition of the natural numbers, but that's not important.

The cool thing about induction (we will henceforth drop the formality of "mathematical induction") is that it allows us to prove infinitely many statements. How does it do this? Suppose we have a proposition $P(n)$ for each natural number $n \in \mathbb{N}$ and we want to prove that for all $n \in \mathbb{N}$, the statement $P(n)$ is true. Well, we prove two things:

1. $P(1)$ (the base case), and
2. $(\forall n \in \mathbb{N})\big(P(n) \implies P(n+1)\big)$ (the inductive step).

Then the set $S = \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$ satisfies the conditions of Theorem 2.4.1 and so $S = \mathbb{N}$.

Example 2.4.2. Suppose we want to prove that for every $n \in \mathbb{N}$, 3 divides $n^3 - n$. Here, our proposition $P(n)$ is that 3 divides $n^3 - n$, and we want to prove $(\forall n \in \mathbb{N})(P(n))$.

We start by proving the base case. Note that $1^3 - 1 = 0 = 3 \cdot 0$, so the claim holds when $n = 1$.

We now prove the inductive step. Let $n \in \mathbb{N}$ be an arbitrary integer and suppose that 3 divides $n^3 - n$, so that $n^3 - n = 3k$ for some $k \in \mathbb{Z}$. Then Now notice that

$$(n+1)^3 - (n+1) = (n+1)\big((n+1)^2 - 1\big)$$

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

Thus 3 divides $(n+1)^3 - (n+1)$.

By the Principle of Mathematical Induction (PMI), for every $n \in \mathbb{N}$, 3 divides $n^3 - n$.

Induction also allows us to *define* infinitely many things at the same time. For example, consider the function $f(n) = n^2 - n + 2$. We will define a sequence of numbers a_n by:

$$a_1 = 0, \qquad a_{n+1} = f(a_n).$$

For those of you familiar with computer science or programming, you may think of this as a *recursively* defined sequence. Induction and recursion are two sides of the same coin; we won't address the difference here.

Definition 2.4.3 (Strong induction)**.**

2.5 Well-Ordering and Strong Induction

In this section we present two properties that are equivalent to induction, namely, the **well-ordering principle**, and **strong induction**.

Theorem 2.5.1 (Strong Induction)**.** *Suppose S is a subset of the natural numbers with the property:*

$$(\forall n \in \mathbb{N})\big(\{k \in \mathbb{N} \mid k < n\} \subseteq S \implies n \in S\big).$$

Then $S = \mathbb{N}$.

Proof. We prove by induction that for every $n \in \mathbb{N}$, $\{1, \ldots, n\}$

Base case. Notice that by taking $n = 1$, we see that $\{k \in \mathbb{N} \mid k < 1\} = \varnothing$ which is clearly a subset of S. Therefore, by the property of S, we find that $1 \in S$, so $\{1\} \subseteq \mathbb{N}$.

Inductive step. Let $n \in \mathbb{N}$ be arbitrary and suppose that $\{1, \ldots, n\} \subseteq S$. This is the same as the set $\{k \in \mathbb{N} \mid k < n+1\}$, so by the property of S, $n+1 \in S$. Therefore, $\{1, \ldots, n+1\} \subseteq S$.By induction, for every $n \in \mathbb{N}$, $\{1, \ldots, n\} \subseteq S$. Hence

$$\mathbb{N} = \bigcup_{n \in \mathbb{N}} \{1, \ldots, n\} \subseteq S.$$

We already knew $S \subseteq \mathbb{N}$, so they must in fact be equal. □

Theorem 2.5.2 (Well-Ordering Principle)**.** *Every nonempty subset of the natural numbers has a least element.*

Proof. Let S be a subset of natural numbers with no least element. Note that $1 \notin S$ (i.e., $1 \in S^c$) since 1 is the smallest natural number. Now let $n \in \mathbb{N}$ be arbitrary and suppose $\{1, \ldots, n\} \subseteq S^c$. Therefore $S \subseteq \{n+1, n+2, \ldots\} = \{k \in \mathbb{N} \mid k \geq n+1\}$. Thus $n+1 \notin S$ because otherwise it would be a least element. Hence $\{0, \ldots, n+1\} \subseteq S^c$. By Strong Induction, $S^c = \mathbb{N}$ and hence $S = \varnothing$. By contraposition, the desired result follows. □

Theorem 2.5.3. *The well-ordering principle implies the principle of mathematical induction.*

Proof. Suppose $\mathbb{N}$ has the well-ordering principle. Let $S \subseteq \mathbb{N}$ be any subset with the property that $1 \in S$ and for every $n \in \mathbb{N}$, $n \in S$ implies $n+1 \in S$. We wish to prove that $S = \mathbb{N}$.

Suppose to the contrary that $S \neq \mathbb{N}$. Then $S^c \neq \varnothing$, and so by the well-ordering principle has a least element $k \in S^c$. Since $1 \in S$, $k \neq 1$, so $k-1 \in \mathbb{N}$. Moreover, we must have $k-1 \in S$ since k is the minimal element of S^c. By the property assumed by S for the value $n = k-1$, we find $k \in S$ which is a contradiction.

Therefore, our assumption that $S \neq \mathbb{N}$ was false, and hence $S = \mathbb{N}$. In other words, $\mathbb{N}$ has the principle of mathematical induction. □

We now recall the division algorithm, but we can provide a proof this time.

Theorem 2.5.4 (Division Algorithm)**.** *For any integers a, b with $a \neq 0$, there exists unique integers q and r for which*

$$b = aq + r, \quad 0 \leq r < |a|\,.$$

The intger b is called the ***dividend****, a the* ***divisor****, q the* ***quotient****, and r the* ***remainder****.*

Proof. Let $a, b \in \mathbb{Z}$ with a nonzero. For simplicity, we will assume that $a > 0$ because the proof when $a < 0$ is similar. Consider the set of integers $A = \{b - ak \mid k \in \mathbb{Z}, b - ak \geq 0$. This set is clearly nonempty, for if $b \geq 0$ then $b - a0 = b \geq 0$ is in A, and if $b < 0$ then $b - ab = b(1-a) \geq 0$ is in A.

By the Well-Ordering Principle, A has a minimum element, which we call r, and some integer which we call q so that $r = b - aq$. Then $r \geq 0$ and notice that $r - a = b - aq - a = b - a(q+1)$. Since $a > 0$, $r - a < r$. By the minimality of r, we know $r - a < 0$ or equivlaently, $r < a$.

Now suppose there are some other integers q', r' with $0 \leq r' < a$ and $b = aq' + r'$. Then $aq + r = aq' + r'$ and hence $r - r' = aq - aq' = a(q - q')$. Now $-a < -r' \leq r - r' \leq r < a$ and hence $a\,|q - q'| = |a(q-q')| = |r - r'| < a$. Dividing through by a, we obtain $|q - q'| < 1$ and since $q - q' \in \mathbb{Z}$ it must be zero. Hence $q = q'$ and so also $r = r'$. □

Lemma 2.5.5. *If $a, b \in \mathbb{Z}$ are nonzero and relatively prime and if a, b divide c, then ab divides c.*

Proof. Let a, b be nonzero relatively prime integers which divide some integer c. Since a, b divides c there exist integers r, s for which $c = ar = bs$. Since $\gcd(a, b) = 1$, by Theorem 1.7.5 there exist integers, x, y for which $ax + by = 1$. Multipliying by c and using the division properties above we find

$$c = acx + bcy = absx + abry = ab(sx + ry),$$

so ab divides c. □

2.6 Principles of counting

It is often useful in both pure and applied mathematics to count the sizes of finite sets. In this section we prove some basic theorems of this sort. If A is a set, let $|A|$ denote the number of elements in A. Note that $\varnothing$ is a finite set with $|\varnothing| = 0$.

Theorem 2.6.1 (Sum Rule)**.** *If A, B are disjoint finite sets then $|A \cup B| = |A| + |B|$. More generally, if $A_1, \ldots, A_n$ is a pairwise disjoint collection of finite sets, then*

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{j=1}^{n} |A_j| \, .$$

Proof. Obvious, but we omit the technical proof until we have a proper discussion of the definition of the *number* of elements in a set, which won't occur until Chapter 5. □

Theorem 2.6.2. *For finite sets A, B, which are not necessarily disjoint,*

$$|A \cup B| = |A| + |B| - |A \cap B| \, .$$

Proof. Obvious when you look at a Venn diagram, but we omit the technical proof for similar reasons. □

Theorem 2.6.3 (Inclusion–Exclusion Principle)**.** *Let $A_1, \ldots, A_n$ be a collection of finite sets. Then*

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{j=1}^{n} \left((-1)^{j+1} \sum_{1 \le n_1 < \cdots < n_j \le n} \left| \bigcap_{k=1}^{j} A_{n_k} \right| \right) .$$

In the above formula the sum is taken over all subcollections of j different sets from among $A_1, \ldots, A_n$. In particular, when $n = 3$, the above becomes

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = \quad & \big(|A_1| + |A_2| + |A_3| \big) \\ & - \big(|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| \big) \\ & + |A_1 \cap A_2 \cap A_3| \end{aligned}$$

Proof. By induction and using Theorem 2.6.3. □

Theorem 2.6.4 (Product Rule)**.** *If A, B are disjoint finite sets then $|A \times B| = |A| \cdot |B|$. More generally, if $A_1, \ldots, A_n$ is a pairwise disjoint collection of finite sets, then*

$$|A_1 \times A_2 \times \cdots \times A_n| = \prod_{j=1}^{n} |A_j| \, .$$

Proof. Using induction and the Sum Rule. □

Definition 2.6.5 (Permutation (combinatorics))**.** A **permutation** of a finite set is an arrangement of the elements in a particular order.

For the next theorem, recall that the **factorial** of a positive integer n is defined inductively by

$$\begin{aligned} 0! &= 1 \\ n! &= n(n-1)! \end{aligned}$$

Equivalently, $n! = n(n-1)(n-2) \cdots 1$.

Theorem 2.6.6. *The number of permutations of a set with n elements is $n!$*

Proof. By induction on the number of elements in the set. □

Theorem 2.6.7. *If $n \in \mathbb{N}$ and $r \in \mathbb{Z}$ with $0 \le r \le n$, then the number of permutations of any r distinct objects from a set of n objects is*

$$\frac{n!}{(n-r)!} = n(n-1)(n-2)\cdots(n-r+1).$$

Proof. By induction on r and Theorem 2.6.6. □

Definition 2.6.8 (Combination)**.** For $n \in \mathbb{N}$ and $r \in \mathbb{Z}$ with $0 \le r \le n$, a **combination** of r elements from a set of size n is just a subset of size r.

The number of combinations is called the **binomial coefficient** and is denoted $\binom{n}{r}$. We read this symbol as "n choose r."

Theorem 2.6.9 (Combination Rule)**.** *We have the following formula for the binomial coefficients:*

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

Proof. Note that the number of permutations of any r distinct objects from a set of n objects is necessarily the number of subsets of size r (i.e., the number of combinations, the binomial coefficient) times the number of ways to arrange those r elements (i.e., permutations of a set of size r). Therefore, by Theorem 2.6.6 and Theorem 2.6.7, we have

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

thereby proving the result. □

Note: the above theorem guarantees $\binom{n}{r} = \binom{n}{n-r}$.

Theorem 2.6.10 (Binomial Theorem)**.** *If $n \in \mathbb{N}$ and $a, b \in \mathbb{R}$, then*

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

Proof. By induction and using the fact that when $r \ge 1$,

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1},$$

which you should prove. This displayed equation essentially says that Pascal's triangle generates the binomial coefficients. □

Chapter 3

Relations and partitions

3.1 Relations

Definition 3.1.1 (Relation)**.** For sets A, B, a **relation** *from A to B* is a subset R of the Cartesian product $A \times B$. Elements $a \in A$ and $b \in B$ are said to be **related** if $(a, b) \in R$. Moreover, we often write a relation with infix notation, as $a \, R \, b$.

When $A = B$, which is perhaps more common, we just call R a *relation on A*.

Note that *any* set of ordered pairs from A and B is a relation. Most of them we don't find particularly interesting, but others are incredibly interesting. Soon we will study some properties of interesting relations.

Example 3.1.2. Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4, 5\}$ and consider the relation R from A to B given by

$$R = \{(1, 2), (1, 4), (2, 3), (2, 5), (3, 2), (3, 1)\}.$$

Then, $2 \, R \, 3$, $3 \, R \, 2$, $1 \, R \, 2$ but $2 \not R \, 1$. Moreover, $1 \, R \, 4$, but saying $4 \, R \, 1$ or $4 \not R \, 1$ doesn't even make sense since $4 \notin A$ and hence $(4, 1) \notin A \times B$.

Example 3.1.3. The "less than" relation $<$ is a relation on $\mathbb{R}$, with which you are undoubtedly familiar. You probably aren't used to thinking of this as a subset of the plane $\mathbb{R}^2$, but it can be. In particular, $x < y$ if and only if the point (x, y) lies *above* the line $y = x$ in the plane. The reason we need to recognize things like less than as a set is because we are using set theory as the foundation of mathematics.

Example 3.1.4. Here is an example of a relation on $\mathbb{Z}$, which is called the **divides** relation. Given $a, b \in \mathbb{Z}$, we say a divides b and write $a \mid b$, if there exists some integer k so that $b = ak$. Note, although technically $\mid$ is a subset of $\mathbb{Z}^2$, we almost never think of it that way, and it would look kind of weird to write $(2, 6) \in \mid$ as opposed to $2 \mid 6$.

Definition 3.1.5 (Domain, Range)**.** The **domain** of a relation R from A to B is the subset of A given by

$$\operatorname{dom}(R) = \{x \in A \mid (\exists y \in B)(x \, R \, y)\}.$$

Similarly, the **range** of R is the subset of B given by

$$\operatorname{rng}(R) = \{y \in B \mid (\exists x \in A)(x \, R \, y)\}.$$

Definition 3.1.6 (Identity relation)**.** The **identity relation** on a set A is the relation $I_A := \{(x,x) \mid x \in A\}$. In other words, a pair of elements from A are related if and only if they are equal. This could also be called the equality relation.

Definition 3.1.7 (Inverse relation)**.** If R is a relation from A to B, the **inverse relation** R^{-1} is the relation from B to A given by

$$R^{-1} = \{(b,a) \in B \times A \mid a \mathrel{R} b\}.$$

Note that $(R^{-1})^{-1} = R$.

Exercise 3.1.8. What is the inverse of the less than relation on $\mathbb{R}$?

Exercise 3.1.9. Consider a relation R on $\mathbb{R}$. Since $R \subseteq \mathbb{R}^2$, we can think of this as some geometric subset of the plane. Describe how R and R^{-1} are related geometrically.

Hint. If you are having trouble, consider a few *very* simple examples along with the less than relation. Remember, whatever the geometric transformation is, applying it twice should give you the original set back since $(R^{-1})^{-1} = R$.

Theorem 3.1.10. *Given a relation R, we have*

1. $\operatorname{dom}(R^{-1}) = \operatorname{rng}(R)$*;*
2. $\operatorname{rng}(R^{-1}) = \operatorname{dom}(R)$*.*

Definition 3.1.11 (Relation Composition)**.** Given relations R, S from A to B and from B to C, respectively, we can form the **composite relation** $S \circ R$ from A to C as

$$\{(a,c) \in A \times C \mid (\exists b \in B)(a \mathrel{R} b \land b \mathrel{R} c)\}.$$

Theorem 3.1.12. *Let A, B, C, D be sets with relations R, S, T from A to B, B to C, and C to D, respectively. Then*

1. $(R^{-1})^{-1} = R$*;*
2. $T \circ (S \circ R) = (T \circ R) \circ S$*;*
3. $I_B \circ R = R$ *and* $R \circ I_A = R$*;*
4. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$*.*

Proof. Left as an exercise for the reader. These follow directly from the definitions. □

3.2 Equivalence relations

Definition 3.2.1 (Reflexive)**.** A relation R on A is said to be **reflexive** if $x \mathrel{R} x$ for all $x \in A$. Analogously, it is said to be **irreflexive** if $x \not\mathrel{R} x$ for all $x \in A$.

Definition 3.2.2 (Symmetric)**.** A relation R on A is said to be **symmetric** if for all $x, y \in A$ $x \mathrel{R} y$ if and only if $y \mathrel{R} x$.

Definition 3.2.3 (Transitive)**.** A relation R on A is said to be **transitive** if for all $x, y, z \in A$, if $x \mathrel{R} y$ and $y \mathrel{R} z$, then $x \mathrel{R} z$

Definition 3.2.4 (Antisymmetric)**.** A relation R on a set A is said to be **antisymmetric** if for all $x, y \in A$, if $x \, R \, y$ and $y \, R \, x$, then $x = y$.

Example 3.2.5. Let us consider a few examples:

- The less than relation on $\mathbb{R}$ is irreflexive, antisymmetric, and transitive.
- The divides relations on $\mathbb{N}$ is reflexive, antisymmetric, and transitive.
- Equality is a relation which is reflexive, symmetric, and transitive.
- The subset relation is reflexive, antisymmetric, and transitive.
- Trust is a relation which is reflexive (probably?), neither symmetric nor antisymmetric, and not transitive.
- For the relation from Example 3.1.2 we cannot even talk about it being reflexive, irreflexive, symmetric, antisymmetric, or transitive because it is a relation between two *different* sets.
- The relation R on $\mathbb{R}$ given by $x \, R \, y$ if and only if $\sin x = \sin y$ is clearly reflexive, symmetric and transitive.

Exercise 3.2.6. Prove that the only relations R on A which are both symmetric and antisymmetric are subsets of the identity relation I_A.

Solution. Recall that $I_A = \{(a, a) \in A^2 \mid a \in A\}$. Let R be a symmetric and antisymmetric relation on A. Then for all $x, y \in A$, if $x \, R \, y$ then $y \, R \, x$ by symmetry, and hence by antisymmetry, $x = y$. Thus, a pair can only be in R if it is of the form (x, x) for some $x \in A$. Hence $R \subseteq I_A$.

A few corollaries of this fact are that the only symmetric, antisymmetric, reflexive relation is the identity, and the only symmetric, antisymmetric, irreflexive relation is the empty relation.

Exercise 3.2.7. Prove that a relation R on a set A is symmetric if and only if $R = R^{-1}$.

Solution. Suppose that R is a symmetric relation on A. Then for all $x, y \in A$, we have $x \, R \, y$ if and only if $y \, R \, x$ (by symmetry) if and only if $x \, R^{-1} \, y$ (by definition of inverse). This proves that symmetric relations are equal to their own inverses.

Now suppose that $R = R^{-1}$, then all we do is rearrange the if and only if statements from above. Then for all $x, y \in A$, we have $x \, R \, y$ if and only if $y \, R^{-1} \, x$ (by definition of inverse) if and only if $y \, R \, x$ (by $R = R^{-1}$). This proves that relations which are equal to their own inverses are symmetric.

Exercise 3.2.8. A relation R on $\mathbb{R}$ can be viewed as a subset of the plane $\mathbb{R}^2$ as we have already disussed. For each of the properties on the relation R given below, provide its geometric equivalent.

1. reflexive
2. irreflexive
3. symmetric
4. antisymmetric
5. transitive

Solution.

1. reflexive: contains the diagonal line $y = x$.
2. irreflexive: does not contain the diagonal line $y = x$.
3. symmetric: symmetric about the line $y = x$, i.e., when reflected about this line, the set doesn't change.
4. antisymmetric: the only points that lie both in this set and its reflection about the line $y = x$ are perhaps some points on the diagonal.
5. transitive: this one is harder to see. If points P and Q lie in the relation, and if Q lies on the vertical line through the reflection of the point P across the line $y = x$, then the point of intersection of the vertical line through P and the horizontal line through Q also lies in the relation.

Exercise 3.2.9. Prove the fact discussed in the example above: the divides relation on $\mathbb{N}$ is reflexive, antisymmetric and transitive.

The divides relation on $\mathbb{Z}$ is also reflexive and transitive, but it is not quite antisymmetric. Why isn't it antisymmetric on $\mathbb{Z}$? Once you have proven it is antisymmetric on $\mathbb{N}$, ask yourself what does wrong in the proof when you switch from $\mathbb{N}$ to $\mathbb{Z}$.

Solution. Let $x, y, z \in \mathbb{N}$ be arbitrary. Clearly, $x \mid x$ since $x = 1x$, so divides is reflexive.

If $x \mid y$ and $y \mid x$, then there exist positive integers m, n so that $y = mx$ and $x = ny$. Then $y = mx = m(ny) = (mn)y$ and hence by cancellation $1 = mn$ and so $m = n = 1$ since $m, n \in \mathbb{N}$. Therefore, $x = y$ and so divides is antisymmetric.

If $x \mid y$ and $y \mid z$, then there exist positive integers p, q so that $y = px$ and $z = qy$. Then $z = qy = q(px) = (qp)x$ so $x \mid z$.

Hopefully, from the previous examples, you saw that a bunch of relations have nice properties. Actually, it is more accurate to say that relations we find interesting have certain collections of nice properties. These are summarized in the next two definitions.

Definition 3.2.10 (Equivalence relation)**.** A relation R on a set A is said to be an **equivalence relation** if it is reflexive, symmetric and transitive.

Definition 3.2.11 (Modular congruence)**.** Let n be a fixed positive integer called the **modulus** of congruence. For $x, y \in \mathbb{Z}$, we say x is **congruent modulo** n to y if n divides $x - y$. In this case we write $x \cong_n y$ or $x = y($ mod $n)$.

