

Contents

1	Mathematical Language and Logic	1
1.1	A Little Symbolic Logic	1
1.2	Quantifiers	8
2	Proving Things	11
2.1	Quantifiers and Proofs	12
2.2	Conditional Statements	14
2.3	Proving Practice	16
2.4	Mathematical Induction	17
3	Naive Set Theory	20
3.1	Sets and Operations on Sets	20
3.2	Indexed Families of Sets	23
4	Functions and Relations	25
4.1	Relations	25
4.2	Order Relations	28
4.3	Functions	30
4.4	The Axiom of Choice	33
4.5	Generalized Products of Sets	34
5	Cardinality of Sets	36
5.1	Finite and Infinite Sets	36
5.2	Countable and Uncountable Sets	38

An Intro to Proving and Basic Math Concepts

M.M.Marsh

August 5, 2015

Chapter 1

Mathematical Language and Logic

1.1 A Little Symbolic Logic

A **statement** is a sentence that, in the absence of subjective judgement, is either true or false, but not both.

Problem 1.1.1 *Which of the following are statements?*

1. $3 + 2$ is equal to 6.
2. *Extraterrestrials have visited the Earth.*
3. *Math is fun.*
4. *It is not raining. (at the closest outside location, right now)*
5. *The digit 8 occurs more times than any other digit in the most recent edition of the Calculus text by Stewart.*
6. *The weather in Sacramento is better than the weather in Los Angeles.*
7. $x + 2 = 6$.

Definition 1.1.1 *Suppose P is a statement. The **negation (or denial, or logical opposite)** of P , denoted $\neg P$, is the statement “It is not the case that P ”.*

If P is true, $\neg P$ is false, and vice versa. As we will see later, it is imperative that when given a statement, we are able to correctly write its negation. Now, from the definition above, this seems ridiculously easy. For example, take the statement

P : “Jim weighs over 200 pounds”.

From the definition, its negation is “It is not the case that Jim weighs over 200 pounds”. Indeed, this is the negation; however, we prefer to write the negation in a more simply stated way, without using the phrase “it is not the case that ...”. That is, we wish to find a simpler statement that is “logically equivalent” to

$\neg P$: “It is not the case that Jim weighs over 200 pounds”.

So, like it or not, we will also have to decide when two statements are logically equivalent to each other. Let’s try a few possible negations for this example; that is, possible equivalent statements to $\neg P$ above.

- (1) “Jim doesn’t weigh over 200 pounds”, or
- (2) “Jim weighs 200 pounds or less”, or
- (3) “Jim weighs 160 pounds”?

Are all of these statements negations of the original statement? Are they all logically equivalent to each other? What about the last two statements, (2) and (3)? It’s possible that Jim weighs 200 pounds or less but doesn’t weigh 160 pounds. That is, statement (2) could be true while at the same time statement (3) is false. Thus, these two aren’t logically equivalent. So, not both are negations. Notice that statements (1) and (2) must both be true or both be false, regardless of what Jim weighs. If “Jim weighs over 200 pounds” is true, they are both false. If “Jim weighs over 200 pounds” is false, they are both true. Let’s look at another example.

Example 1.1.1 Consider statements P and possible negations Q below.

P	Q
1. $3 + 2 = 6$	$3 + 2 \neq 6$ $3 + 2 = 5$ <i>there are more than two people in this class</i> <i>the word "math" has exactly four letters</i> $4 \times 2 = 8$ <i>this course is extra fun</i> <i>logic is not very logical</i>
2. $e^\pi = 26.412$	$e^\pi \neq 26.412$ $e^\pi = 4$
3. <i>it is raining</i>	<i>it is not raining</i> <i>it is sunny</i>

Discussion. Notice that in 1 of this example, statement P is false and all of the possible negation statements Q are true. (Pretend that the last two are really statements, and that they are true.) Does this mean that all of the statements Q are negations of P ? It seems unlikely. In fact, some of the candidates for Q don't even have a 3, 2, or 6 in them. So, surely, they're not all logically equivalent to each other.