Exercise 3.2.12. Show that congruence modulo n ($\cong_n$) is an equivalence relation.

Definition 3.2.13 (Equivalence class)**.** Let $\sim$ be an equivalence relation on a set A. For $x \in A$, the equivalence class of x is

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

The set of equivalence classes of elements of A is denoted by $A/\sim$

Definition 3.2.14 (Partition)**.** A **partition** of a set A is a collection $\mathcal{P}$ of subsets of A which is pairwise disjoint and whose union is A.

Theorem 3.2.15. *Let $\sim$ be an equivalence relation on the set A. Then the set of equivalences class $A/\sim$ partitions A.*

Proof. Notice that since $\sim$ is reflexive, for every $x \in A$, $x \sim x$ and therefore $x \in [x] \in A/\sim$. Therefore, the union over $A/\sim$ is A.

Now suppose $[x], [y] \in A/\sim$ and $[x] \cap [y] \not\emptyset$. Then there is some $z \in [x] \cap [y]$, so $x \sim z$ and $z \sim y$ (by definition and symmetry of $\sim$. Therefore $x \sim y$ by transitivity. Now let $w \in [x]$, then $w \sim x$, so $w \sim y$ by transitivity, and hence $w \in [y]$. Thus $[x] \subseteq [y]$. A symmetric argument proves the reverse inclusion, and thus $[x] = [y]$. So we have proven that equivalence classes are either disjoint, or they are the same set, and hence $A/\sim$ is a pairwise disjoint collection, and hence also forms a partition of A. □

Theorem 3.2.16. *Let $\mathcal{A}$ be a partition of A. Define a relation $\sim$ on A by $x \sim y$ if and only if there is some $[z] \in A/\sim$ with $x, y \in [z]$. Prove that $\sim$ is an equivalence relation on A.*

Proof. Exercise on the review sheet with a solution there. □

3.3 Order relations

Definition 3.3.1 (Partial order, total order)**.** A relation R on a set A is said to be a **partial order** if it is reflexive, antisymmetric, and transitive. A partial order is said to be a **total order** if for any $x, y \in A$ either $x\,R\,y$ or $y\,R\,x$.

Remark 3.3.2. Note, some authors require partial orders to be irreflexive instead of reflexive. All that this requires is to delete the diagonal from the relation. Basically everything that can be proven about partial orders in our formulation can be proven in the other formulation, and vice versa. Instead, we we call a relation that is irreflexive, symmetric and transitive a **strict partial order**.

Definition 3.3.3 (Minim(al/um), Maxim(al/um))**.** Let $\prec$ be a partial order on a set A. An element $x \in A$ is said to be **minimal** relative to the ordering $\prec$ if for every $y \in A$, $y \not\prec x$. In other words, there are no elements smaller than x. **Maximal** elements are defined analogously.

An element $x \in A$ is said to be a **minimum** if for all $y \in A$, $x \prec y$. **Maximum** elements are defined analogously.

Exercise 3.3.4. Prove that if A has a minimum element relative to the partial order $\prec$, then it is unique (similarly for maximum elements).

Exercise 3.3.5. Consider the less than partial order $<$ on the real numbers $\mathbb{R}$. Does it have maximum or minimum elements? What about maximal or minimal elements?

Exercise 3.3.6. Consider a universe U and the subset relation on the subsets of U. Does U have maximum and minimum elements?

Exercise 3.3.7. Consider the divides partial order on $\mathbb{N} \setminus \{1\}$, i.e., then integers greater than or equal to 2. Describe the minimal elements of this partial order and explain your reasoning.

Exercise 3.3.8. Suppose $\prec$ is a total order on A. There is an induced ordering $\prec_n$ on A^n call the **lexicographical ordering** or **dictionary order**.

It works like this, given $(x_1, \dots, x_n), (y_1, \dots, y_n) \in A^n$, if $x_j = y_j$ for all $j = 1, \dots, n$ then $(x_1, \dots, x_n) \prec_n (y_1, \dots, y_n)$. Otherwise, let k be the first index for which $x_k \neq y_k$. If $x_k \prec y_k$, then $(x_1, \dots, x_n) \prec_n (y_1, \dots, y_n)$, and otherwise $(y_1, \dots, y_n) \prec_n (x_1, \dots, x_n)$.

Prove that $\prec_n$ is a total order on A^n.

Definition 3.3.9 (Well order)**.** A total order $\prec$ on A is said to be a **well order** if every nonempty subset of A has a minimum element with respect to A.

Remark 3.3.10. On $\mathbb{N}$, we know that $<$ is a well-order. This is precisely the content of the Well-Ordering Principle.

Exercise 3.3.11. Is $<$ a well ordering on $\mathbb{R}, \mathbb{Q}$ or $\mathbb{Z}$?

Do you think $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ have well-orders of some form or another?

Theorem 3.3.12. *Every set can be well-ordered.*

Remark 3.3.13. This theorem seems absolutely ridiculous. What does a well-order of $\mathbb{R}$ look like? The answer is, in short, we don't know. It is actually impossible to write down a formula for one. However, the proof of this theorem and hence the existence of such a well-order is a consequence of the **Axiom of Choice**, which was originally the most highly contested axiom of early set theory, but not it is almost ubiquitously accepted. Why? Because it makes lots of nice theorems true, like the previous ones (it also makes some very annoying theorems true, but that is a discussion for another day). We will state the Axiom of Choice after we discussion functions.

Theorem 3.3.14. *Let $\prec$ be a partial order on A and let $a \in A$ be a minimum. Then a is the unique minimal element.*

Proof. We first show a is minimal. Notice that for any $b \in A$, we have $a \prec b$ since a is a minimum. If $a \neq b$, then by antisymmetry $b \not\prec a$, so a is minimal.

Now suppose that c is minimal. Since a is a minimum, $a \prec c$. By minimality, this can only happen if $a = c$. □

Remark 3.3.15. There is an analogue of Theorem 3.3.14 for maximum and maximal elements.

3.4 Graphs

A **graph** is a fundamental and important object in modern mathematics. Graphs often connect pure and applied math, as well as linking both of these with statistics.

Definition 3.4.1 (Graph)**.** A **graph** is a pair $G = (V, E)$ of **vertices** V and **edges** $E \subseteq V^2$.

It is useful to think of a graph as a bunch of nodes (the vertices) connected in a network (the edges).

Chapter 4

Functions

4.1 Functions as relations

Definition 4.1.1 (Function)**.** A **function** f from A to B, denoted $f : A \to B$, is a relation from A to B such that for every $x \in A$ there exists a unique $y \in B$ for whcih $(x, y) \in f$. Instead, we use the more familiar notation $f(x) = y$ to mean the same thing. In this context, x is called the **argument**, y the **value**. We could also refer to f as a **map** (or **mapping**), and sometimes we call y the **image** of x under f. The set A is called the **domain**, and B is the **codomain**. A function cannot be specified without also specifying it domain and codomain!

So, functions are just special relations, and relations are just sets. Thus, all your familiar mathematical objects are turning into sets! Now, since functions are just sets, what we mean when we say that two functions are equal is that they are equal *as sets!* Thankfully, the following theorem establishes that this means precisely what we would expect.

Theorem 4.1.2. *Functions f, g are equal if and only if*

1. $\operatorname{dom} f = \operatorname{dom} g$*, and*

2. *for all $x \in \operatorname{dom} f$, $f(x) = g(x)$.*

Proof. See the textbook. □

Theorem 4.1.3. *Let $f : A \to B$, $g : B \to C$ be functions. Then the composite relation $g \circ f$ is also a function.*

Proof. Let $x \in A$. Then since f is a function, there is a *unique* $y \in B$ for which $(x, y) \in f$. Since g is a function, there is a *unique* $z \in C$ for which $(y, z) \in g$. Therefore, $(x, z) \in g \circ f$. Now suppose $(x, c) \in g \circ f$. Then there exists some $b \in B$ for which $(x, b) \in f$ and $(b, c) \in g$. Since y is unique, $b = y$, and then since z is unique $c = z$. Thus, for every $x \in A$ there exists a unique $z \in C$ for which $(x, z) \in g \circ f$, so $g \circ f$ is a function. □

Remark 4.1.4. Recall the identity relation on A defined by $I_A := \{(a, a) \mid a \in A\}$. Note that I_A is actually a function because if $(a, b) \in I_A$, then $b = a$, so there is only one value associated to the argument a, namely, a itself. So, $I_A : A \to A$ is just the function $I_A(a) = a$.

By properties of relations that we discussed before, if $f : A \to B$ is any function, then $f \circ I_A = f$ and $I_B \circ f = f$.

Some functions are related to others by changing only the domain. For example, one could have a larger domain than the other, but on the smaller domain, the functions are equal. The next definition provides us the means to talk about such functions.

Definition 4.1.5 (Restriction)**.** Let $f : A \to B$ and suppose $D \subseteq A$. The **restriction** of f to D is the function

$$f|_D = \{(x, y) \mid x \in D, y = f(x)\}.$$

If g, h are functions and g is a restriction of h, we also say that h is an **extension** of g.

Theorem 4.1.6. *Composition of functions is associative. That is, if $f : A \to B$, $g : B \to C$, $h : C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$.*

Proof. Suppose $(w, z) \in (h \circ g) \circ f$. Then there exists some $x \in B$ for which $(w, x) \in f$ and $(x, z) \in h \circ g$. Then there also exists some $y \in C$ for which $(x, y) \in g$ and $(y, z) \in h$. Thus, $(w, y) \in (g \circ f)$ and hence $(w, z) \in h \circ (g \circ f)$. Therefore $(h \circ g) \circ f \subseteq h \circ (g \circ f)$.

Suppose $(w, z) \in h \circ (g \circ f)$. Then there exists some $y \in C$ for which $(w, y) \in g \circ f$ and $(y, z) \in h$. Then there also exists some $x \in B$ for which $(w, x) \in f$ and $(x, y) \in g$. Thus, $(x, z) \in (h \circ g)$ and hence $(w, z) \in (h \circ g) \circ f$. Therefore $h \circ (g \circ f) \subseteq (h \circ g) \circ f$. □

Theorem 4.1.7. *Let $f : A \to B$ and $g : C \to D$. If the functions agree on their common domain $A \cap C$, i.e., if the restrictions satisfy $f|_{A\cap C} = g|_{A\cap C}$, then the set $f \cup g$ is a function from $A \cup C$ to $B \cup D$ and it is defined by*

$$(f \cup g)(x) := \begin{cases} f(x) & \text{if } x \in A, \\ g(x) & \text{if } x \in C. \end{cases}$$

Proof. Exercise for the reader. □

Definition 4.1.8. Let A, B be sets with (strict) partial orders $\prec_A, \prec_B$. A function $f : A \to B$ is said to be (resp., strictly) **increasing** if whenever $x, y \in A$ with $x \prec_A y$, then $f(x) \prec_B f(y)$. Simiarly, it is said to be (resp., strictly) **decreasing** if whenever $x, y \in A$ with $x \prec_A y$, then $f(y) \prec_B f(x)$.

Exercise 4.1.9. Prove that the function $f : (0, \infty) \to \mathbb{R}$ given by the formula $f(x) = \frac{1}{x}$ is strictly decreasing.

4.2 Injective, surjective and bijective functions

Definition 4.2.1. A function $f : A \to B$ is said to be **injective** (or **one-to-one**, or **1-1**) if for any $x, y \in A$, $f(x) = f(y)$ implies $x = y$. Alternatively, we can use the contrapositive formulation: $x \neq y$ implies $f(x) \neq f(y)$, although in practice usually the former is more effective.

Note: injective functions are precisely those functions f whose inverse relation f^{-1} is also a function. You should prove this to yourself as an exercise.

Exercise 4.2.2. Let $f : A \to B$ be a function and f^{-1} its inverse relation. Then f is injective if and only if the restriction $f^{-1}|_{\text{rng}(f)}$ is a function.

Definition 4.2.3. A function $f : A \to B$ is said to be **surjective** (or **onto**) if $\text{rng}(f) = B$. That is, for every $b \in B$ there is some $a \in A$ for which $f(a) = b$.

Definition 4.2.4. A function $f : A \to B$ is said to be **bijective** (or **one-to-one and onto**) if it is both injective and surjective. We also say that f is a **one-to-one correspondence**.

Theorem 4.2.5. *The composition of injective functions is injective and the compositions of surjective functions is surjective, thus the composition of bijective functions is bijective. That is, let $f : A \to B$ and $g : B \to C$.*

1. *If f, g are injective, then so is $g \circ f$.*
2. *If f, g are surjective, then so is $g \circ f$.*
3. *If f, g are bijective, then so is $g \circ f$.*

Proof. Suppose f, g are injective and suppose $(g \circ f)(x) = (g \circ f)(y)$. That means $g(f(x)) = g(f(y))$. Since g is injective, $f(x) = f(y)$. Since f is injective, $x = y$. Thus $g \circ f$ is injective.

Suppose f, g are surjective and suppose $z \in C$. Since g is surjective, there exists some $y \in B$ with $g(y) = z$. Since f is surjective, there exists some $x \in A$ with $f(x) = y$. Therefore $z = g(f(x)) = (g \circ f)(x)$ and so $z \in \operatorname{rng}(g \circ f)$. Thus $g \circ f$ is surjective.

If f, g are bijective then $g \circ f$ is also bijective by what we have already proven. □

Exercise 4.2.6. Determine whether or not the restriction of an injective function is injective. If it is, prove your result. If it isn't, provide a counterexample.

As we established earlier, if $f : A \to B$ is injective, then the restriction of the inverse relation $f^{-1}|_{\operatorname{rng}(f)} : \operatorname{rng}(f) \to A$ is a function. Moreover, if $f : A \to B$ is bijective, then $\operatorname{rng}(f) = B$, and so the inverse relation $f^{-1} : B \to A$ is a function itself. The next theorem says that even more is true: if $f : A \to B$ is bijective, then $f^{-1} : B \to A$ is also bijective.

Theorem 4.2.7. *Suppose $f : A \to B$ is bijective, then the inverse function $f^{-1} : B \to A$ is also bijective.*

Proof. Suppose $b, y \in B$ with $f^{-1}(b) = a = f^{-1}(y)$. Thus $b = f(a) = y$, so f^{-1} is injective.

Now suppose $a \in A$ and let $b = f(a)$. Then $f^{-1}(b) = a$. Thus $A = \operatorname{rng}(f^{-1})$ and so f^{-1} is surjective. □

Definition 4.2.8. Let A be a nonempty set. A **permutation** of A is a bijection from A to itself.

Notice that we now have two different instances of the word permutation, doesn't that seem confusing? Well, let's see that they aren't that different after all. Let A be a nonempty finite set with n elements $a_1, \ldots, a_n$. Then let $f : A \to A$ be a permutation (as defined above). Then $f(a_1), \ldots, f(a_n)$ is some ordering of the elements of A, i.e. a permutation in the sense of combinatorics. Notice that nothing in this list is repeated (because f is injective) and every element of A is listed (because f is surjective). So, every function permutation gives us a combinatorial permutation.

However, we also need to go the other way. Let $b_1, \ldots, b_n$ be a (combinatorial) permutation of the elements of A. Define a function $f : A \to A$ by $f(a_1) = b_1$. Since any element of A is only listed once in the list $b_1, \ldots, b_n$, then f is injective. Since every element of A occurs somewhere in the list $b_1, \ldots, b_n$, then f is surjective.

So, what is the difference between a combinatorial permutation and a function permutation? Well, two things: one is the way we think about it, but here each viewpoint provides some perspective on the other. However, the other difference is perhaps much more interesting: combinatorial permutations can only be applied to *finite* sets, while function permutations can apply even to *infinite* sets! This means that a permutation $f : \mathbb{N} \to \mathbb{N}$ can be thought of as "reordering" the elements of $\mathbb{N}$.

Theorem 4.2.9. *Let A be a nonempty set.*

1. *The identity map I_A is a permutation.*
2. *The composition of permutations is a permutation.*
3. *The inverse of a permutation is a permutation.*
4. *If f is a permutation, then $f \circ I_A = f = I_A \circ f$.*
5. *If f is a permutation, then $f \circ f^{-1} = I_A = f^{-1} \circ f$.*
6. *If f, g are permutations of A, then $(g \circ f) = f^{-1} \circ g^{-1}$.*

Proof. All of these statements follow directly from already proven results. □

The above theorem is probably one of the most important we have encountered. Basically, it says that the permutations of a set A form a mathematical structure called a **group**. A group is just a set of things (in this case, permutations) together with a binary operation (in this case, composition of functions) that satisfy a few properties:

- the binary operation is associate (we already proved this about function composition),
- applying the binary operation to two things in the set keeps you in the set (Item 2 above),
- there is an identity for the binary operation, i.e., an element such that applying the operation with something else leaves that thing unchanged (Item 1 and Item 4 above),
- every element has an inverse for the binary operation, i.e., an element such that applying the operation to an element and its inverse yeilds the identity (Item 3 and Item 5 above),

Chances are, you have never heard of a group, but they are a fundamental tool in modern mathematics, and they are the foundation of modern algebra. Groups will be the sole object of study for the entirety of MATH-320!

Groups were invented (or discovered, depending on your metamathematical philosophy) by Évariste Galois, a French mathematician who died in a duel (over a girl) at the age of 20 on 31 May, 1832, during the height of the French revolution. Galois invented groups in order to solve, or rather, *not* to solve an interesting open problem.

In high school algebra, you learn that a quadratic equation of the form $ax^2+bx+c = 0$ has two (or one repeated) solutions of the form $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$, and these solutions always exist provided we allow for complex numbers. This formula was known even to the Greeks, although they dismissed the complex solutions.

There is a similar, albeit significanlty more complicated, fomula for the solutions of a cubic equation $ax^3 + bx^2 + cx + d = 0$ in terms of the coefficients a, b, c, d and using only the operations of addition, subtraction, multiplication, division and extraction of roots. There is another similar formula for quartic equations, but the cubic and the quartic forumlae were not discovered until the middle of the second millenia A.D.!

Then for a few hundred more years, mathematicians search for a formula to the quintic equation satisfying these same properties. Galois invented groups in order to solve this problem. Although, instead of finding a formula, he proved that *no such formula exists* for the quintic, or indeed for any higher degree polynomial. When we say that no such formula exists, we mean there is no formula involving only the coefficients and the operations mentioned; there are other ways to find roots of higher degree polynomials. It should be noted that Niels Henrik Abel *also* proved that the quintic is unsolvable, and his solution appeared earlier than that of Galois, although Abel did not generalize his result to all higher degree polynomials. It is clear, however, that Galois did not know of Abel's solution, and the idea of a group was revolutionary.

Chapter 5

Homework

5.1 Intro

Here you will find the homework listed for each week. Homework is due on the Tuesday following the week it is assigned, e.g., homework assigned for Week One is due on the following Tuesday of Week 2, which means you will have 5 days to complete the homework.

If you wish, you may type your solutions to the homework (I would be forever grateful). However, please do not use Microsoft Word or similar word processing software. Instead, use LaTeX, which is typesetting software which is especially good for mathematics. If you are a math major, you must learn LaTeX anyway in order to complete your senior project. It is particularly important to learn if you plan on going to graduate school in mathematics or physics. If you are interested in using LaTeX, please consult the following simple installation guide. After installing and testing your installation, let me know and I will show you the basics.

5.2 Homework, 2/22/18

1. Pages 86,87 of section 2.2: problems 9(b),(f),(g). 10(a),(b),(c), 11(d)

2. Pages 96,97 of section 2.3: problems 1(h),(k),(m). 6(a),(b). 7(a),(b). 10(a),(c).

5.3 Test corrections, due Tuesday, 02/27/2018

Complete each of the following problems. You are allowed to use the textbook and your notes, but you may not consult classmates nor online resources. Each problem will be graded on a pass/fail basis, and it needs to be essentially flawless to pass. For each correct problem, you will receive a 2 percent increase to your Exam 1 score.

1. Page 79 of section 2.1: problem 13.

2. Page 68 of section 1.7: problem 17.

3. Page 67 of section 1.7: problem 14(a).

4. Page 47 of section 1.5: problem 6(a).

5. Page 47 of section 1.5: problem 8.

5.4 Homework, due Tuesday 02/27/2018

1. Pages 110,111 of section 2.4: problems 6(b),(f),(l); 7(a),(k),(m); 8(f),(h)

5.5 Homework, due Tuesday 03/01/2018

1. Page 120 of section 2.5: problems 2; 5(b),(d); 6(b),(d). Note: What your book calls “PMI” we have just been calling “induction,” and what your book calls “PCI” we have been calling “strong induction.”

5.6 Practice problems 1

1. This exercise is vital to your success in this course because definition will be written in English. It is imperative that you are able to translate them into precise logical statements.
Translate each of the following English sentences into logical statements if it is a proposition. If it is not a proposition, say so and explain why. For the atomic propositions (i.e., the ones that cannot be further broken down), assign them a letter. For example, for the sentence “my dog is cute and I am not a construction worker,” you should provide the answer $P \wedge (\neg Q)$ where P is the proposition “my dog is cute” and Q is the proposition “I am a construction worker.”

(a) I am neither a good basketball player nor a good baseball player.

(b) I am not both American and Japanese.

(c) 17 is prime and divides 476 implies 17 divides either 68 or 7.

(d) What time is the movie?

(e) If I owe you a dollar, then either I am in debt or you owe me more than a dollar.

(f) $\frac{x}{2}$ is a rational number.

(g) $2 < 5$ is necessary and sufficient for $4 < 25$.

(h) I am not a quick reader, but I can do mathematics easily.

(i) This statement is not true.

(j) There are clouds whenever it is raining.

(k) $3 + 2 = 5$ if and only if $3 \cdot 2 \neq 7$.

For the next sentences, you may need to use quantifiers. Be sure to specify the universe of discourse in each case. Moreover, you should not use abbreviations like in the previous problem, you need to determine how to state each of the properties mathematically.

(a) There is a unique smallest positive integer.

(b) Each real number is either positive or negative.

(c) Every integer exceeds another.

(d) Some integer is greater than the rest.

(e) Rational numbers are real.

Solution.

(a) $(\neg P)\wedge(\neg Q)$ (or equivalently, $\neg(P \vee Q)$ where P is “I am a good basketball player,” and Q is “I am a good baseball player.”

(b) $\neg(P \wedge Q)$ where P is “I am american,” and Q is “I am Japanese.”

(c) $(P \wedge Q) \implies (R \vee S)$ where P is “17 is prime,” Q is “17 divides 476,”, R is “17 divides 68,” and S is “17 divides 7.”

(d) Not a proposition because it is a question and so has no truth value.

(e) $P \implies (Q \vee R)$ where P is “I owe you a dollar,” Q is “I am in debt,” and R is “you owe me more than a dollar.”

(f) Not a proposition because x is an unquantified variable; this is an open sentence.

(g) $P \iff Q$ where P is $2 < 5$ and Q is $4 < 25$.

(h) $(\neg P) \wedge Q$ where P is “I am a quick reader,” and Q is “I can do mathematics easily.”

(i) Not a proposition. If this statement were true, then by its meaning it would be false, which is a contradiction. If this statement were false, then by its meaning it would be true, which is a contradiction. Thus this statement can be neither true nor false.

(j) $P \implies Q$ where P is “it is raining,” and Q is “there are clouds.”

(k) $P \iff \neg Q$ where P is $3 + 2 = 5$, and Q is $3 \cdot 2 = 7$.

For the quantified sentences, we have

(a) $(\exists! x \in \mathbb{N})(\forall y \in \mathbb{N})(x \leq y)$

(b) $(\forall x \in \mathbb{R})\big((x < 0) \vee (x > 0)\big)$

(c) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x > y)$

(d) $(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})\big((x \neq y) \implies (x > y)\big)$

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

2. Using associativity, commutativity and distributivity properties of conjunction and disjunction, along with DeMorgan’s Laws and the fact that $\neg P \vee Q$ is equivalent to $P \implies Q$, establish the following equivalences.

(a) $P \implies Q$ is equivalent to $\neg Q \implies \neg P$ (this is called the **contrapositive** of the conditional statement).

(b) $P \implies (Q \implies R)$ is equivalent to $(P \wedge Q) \implies R$.

(c) $\neg(P \wedge Q)$ is equivalent to $P \implies \neg Q$ and also to $Q \implies \neg P$. (Hint: for the second equivalence, try using an equivalence you have already proven; this is part of the reason we prove things: so that we can use them later.)

Solution. For the first equivalence, we have the following chain:

$$\begin{aligned} P \implies Q &\iff \neg P \vee Q \\ &\iff Q \vee \neg P \\ &\iff \neg\neg Q \vee \neg P \\ &\iff \neg Q \implies \neg P \end{aligned}$$

For the second equivalence, we have the following chain:

$$\begin{aligned} P \implies (Q \implies R) &\iff \neg P \vee (Q \implies R) \\ &\iff \neg P \vee (\neg Q \vee R) \\ &\iff (\neg P \vee \neg Q) \vee R \\ &\iff \neg(P \wedge Q) \vee P \\ &\iff (P \wedge Q) \implies R \end{aligned}$$

For the last equivalence, we have the following chain:

$$\begin{aligned}\neg(P \wedge Q) &\iff \neg P \vee \neg Q \\ &\iff P \implies \neg Q \\ &\iff \neg\neg Q \implies \neg P \\ &\iff Q \implies \neg P\end{aligned}$$

3. Do problems 9 and 10 of section 1.3 on pages 26 and 27. Since some of you are unable to obtain the book, I restate the problems here.
#9. Give an English translation for each sentence.

(a) $\forall x \in \mathbb{N}, x \geq 1$.

(b) $\exists! x \in \mathbb{R}, x \geq 0 \wedge x \leq 0$.

(c) $\forall x \in \mathbb{N}, x$ is prime $\wedge x \neq 2 \implies x$ is odd.

(d) $\exists! x \in \mathbb{R}, \ln x = 1$.

(e) $\neg(\exists x \in \mathbb{R}, x^2 < 0$.

(f) $\exists! x \in \mathbb{R}, x^2 = 0$.

(g) $\forall x, x$ is odd $\implies x^2$ is odd.

#10. Which of the following are true in the universe of all real numbers?

(a) $\forall x, \exists y, x + y = 0$.

(b) $\exists x, \forall y, x + y = 0$.

(c) $\exists x, \exists y, x^2 + y^2 = -1$.

(d) $\forall x, (x > 0 \implies (\exists y, y < 0 \wedge xy > 0))$.

(e) $\forall y, \exists x, \forall z, xy = xz$.

(f) $\exists x, \forall y, x \leq y$.

(g) $\forall x, \exists y, x \leq y$.

(h) $\exists! y, y < 0 \wedge y + 3 > 0$.

(i) $\exists! x, \forall y, x = y^2$.

(j) $\forall y, \exists! x, x = y^2$.

(k) $\exists! x, \exists! y, \forall w, w^2 > x - y$.

Solution. 9.

(a) Every natural number is greater than or equal to one.

(b) There exists a unique real number which is both greater than or equal to zero and less than or eqaul to zero.

(c) For any prime natural number x, if x is not equal to 2, then x is odd. Alternatively, you could say: every prime natural number other than 2 is odd.

(d) There exists a unique real number x for which is the base-e logarithm of x is 1.

(e) There is no real number whose square is negative.

(f) There exists a unique real number whose square is zero.

(g) For every natural number x, if x is odd, then x^2 is also odd. Alternatively, you could say: The square of any odd natural number is itself odd.

10. Here I provide the truth value as well as an English translation to help you see why it has that truth value.

(a) True, “for every real number, there is some other number so that the sum of the two is zero.”

(b) False, “there exists some real number so that when you add it to any other real number, the sum is zero.”

(c) False, “there exist two real numbers x, y so that $x^2 + y^2 = -1$.”

(d) False, “for every positive real number there exists some negative real number so that the product is positive.”

(e) True, “for every real number y there is some real number x so that no matter which real number z is given, the products xy, xz are equal.”

(f) False, “there exists a smallest real number.”

(g) True, “every real number is at least as small as some real number.”

(h) False, “there exists a unique negative real number which, becomes positive upon adding 3.”

(i) False, “there exists a unique number which is the square root of every real number.”

(j) False, “every real number has a unique sqaure root.”

(k) False, “there exist unique real numbers x, y whose difference is less than the square of every real number w.”

4. On pages 37, 38 and 39 of section 1.4, do problems 1(a)-1(c), 5(a), 5(c), 7(j), 7(k), 7(l). 11(a)-11(c).

Solution. 1(a). Suppose $(G, *)$ is a cyclic group, $\ldots$, therefore $(G, *)$ is abelian.
1(b). Suppose B is a nonsingular matrix, $\ldots$, hence $\det B \neq 0$.
1(c). Suppose A, B, and C are sets and that A is a subset of B and that B is a subset of C, $\ldots$, thus A is a subset of C.
5(a). Suppose x, y are even integers. By the definition of even, we have $x = 2m$ and $y = 2n$ for some integers $m, n \in \mathbb{Z}$. So $x + y = 2m + 2n = 2(m + n)$. Since the sum of integers is an integer, $m + n \in \mathbb{Z}$ is an integer, and so by the definition of even, $x + y$ is even.
5(c). Suppose x, y are even integers. By the definition of even, we have $x = 2m$ and $y = 2n$ for some integers $m, n \in \mathbb{Z}$. So $xy = (2m)(2n) = 4(mn)$. Since the product of integers is an integer, $mn \in \mathbb{Z}$ is an integer, and so using the definition of divisibility, we see 4 divides xy.
7(j). Suppose a, b are positive integers and a divides b and b divides a. By the definition of divisibility, there are some integers m, n so that $b = am$ and $a = bn$. Since, a, b are positive, m, n must be positive as well. Thus $a = bn = (am)n = a(mn)$. Since, $a \neq 0$, we may cancel it on both sides to obtain $1 = mn$. Because m, n are positive integers, $m, n \geq 1$. Therefore, $1 \leq m \leq mn = 1$ and thus $m = 1 = n$. Finally, $b = am = a$.
An alternate proof proceeds as follows. Suppose a, b are positive integers and a divides b and b divides a. By a result proven in class, if a positive integer x divides another positive integer y, then $x \leq y$. Therefore, we find that $a \leq b$ and $b \leq a$, therefore $a = b$.
7(k). Suppose $a, b, c, d \in \mathbb{Z}$ and a divides b and c divides d. By the definition of divisibility, there are some integers m, n so that $b = am$ and $d = cn$. Thus $bd = (am)(cn) = (ac)(mn)$. Since the product of integers is an integer, $mn \in \mathbb{Z}$ is an integer, and so using the definition of divisibility, we see bd divides ac.
7(l). Suppose $a, b, c \in \mathbb{Z}$ and ab divides c. By the definition of divisibility, there is some integer m so that $c = (ab)m$. Thus $c = a(bm)$. Since the product of integers is an integer, $bm \in \mathbb{Z}$ is an integer, and so using the definition of divisibility, we see a divides c.

5. Prove that for every integer k, the product $k(k+1)$ is even.

Hint. Use proof by cases.

Solution. Suppose that $k \in \mathbb{Z}$.
Case 1: k is even. Then $k = 2n$ for some integer $n \in \mathbb{Z}$, so $k(k+1) = (2n)(k+1) = 2(n(k+1))$, which is even since $n(k+1)$ is an integer.
Case 2: k is odd. Then $k = 2n+1$ for some integer $n \in \mathbb{Z}$, so $k+1 = 2n+2 = 2(n+1). Then k(k+1) = k(2(n+1)) = 2(k(n+1))$, which is even since $k(n+1)$ is an integer.

6. Prove by contraposition that for any integers x, y, if xy is even then either x is even or y is even.

Solution. Note that the contrapositive of this statement is that if both x, y are not even, then xy is not even. This is equivalent to saying that if both x, y are odd, then xy is odd. This is the statement we will prove.
Suppose x, y are arbitrary integers. Assume that x is odd and y is odd. So there exist $m, n \in \mathbb{Z}$ with $x = 2m+1$ and $y = 2n+1$. Hence $xy = (2m+1)(2n+1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$ is odd since $2mn + m + n \in \mathbb{Z}$.

7. From section 1.6 on pages 57, 58, 59, do problems 1(d), 1(h), 2(c), 4(c), 4(d), 4(f), 5(a).

Solution. 1(d). To prove this statement $(\neg(\exists m, n \in \mathbb{Z})P(m,n))$ we will prove the equivalent form $((\forall m, n \in \mathbb{Z})(\neg P(m,n)))$. To this end, suppose $m, n \in \mathbb{Z}$ are arbitrary. Then $12m + 15n = 3 \cdot 4m + 3 \cdot 5n = 3(4m + 5n)$. Since $4m + 5n$ is an integer, we see that 3 divides $12m + 15n$. But 3 does not divide 1, and so $12m + 15n \neq 1$.
1(h). Let m be an arbitrary odd integer. Then there exists $k \in \mathbb{Z}$ with $m = 2k + 1$, and hence

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

By a previous problem, $k(k+1)$ must be even, and so there is some $j \in \mathbb{Z}$ so that $k(k+1) = 2j$. Hence,

$$m^2 = 4k(k+1) + 1 = 4(2j) + 1 = 8j + 1.$$

2(c). Suppose $a, b \in \mathbb{Z}$ are aribtrary and a divides b. Then $b = ka$ for some $k \in \mathbb{Z}$. Let $n \in \mathbb{N}$ be any natural number. Then $b^n = (ka)^n = k^n a^n$. Since $k^n \in \mathbb{Z}$, a^n divides b^n. Because $n \in \mathbb{N}$ was arbitrary, this proves the result.
4(c). False. Counterexample: $x = 2$, $y = \frac{1}{2}$, then $y^x = \left(\frac{1}{2}\right)^2 = \frac{1}{4} \leq 2 = x$.
4(d). False. Counterexample: $a = 6$, $b = 2$, $c = 3$. Certainly $a = 6$ divides $bc = 2 \cdot 3 = 6$ since $6 = 6 \cdot 1$ and $1 \in \mathbb{Z}$. However, $a = 6$ cannot divide either of $b = 2$ or $c = 3$ since these are less than 6.
4(f). False. Counterexample: $x = \frac{1}{2}$. $x^2 - x = \left(\frac{1}{2}\right)^2 - \frac{1}{2} = \frac{1}{4} - \frac{1}{2} = -\frac{1}{4} < 0$. Alternative counterexample: Consider *any* $0 < x < 1$. Then $x > 0$ but $x - 1 < 0$. Hence $x^2 - x = x(x-1) < 0$ since it is the product of a negative and a positive.
5(a). We will use a two-part proof.
Suppose x is any prime natural number. That means $x > 1$ and x has no divisor y in the range $1 < y < x$. Since $\sqrt{x} < x$ (because $x > 1$), x has no divisor y in the range $1 < y \leq \sqrt{x}$.
For the other direction, we will prove the statement using contraposition. Suppose x is a natural number which is not prime. There are two cases:
Case 1: $x = 1$. Then clearly x is not greater than one.
Case 2: $x > 1$. Since x is greater than one and not prime, it is composite (by definition). Thus $x = ab$ for some positive integers $1 < a, b < x$. Either $a \leq b$

or $b \leq a$. Without loss of generality, we may assume $a \leq b$. Then multiplying both sides by a, we find

$$a^2 \leq ab = x = (\sqrt{x})^2.$$

Hence $a \leq \sqrt{x}$ (by properties of square roots, in particular, because it is an increasing function). So, a is a divisor of x which is greater than one (because it is a prime) and less than or equal to the sqaure root of x. By contraposition, we have proven the desired result.

8. From section 1.5 on pages 47 and 48 do problems 12(a), 12(b).

Solution. 12(a). Grade: F. The student tried to prove the **inverse** $((\neg P) \implies (\neg Q))$ of the implication $P \implies Q$ given in the problem. However, this is a logical error since the two are not equivalent.
12(b). Grade: A. The student correctly proved this statement by contraposition. There are no errors.

9. For a nonzero rational number a, a **multiplicative inverse** of a is a rational number b so that $ab = 1$. Remember a rational number is a fraction of integers where the denominator is nonzero. Prove that every nonzero rational number has a unique multiplicative inverse.

Solution. Suppose a is a nonzero rational number. Then there exist integers $p, q \in \mathbb{Z}$ with $q \neq 0$ so that $a = \frac{p}{q}$. Since $a \neq 0$, we know $p \neq 0$, and hence $\frac{q}{p}$ is a rational number. Moreover, $a \cdot \frac{q}{p} = \frac{p}{q} \cdot \frac{q}{p} = \frac{pq}{qp} = 1$. Therefore, $\frac{q}{p}$ is a multiplicative inverse for a. Thus every nonzero $a \in \mathbb{Q}$ has a multiplcative inverse.
Now suppose $b, c \in \mathbb{Q}$ are multiplicative inverses of a. Then $ab = 1$ and $ac = 1$, and hence $ab = ac$. Since $a \neq 0$, we may cancel to obtain $b = c$. Thus the multiplicative inverse of a is unique.

10. Prove or find a counterexample: For nonzero $a, b \in \mathbb{Z}$ with $a \neq b$, there exist *unique* $x, y \in \mathbb{Z}$ so that $ax + by = \gcd(a, b)$.

Solution. Notice that without the word “unique,” this statement is precisely Bezout’s identity. So, certainly x, y exist, the question is whether they are unique. We show below that they are not unique.
Counterexample: $a = 2$ and $b = 3$. Two different solutions are $x = -1$. $y = 1$ and $x = 2$, $y = -1$.
Comment: In fact, it is possible to list out precisely all the pairs that satisfy Bezout’s identity by starting with a single pair x, y. I will state this without proof. Given nonzero integers a, b with $d := \gcd(a, b) = ax + by$, then all other solutions to Bezout’s identity have the form:

$$x' = x + k\frac{b}{d}, \quad y' = y - k\frac{a}{d}, \quad k \in \mathbb{Z}.$$

11. Show that if $x \in \mathbb{R}$ and $x^2 = p$ for some prime number p, then x is irrational.

Hint. Mimic the proof that $\sqrt{2}$ is irrational that I provided in class, except use Euclid’s Lemma for the key steps.

Solution. Assume to the contrary that $x \in \mathbb{Q}$ and $x^2 = p$ for some prime p. Then we may write $x = \frac{a}{b}$ for $a, b \in \mathbb{Q}$ with $b \neq 0$. Moreover, by ⟨⟨Unresolved xref, reference "lem-rational-lowest-terms"; check spelling or use "provisional" attribute⟩⟩ we may even assume $\gcd(a, b) = 1$. Since $p = x^2 = \frac{a^2}{b^2}$ we know $pb^2 = a^2$, which means that p divides a^2 since b^2 is an integer. By Euclid’s Lemma we know that p must divide a as well. Thus $a = pk$ for some $k \in \mathbb{Z}$.

Therefore, $pb^2 = a^2 = (pk)^2 = p^2k^2$ and so $b^2 = pk^2$. Thus, p divides b^2 since $k^2 \in \mathbb{Z}$. By Euclid's Lemma we know that p must divide b as well. Hence, p is a common divisor of a, b, which contradicts the fact that $\gcd(a, b) = 1$. Therefore our assumption was wrong and instead $x \notin \mathbb{Q}$.

12. Prove that if a, b are relatively prime integers and both a and b divide c, then ab divides c.

Solution. Suppose that a, b are relatively prime integers and each divides c. Then $c = am$ and $c = an$ for some $m, n \in \mathbb{Z}$. Moreover, by Bezout's identity, $1 = \gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$. Multiplying this last equation by c, we find

$$c = cax + cby = (bn)ax + (am)by = ab(nx + my),$$

and therefore ab divides c.

5.7 Exam 1 Review

1. Recall all the definitions we have discussed, both in plain English, and their logical form.

2. Recall all the proof structures we have discussed, and know how to implement them.

3. Suppose that a, b are nonzero integers. Let q, r be the quotient and remainder obtained from the Division Algorithm. Prove that $\gcd(a, b) = \gcd(b, r)$.

Solution. Suppose that a, b are nonzero integers and q, r are the quotient and remainder from the Division Algorithm, so that $a = qb + r$. We will prove that the common divisors of a, b are the same as the common divisors of b, r, and therefore these pairs have the same gcd.
Suppose that c is a common divisor of a, b, so that $a = cm$ and $b = cn$ for some $m, n \in \mathbb{Z}$. Then $r = a - bq = cm - cnq = c(m - nq)$, so c divides r. Since it already divides b, this means c is a common divisor of b, r.
The proof that a common divisor of b, r is also a common divisor of a, b is almost identical to the previous paragraphy, so we omit it.

4. Prove that if m^2 is odd, then m is odd. *Note: you should be able to provide two different proofs of this result (see the hint for two different ideas).*

Hint. You should be able to prove this using parity. You should also be able to provide a different proof using Euclid's lemma.

Solution 1. We prove the contrapositive, namely, if m is not odd, then m^2 is not odd. By parity, this is equivalent to: if m is even, then m^2 is even.
Suppose that m is even. Then $m = 2k$ for some $k \in \mathbb{Z}$. Thus $m^2 = 4k^2 = 2(2k^2)$. Snice $2k^2$ is an integer, m^2 is even.

Solution 2. Suppose that m^2 is odd. Then $m^2 = 2k + 1$ for some integer k. Thus $2k = m^2 - 1 = (m - 1)(m + 1)$. Since 2 is prime and divides the product $(m - 1)(m + 1)$, by Euclid's Lemma we know that either 2 divides $m - 1$ or $m + 1$.
Case 1: Suppose 2 *divides* $m - 1$. Then $m - 1 = 2j$ for some $j \in \mathbb{Z}$, and so $m = 2j + 1$, so m is odd.
Case 2: Suppose 2 *divides* $m + 1$. Then $m + 1 = 2j$ for some $j \in \mathbb{Z}$, and so $m = 2j - 1 = 2(j - 1) + 1$, so m is odd.

5. Prove that the product of three consecutive integers is divisible by 3.

Solution. Let $n, (n + 1), (n + 2)$ be an arbitrary choice of three consecutive integers. Notice that to prove that 3 divides $n(n+1)(n+2)$ it suffices to prove

that 3 divides one of the factors in the product. By the Division Algorithm, $n = 3q + r$ for some integers r, q with $r \in \{0, 1, 2\}$.
Case 1: $r = 0$. Then $n = 3q$ so 3 divides n.
Case 2: $r = 1$. Then $n + 2 = (3q + 1) + 2 = 3(q + 1)$ so 3 divides $n + 2$.
Case 3: $r = 2$. Then $n + 1 = (3q + 2) + 1 = 3(q + 1)$ so 3 divides $n + 1$.

6. Prove that if p, q are *distinct* primes (i.e., $p \neq q$) and p, q each divide a, then pq divides a.

Solution 1. Since p, q are primes, the only divisors of p are $1, p$, and the only divisors of q are $1, q$. Since $p \neq q$, the only commmon divisor is 1, so $\gcd(p, q) = 1$. By a previous problem, if relatively prime integers each divides an integer a, then so does their product. Thus pq divides a.

Solution 2. Suppose p, q each divide a. Then $pm = a = qn$ for some $m, n \in \mathbb{Z}$. Thus p divides the product qn. Since p is prime, by Euclid's Lemma, either $p \mid q$ or $p \mid n$. Since q is prime, it's only divisors are $1, q$, and hence $p \not| q$ since $p \neq q$. Therefore $p \mid n$. Hence $n = pk$ for some $k \in \mathbb{Z}$. Finally, $a = qn = q(pk) = (pq)k$, so $pq \mid a$.

7. Suppose m is an odd integer. Prove that m^2 has remainder 1 when divided by 4.

Solution. Assume m is an odd integer. Then $m = 2k + 1$ for some $k \in \mathbb{Z}$. Thus $m^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. Therefore m^2 has remainder 1 when divided by 4 (since we can write it as 4 times an integer plus 1).

8. Prove that if $x \in \mathbb{R}$ and $x^2 = 2$, then x is irrational.

Hint. Assume x is rational and express the fraction in *lowest terms*, i.e., where the numerator and the denominator are relatively prime.

Solution. Assume to the contrary that $x \in \mathbb{Q}$ and $x^2 = 2$. Then we may write $x = \frac{a}{b}$ for $a, b \in \mathbb{Q}$ with $b \neq 0$. Moreover, by ⟨⟨Unresolved xref, reference "lem-rational-lowest-terms"; check spelling or use "provisional" attribute⟩⟩ we may even assume $\gcd(a, b) = 1$. Since $2 = x^2 = \frac{a^2}{b^2}$ we know $2b^2 = a^2$, which means that a^2 is even since b^2 is an integer. By Proposition 1.4.13 we know that a must be even as well. Thus $a = 2k$ for some $k \in \mathbb{Z}$. Therefore, $2b^2 = a^2 = (2k)^2 = 4k^2$ and so $b^2 = 2k^2$. Thus, b^2 is even since $k^2 \in \mathbb{Z}$. By Proposition 1.4.13 we know that b must be even as well. Hence, a, b are both even which means they have a common divisor of 2, which contradicts the fact that $\gcd(a, b) = 1$. Therefore our assumption was wrong and instead $x \notin \mathbb{Q}$.

9. Prove that for any natural number n, we have $\gcd(n, n + 1) = 1$.

Solution 1. Suppose that $n \in \mathbb{N}$. Then $(-1) \cdot n + 1 \cdot (n + 1) = 1$ is a linear combination of n and $n + 1$, and clearly it is the smallest positive linear combination (since any such combination must be an integer). Therefore, by Bezout's Identity, $1 = \gcd(n, n + 1)$.

Solution 2. Suppose that $n \in \mathbb{N}$. Let c be any positive common divisor of $n, n + 1$. Then $n = cj$ and $n + 1 = ck$ for some integers j, k. Thus $1 = (n + 1) - n = ck - cj = c(k - j)$, and so c divides 1. Therefore $c \leq 1$. Since c was an arbitrary positive common divisor, $\gcd(n, n + 1) = 1$.

10. Use the previous problem to prove that there are infinitely many prime numbers.

Hint. Use contradiction and let n be the product of all the prime numbers.

Solution. Suppose to the contrary that there are only finitely many prime numbers, which we will list as $p_1, p_2, \ldots, p_k$. Let $n = p_1 p_2 \cdots p_k$ be the product of all these primes. Note, all the primes divide n. By the previous problem,

$\gcd(n, n+1) = 1$. By the fundamental theorem of arithmetic, there is a prime q dividing $n+1$ (it is possible $q = n+1$, but that is not necessarily the case). Note that q must not divide n (because then it would be a common divisor of $n, n+1$ greater than 1). Therefore, q is a prime not equal to any of $p_1, p_2, \ldots, p_k$, contradicting that this is the list of all the primes. Therefore there must be infinitely many prime numbers.
Note, we used the fundamental theorem of arithmetic to say that $n+1$ had a prime dividing it. This is overkill. All we really need is that any natural number greater than 1 has a prime dividing it, which is much easier to prove than the fundamental theorem of arithmetic. We will learn how to prove this simpler fact in a few weeks.

11. Prove that if every even natural number greater than 2 is the sum of two primes, then every odd natural number greater than 5 is the sum of three primes.

Solution. Suppose that every even natural number greater than 2 is the sum of two primes. Now let n be an odd natural number greater than 5. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, and so $n - 3 = 2k + 1 - 3 = 2(k-1)$ is even. Morevoer, $n - 3 > 5 - 3 = 2$ since $n > 5$. Therefore, we can write $n - 3 = p + q$ for some primes p, q. Finally, $n = 3 + p + q$, and since 3 is also prime, we have written n as the sum of three primes.

12. Prove that if a divides both $b-1$ and $c-1$, then a divides $bc-1$.

Solution. Suppose that a divides both $b-1$ and $c-1$. Then $b - 1 = am$ and $c - 1 = an$ for some $m, n \in \mathbb{Z}$. Now

$$bc - 1 = bc - b + b - 1 = b(c-1) + (b-1)ban + am = a(bn + m).$$

Thus a divides $bc - 1$.
Note, we could have also reasoned like this:

$$bc - 1 = bc - c + c - 1 = c(b-1) + (c-1)cam + an = a(cm + n).$$

Using this equation and the one above, we find that $a(bn + m) = a(cm + n)$, and thus $bn + m = cm + n$ by cancellation. Thus $b(n-1) = c(m-1)$, which is a perhaps unexpected relationship.

13. Prove that if x is prime, then $x + 7$ is composite.

Solution. Suppose that x is prime. Then either $x = 2$ or x is odd (because if $x > 2$ and x is even, then x is divisible by 2 and therefore wouldn't be prime).
Case 1: $x = 2$. Then $x + 7 = 9 = 3 \cdot 3$ is composite.
Case 2: x is odd. Then $x = 2k + 1$ for some $k \in \mathbb{Z}$. Moreover, $x + 7 = 2k + 1 + 7 = 2(k+4)$, so $x + 7$ is divisible by 2. Also, $x + 7 > 2$, so $x + 7$ is composite.

14. Prove that for sets A, B, C, we have the following two set equalities:

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

Solution. First equality. Let x be arbitrary. Then

$$\begin{aligned} x \in A \cap (B \cup C) &\iff (x \in A) \wedge (x \in B \cup C) \\ &\iff (x \in A) \wedge (x \in B \vee x \in C) \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \end{aligned}$$

$$\begin{aligned}
&\iff (x \in A \cap B) \vee (x \in A \cap C) \\
&\iff x \in (A \cap B) \cup (A \cap C)
\end{aligned}$$

Second equality. Let x be arbitrary. Then

$$\begin{aligned}
x \in A \cup (B \cap C) &\iff (x \in A) \vee (x \in B \cap C) \\
&\iff (x \in A) \vee (x \in B \wedge x \in C) \\
&\iff (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\
&\iff (x \in A \cup B) \wedge (x \in A \cup C) \\
&\iff x \in (A \cup B) \cap (A \cup C)
\end{aligned}$$

15. Prove that if A, B, C are sets and $A \subseteq B$, $B \subseteq C$, and $C \subseteq A$, then $A = B = C$.

Solution. Assume $A \subseteq B$, $B \subseteq C$, and $C \subseteq A$.
By a result proven in class, since $A \subseteq B$ and $B \subseteq C$, we also have $A \subseteq C$. Since $C \subseteq A$, this means $A = C$. Similarly, since $B \subseteq C$ and $C \subseteq A$, by the same result from class, we know $B \subseteq A$. Since $A \subseteq B$ this entails $A = B$. Thus $B = A = C$.

16. You should also be able to do problems 8, 9, 10(a), 10(c), 13, 17 from Section 2.3 on pages 96–99.

Solution. #8.

(a) Suppose $B = \{a, b\}$, $\Delta = \{1, 2\}$, $A_1 = \{a\}, A_2 = \{b\}$. Then $B \setminus A_1 = \{b\}$ and $B \setminus A_2 = \{a\}$. Moreover, $\bigcap_{\alpha \in \Delta} A_\alpha = \varnothing$. Therefore,

$$B \setminus \left(\bigcap_{\alpha \in \Delta} A_\alpha \right) = B \setminus \varnothing = \{a, b\} \neq \varnothing = \{a\} \cap \{b\} = \bigcap_{\alpha \in \Delta} (B \setminus A_\alpha).$$

(b) Suppose $B = \{a, b\}$, $\Delta = \{1, 2\}$, $A_1 = \{a\}, A_2 = \{b\}$. Then $B \setminus A_1 = \{b\}$ and $B \setminus A_2 = \{a\}$. Moreover, $\bigcup_{\alpha \in \Delta} A_\alpha = \{a, b\} = B$. Therefore,

$$B \setminus \left(\bigcup_{\alpha \in \Delta} A_\alpha \right) = B \setminus B = \varnothing \neq \{a\} \cup \{b\} = \bigcup_{\alpha \in \Delta} (B \setminus A_\alpha).$$

(c) We will prove this with a series of if and only if statements.

$$\begin{aligned}
x \in \left(\bigcap_{\alpha \in \Delta} A_\alpha \right) \setminus B &\iff \left(\left(x \in \bigcap_{\alpha \in \Delta} A_\alpha \right) \wedge (x \notin B) \right) \\
&\iff ((\forall \alpha \in \Delta, x \in A_\alpha) \wedge (x \notin B)) \\
&\iff (\forall \alpha \in \Delta, (x \in A_\alpha) \wedge (x \notin B)) \\
&\iff (\forall \alpha \in \Delta, x \in (A_\alpha \setminus B)) \\
&\iff x \in \left(\bigcap_{\alpha \in \Delta} (A_\alpha \setminus B) \right)
\end{aligned}$$

(d) We will prove this with a series of if and only if statements.

$$\begin{aligned}
x \in \left(\bigcup_{\alpha \in \Delta} A_\alpha \right) \setminus B &\iff \left(\left(x \in \bigcup_{\alpha \in \Delta} A_\alpha \right) \wedge (x \notin B) \right) \\
&\iff ((\exists \alpha \in \Delta, x \in A_\alpha) \wedge (x \notin B))
\end{aligned}$$

$$\begin{aligned}
&\iff (\exists \alpha \in \Delta, (x \in A_\alpha) \wedge (x \notin B)) \\
&\iff (\exists \alpha \in \Delta, x \in (A_\alpha \setminus B)) \\
&\iff x \in \left(\bigcup_{\alpha \in \Delta} (A_\alpha \setminus B) \right)
\end{aligned}$$

#9.

(a) Suppose that $x \in \bigcup_{\alpha \in \Gamma} A_\alpha$. Then there exists some $\gamma \in \Gamma$ for which $x \in A_\gamma$. Since $\Gamma \subseteq \Delta$, $\gamma \in \Delta$ as well. Therefore $x \in \bigcup_{\alpha \in \Delta} A_\alpha$.

(b) Suppose that $x \in \bigcup_{\alpha \in \Delta} A_\alpha$. Take any $\gamma \in \Gamma$. Since $\Gamma \subseteq \Delta$, $\gamma \in \Delta$. Since $x \in \bigcup_{\alpha \in \Delta} A_\alpha$, $x \in A_\gamma$. Since γ was chosen arbitrarily from Γ, this proves $x \in \bigcup_{\alpha \in \Gamma} A_\alpha$.

#10.

(a) Suppose $B \subseteq A$ for every $A \in \mathcal{A}$. Then, take any $x \in B$ and any $C \in \mathcal{A}$. Since $B \subseteq C$, we must have $x \in C$. Since C was arbitrary in $\mathcal{A}$, this shows that $x \in \bigcap_{A \in \mathcal{A}} A$. Since x was arbitrary in B, this proves the result.

(b) The largest X such that $X \subseteq A$ for all $A \in \mathcal{A}$ is precisely their intersection: $\bigcap_{A \in \mathcal{A}} A$.

(c) Suppose that $A \subseteq D$ for every $A \in \mathcal{A}$. Take any $x \in \bigcup_{A \in \mathcal{A}} A$. Then there is some $C \in \mathcal{A}$ for which $x \in C$. But we know $C \subseteq D$ by hypothesis, and thus $x \in D$. Since x was arbitrarily chosen from the union, this proves the result.

(d) The smallest set Y such that $A \subseteq Y$ for all $A \in \mathcal{A}$ is precisely their union: $\bigcup_{A \in \mathcal{A}} A$.

#13. Suppose that $\mathcal{A}$ is a family of pairwise disjoint sets and assume $\mathcal{B} \subseteq \mathcal{A}$ is another family of sets. Take any $C, D \in \mathcal{B}$. Since $\mathcal{B} \subseteq \mathcal{A}$, we also have $C, D \in \mathcal{A}$. Because $\mathcal{A}$ is a pairwise disjoint family, either $C = D$ or $C \cap D = \varnothing$. Since C, D were arbitrarily chosen from $\mathcal{B}$, we know $\mathcal{B}$ is a pairwise disjoint family.
#17.

(a) $A_i := \left[-\frac{1}{i}, 1 + \frac{1}{i}\right]$.

(b) $A_i := (0, 1)$.

(c) $A_i := \left[0, \frac{1}{i}\right) \cup \left(1 - \frac{1}{i}, 0\right]$.

(d) $A_i := \left(0, \frac{1}{i}\right)$.

5.8 Exam 2 Review

1. Prove that $\{5m + 2 \mid m \in \mathbb{Z}\} = \{5n - 3 \mid n \in \mathbb{Z}\}$.

Solution. Call the left-hand set A and the right-hand set B.
($\subseteq$). Suppose that $x \in A$. Then $x = 5m + 2$ for some $m \in \mathbb{Z}$. Thus $x = 5m + 2 + 3 - 3 = 5(m + 1) - 3$. Since $m + 1 \in \mathbb{Z}$, we find $x \in B$.
($\supseteq$). Suppose that $x \in B$. Then $x = 5n - 3$ for some $n \in \mathbb{Z}$. Thus $x = 5n - 3 - 2 + 2 = 5(n - 1) + 2$. Since $n - 1 \in \mathbb{Z}$, we find $x \in A$.

2. For an integer $m \in \mathbb{Z}$, define $m\mathbb{Z} := \{x \mid x = mk, \text{for some } k \in \mathbb{Z}\}$. In English, $m\mathbb{Z}$ is the set of multiples of m. Prove that $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $n \mid m$.

Solution. Let $m, n \in \mathbb{Z}$ be arbitrary.
($\Rightarrow$). Suppose that $m\mathbb{Z} \subseteq n\mathbb{Z}$. Since $m = m \cdot 1 \in m\mathbb{Z}$, we know that $m \in n\mathbb{Z}$. Therefore $m = nk$ for some $k \in \mathbb{Z}$. Thus $n \mid m$.
($\Leftarrow$). Suppose that $n \mid m$. Then $m = nk$ for some $k \in \mathbb{Z}$. Now take any element $x \in m\mathbb{Z}$. By definition of $m\mathbb{Z}$, we find $x = mj$ for some integer j. Hence $x = mj = (nk)j = n(kj)$. Since kj is an integer, we find $x \in n\mathbb{Z}$.

3. On pages 86–87 of Section 2.2, do problems 6, 9, 10, 15(a), (c), (d), 16(a).

Solution. #6.

(a) $A = \{1, 2\}, B = \{2\}, C = \{1\}$

(b) $A = B = C = \{1\}$

(c) $A = B = \{1\}, C = \{1, 2\}$

(d) $A = \{1, 3\}, B = \{2, 3\}, C = \{3\}$

(e) $A = \{1\}, B = C = \{1, 2\}$

(f) $A = B = C = \{1\}$

#9.

(a) Note that $A \subseteq B$ if and only if $\forall x, x \in A \implies x \in B$ if and only if $\forall x, \neg(x \in A \wedge x \notin B)$ if and only if $\forall x, \neg(x \in A \setminus B)$ if and only if $\forall x, x \notin A \setminus B$ if and only if $A \setminus B = \varnothing$. Note that the second "if and only if" uses the equivalence $(P \implies Q) \iff \neg(P \wedge \neg Q)$, and the last "if and only if" uses the definition of the empty set.

(b) Suppose $A \subseteq B \cup C$ and $A \cap B = \varnothing$. Take an $x \in A$. Then since $A \subseteq B \cup C$, $x \in B \cup C$, so either $x \in B$ or $x \in C$. But since $A \cap B = \varnothing$, it cannot be the case that $x \in B$ (for otherwise $x \in A \cap B$), and therefore $x \in C$. Hence $A \subseteq C$.

(c) ($\Rightarrow$) Suppose that $C \subseteq A \cap B$. Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, we can use the small lemma we proved in class to conclude $C \subseteq A$ and $C \subseteq B$.
($\Leftarrow$) Suppose that $C \subseteq A$ and $C \subseteq B$. Now take any $x \in C$. By the first condition, $x \in A$, and by the second condition, $x \in B$. Therefore $x \in A \cap B$. Thus $C \subseteq A \cap B$.

(d) Suppose $A \subseteq B$. Now take any $x \in A \setminus C$. Then $x \in A$ and $x \notin C$. Since $A \subseteq B$, we have $x \in B$. Thus $x \in B \setminus C$. Therefore $A \setminus C \subseteq B \setminus C$.

(e) Notice that for any x,

$$\begin{aligned}
x \in (A \setminus B) \setminus C &\iff x \in A \setminus B \wedge x \notin C \\
&\iff x \in A \wedge x \notin B \wedge x \notin C \\
&\iff (x \in A \wedge x \notin C \wedge x \notin B) \vee (x \in A \wedge x \notin C \wedge x \in C) \\
&\iff (x \in A \wedge x \notin C) \wedge (x \notin B \vee x \in C) \\
&\iff (x \in A \wedge x \notin C) \wedge \neg(x \in B \wedge x \notin C) \\
&\iff x \in (A \setminus C) \wedge x \notin (B \setminus C) \\
&\iff x \in (A \setminus C) \setminus (B \setminus C)
\end{aligned}$$

(f) Suppose $A \subseteq C$ and $B \subseteq C$. Take any $x \in A \cup B$. Then either $x \in A$ or $x \in B$. If $x \in A$, then $x \in C$ since $A \subseteq C$. If $x \in B$, then $x \in C$ since $B \subseteq C$. Either way, $x \in C$. Thus $A \cup B \subseteq C$.

(g) Take any $x \in (A \cup B) \cap C$. Then $x \in A \cup B$ and $x \in C$. So, either $x \in A$ or $x \in B$. *Case 1:* $x \in A$. Then certainly $x \in A \cup (B \cap C)$. *Case 2:* $x \in B$. Then since $x \in C$ also, we have $x \in B \cap C$. Hence $x \in A \cup (B \cap C)$.

(h) To show $(A \setminus B) \cap B = \varnothing$, we will use a proof by contradiction. That is, suppose this set is nonempty. Then there is some $x \in (A \setminus B) \cap B$, so $x \in A \setminus B$ and $x \in B$. But the first statement means $x \in A$ and $x \notin B$, contradicting the fact that $x \in B$. Hence our assumption (that $(A \setminus B) \cap B \neq \varnothing$), was false. Therefore $(A \setminus B) \cap B = \varnothing$.

#10. Let A, B, C, D be sets.

(a) Suppose $C \subseteq A$ and $D \subseteq B$. Take any $x \in C \cap D$. Then $x \in C$ and $x \in D$. Since $C \subseteq A$ we have $x \in A$. Since $D \subseteq B$ we have $x \in B$. Thus $x \in A \cap B$.

(b) Suppose $C \subseteq A$ and $D \subseteq B$. Take any $x \in C \cup D$. Then $x \in C$ or $x \in D$. Case 1: suppose $x \in C$. Since $C \subseteq A$ we have $x \in A$. Case 2: suppose $x \in D$. Since $D \subseteq B$ we have $x \in B$. So $x \in A$ or $x \in B$. Thus $x \in A \cup B$.

(c) Suppose $C \subseteq A$ and $D \subseteq B$, and A, B are disjoint. Then $A \cap B = \varnothing$, and by #10(a), $C \cap D \subseteq A \cap B = \varnothing$. But trivially $\varnothing \subseteq C \cap D$, so they must be equal.

(d) Suppose $C \subseteq A$ and $D \subseteq B$. Take any $x \in D \setminus A$. Then $x \in D$ and $x \notin A$. Since $D \subseteq B$ we have $x \in B$. Since $C \subseteq A$, by an earlier problem, we have $x \notin C$. Thus $x \in B \setminus C$.

(e) Suppose $A \cup B \subseteq C \cup D$, $A \cap B = \varnothing$, and $C \subseteq A$. Take $x \in B$, then $x \in A \cup B$, and hence $x \in C \cup D$. Since $A \cap B = \varnothing$, $x \notin A$, and hence $x \notin C$. But because $x \in C \cup D$ and $x \notin C$, we must have $x \in D$. Therefore $B \subseteq D$.

4. For each natural number n, let $A_n = \{5n, 5n+1, \ldots, 6n\}$. Find the union and intersection over $\mathcal{A} := \{A_n \mid n \in \mathbb{N}\}$. Be sure to prove your claim.

Solution. Claim: $\bigcup_{n=1}^{\infty} A_n = B \cup C$ where $B := \{5, 6, 10, 11, 12, 15, 16, 17, 18\}$ and $C := \{n \in \mathbb{N} \mid n \geq 20\}$.
"$\subseteq$" Suppose $x \in \bigcup_{n=1}^{\infty} A_n$. Then there is some $k \in \mathbb{N}$ so that $x \in A_k$.
Case 1: $k = 1, 2, 3$. Then $x \in A_k \subseteq A_1 \cup A_2 \cup A_3 = B$, and hence $x \in B \cup C$.
Case 2: $k \geq 4$. Then $20 = 5 \cdot 4 \leq 5k \leq x \leq 6k$, and hence $x \in C$, so $x \in B \cup C$.
"$\supseteq$" Suppose that $x \in B \cup C$. If $x \in B = A_1 \cup A_2 \cup A_3$, then clearly $x \in \bigcup_{n=1}^{\infty} A_k$. If $x \in C$, then by the division algorithm we can write $x = 5m + r$ with $m, r \in \mathbb{Z}$ and $0 \leq r < 5$. Moreover, since $20 = 5 \cdot 4$ and $x \geq 20$ we know $m \geq 4$. Furthermore, $x = 5m + r \leq 5m + 4 \leq 5m + m = 6m$. Thus $5m \leq x \leq 6m$. And therefore $x \in A_m$, so $x \in \bigcup_{n=1}^{\infty} A_n$.

5. Give an example of an indexed collection of sets $\{A_n \mid n \in \mathbb{N}\}$ which are pairwise disjoint and for which $A_n \subseteq (0, 1)$ (the open interval). Be sure to prove your collection satisfies the listed properties.

Solution. Simple example: set $A_n = \{\frac{1}{n+1}\}$. Clearly these are pairwise disjoint because each only contains one element and none of those are the same one. Moreover, $0 < \frac{1}{n+1} < 1$, so $A_n \subseteq (0, 1)$.

6. Give an example of an indexed collection of sets $\{A_n \mid n \in \mathbb{N}\}$ no two of which are disjoint and such that each $A_n \subseteq (0, 1)$ (the open interval), but $\displaystyle\bigcap_{n \in \mathbb{N}} A_n = \varnothing$. Be sure to prove your collection satisfies the listed properties.

Solution. Consider $A_n = (0, \frac{1}{n})$. Clearly, if $n < m$, then $\frac{1}{m} < \frac{1}{n}$, so $A_m \subseteq A_n$ and thus $A_m \cap A_n = A_m \neq \varnothing$.
We now prove the intersection over all the sets is empty. Let $x \in \mathbb{R}$. If $x \leq 0$, then $x \notin A_1$, so x is not in the intersection either. Now suppose $x > 0$. Then by the Archimedean Principle, there is some $n \in \mathbb{N}$ so that $\frac{1}{n} < x$. Therefore

$x \notin A_n$ and hence x is not in the intersection either. This proves that every x is not in the intersection, so the intersection is empty.

7. Let $\{A_\alpha \mid \alpha \in I\}$ be an indexed family of sets and let B be any set. Prove that

(a) $B \cap \bigcup_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I}(B \cap A_\alpha)$

(b) $B \cup \bigcap_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in I}(B \cup A_\alpha)$

Solution 1. Subset based solution.
"$\subseteq$" Suppose that $x \in B \cap \bigcup_{\alpha \in I} A_\alpha$, then $x \in B$ and $x \in \bigcup_{\alpha \in I} A_\alpha$. Thus there is some $\beta \in I$ so that $x \in A_\beta$. Therefore $x \in B \cap A_\beta$. Hence $x \in \bigcup_{\alpha \in I}(B \cap A_\alpha)$.
"$\supseteq$" Suppose that $x \in \bigcup_{\alpha \in I}(B \cap A_\alpha)$, then there is some $\beta \in I$ so that $x \in B \cap A_\beta$. Thus $x \in B$ and $x \in B \cap A_\beta$. Hence $x \in \bigcup_{\alpha \in I} A_\alpha$. Therefore $x \in B \cap \bigcup_{\alpha \in I} A_\alpha$.
The equality $B \cup \bigcap_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in I}(B \cup A_\alpha)$ follows from a similar proof.

Solution 2. Iff based solution.
Note that

$$\begin{aligned} x \in B \cap \bigcup_{\alpha \in I} A_\alpha &\iff (x \in B) \wedge (\exists \alpha \in I)(x \in A_\alpha) \\ &\iff (\exists \alpha \in I)\big((x \in B) \wedge (x \in A_\alpha)\big) \\ &\iff (\exists \alpha \in I)(x \in B \cap A_\alpha) \\ &\iff x \in \bigcup_{\alpha \in I}(B \cap A_\alpha), \end{aligned}$$

and

$$\begin{aligned} x \in B \cup \bigcap_{\alpha \in I} A_\alpha &\iff (x \in B) \vee (\forall \alpha \in I)(x \in A_\alpha) \\ &\iff (\forall \alpha \in I)\big((x \in B) \vee (x \in A_\alpha)\big) \\ &\iff (\forall \alpha \in I)(x \in B \cup A_\alpha) \\ &\iff x \in \bigcap_{\alpha \in I}(B \cup A_\alpha). \end{aligned}$$

8. For each natural number n, define $A_n := \{n, n+1, n+2, \ldots,\}$ (i.e., $A_n = \{k \in \mathbb{N} \mid k \geq n\}$). Determine $\bigcap_{n=1}^{\infty} A_n$ and prove your claim.

Solution. We claim that $\bigcap_{n=1}^{\infty} A_n = \varnothing$.
Since our universe is $\mathbb{N}$, it suffices to show that every $k \in \mathbb{N}$ is *not* in this intersection. So, let $k \in \mathbb{N}$ be arbitrary. Notice that $k < k+1$, so $k \ngeq k+1$. Therefore $k \notin A_{k+1}$. Hence $k \notin \bigcap_{n=1}^{\infty} A_n$.

9. (Pg. 110, #5(c,d,e,f)). Give an inductive definition for each:

- $\{n \mid n = 2^k \text{ for some } k \in \mathbb{N}\}$
- $\{a, a+d, a+2d, a+3d, \ldots\}$, where $a, d \in \mathbb{R}$. (The elements in this set form an **arithmetic progression**.
- $\{a, ar, ar^2, ar^3, \ldots\}$, where $a, d \in \mathbb{R}$. (The elements in this set form an **geometric progression**.
- $\bigcup_{i=1}^{n} A_i$, for some indexed family $\{A_i \mid i \in \mathbb{N}\}$.

Solution.

- $\{n \mid n = 2^k \text{ for some } k \in \mathbb{N}\} := \{a_n \mid n \in \mathbb{N}\}$, where $a_1 := 2$ and $a_{n+1} = 2a_n$.

- $\{a, a+d, a+2d, a+3d, \ldots\} := \{a_n \mid n \in \mathbb{N}\}$, where $a_1 := a$ and $a_{n+1} = a_n + d$.
- $\{a, ar, ar^2, ar^3, \ldots\} := \{a_n \mid n \in \mathbb{N}\}$, where $a_1 := a$ and $a_{n+1} = a_n r$.
- $\bigcup_{i=1}^n A_i$, for some indexed family $\{A_i \mid i \in \mathbb{N}\}$. $\bigcup_{i=1}^1 A_i := A_1$, and $\bigcup_{i=1}^{n+1} A_i := (\bigcup_{i=1}^n A_i) \cup A_{n+1}$.

10. (Pg. 110, #6(d)). Use induction to prove that for all $n \in \mathbb{N}$,

$$\sum_{j=1}^{n} j \cdot j! = (n+1)! - 1.$$

Solution. For the base case, notice that

$$\sum_{j=1}^{1} j \cdot j! = 1 \cdot 1! = 1 = 2 - 1 = (1+1)! - 1.$$

Now let $k \in \mathbb{N}$ be arbitrary and assume $\sum_{j=1}^k j \cdot j! = (k+1)! - 1$. Then we find

$$\begin{aligned}\sum_{j=1}^{k+1} j \cdot j! &= \sum_{j=1}^{k} j \cdot j! + (k+1) \cdot (k+1)! \\ &= ((k+1)! - 1) + (k+1) \cdot (k+1)! \\ &= (1 + k + 1)(k+1)! - 1 \\ &= (k+2)! - 1\end{aligned}$$

11. (Pg. 110, #6(g)). Use induction to prove that for all $n \in \mathbb{N}$,

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

Solution. For the base case, notice that

$$\sum_{j=1}^{1} \frac{1}{j(j+1)} = \frac{1}{1 \cdot 2} = \frac{1}{2} = \frac{1}{1+1}.$$

Now let $k \in \mathbb{N}$ be arbitrary and assume $\sum_{j=1}^k \frac{1}{j(j+1)} = \frac{k}{k+1}$. Then we find

$$\begin{aligned}\sum_{j=1}^{k+1} \frac{1}{j(j+1)} &= \sum_{j=1}^{k} \frac{1}{j(j+1)} + \frac{1}{k(k+1)} \\ &\frac{k}{k+1} + \frac{1}{k(k+1)} \\ &\frac{k(k+2)}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)} \\ &\frac{k^2 + 2k + 1}{(k+1)(k+2)} \\ &\frac{(k+1)^2}{(k+1)(k+2)} \\ &\frac{(k+1)}{(k+2)}\end{aligned}$$

12. (Pg. 110, #6(j)). Use induction to prove that for all $n \in \mathbb{N}$,

$$\prod_{j=1}^{n} \left(1 - \frac{1}{j+1}\right) = \frac{1}{n+1}.$$

Solution. For the base case, notice that

$$\prod_{j=1}^{1} \left(1 - \frac{1}{j+1}\right) = 1 - \frac{1}{1+1} = \frac{1}{1+1}.$$

Now let $k \in \mathbb{N}$ be arbitrary and assume $\prod_{j=1}^{k} \left(1 - \frac{1}{j+1}\right) = \frac{1}{n+1}$. Then we find

$$\begin{aligned}
\prod_{j=1}^{k+1} \left(1 - \frac{1}{j+1}\right) = & \left(\prod_{j=1}^{k} \left(1 - \frac{1}{j+1}\right)\right) \cdot \left(1 - \frac{1}{k+2}\right) \\
& \frac{1}{k+1} \cdot \left(\frac{k+2}{k+2} - \frac{1}{k+2}\right) \\
& \frac{1}{k+1} \cdot \frac{k+1}{k+2} \\
& \frac{1}{k+2}.
\end{aligned}$$

13. (Pg. 111, #6(k)). Use induction to prove that for all $n \in \mathbb{N}$,

$$\prod_{j=1}^{n} (2i - 1) = \frac{(2n)!}{n! 2^n}.$$

Solution. For the base case, notice that

$$\prod_{j=1}^{1} (2j - 1) = 2 \cdot 1 - 1 = 1 = \frac{2 \cdot 1}{1 \cdot 2} = \frac{2!}{1! 2^1}.$$

Now let $k \in \mathbb{N}$ be arbitrary and assume $\prod_{j=1}^{k} (2j - 1) = \frac{(2k)!}{k! 2^k}$. Then we find

$$\begin{aligned}
\prod_{j=1}^{k+1} (2j - 1) = & \left(\prod_{j=1}^{k} (2j - 1)\right) \cdot \left((2(k+1) - 1\right) \\
& \frac{(2k)!}{k! 2^k} \cdot (2k + 1) \\
& \frac{(2k+1)!}{k! 2^k} \cdot \frac{2k+2}{(k+1)2} \\
& \frac{(2k+2)!}{(k+1)! 2^{k+1}} \\
& \frac{(2(k+1))!}{(k+1)! 2^{k+1}}.
\end{aligned}$$

14. (Pg. 111, #6(l)). (Sum of finite geometric series.) Use induction to prove that for all $n \in \mathbb{N}$,

$$\sum_{j=0}^{n-1} ar^j = \frac{a(r^n - 1)}{r - 1}.$$

Solution. For the base case, notice that

$$\sum_{j=0}^{1-1} ar^j = ar^0 = a = \frac{a(r^1-1)}{r-1}.$$

Now let $k \in \mathbb{N}$ be arbitrary and assume $\sum_{j=0}^{k-1} ar^j = \frac{a(r^k-1)}{r-1}$. Then we find

$$\begin{aligned}\sum_{j=0}^{k} ar^j &= \sum_{j=0}^{k-1} ar^j + ar^k \\ &= \frac{a(r^k-1)}{r-1} + ar^k \\ &= \frac{ar^k-a}{r-1} + \frac{ar^k(r-1)}{r-1} \\ &= \frac{ar^k-a}{r-1} + \frac{ar^{k+1}-ar^k}{r-1} \\ &= \frac{ar^{k+1}-a}{r-1} \\ &= \frac{a(r^{k+1}-1)}{r-1}\end{aligned}$$

15. (Pg. 111, #7(g)). Use induction to prove that for all $n \in \mathbb{N}$, 8 divides $9^n - 1$

Solution. For the base case, notice that $8 = 1 \cdot 8$, so $8 \mid 8 = 9^1 - 1$. Now let $k \in \mathbb{N}$ be arbitrary and assume $8 \mid 9^k - 1$. Then there is some $j \in \mathbb{Z}$ for which $9^k - 1 = 8j$. Thus

$$9^{k+1} - 1 = 9 \cdot 9^k - 1 = 9(8j+1) - 1 = 8(9j) + 9 - 1 = 8(9j+1).$$

Since $9j + 1 \in \mathbb{Z}$, we have shown $8 \mid 9^{k+1} - 1$. By induction we have proven the result.

16. (Pg. 111, #7(k)). Use induction to prove that for all $n \in \mathbb{N}$,

$$\sum_{j=1}^{n} \frac{1}{j^2} \le 2 - \frac{1}{n}.$$

Solution. For the base case, notice that

$$\sum_{j=1}^{1} \frac{1}{j^2} = \frac{1}{1^2} = 1 = 2 - \frac{1}{1}.$$

Now let $k \in \mathbb{N}$ be arbitrary and assume $\sum_{j=1}^{k} \frac{1}{j^2} \le 2 - \frac{1}{k}$. Before we continue, recall the following elementary fact: for any $m \in \mathbb{N}$, $\frac{1}{m(m+1)} = \frac{1}{m} - \frac{1}{m+1}$. Then we find

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

$$\begin{aligned}&\le \left(2-\frac{1}{k}\right)+\left(\frac{1}{k}-\frac{1}{k+1}\right)\\&=2-\frac{1}{k+1}\end{aligned}$$

By induction we have proven the result.

17. (Pg. 111, #7(l)). Use induction to prove that for all $n \in \mathbb{N}$, and every positive real number x,

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

Solution. For the base case, notice that $(1+x)^1 = 1+x = 1+1x$. Now let $k \in \mathbb{N}$ be arbitrary and assume $(1+x)^k \ge 1+kx$. Then we find (be careful! the first inequality only works because $1+x>0$ since $x>0$. When you start introducing other variables, you have to pay attention to such things!)

$$\begin{aligned}(1+x)^{k+1} &= (1+x)^k(1+x)\\&\ge (1+kx)(1+x)\\&= 1+kx+x+kx^2\\&= 1+(k+1)x+kx^2\\&> 1+(k+1)x,\end{aligned}$$

where the last inequality follows because $k \in \mathbb{N}$ and so $kx^2 > 0$. By induction we have proven the result.

18. (Pg. 111, #7(n)). Assume the differentiation formulas $\frac{d}{dx}(x) = 1$ and $\frac{d}{dx}(fg) = f\frac{dg}{dx} + g\frac{df}{dx}$ (product rule). Use induction to prove that for all $n \in \mathbb{N}$, $\frac{d}{dx}(x^n) = nx^{n-1}$.

Solution. The base case is one of our assumptions, so we are done. Now let $k \in \mathbb{N}$ be arbitrary and assume $\frac{d}{dx}(x^k) = kx^{k-1}$. Then notice that $x^{k+1} = x^k \cdot x$, so applying the product rule to the functions $f(x) = x^k$ and $g(x) = x$, we find

$$\begin{aligned}\frac{d}{dx}(x^{k+1}) &= \frac{d}{dx}(x^k \cdot x)\\&= x^k\frac{d}{dx}(x) + x\frac{d}{dx}(x^k)\\&= x^k \cdot 1 + x \cdot kx^{k-1}\\&= x^k + kx^k\\&= (k+1)x^k.\end{aligned}$$

By induction we have proven the result.

19. (Pg. 111, #8(g)). Use generalized induction to prove that for all $n > 2$, the sum of the angle measures of the interior angles of a convex polygon of n sides is $(n-2)\pi$ (measured in radians).

Hint. Use a standard fact from geometry.

Solution. The base case, when $n = 3$ is just the standard geometry fact that the sum of the interior angle measures of a triangle is always π.

Now suppose $k \in \mathbb{N}$ and $k > 2$ (i.e., $k \ge 3$) and the sum of the interior angle measures of any k-sided polygon is $(k-2)\pi$. Then consider any $(k+1)$-sided polygon. Pick a vertex v with an interior angle less than π. Since $k+1 \ge 4$, we can divide our polygon into a triangle and a k-sided polygon by drawing a line between the vertices adjacent to v. Moreover, the sum of the interior angles of the original $(k+1)$-gon is the same as the sum of the interior angles of the k-gon (which has total angle measure $(k-2)\pi$) added to the sum of the interior angles of the triangle (which has total angle measure π. Therefore, the total angle measure for the $(k+1)$-gon is $(k-2)\pi + \pi = ((k+1)-2)\pi$, as desired.

20. (Pg. 153–154, #1(f,h,k,m)).

Solution. For each relation, determine if it is reflexive, symmetric or transitive.

(a) #1(f). The relation is $\neq$ on $\mathbb{N}$. This is *not* reflexive since $x = x$ for any $x \in \mathbb{N}$. This relation is symmetric since $x \neq y$ if and only if $y \neq x$. This relation is not transitive on $\mathbb{N}$ since $0 \neq 1$ and $1 \neq 0$, but $0 = 0$.

(b) #1(h). The relation is $R := \{(x,y) \in \mathbb{Z}^2 \mid x+y = 10\}$ on $\mathbb{Z}$. This relation is not reflexive since $0+0 = 0 \neq 10$ and hence $(0,0) \notin R$. This relation is symmetric since $(x,y) \in R$ if and only if $x+y = 10$ if and only if $y+x = 10$ if and only if $(y,x) \in R$. This relation is not transitive since $(4,6) \in R$ and $(6,4) \in R$, but $(4,4) \notin R$.

(c) #1(k). The relation is R on $\mathbb{R}^2$ where $(x,y)\ R\ (z,w)$ if and only if $x+z \leq y+w$. This relation is not reflexive since $1+1 \not\leq 0+0$, so $(1,0) \ \not R\ (1,0)$. This relation is symmetric since $(x,y)\ R\ (z,w)$ if and only if $x+z \leq y+w$ if and only if $z+x \leq w+y$ if and only if $(z,w)\ R\ (x,y)$. This relation is not transitive since $(1,0)\ R\ (0,1)$ and $(0,1)\ R\ (1,0)$, but $(1,0) \ \not R\ (1,0)$.

(d) #1(m). The relation is T on $\mathbb{R}^2$ where $(x,y)\ R\ (z,w)$ if and only if $x+y \leq z+w$. This relation is reflexive since for any $(x,y) \in \mathbb{R}^2$, $x+y \leq x+y$ and so $(x,y)\ T\ (x,y)$. This relation is not symmetric since $0+0 \leq 1+1$ but $1+1 \not\leq 0+0$, so $(0,0)\ T\ (1,1)$ but $(1,1) \ \not T\ (0,0)$. This relation is transitive. Indeed, if $(x,y)\ T\ (z,w)$ and $(z,w)\ T\ (a,b)$, then $x+y \leq z+w$ and $z+w \leq a+b$, and therefore $x+y \leq a+b$. Thus $(x,y)\ T\ (a,b)$ and so T is transitive.

21. (Pg. 154, #5(a)).

Solution. We will prove that the relation R on $\mathbb{R}$ given by $x\ R\ y$ if and only if $x - y \in \mathbb{Q}$ is an equivalence relation. Note that this relation is reflexive since for any $x \in \mathbb{R}$, $x - x = 0 \in \mathbb{Q}$, and hence $x\ R\ x$. This relation is also symmetric since for any $x, y \in \mathbb{R}$, we have $x - y \in \mathbb{Q}$ if and only if $y - x = -(x-y) \in \mathbb{Q}$. This relation is also transitive since for any $x, y, z \in \mathbb{R}$, if $x\ R\ y$ and $y\ R\ z$, then $x - y, y - z \in \mathbb{Q}$, and hence $x - z = (x-y) + (y-z) \in \mathbb{Q}$.
We give the equivalence classes of $0, 1, \sqrt{2}$ below.

$$[0] = [1] = \mathbb{Q}$$
$$[\sqrt{2}] = \{x + \sqrt{2} \mid x \in \mathbb{Q}\}$$

22. (Pg. 154, #5(c)).

Solution. We will prove that the relation V on $\mathbb{R}$ given by $x\ V\ y$ if and only if $x = y$ or $xy = 1$ is an equivalence relation.
This relation is reflexive since for any $x \in \mathbb{R}$, $x = x$ and hence $x\ V\ x$. This relation is symmetric since $x = y$ or $xy = 1$ if and only if $y = x$ or $yx = 1$. This relation is also transitive, for if $x, y, z \in \mathbb{R}$ and $x\ V\ y$ and $y\ V\ z$, then if either $x = y$ or $y = z$, the conclusion $x\ V\ z$ is trivial. So suppose $x \neq y \neq z$. Thus $xy = 1 = yz$, and so none of x, y, z are zero. Dividing by z we obtain $x = z$. Thus $x\ V\ z$.
We give the equivalence classes of $3, -\frac{2}{3}, 0$ below.

$$[3] = \left\{3, \frac{1}{3}\right\} \quad \left[-\frac{2}{3}\right] = \left\{-\frac{2}{3}, -\frac{3}{2}\right\} \quad [0] = \{0\}.$$

23. (Pg. 155, #5(h)).

Solution. Consider the relation R on the set of differentiable functions defined by $f \; R \; g$ if and only if f and g have the same first derivative. This relation is obviously an equivalence relation because it is a notion of "sameness." By the Fundamental Theorem of Calculus, the elements of any equivalence class are things of the form $f + C$ where C is an arbitrary constant.

Consider the following inductively (recursively) defined sequence. Let $f_1 = 1, f_2 = 1$ and for all $n \geq 3$, let $f_n = f_{n-1} + f_{n-2}$. The sequence of positive integers f_n is call the **Fibonacci sequence**.

24. Prove that

(a) For every positive integer n, f_{3n} is even and f_{3n+1}, f_{3n+2} are both odd.

(b) For every positive integer n, $\gcd(f_n, f_{n+1}) = 1$ and $\gcd(f_n, f_{n+2}) = 1$.

(c) For every positive integer n,

$$\sum_{j=1}^{n} f_j = f_{n+2} - 1.$$

Solution. For each of these, we will use strong induction.

(a) Notice that $f_1 = 1 = f_2$, so these are both odd. Now suppose that $m \geq 3$ and for any $k < m$, f_k is even if and only if k is divisible by 3. Now we apply the division algorithm to divide m by 3 to get $m = 3q + r$ for some $q, r \in \mathbb{Z}$ with $r \in \{0, 1, 2\}$. Case 1: $r = 0$. Then $f_m = f_{m-1} + f_{m-2} = f_{3(q-1)+2} + f_{3(q-1)+1}$ and by the strong inductive hypothesis, these last two terms are odd since the subscripts are not divisible by 3, and therefore their sum is even. Case 2: $r = 1$. Then $f_m = f_{m-1} + f_{m-2} = f_{3q} + f_{3(q-1)+2}$ and by the strong inductive hypothesis, f_{3q} is even and $f_{3(q-1)+2}$ is odd, therefore their sum is odd. Case 2: $r = 2$. Then $f_n = f_{m-1} + f_{m-2} = f_{3q+1} + f_{3q}$ and by the strong inductive hypothesis, f_{3q} is even and f_{3q+1} is odd, therefore their sum is odd. Thus f_m is even if and only if m is divisible by 3. By strong induction, the proof is complete.

(b) Notice that $f_1 = f_2 = 1$ and $f_3 = 2$, and so $\gcd(f_1, f_2) = \gcd(1, 1) = 1$ and similarly, $\gcd(f_1, f_3) = \gcd(1, 2) = 1$. Now, let $m \geq 2$ and suppose that for any $k < m$, we have $\gcd(f_k, f_{k+1}) = 1 = \gcd(f_k, f_{k+2})$. Then we find that $f_{m+1} = f_m + f_{m-1}$. Let c be any common divisor of f_m, f_{m+1}. Then it is also a divisor of $f_{m-1} = f_{m+1} - f_m$, so it is a common divisor of f_{m-1}, f_m. Therefore, by the strong inductive hypothesis, $c = 1$. Hence $\gcd(f_m, f_{m+1}) = 1$. Now let c be any common divisor of f_m, f_{m+2}. Since $f_{m+2} = f_{m+1} + f_m$, we see that c is also a divisor of $f_{m+1} = f_{m+2} - f_m$. Therefore it is a common divisor of f_m, f_{m+1}. By the previous paragraph, this implies that $c = 1$. Hence $\gcd(f_m, f_{m+2}) = 1$. By strong induction, we have established the result.

(c) Notice that $\sum_{j=1}^{1} f_j = f_1 = 1 = 2 - 1 = f_{1+2} - 1$. For the inductive step, assume that $m > 1$ and for any $k < m$, $\sum_{j=1}^{k} f_j = f_{k+2} - 1$. Then

$$\begin{aligned} f_{m+2} - 1 &= f_{m+1} + f_m - 1 \\ &= \sum_{j=1}^{m-1} f_j + f_m - 1 \\ &= \sum_{j=1}^{m} f_j - 1. \end{aligned}$$

By strong induction we have proven the result.

25. Let α, β be the (positive, negative) solutions to the quadratic equation $x^2 = x + 1$. That is, $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Prove that for every $n \in \mathbb{N}$,

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Solution. We will prove this by strong induction. Notice that $\frac{\alpha^1 - \beta^1}{\alpha - \beta} = 1 = f_1$ and also

$$\frac{\alpha^2 - \beta^2}{\alpha - \beta} = \alpha + \beta = 1 = f_2.$$

Now let $m \geq 3$ and assume that for all $k < m$, we have

$$f_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}.$$

Then

$$\begin{aligned} f_m &= f_{m-1} + f_{m-2} \\ &= \frac{\alpha^{m-1} - \beta^{m-1}}{\alpha - \beta} + \frac{\alpha^{m-2} - \beta^{m-2}}{\alpha - \beta} \\ &= \frac{\alpha^{m-2}(\alpha + 1) - \beta^{m-2}(\beta + 1)}{\alpha - \beta} \\ &= \frac{\alpha^{m-2}(\alpha^2) - \beta^{m-2}(\beta^2)}{\alpha - \beta} \\ &= \frac{\alpha^m - \beta^m}{\alpha - \beta}. \end{aligned}$$

26. Let $a_1 = 2, a_2 = 4$ and $a_{n+2} = 5a_{n+1} - 6a_n$ for all $n \geq 1$. Prove that $a_n = 2^n$ for every $n \in \mathbb{N}$.

Solution. Notice that $a_1 = 2 = 2^1$ and $a_2 = 4 = 2^2$. Now let $m \geq 3$ and suppose that for all $k < m$, $a_k = 2^k$. Then by the definition of a_m and the strong inductive hypothesis, we find

$$\begin{aligned} a_m &= 5a_{m-1} - 6a_{m-2} \\ &= 5 \cdot 2^{m-1} - 6 \cdot 2^{m-2} \\ &= 5 \cdot 2^{m-1} - 3 \cdot 2^{m-1} \\ &= (5 - 3) \cdot 2^{m-1} \\ &= 2^m \end{aligned}$$

27. For every natural number n, 5 divides $8^n - 3^n$.

Solution. Notice that 5 obviously divides $5 = 8 - 3 = 8^1 - 3^1$. Now suppose $m \in \mathbb{N}$ and assume 5 divides $8^m - 3^m$ so that $8^m - 3^m = 5k$ for some integer k. Then

$$\begin{aligned} 8^{m+1} - 3^{m+1} &= 8 \cdot 8^m - 3 \cdot 3^m \\ &= 8 \cdot 8^m - 3 \cdot 3^m - 5 \cdot 3^m + 5 \cdot 3^m \\ &= 8 \cdot 8^m - (3 + 5) \cdot 3^m + 5 \cdot 3^m \\ &= 8(8^m - 3^m) + 5 \cdot 3^m \end{aligned}$$

$$\begin{aligned} &= 8 \cdot 5k + 5 \cdot 3^m \\ &= 5(8k + 3^m). \end{aligned}$$

28. Every natural number $n > 1$ has a prime divisor.

Solution. Suppose to the contrary that not every natural number greater than 1 has a prime divisor. Then by the Well-Ordering Principle, there is a smallest such natural number, which we will call n. Note that n cannot be prime, for otherwise it would be its own prime divisor. Therefore, since $n > 1$, it must be composite, and thus $n = mk$ for $1 < m, k < n$. By the minimality of n, k must have a prime divisor, which we call p. Thus $k = xp$ for some integer x. Finally, $n = mk = mxp$ and hence p is a prime divisor of n, which is a contradiction. Therefore, every natural number greater than 1 has a prime divisor.

29. Give examples of relations (on any set or sets of your choosing) which satisfy each of the following combinations of properties.

(a) neither reflexive nor irreflexive

(b) reflexive and symmetric, but not transitive

(c) reflexive and antisymmetric, but not transitive

(d) reflexive and transitive, but not symmetric

Solution.

(a) $A = \{0, 1\}$, $R = \{(0, 0)\}$. R is not reflexive because $1 \not R\, 1$, and it is not irreflexive because $0\, R\, 0$.

(b) $A = \{0, 1, 2, \}$, $R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0), (1, 2), (2, 1)\}$. This is clearly reflexive and symmetric, but it is not transitive because $0\, R\, 1$ and $1\, R\, 2$ but $0 \not R\, 2$.

(c) $A = \{0, 1, 2, \}$, $R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 2)\}$. This is clearly reflexive and antisymmetric, but it is not transitive because $0\, R\, 1$ and $1\, R\, 2$ but $0 \not R\, 2$.

(d) $A = \{0, 1, 2, \}$, $R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 2), (0, 2)\}$. This is reflexive and transitive, but it is not symmetric because $0\, R\, 1$ but $1 \not R\, 0$. As an alternative example you could take $\leq$ on $\mathbb{R}$.

30. Let $r \in \mathbb{R}$ be a fixed real number. Define a relation $\sim_r$ on $\mathbb{R}^2$ in the following way. For any distinct points $(x, y), (w, z) \in \mathbb{R}^2$, set $(x, y) \sim_r (w, z)$ if and only if the slope of the line through these two points is r. Moreover, set $(x, y) \sim_r (x, y)$ always. Prove that $\sim_r$ is an equivalence relation (note: reflexivitiy is very easy).

Solution. This relation $\sim_r$ is reflexive by definition.
For symmetry, let $(x, y), (w, z) \in \mathbb{R}^2$ be any distinct points with $(x, y) \sim_r (w, z)$. Thus the slope of the line through these points is r, i.e.

$$\frac{z-y}{w-x} = r.$$

Now let us compute the slope of the line through the points in the other order:

$$\frac{y-z}{x-w} = \frac{-(z-y)}{-(w-x)} = \frac{z-y}{w-x} = r.$$

For transitivity, suppose that $(x, y) \sim_r (w, z) \sim_r (a, b)$. Then let's look at the slope of the line through $(x, y), (a, b)$:

$$\begin{aligned}\frac{b-y}{a-x} = \frac{(b-z)+(z-y)}{a-x} &= \frac{b-z}{a-x} + \frac{z-y}{a-x} \\ &= \frac{b-z}{a-x} \cdot \frac{a-w}{a-w} + \frac{z-y}{a-x} \cdot \frac{w-x}{w-x} \\ &= r\frac{a-w}{a-x} + r\frac{w-x}{a-x} = r\frac{a-w+w-x}{a-x} = r.\end{aligned}$$

Thus $(x, y) \sim_r (a, b)$.

31. When $r = 5$, describe the equivalence class $[(3, 10)]$.

Solution. The equivalence class $[(3, 10)]$ is the set of points such that the line through that point and $[(3, 10)]$ has slope 5. However, each of these lines passes through $(3, 10)$ and have the slope 5, but there is only one such line. In particular, the equivalence class is this line. In other words,

$$[(3, 10)] = \{(x, y) \in \mathbb{R}^2 \mid y = 5(x-3) + 10\}.$$

32. Give a geometric description of the partition of $\mathbb{R}^2$ induced by the equivalence relation $\sim_r$.

Solution. The elements of the partition induced by $\sim_r$ are just all the lines of slope $\sim_r$ in the plane.

33. This is problem 3 on page 162 of your textbook.
Describe the partition for each of the following equivalence relations.

(a) For $x, y \in \mathbb{R}$, $x \sim y$ iff $x - y \in \mathbb{Z}$.

(b) For $x, y \in \mathbb{R}$, $x \sim y$ iff $\sin x = \sin y$.

(c) For $x, y \in \mathbb{R}$, $x \sim y$ iff $x^2 = y^2$.

(d) For $(x, y), (u, v) \in \mathbb{R}^2$, $(x, y) \sim (u, v)$ iff either $xy = uv = 0$ or $xyuv > 0$.

Solution.

(a) The equivalence classes consist of sets of points whose two nearest neighbors are exactly distance 1 apart. One of these equivalence class is just $\mathbb{Z}$ itself, and the others are just shifted copies of $\mathbb{Z}$.

(b) Notice that $\sin x = \sin y$ if and only if either $y = x + 2\pi k$ for some integer k or if $y = (\pi - x) + 2\pi k$ for some integer k. So the equivalence classes are the union of two sets of points each having an equal spacing of 2π. Alternatively, you can view the equivalence classes as the set of points of intersection of a horizontal line (between -1 and 1 on the vertical axis) with the graph of $\sin(x)$.

(c) The equivalence classes from this equivalence relation are just the union of a point with its negative, e.g. $\{2, -2\}$. These are all two point sets except the line $\{0\}$ which is a singleton. As in the previous example, you can also think of this as the set of points of intersection of a horizontal line with the graph of the parabola x^2.

(d) Given two points $(x, y), (u, v)$, $xy = 0$ if and only if either $x = 0$ or $y = 0$, that is, if (x, y) lies on one of the axes. So, two points are similar if either $xy = uv = 0$ (i.e. they both lie on the axes) or $xyuv > 0$ (which can only happen if both points are *not* on the axes). Thus the axes are one of the partitions. Now, how can $xyuv > 0$? Consider the different quadrants: if (x, y) is in: quadrant 1, then $xy > 0$; quadrant 2, then $xy < 0$; quadrant 3, then $xy > 0$; quadrant 4, then $xy < 0$. So, the only way for $xyuv > 0$ is if both $(x, y), (u, v)$ are in quadrants 1,3 or both are in quadrants 2,4. Thus the partition has 3 sets, the axes, the union of quadrants 1 and 3, and the union of quadrants 2 and 4.

34. Consider the following relation on $\mathbb{N}^2$. For $(x, y), (u, v) \in \mathbb{N}^2$, $(x, y) \sim (u, v)$ iff $x + v = y + u$. Prove that $\sim$ is an equivalence relation.

Solution. Reflexivity: since $x + y = y + x$ for any $(x, y) \in \mathbb{N}^2$, then $(x, y) \sim (x, y)$.

Symmetry: if $(x, y) \sim (u, v)$, then $x + v = y + u$ so $u + z = w + v$, thus $(u, v) \sim (x, y)$.

Transitivitiy: if $(x, y) \sim (u, v) \sim (w, z)$ then $x + v + z = y + u + z = y + w + v$. By cancelling the v we obtain $x + z = w + y$ and hence $(x, y) \sim (w, z)$.

35. Describe the equivalence class $[(1, 1)]$.

Solution. Note that $(n, m) \in [(1, 1)]$ if and only if $n + 1 = m + 1$ if and only if $n = m$. Thus $[(1, 1)] = \{(n, n) \mid n \in \mathbb{N}\}$.

36. Show that every equivalence class has one of the following forms:

- $[(n + 1, 1)]$ for some $n \in \mathbb{N}$.
- $[(1, 1)]$.
- $[(1, n + 1)]$ for some $n \in \mathbb{N}$.

What common set do you think it would be natural to identify with the set of equivalence classes $\mathbb{N}^2/\sim$?

Solution. Consider the equivalence class $[(n, m)]$. If $n = m$ then we have already shown that this is $[(1, 1)]$ in the previous problem.

If $n < m$, then there is some $k \in \mathbb{N}$ for which $n + k = m$. Thus $n + (k + 1) = m + 1$, and hence $(n, m) \sim (1, k + 1)$ so their equivalence class are the same.

If $n > m$, then just reverse their roles in the previuos paragraph.

37. Consider the relation $\sim$ on the set $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ defined by $(p,q)\sim(a,b)$ if and only if $pb=aq$. Prove that $\sim$ is an equivalence relation.

Solution. Reflexivity: since $pq=pq$, we know $(p,q)\sim(p,q)$.

Symmetry: suppose $(p,q)\sim(a,b)$, then $pb=aq$, and so obviously $aq=pb$, hence $(a,b)\sim(p,q)$.

Transitivity: suppose $(p,q)\sim(a,b)\sim(r,s)$, then $pb=aq$ and $as=rb$. Then $pbs=aqs=qrb$ and since $b\neq 0$ we may cancel it to obtain $ps=rq$. Hence $(p,q)\sim(r,s)$.

38. Prove that in every equivalence class $[(p,q)]$ with $p\neq 0$ there is some element (a,b) in this equivalence class for which $\gcd(a,b)=1$. Moreover, prove that if we add the constraint that $b>0$ then this element is actually unique.

Solution. Recall from a previous homework exercise that if $p,q\neq 0$ and $d=\gcd(p,q)$, then $\gcd(\frac{p}{d},\frac{q}{d})=1$. (Note: here what we mean by $\frac{p}{d}$ is the quotient from the division algorithm, and similarly for $\frac{q}{d}$.) Set $a=\frac{p}{d}$ and $b=\frac{q}{d}$. Since $p,q\neq 0$ so also $a,b\neq 0$. Finally, notice that $pbd=ab=aqd$ and by cancellation, we may drop the d to obtain $pb=aq$.

Now, suppose that there are two of these elements in a given equivalence class with the second coordinate positive. Call them $(a,b)\sim(p,q)$ and $\gcd(a,b)=\gcd(p,q)=1$ and $b,q>0$. Then $pb=aq$. Mutliplying by a we obtain $pab=a^2q$. Since $\gcd(a,b)=1$, and ab divides a^2q, by a result proved after the first exam for relatively prime numbers, we can conclude that either ab divides a^2 (in which case $a=b=1$ and hence also $p=q=1$) or ab divides q. If the former, then we are done, so assume ab divides q. Then there is some integer k so that $q=abk$, and hence $pb=aq=a^2bk$. But then ab divides pb and so by that same earlier result, ab divides p or b. If it divides b, then everything collapses and we are done. If it divides p, then p,q would have a common factor, ab violating $\gcd(p,q)=1$ unless $a=b=1$.

39. Consider the following relation R,S,T,U on $A=\{0,1,2\}$.

$$R=\{(0,0),(0,1),(1,1),(1,2),(2,2),(0,2),(1,0)\}.$$
$$S=\{(0,0),(0,1),(1,1),(1,2),(2,2),(0,2)\}.$$
$$T=\{(0,0),(0,1),(1,1)\}.$$
$$U=\{(0,0),(0,1),(1,1),(1,2),(2,2)\}.$$

Are any of R,S,T,U a partial order on A? Provide justification.

Solution. R is not antisymmetric since $(0,1),(1,0)\in R$.
S is a partial order because it is reflexive (contains $(0,0),(1,1),(2,2)$), antisymmetric (contains $(0,1),(1,2),(0,2)$ but not any of $(1,0),(2,1),(2,0)$), and transitive (it contains $(0,1),(1,2)$ and also $(0,2)$). Note that S is just the partial order $\leq$ on A.
T is not reflexive since $(2,2)\notin T$.
U is not transitive since $(0,1),(1,2)\in U$ but $(0,2)\notin U$.

40. Define a relation $\prec$ on $\mathbb{R}^2$ by $(a,b)\prec(x,y)$ if and only if $a\leq x$ and $b\leq y$. Prove that $\prec$ is a partial order on $\mathbb{R}^2$. Is it a total order?

Solution. We first prove that $\prec$ is reflexive. Note that for any $(x,y)\in\mathbb{R}^2$, we have $x\leq x$ and $y\leq y$, and therefore $(x,y)\prec(x,y)$.
To see that $\prec$ is antisymmetric, note that for any $(x,y),(a,b)\in\mathbb{R}^2$, if $(x,y)\prec(a,b)$ and $(a,b)\prec(x,y)$, then $x\leq a$ amd $y\leq b$, and also $a\leq x$ and $b\leq y$.

Therefore, by the antisymmetry of $\leq$, we find $x = a$ and $y = b$, therefore $(x, y) = (a, b)$.
To see that $\prec$ is transitive, note that for any $(x, y), (a, b), (w, z) \in \mathbb{R}^2$, if $(x, y) \prec (a, b)$ and $(a, b) \prec (w, z)$, then $x \leq a$ and $y \leq b$, and also $a \leq w$ and $b \leq z$. Therefore, by the transitivity of $\leq$, we find $x \leq w$ and $y \leq z$. Hence $(x, y) \prec (w, z)$.
We have shown that $\prec$ is a partial order on $\mathbb{R}^2$ because it is reflexive, antisymmetric and transitive, but it is not a total order because there are incomparable elements. In particular, $(1, 2) \not\prec (0, 3)$ since $1 \not\leq 0$, but also $(0, 3) \not\prec (1, 2)$ since $3 \not\leq 2$.

41. Define the relation R on $\mathbb{C}$ by $(a+bi)R(c+di)$ if and only if $a^2+b^2 \leq c^2+d^2$. Is R a partial order on $\mathbb{C}$? Justify your answer.

Solution. The relation R is not a partial order on $\mathbb{C}$ because it is not antisymmetric. In particular, $1\ R\ i$ and $i\ R\ 1$ since $1^2 + 0^2 = 0^2 + 1^2$, but $1 \neq i$. This completes the solution to this problem.
Note however that this relation *is* reflexive and transitive. A relation like this is called a **pre-order**. If S is any pre-order (reflexive, transitive) on a set A, then we can create an equivalence relation $\sim$ on A by $x \sim y$ if and only if $x\ S\ y$ and $y\ S\ x$. This is easily seen to be symmetric, and the reflexivity and transitivity follow from those same properties of S. Then there is a natural partial order $S/\sim$ on the set of equivalence classes $A/\sim$ defined by $[x]S/\sim[y]$ if and only if $x\ S\ y$.
If we were to apply the procedure in the last paragraph to the relation R given in this problem, then the equivalence relation on $\mathbb{C}$ we would obtain is the one in which $x \sim y$ if and only if x, y lie on the same circle centered at 0. So the equivalence classes are circles centered at 0. Then the partial order $R/\sim$ on the set of these circles is precisely the one that says one circle is less than or equal to another circle if and only if its radius is less than or equal to the radius of the other.

5.9 Function Review

1. Find a bijection between the closed intervals $[a, b]$ and $[c, d]$ with $a < b$ and $c < d$. You must *prove* that the function you construct *is* a bijection.

Solution. You really want to use a line segment. Let's start by finding a bijection $f : [0, 1] \to [a, b]$. So, we could make the graph of our function a line through $(0, a)$ and $(1, b)$. The formula for such a line is $f(x) = (b - a)x + a$.
We claim that f is a bijection. First, notice that since $0 \leq x \leq 1$ and $b-a > 0$, we have $a \leq (b - a)x + a \leq (b - a) + a = b$, so $[a, b]$ is a valid codomain. Now suppose $f(x) = f(y)$. Then $(b-a)x+a = (b-a)y+a$ so $(b-a)x = (b-a)y$ and hence $x = y$ since $b-a > 0$. Thus f is injective. Now let $z \in [a, b]$ and consider $x = \frac{z-a}{b-a}$ which lies in $[0, 1]$ since $z \in [a, b]$. Then a computation guarantees that $f(x) = z$, so f is surjective.
Now, the function $g : [0, 1] \to [c, d]$ given by $g(x) = (d - c)x + c$ is also a bijection, and its inverse is given by the formula $g^{-1}(x) = \frac{x-c}{d-c}$. Then $f \circ g^{-1} : [c, d] \to [a, b]$ is a bijection and $(f \circ g^{-1})(x) = (b - a)\frac{x-c}{d-c} + a$.

2. Let $f : A \to B$ and $g : C \to D$ be functions. Define $f \times g = \{\big((a, c), (b, d)\big) \mid (a, b) \in f \wedge (c, d) \in g\}$. Prove that $f \times g$ is a function from $A \times C$ to $B \times D$ and find a formula for $(f \times g)(a, c)$ in terms of $f(a)$ and $g(c)$.

3. In each case, find functions $f : A \to B$ and $g : B \to C$ (you get to pick the sets in each case) with the stated properties:

(a) f is surjecetive, but $g \circ f$ is not surjective.

(b) g is surjective, but $g \circ f$ is not surjective.

(c) $g \circ f$ is surjective, but f is not surjective.

(d) f is injective, but $g \circ f$ is not injective.

(e) g is injective, but $g \circ f$ is not injective.

(f) $g \circ f$ is injective, but g is not injective.

4. Consider the functions $f : (-\infty, 0] \to \mathbb{R}$ and $g : [0, \infty) \to \mathbb{R}$ given by the formulae $f(x) = x^2$ and $g(x) = \cos x$. Is $f \cup g$ a function? Justify.

Solution. No, $f \cup g$ is not a function because $f(0) = 0$ (so $(0,0) \in f$) and $g(0) = \cos 0 = 1$ (so $(0,1) \in g$), and hence $(0,0), (0,1) \in f \cup g$. Thus there is an element in the domain of $f \cup g$ which is related to *two* different elements, and so $f \cup g$ cannot be a function.

5. Suppose $f : A \to B$ and $g : A \to C$ are functions with the same domain. Prove that

$$\langle f, g\rangle := \{(a,(b,c)) \in A \times (B \times C) \mid (a,b) \in f, (a,c) \in g\}$$

is a function.

Solution. Consider any element $a \in A$, then $f(a) \in B, g(a) \in C$ and so $(a, f(a)) \in f$ and $(a, g(a)) \in g$. Hence $(a, (f(a), g(a)) \in \langle f, g\rangle$. Moreover, suppose $(a, (b, c)) \in \langle f, g\rangle$. Then $(a, b) \in f$ and $(a, c) \in g$. Since f, g are functions, their outputs are unique, so $b = f(a)$ and $c = g(a)$. Therefore, $(a, (b, c)) = (a, (f(a), g(a)))$. Thus $\langle f, g\rangle$ is a function.

6. Prove that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x^3 + 5$ is injective and surjective.

Hint. Injectivity should be very easy. For surjectivity, try using the intermediate value theorem from calculus (I will allow you to assume without proof that f is continuous).

Solution. Let $x, y \in \mathbb{R}$ and suppose $f(x) = f(y)$. Then $3x^3 + 5 = 3y^3 + 5$ and so $3x^3 = 3y^3$ and also $x^3 = y^3$. Taking cube roots we find $x = y$. Thus f is injective.
Suppose $z \in \mathbb{R}^2$. Then $z \le |z|$. If $|z| \le 1$, then $|z| \le 5$ and if $|z| \ge 1$, then $|z| \le 3|z|^3$. Either way $|z| \le f(|z|)$.
We know $(-|z|-2)^3 = -|z|^3 - 6|z|^2 - 12|z| - 8 \le -|z| - 8$. Thus $f(-|z|-2) = 3(-|z|-2)^3 + 5 \le -3|z| - 24 + 5 \le -|z| \le z$.
Thus $f(-|z|-2) \le z \le f(|z|)$. Therefore, since f is continuous, by the intermediate value theorem there is some $x \in [-|z|-2, |z|]$ for which $f(x) = z$.

7. Prove that $\sqrt{\cdot} : \{x \in \mathbb{R} \mid x \ge 0\} \to \mathbb{R}$ is injective.

Solution. Suppose $y, z \in \{x \in \mathbb{R} \mid x \ge 0\}$ and $\sqrt{y} = \sqrt{z}$. Then, by the definition of square root, $y = (\sqrt{y})^2 = (\sqrt{z})^2 = z$. Therefore $\sqrt{\cdot}$ is injective on this domain.
Note, we could have also proved this by noting that this is the inverse of the squaring function $(\cdot)^2$ restricted to the nonnegative real numbers, and inverses of functions are always injective by another exercise.

8. Is $f(x) = x^3 - x$ injective if the domain and codomain are both $\mathbb{R}$?

Solution. No, since $f(-1) = f(0) = f(1) = 0$.
Facts about injections, surjections and inverses.

9. Suppose that $f : A \to B$ and $g : B \to C$ are functions. Prove that if $g \circ f$ is injective, then f is injective. Prove that if $g \circ f$ is surjective, then g is surjective.

Solution. We prove the first statement by contraposition. Suppose f is not injective. Then there exist $x, y \in A$ with $x \neq y$ so that $f(x) = f(y)$. Applying g we find that $(g \circ f)(x) = g(f(x) = g(f(y)) = (g \circ f)(y)$, so $g \circ f$ is not injective.

We prove the second statement by contraposition as well. Recall that even for relations, we have $\operatorname{rng}(g \circ f) \subseteq \operatorname{rng}(g)$. Therefore, if g is not surjective, then $\operatorname{rng}(g) \subsetneq C$ and hence $\operatorname{rng}(g \circ f) \neq C$, so $g \circ f$ is not surjective either.

10. Suppose that $f : A \to B$ is a function. Prove that if f is injective, then there is a function $g : B \to A$ so that $g \circ f = Id_A$. Prove that if f is surjective, then there is a function $h : B \to A$ so that $f \circ h = Id_B$.

Solution. Suppose f is injective. Let $f^{-1} : \operatorname{rng}(f) \to A$ be its inverse. Let $a \in A$ be any element. Define $\tilde{g} : B \setminus \operatorname{rng}(f) \to A$ by $\tilde{g}(y) = a$ for all $y \in B \setminus \operatorname{rng}(f)$. Then let $g = f \cup \tilde{g} : B \to A$. Now, for any element $x \in A$, $f(x) \in \operatorname{rng}(f)$, so $g(f(x)) = f^{-1}(f(x)) = x = Id_A(x)$. Thus $g \circ f = Id_A$.

Suppose now that f is surjective. Then for each $y \in B$ the preimage set $f^{-1}(y) := \{x \in A \mid f(x) = y\}$ is nonempty since f is surjective. By the Axiom of Choice we may choose one element from each set. More specifically, there is some function $h : B \to A$ such that $h(y) \in f^{-1}(y)$. Thus, $(f \circ h)(y) = f(h(y)) = y = Id_B(y)$ by the definition of $f^{-1}(y)$, so $f \circ h = Id_B$.

11. Use the previous two exercises to prove that $f : A \to B$ is bijective if and only if there exists a *single* function $g : B \to A$ for which $g \circ f = Id_A$ and $f \circ g = Id_B$.

Solution. If f is bijective, we may simply choose $g = f^{-1}$.

If there exists $g : B \to A$ so that $f \circ g = Id_B$ and $g \circ f = Id_A$ are both bijections. Since $f \circ g$ is surjective, f must be surjective as well. since $g \circ f$ is injective, f must be injective as well. Hence f is a bijection.

12. Find a bijection between $\mathbb{N}$ and $\mathbb{N} \setminus \{1\}$.

Solution. Define $f : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ by $f(n) = n + 1$. The claimed codomain is valid since if $n \in \mathbb{N}$ then $n \geq 1$ and hence $n + 1 \in \mathbb{N}$ and $n + 1 \geq 2$, so $n + 1 \in \mathbb{N} \setminus \{1\}$.

The function f is clearly injective because if $f(n) = f(m)$ then $n + 1 = m + 1$ and hence $m = n$ by cancellation.

The function f is surjective because if $m \in \mathbb{N} \setminus \{1\}$, then $m - 1 \in \mathbb{N}$, and moreover, $f(m - 1) = (m - 1) + 1 = m$.

13. Provide an example of an injective function $f : \mathbb{R} \to \mathbb{R}$ which is not surjective.

Solution. Consider $f(x) = e^x$. Then f is injective because it has an inverse (namely, $\ln(x)$), and it is not surjective because $e^x > 0$ for all x (so no nonpositive values are in the range).

14. Provide an example of a surjective function $f : \mathbb{R} \to \mathbb{R}$ which is not injective.

Solution. The function $f(x) = x(x + 1)(x - 1) = x^3 - x$ is not injective because $f(0) = f(1) = f(-1) = 0$, but it is surjective. The proof of surjectivity uses the intermediate value theorem and is similar to the one given above in a different exercise.

15. Prove by any means that $\mathbb{N}, \mathbb{Z}$ have the same cardinality.

16. For $a, b, c, d \in \mathbb{R}$ with $a < b$ and $c < d$, prove that the intervals $[a, b)$ and $(c, d]$ have the same cardinality by finding a bijection between them.

Solution. By a proof analogous to the homework, the function $g : [0, 1) \to (c, d]$ given by $g(x) = (c-d)x + d$ is a bijection. Moreover, from the homework we know the function $f : [a, b) \to [0, 1)$ given by $f(x) = \frac{x-a}{b-a}$ is a bijection. Therefore $g \circ f : [a, b) \to (c, d]$ is a bijection given by the formula

$$(g \circ f)(x) = g(f(x)) = \frac{c-d}{b-a}(x-a) + d.$$

17. Prove by finding a bijection that $(0, 1)$ and $(0, \infty)$ have the same cardinality. You may use standard facts about functions from calculus to prove your claims.

Solution. Chose $f : (0, 1) \to (0, \infty)$ to be $f(x) = -\ln(x)$. The claimed codomain is valid because $\ln(x) < 0$ if $0 < x < 1$. This function is bijective because it has an inverse, namely, $f^{-1}(x) = e^{-x}$.

18. Recall that $[0, 1]$ is uncountable by Cantor's diagonal argument. Prove that any subset of $\mathbb{R}$ which contains an interval (open, closed, half-open), no matter how small, is uncountable.

Solution. Suppose A is a subset of $\mathbb{R}$ which contains an interval (a, b); if it contains a closed or half-open interval, then it contains this open interval. By earlier exercises, this open interval can be mapped bijectively to $(0, 1)$, and so the inverse of this function is an injection from $(0, 1)$ to A. Thus, the cardinality of A is at least as large as the cardinality of $(0, 1)$, which is uncountable by Cantor's diagonal argument.

19. Prove by any means that the unit circle $\mathbb{T} := \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ has the same cardinality as the unit interval $(0, 1)$.

20. Prove (by any method) that the unit square $[0, 1]^2$ and the unit disk $\mathbb{D} = \{(x, y) \mid x^2 + y^2 < 1\}$ have the same cardinality.

Solution. Consider the function $f : [0, 1]^2 \to \mathbb{D}$ given by the formula $f(x, y) = \left(\frac{x}{2}, \frac{y}{2}\right)$. Note that if $(x, y) \in [0, 1]^2$ then $0 \leq x, y \leq 1$ and hence $0 \leq \frac{x}{2}, \frac{y}{2} \leq \frac{1}{2}$. Therefore, $\left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 \leq \frac{1}{2} < 1$ and hence $f(x, y) \in \mathbb{D}$ as claimed.
We now prove f is injective. Suppose $f(x, y) = f(u, v)$. Then $\left(\frac{x}{2}, \frac{y}{2}\right) = \left(\frac{u}{2}, \frac{v}{2}\right)$ and hence $\frac{x}{2} = \frac{u}{2}$ and similarly $\frac{y}{2} = \frac{v}{2}$. So $x = u$ and $y = v$, hence $(x, y) = (u, v)$, so f is injective.
Consider the function $g : \mathbb{D} \to [0, 1]^2$ given by $f(x, y) = \left(\frac{x+1}{2}, \frac{y+1}{2}\right)$. Note that if $(x, y) \in \mathbb{D}$, then $x^2 + y^2 < 1$ and hence $-1 < x, y < 1$. Adding 1 and dividing by 2 yields $0 < \frac{x+1}{2}, \frac{y+1}{2} < 1$. Thus $f(x, y) \in [0, 1]^2$, as claimed.
We now prove g is injective. The argument that g is injective is very similar to the one for f.
By the Cantor–Schroeder–Bernstein theorem, there is a bijection between $[0, 1]^2$ and $\mathbb{D}$.

5.10 Comprehensive Final Exam Review

1. Show that the statements $(P \land Q) \implies R$ and $(P \land \neg R) \implies \neg Q$ are equivalent by whatever means you prefer.

Solution. Each of the following statements are equivalent.

$$(P \wedge Q) \implies R$$

$$\neg(P \wedge Q) \vee R \text{ definition of } \implies$$

$$(\neg P \vee \neg Q) \vee R \text{ DeMorgan's Laws}$$

$$(\neg P \vee (\neg\neg R)) \vee \neg Q \text{ double negation and associativity/commutativity of disjunction}$$

$$\neg(P \wedge \neg R) \vee \neg Q \text{ DeMorgan's Laws}$$

$$(P \wedge \neg R) \implies \neg Q$$

2. Prove that if $a, b \in \mathbb{Z}$ are relatively prime and for some $c \in \mathbb{Z}$, we have $a \mid c$ and $b \mid c$, then $ab \mid c$.

Solution. Since a, b are relatively prime, we have $\gcd(a, b) = 1$, and by a theorem from class there are integers x, y for which $ax + by = 1$. Multiplying by c we find $acx + bcy = c$. Now since a, b both divide c, there exist integers j, k so that $c = aj$ and $c = bk$. Applying these to the above equation yields

$$c = acx + bcy = abkx + abjy = ab(kx + jy).$$

Thus ab divides c since $kx + jy$ is a integer.

3. Translate the following sentence into a mathematical formula: "Not every real number is the square of a real number."

Solution. $\neg(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^2 = x)$.

4. Prove that for positive integers $a, b, c \in \mathbb{N}$, if $a \mid b$ and $b \mid c$, then $a \mid c$. What does this mean about the divides relation on the positive integers?

Solution. Since $a \mid b$ and $b \mid c$ there are integers m, n so that $b = ma$ and $c = nb$. Therefore $c = nb = n(ma) = (nm)a$. Since nm is an integer, $a \mid c$. This shows that the divides relation on $\mathbb{N}$ is *transitive*.

5. Describe the minimal elements of the divides relation on $N = \mathbb{N} \setminus \{1\}$. You should also prove these elements are minimal and that the elements you propose are the only minimal elements.

Solution. The minimal elements of the divides relation on N are precisely the prime numbers. Indeed, suppose $p \in \mathbb{N}$ is prime. Then its only divisors are $1, p$, but $1 \notin N$. Therefore, for $a \in N$, $a \mid p$ if and only if $a = p$, hence p is minimal.

Similarly, if $b \in N$ is *not* prime, then there is some divisor a with $1 < a < b$, so $a \in N$ and $a \mid b$. Therefore, b is not minimal.

6. Prove that for any odd positive integer n, the quantity n^2+4n+3 is divisible by 8.

Solution 1. Suppose n is odd so that there is an integer m satisfying $n = 2m + 1$. Then

$$n^2+4n+3 = (n+1)(n+3) = (2m+1+1)(2m+1+3) = 2(m+1)2(m+2) = 4(m+1)(m+2).$$

Since $(m + 1)(m + 2)$ is the product of two consecutive integers, it must be even (we proved this elsewhere), and hence there is some integer k so that $(m + 1)(m + 2) = 2k$. Hence $n^2 + 4n + 3 = 8k$.

Solution 2. Given an odd positive integer n, we can write it as $2m+1$ for some nonnegative integer m. Our proof will proceed by induction on m.
Base case: $m = 0$. Notice that when $m = 0$, then $n = 1$, and $n^2 + 4n + 3 = 1 + 4 + 3 = 8$ which is obviously divisible by 8.
Inductive step. Suppose that m is a nonnegative integer and for $n = 2m + 1$, the quantity $n^2 + 4n + 3$ is divisible by 8 so that there is some integer k for which $n^2 + 4n + 3 = 8k$. Then consider $r = 2(m + 1) + 1 = 2m + 3 = n + 2$. Then

$$r^2+4r+3 = (n+2)^2+4(n+2)+3 = (n^2+4n+3)+4n+4+8 = 8k+4(2m+1)+4+8 = 8k+8m*16 = 8(k+m+2),$$

which is divisible by 8.
By induction, we have proven the desired result.

7. Prove that $\sqrt{p}$ is irrational for any prime p.

Solution. Supose $\sqrt{p}$ were rational, so that $\sqrt{p} = \frac{a}{b}$ for some integers a, b. We may assume that the fraction is in lowest terms, i.e., $\gcd(a, b) = 1$. Then squaring our equation and multiplying both sides by b^2, we find $b^2p = a^2$. In particular, this means p divides a^2. Since p is prime, by Euclid's lemma we know p divides a. Thus $a = pk$ for some integer k. Hence $b^2p = a^2 = (pk)^2 = p^2k^2$. Cancelling one of the factors of p, we obtain $b^2 = pk^2$, and hence p divides b. This implies $\gcd(a, b) \geq p > 1$, contradicting the fact that $\frac{a}{b}$ is in lowest terms. Therefore $\sqrt{p}$ is irrational.

8. Fix nonzero integers a, b. Consider the function $f : \mathbb{Z}^2 \to \mathbb{Z}$ given by $f(x, y) = ax + by$. Prove that f is surjective if and only if $\gcd(a, b) = 1$.

Solution. Notice that $\gcd(a, b)$ divides $f(x, y) = ax + by$ for any x, y since it divides each of a, b. Therefore, if $\gcd(a, b) > 1$, then $f(x, y) \neq 1$ for any $x, y \in \mathbb{Z}$, hence f is not surjective.
Now suppose $\gcd(a, b) = 1$. Then by a theorem from class, there exist some integers $r, s \in \mathbb{Z}$ so that $ar + bs = 1$. Now let $c \in \mathbb{Z}$ be arbitrary. Notice that $arc + bsc = (ar + bs)c = c$, and so letting $x = rc \in \mathbb{Z}$, $y = sc\mathbb{Z}$, we have $f(x, y) = c$. Since $c \in \mathbb{Z}$ was arbitrary, f is surjective.

9. Prove that a relation R on A is antisymmetric if and only if for every $x, y \in A$, if $x \, R \, y$ and $x \neq y$, then $y \not R \, x$.

Solution. Apply the equivalence from the first question in this review.

10. Consider $f : \mathbb{R} \to \mathbb{Q}$ given by the formula

$$f(x) = \begin{cases} \frac{1}{q} & \text{if } x = \frac{p}{q} \in \mathbb{Q}, \\ 0 & \text{if } x \notin \mathbb{Q}. \end{cases}$$

Is f well-defined? If so, prove it. If not, explain why and give a counterexample.

Solution. No, f is not well-defined because $f(\frac{1}{2}) = \frac{1}{2}$, and $f(\frac{2}{4}) = \frac{1}{4}$, but $\frac{1}{2} \neq \frac{1}{4}$

11. Find a bijection between the integers $\mathbb{Z}$ and the set A of integers with remainder 2 when divided by 5.

Solution. Let $f : A \to \mathbb{Z}$ be defined as follows: for $n \in A$, let $f(n)$ be the quotient (from the Division Algorithm) of n divided by 5. This function is well-defined because the quotient from the Division Algorithm always exists, and is a unique integer.
Now consider the function $g : \mathbb{Z} \to A$ defined by $g(k) = 5k + 2$. Clearly, $g(k) \in A$ since it has remainder 2 when divided by 5, and so A is a valid

codomain.
Now consider $g \circ f$. Let $n \in A$. By the Division Algorithm, there exist unique integers q, r with $0 \leq r < 5$ so that $n = 5q + r$. Since $n \in A$, $r = 2$. Moreover, by definition $f(n) = q$. Therefore $(g \circ f)(n) = g(f(n)) = g(q) = 5q + 2 = n$. Hence $g \circ f = Id_A$.
Now consider $f \circ g$. Let $n \in \mathbb{Z}$. Notice that $g(n) = 5n + 2$. Since the quotient from the division algorithm is unique, it is clear that $(f \circ g)(n) = f(5n+2) = n$ so that $f \circ g = Id_{\mathbb{Z}}$.
By a result proven previously, since $f \circ g$ and $g \circ f$ are the identity on their respective domains, we know that f, g are bijective and in fact $f^{-1} = g$, thereby proving the result.

12. Use the Cantor–Schröder–Bernstein theorem to prove that $\mathbb{R}$ and $[0, \infty)$ have the same cardinality.

Solution. Notice that the inclusion map $f : [0, \infty) \to \mathbb{R}$ givne by $f(x) = x$ is obviously injective. Moreover, consider the function $g : \mathbb{R} \to [0, \infty)$ given by $g(x) = 2^x$. The codomain $[0, \infty)$ is valid since $2^x > 0$ for all $x \in \mathbb{R}$. Moreover, g is strictly increasing (using, say, the first derivative test from calculus), and therefore injective. Indeed, if $x \neq y$, then $x < y$ (or $y < x$). Thus, $g(x) < g(y)$ (or $g(y) < g(x)$), and hence $g(x) \neq g(y)$. Since we have injective functions in both directions, by the Cantor–Schröder–Bernstein theorem, these sets have the same cardinality.

13. Give an example of a partition of $\mathbb{Z}$ into two sets. If it has a simple expression, determine the equivalence relation which generates this partition.

Solution. Let $2\mathbb{Z}$ be the even integers and $2\mathbb{Z}+1$ be the odd integers. Clearly these sets are disjoint since no integer is both even and odd. Moreover, any integer is either even or odd, so the union of these two sets is all of $\mathbb{Z}$. Therefore this set is a partition.
The equivalence relation which generates this partition is congurence moduluo 2.

14. Give an example of a partition of $\mathbb{Z}$ into infinitely many sets.

Solution. Consider the family of *singletons* (i.e., sets with only one element) $\mathcal{A} := \{\{x\} \mid x \in \mathbb{Z}\}$. Clearly, any two sets from this family are either the same or disjoint since they each only contain a single element. Moreover, the union is all of $\mathbb{Z}$ since for any $x \in \mathbb{Z}$, $x \in \{x\} \subset \bigcup_{A \in \mathcal{A}} A$.
The equivalence relation which generates this partition is equality.

15. Consider the following equivalence relation on $\mathbb{N}^2$: $(x, y) \sim (a, b)$ if and only if $x - y = a - b$. Prove that $\sim$ is an equivalence relation and find the number of elements in each of the equivalence classes $[(1, 1)]$ and $[(3, 1)]$.

Solution. This appeared on a previous review sheet.

16. For an integer $m \in \mathbb{N}$ let $m\mathbb{N}$ denote all the positive multiples of m, i.e., $m\mathbb{N} = \{mk \mid k \in \mathbb{N}\}$. Prove that

$$\bigcup_{p \text{ prime}} p\mathbb{N} = \mathbb{N} \setminus \{1\}.$$

Solution. For any prime p, we know that $p > 2$ and therefore $p\mathbb{N} \subseteq \mathbb{N} \setminus \{1\}$. Taking the union over all p prime, we find

$$\bigcup_{p \text{ prime}} p\mathbb{N} \subseteq \mathbb{N} \setminus \{1\}.$$

We now prove the other inclusion by using the well-ordering principle. Suppose the difference $D := (\mathbb{N} \setminus \{1\}) \setminus \left(\bigcup_{p \text{ prime}} p\mathbb{N}\right)$ is nonempty. Then since $\mathbb{N}$ is well-ordered, D has a minimum element which we will call n.
Since $n > 1$, are two possibilities, either n is prime, in which case $n \in n\mathbb{N}$ contradicting the fact that $n \in D$; or n is composite. In this case, $n = ab$ for some $1 < a, b < n$. Since $1 < a < n$, $a \notin D$, and therefore $a \in p\mathbb{N}$ for some prime p. Hence, $a = pk$ for some $k \in \mathbb{N}$. Finally, $n = ab = p(kb) \in p\mathbb{N}$, contradicting the fact that $n \in D$. Therefore our assumption that D is nonempty is false. This proves the other inclusion.

17. Given sets A, B prove that $A = B$ if and only if $A \setminus B = \varnothing = B \setminus A$.

Solution. It is clear that if $A = B$ then $A \setminus B = B \setminus A = A \setminus A = \varnothing$.
For the other direction, suppose that $A \setminus B = \varnothing = B \setminus A$. Let $x \in A$. Then since $A \setminus B = \varnothing$, we know that $x \in B$ (for otherwise $x \in A \setminus B$). Therefore $A \subseteq B$. A symmetric argument proves $B \subseteq A$.

18. Give an example of a tautology. Give an example of a contradiction.

Solution. tautology: $P \vee \neg P$. contradiction: $P \wedge \neg P$.

19. There is a result which says that if $a, b \in \mathbb{N}$ and a divides b and b divides a, then $a = b$. What does this tell you about the divides relation on $\mathbb{N}$? Does the same result hold for the divides relation on $\mathbb{Z}$?

Solution. This result says precisely that the divides relation is antisymmetric on $\mathbb{N}$. No, it does not hold on $\mathbb{Z}$. Indeed, if $m \in \mathbb{Z}$ and $m \neq 0$, then $m = (-1)(-m)$, and therefore $m \mid -m$. Similarly $-m = (-1)m$ so $-m \mid m$. But $m \neq -m$ since $m \neq 0$.

20. Prove by (strong) induction on n that

$$\sum_{k=1}^{n}(-1)^{n-1}(n-1) = \begin{cases} \frac{n}{2} & n \text{ even;} \\ \frac{-n+1}{2} & n \text{ odd.} \end{cases}$$

Solution. *Base case.* For $n = 1$, the quantity on the left is $\sum_{k=1}^{1}(-1)^{1-1}(1-1) = 0 = \frac{-1+1}{2}$.
Inductive step. Now suppose $n \in \mathbb{N}$ and the formula holds for n.
Case 1: n even. In this case, $(-1)^{n+1} = -1$ since $n+1$ is odd. By the inductive hypothesis, we have

$$\sum_{k=1}^{n+1}(-1)^n(n-1) = \sum_{k=1}^{n}(-1)^n(n-1) + (-1)^{n+1}n = \frac{n}{2} - n = -\frac{n}{2} = \frac{-(n+1)+1}{2},$$

as desired.
Case 1: n odd. In this case, $(-1)^{n+1} = 1$ since $n+1$ is even. By the inductive hypothesis, we have

$$\sum_{k=1}^{n+1}(-1)^n(n-1) = \sum_{k=1}^{n}(-1)^n(n-1) + (-1)^{n+1}n = \frac{-n+1}{2} + n = \frac{n+1}{2},$$

as desired.
Don't look now, but if we use this formula to define a function $f : \mathbb{N} \to \mathbb{Z}$, by $f(n) = \sum_{k=1}^{n}(-1)^n(n-1)$, then f is just our usual bijection between $\mathbb{N}$ and $\mathbb{Z}$.

21. Consider $\mathbb{N}^2$ equipped with the equivalence relation $(x, y) \sim (a, b)$ if and only if $x - y = a - b$. Define an addition on the collection of equivalence classes

$\mathbb{N}^2/\sim$ defined by $+ : \left(\mathbb{N}^2/\sim\right)^2 \to \mathbb{N}^2/\sim$ with the formula

$$[(x,y)] + [(a,b)] = [(x+a, y+b)].$$

Show that $+$ is well-defined.

Solution. We need to show that the resulting equivalence class under addition is *independent* of the choice of representatives from the original equivalence classes. So, suppose $(x',y') \in [(x,y)]$ and $(a',b') \in [(a,b)]$. Then $x-y = x'-y'$ and $a-b = a'-b'$. Therefore,

$$(x+a)-(y+b) = (x-y)+(a-b) = (x'-y')+(a'-b') = (x'+a')-(y'+b'),$$

and hence $[(x+a, y+b)] = [(x'+a', y'+b')]$. Thus $+$ is well-defined.

22. Consider the relation on $\mathbb{R}$ given by $x \sim y$ if and only if $x - y \in \mathbb{Q}$. Prove that $\sim$ is an equivalence relation.

Solution. Clearly $\sim$ is reflexive since for any $x \in \mathbb{R}$, $x - x = 0 \in \mathbb{Q}$ and so $x \sim x$.
Now suppose $x, y \in \mathbb{R}$ and $x \sim y$. Then $x - y \in \mathbb{Q}$ and hence $y - x = -(x-y) \in \mathbb{Q}$. Therefore $\sim$ is symmetric.
For transitivity it will be helpful to remember that $\mathbb{Q}$ is closed under addition since $\frac{p}{q} + \frac{a}{b} = \frac{pb+aq}{qb}$. Suppose that $x \sim y$ and $\sim z$. Then $x - y \in \mathbb{Q}$ and $y - z \in \mathbb{Q}$. Therefore $x - z = (x-y) + (y-z) \in \mathbb{Q}$ and hence $x \sim z$. Thus $\sim$ is transitive.
Since $\sim$ is reflexive, symmetric and transitive, it is an equivalence relation.

23. Prove that if n^2 is even if *and only if* n is even.

Solution. Suppose n is even. Then $n = 2k$ for some integer k. Thus $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ which is even since $2k^2 \in \mathbb{Z}$.
For the other direction we use contraposition. Suppose n is not even. Then by parity n is odd and hence $n = 2k+1$ for some integer k. Thus

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

which is odd since $2k^2 + 2k \in \mathbb{Z}$. Thus n^2 is not even. By contraposition, if n^2 is even then n is even.

24. Generalize the previous exercise to arbitrary primes p in the following manner: Prove that n^2 is a multiple of p if and only if n is a multiple of p.

Hint. Euclid's lemma.

Solution. If n is a multiple of p, then $n = pk$ for some integer k. Thus $n^2 = (pk)^2 = p(pk^2)$ is a multiple of p as well.
For the oher direction, if n^2 is a multiple of p then $n^2 = pk$ for some integer p. This means that p divides n^2. By Euclid's lemma p divides n.

25. Give an example to show that the result from the previous exercise doesn't necessarily hold if p is not prime.

Solution. Consider $p = 4$ and $n = 2$. Then $n^2 = 4 = p$ is a multiple of p, but n is not a multiple of p since it is less than p.

Chapter 6

List of Definitions

Definition 1.1.1 Proposition
Definition 1.1.2 Conjunction, Disjunction, Negation
Definition 1.1.3 Well-formed formula
Definition 1.1.4 Equivalent forms
Definition 1.1.5 Tautology
Definition 1.1.7 Contradiction
Definition 1.1.9 Denial
Definition 1.2.1 Conditional, Antecedent, Consequent
Definition 1.2.4 Converse, Contrapositive
Definition 1.2.6 Biconditional
Definition 1.3.1 Quantifiers
Definition 1.3.3 Uniqueness quantifier
Definition 1.4.1 Definition, Axiom, Theorem
Definition 1.7.2 Greatest Common Divisor
Definition 1.7.6 Relatively Prime, Coprime
Definition 2.1.1 Set
Definition 2.1.2 Empty Set
Definition 2.1.3 Subset
Definition 2.1.5 Set equality
Definition 2.1.6 Power set
Definition 2.2.1 Union, intersection, difference
Definition 2.2.3 Disjoint
Definition 2.2.4 Set complement
Definition 2.2.6 Cartesian product
Definition 2.3.1 Family, collection
Definition 2.3.2 Arbitrary union
Definition 2.3.3 Arbitrary intersection
Definition 2.3.5 Pairwise disjoint
Definition 2.4.3 Strong induction
Definition 2.6.5 Permutation (combinatorics)
Definition 2.6.8 Combination
Definition 3.1.1 Relation
Definition 3.1.5 Domain, Range
Definition 3.1.6 Identity relation
Definition 3.1.7 Inverse relation

(Continued on next page)

Definition 3.1.11	Relation Composition
Definition 3.2.1	Reflexive
Definition 3.2.2	Symmetric
Definition 3.2.3	Transitive
Definition 3.2.4	Antisymmetric
Definition 3.2.10	Equivalence relation
Definition 3.2.11	Modular congruence
Definition 3.2.13	Equivalence class
Definition 3.2.14	Partition
Definition 3.3.1	Partial order, total order
Definition 3.3.3	Minim(al/um), Maxim(al/um)
Definition 3.3.9	Well order
Definition 3.4.1	Graph
Definition 4.1.1	Function
Definition 4.1.5	Restriction
Definition 4.1.8	
Definition 4.2.1	
Definition 4.2.3	
Definition 4.2.4	
Definition 4.2.8	
Definition A.1.1	
Definition A.1.2	Even integers
Definition A.1.3	Odd integers
Definition A.1.6	Divisibility
Definition A.1.7	Prime

Appendix A

Prerequisites

A.1 Number classes

Although mathematicians ultimately regard the fundamental undefined object as the set, in the context of this course we will ultimately work with several mathematical

Definition A.1.1. We will take several familiar number classes as objects which we assume we already understand. These are:

natural numbers, $\mathbb{N}$ the set of positive integers (also known as whole numbers or counting numbers), which we enumerate as $1, 2, 3, \ldots$ We will not define these at any point during the course.

integers, $\mathbb{Z}$ the set of integers, including those positive, negative and zero, which we enumerate as $\ldots \quad -2, -1, 0, 1, 2, \ldots$ We will not formally define these at any point in the course, although we will discuss how they could be defined in terms of the set $\mathbb{N}$.

rational numbers, $\mathbb{Q}$ the set of rational numbers, i.e., those numbers which may be written as a fraction of two integers of which the denominator is nonzero. After covering equivalence relations, we will formally define $\mathbb{Q}$ in terms of $\mathbb{Z}$.

algebraic numbers, $\overline{\mathbb{Q}}$ the set of algebraic numbers, i.e., those numbers which are roots of a polynomial with integer coefficients. For example, $\sqrt{2}$ is algebraic because it is a root of the polynomial $x^2 - 2$. Similarly, the imaginary unit i is algebraic because it is a root of $x^2 + 1$. Although it is not easy to prove, π is *not* an algebraic number. While you may not be familiar with algebraic numbers, they are in many ways a more natural class to work with than the real numbers.

real numbers, $\mathbb{R}$ the set of real numbers, i.e., those numbers which correspond to all possible places on a number line, or alternatively, all numbers represented by infinite decimal expansions. These include, for example, $\sqrt{2}, \pi, e$ and others, but not any numbers involving the imaginary unit i. If time allows and there is sufficient interest, we will cover the construction of the real numbers at the end of the semester.

complex numbers, $\mathbb{C}$ the set of complex numbers, i.e., all those numbers of the form $a + bi$ where $a, b \in \mathbb{R}$ and i is the imaginary unit satisfying the relation $i^2 = -1$. These can also be defined as those numbers which are roots of a polynomial with real coefficients (in fact, we can even restrict the polynomial to have degree two or less). This set includes all previous classes mentioned.

Definition A.1.2 (Even integers)**.** An integer $n \in \mathbb{Z}$ is said to be **even** if it can be written as $n = 2k$ for some integer $k \in \mathbb{Z}$.

Definition A.1.3 (Odd integers)**.** An integer $n \in \mathbb{Z}$ is said to be **odd** if it can be written as $n = 2k + 1$ for some integer $k \in \mathbb{Z}$.

Exercise A.1.4 (Parity)**.** Prove that every integer is either even or odd, but never both.

Theorem A.1.5 (Properties of number classes)**.** *Let* $\mathbb{F}$ *denote* any *of the number classes mentioned in Definition 1. Then*

- $\mathbb{F}$ *is closed under addition and multiplication. That is, if* $x, y \in \mathbb{F}$ *then* $x + y, xy \in \mathbb{F}$.

- *Addition and multiplication are* ***commutatitive*** *in* $\mathbb{F}$*. That is, if* $x, y \in \mathbb{F}$ *then*
$$x + y = y + x, \qquad xy = yx.$$

- *Addition and multiplication are* ***associative*** *in* $\mathbb{F}$*. That is, if* $x, y \in \mathbb{F}$ *then*
$$(x + y) + z = x + (y + z), \qquad (xy)z = x(yz).$$

- *Multiplication* ***distributes*** *over addition in* $\mathbb{F}$*. That is, if* $x, y \in \mathbb{F}$ *then*
$$(x + y)z = xz + yz, \qquad z(x + y) = zx + zy.$$

- *For any class* $\mathbb{F}$ *except for* $\mathbb{N}$, ***additive inverses*** *exist. That is, for any* $x \in \mathbb{F}$*, there exists* $y \in \mathbb{F}$ *(namely,* $y = -x$*) so that*
$$x + y = 0.$$

- *For any class* $\mathbb{F}$ *except for* $\mathbb{N}, \mathbb{Z}$*, every nonzero element has a* ***multiplicative inverse****. That is, for any* $x \in \mathbb{F}$*, if* $x \neq 0$*, then there exists* $y \in \mathbb{F}$ *(namely,* $y = \frac{1}{x}$*) so that*
$$xy = 1.$$

Definition A.1.6 (Divisibility)**.** For integers $a, b \in \mathbb{Z}$, we say a **divides** b if there is some integer $k \in \mathbb{Z}$ for which $b = ak$. In this case we say a is a **divisor** or **multiple** of b.

Definition A.1.7 (Prime)**.** A natural number $p \in \mathbb{N}$ is said to be **prime** if $p > 1$ and the only divisors of p are 1 and itself. A natural number greater than 1 which is not prime is said to be **composite**.

Appendix B

Notation

Symbol	**Description**	**Page**
$P \vee Q$	Disjunction of propositions	1
$P \wedge Q$	Conjunction of propositions	1
$\neg P$	Negation of a proposition	1
$P \implies Q$	Conditional implication	2
$P \iff Q$	Biconditional implication	3
$\forall$	Universal quantifier	5
$\exists$	Existential quantifier	5
$\exists!$	Unique existential quantifier	6
$\gcd(a, b)$	greatest common divisor of two integers	12
$\subseteq$	subset	16
$\mathscr{P}(A)$	power set	16
$\cup$	union	16
$\cap$	intersection	16
$\setminus$	difference	16
A^c	complement of a set A	17
$\displaystyle\bigcup_{A \in \mathcal{A}} A$	union over a family A	19
$\displaystyle\bigcap_{A \in \mathcal{A}} A$	intersection over a family A	19
$\mathbb{N}$	Set of natural numbers	75
$\mathbb{Z}$	Set of integers	75
$\mathbb{Q}$	Set of rational numbers	75
$\overline{\mathbb{Q}}$	Set of algebraic numbers	75
$\mathbb{R}$	Set of real numbers	75
$\mathbb{C}$	Set of complex numbers	75

Index

1-1, *see* injective

1729, 11

antecedent, 2
antisymmetric, 26, 27
argument, 31
associativity
  of addition, 76
  of multiplication, 76
axiom, 7
Axiom of Choice, 30

biconditional, 3
bijective, 33
binomial coefficient, 24
binomial theorem, 24
boilerplate, 11

closed
  under addition, 76
  under multiplication, 76
codomain, 31
collection, 19
combination, 24
combination rule, 24
common divisor, 12
commutativity
  of addition, 76
  of multiplication, 76
complement, 17
composite, 76
conditional, 2
congruent, 28
conjunction, 1
consequent, 2
contradiction, 2
contrapositive, 3
converse, 3
coprime, 13

De Morgan's Laws, 3
decreasing
  strictly, 32
definition, 7
denial, 2
difference, 16
disjoint, 17
disjunction, 1
distributivity, 76
dividend, 12
divides, 25, 76
division algorithm, 12
divisor, 12, 76
domain, 25, 31

edge, 30
empty set, 15
equivalent, 1
Euclid's lemma, 13
extension, 32

factorial, 23
family, 19
function, 31

Goldbach conjecture, 7
graph, 30
greatest common divisor, 12

Hardy–Ramanujan number, 11
hypothesis, 8

if and only if, *see also* equivalent
iff, 10
image, 31
implication, 2
Inclusion–Exclusion Principle, 23
increasing
  strictly, 32
index set, 19
induction, 20
inductive set, 20
injective, 32
integer
  even, 76

odd, 76
intersection, 16
inverse
additive, 76
multiplicative, 76

Law of Excluded Middle, 2
lemma, 7
linear combination, 12

map, *see* function
mapping, *see* function
maximal, 29
maximum, 29
minimal, 29
minimum, 29
modulus, 28
modus ponens, 7
multiple, 76

negation, 1
number
algebraic, 75
complex, 75
integer, 75
natural, 75
rational, 75
real, 75

one-to-one, *see* injective
one-to-one correspondence, *see* bijective
onto, 32
open sentence, *see also* predicate

pairwise disjoint, 20
partial order, 29
strict, 29
partition, 28
permutation, 23
power set, 16
predicate, 5
prime, 76
relatively, 13
product rule, 23
proof, 7
biconditional, 10
by cases, 8
by contradiction, 9
by contraposition, 9
direct, 7
two-part, 9
with existential quantifier, 10
with unique existential quantifier, 11
with universal quantifier, 10
proposition, 1

quantifier, 5
existential, 5
unique existential, 6
universal, 5
quotient, 12

range, 25
reflexive, 26
relation, 25
composite, 26
equivalence, 28
identity, 26
inverse, 26
remainder, 12
restriction, 32

set membership, 5
strong induction, 21
subset, 16
sujective, 32
sum rule, 23
symmetric, 26

tautology, 2
total order, 29
transitive, 26
truth value, 1

union, 16
universe, 5

value, 31
vertex, 30

well order, 30
well-formed formula, 1
well-ordering principle, 21