In 2, some of you may not know if statement P is true or false. Should this lack of knowledge affect which statement Q is the appropriate negation? And in 3, statement P may be false now, but at another time it may be true. Surely, none of these considerations should influence whether one statement is the logical negation of another.

Here's a way to think about it. Knowing the actual truth values of two statements doesn't give us any information about their meanings; nor does it indicate if they are "related in meaning". To determine if there is any relationship in meaning, we assume all possible truth values of one and see if the truth values of the other are affected by these assumptions. Statements P and Q are logically equivalent if the assumption that P is true implies that Q is true, AND the assumption that P is false implies that Q is false. Analogously, if P and Q can have opposite truth values, then they're not logically equivalent, as we observed in the example about Jim's weight.

To check if statements P and Q are negations of each other, we ask if under the assumption that P is true, must Q be false AND under the assumption that P is false, must Q be true. Analogously, it is not possible for P and Q to have the same truth values.

Problem 1.1.2 State negations of the statements below. Do not use the phrase “it is not the case that”.

1. Extraterrestrials have visited the earth.
2. The front wall in this room is green.
3. Saturn is larger (in diameter) than Neptune.
4. Saturn is the largest of all the planets in our solar system.
5. $\sqrt{2}$ is an irrational number.
6. There is a direct airline flight from San Francisco to New Orleans.

The statements in Problem 1.1.1 and Problem 1.1.2 are called **simple statements**. Statements can be combined with other statements to make new statements, called **compound statements**. We now consider the three basic types of compound statements.

Definition 1.1.2 Suppose P and Q are statements. The **conjunction of P and Q** , denoted $P \wedge Q$, is the statement “ P and Q ”. The **disjunction of P and Q** , denoted $P \vee Q$, is the statement “ P or Q ”.

Problem 1.1.3 What should be the truth values of $P \wedge Q$ and $P \vee Q$ for the various combinations of truth values of P and Q ? I.e., fill in the following “truth table”.

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

Should $P \vee Q$ and $Q \vee P$ be equivalent (have the same truth values)? What about $P \wedge Q$ and $Q \wedge P$? If we have conjunctions of three or more statements, “when” would we expect the resulting compound statement to be true? What about finite disjunctions? Since our truth table gives “true or false” of conjunction and disjunction for two statements at a time, are parentheses necessary in these “extended finite versions” of conjunction and disjunction? When we write or speak conjunctions (or disjunctions) of three or more statements, parentheses certainly aren’t present. So, could the “meaning” be unclear?

Definition 1.1.3 Suppose P and Q are statements. The statement “If P , then Q ” is called a **conditional statement** and is denoted $P \Rightarrow Q$. P is called the **hypothesis** of the statement and Q is called the **conclusion**. The **biconditional statement** is the statement $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ and is denoted $P \Leftrightarrow Q$. We say “ P if and only if Q ” for biconditional statements.

The following terminology is considered to be equivalent in meaning to “if P , then Q ”.

- ◇ P only if Q ◇ P is a sufficient condition for Q
- ◇ Q if P ◇ Q is a necessary condition for P
- ◇ Q provided that P ◇ P implies Q

The meaning of the conditional statement “if P , then Q ” is the same as the meaning of the statement “it’s not the case that $(P \wedge \neg Q)$ ”. Does this seem reasonable? Make up some examples. Here’s one example to get you started.

“If I finish the semester with a 90% average or better, then I’ll get an A.”

Equivalently,

“It’s not the case that (I will finish the semester with a 90% average or better and I won’t get an A).” or

“It won’t happen that (I finish the semester with a 90% average or better and I don’t get an A).”

Since parentheses are not used in this way in written English and can’t be discerned in spoken English, the second and third statements aren’t typical of what one would actually say. We simply wish to observe here that the three statements express the same thought.

Problem 1.1.4 Accepting the comment above, we wish for $P \Rightarrow Q$ and $\neg(P \wedge \neg Q)$ to be equivalent in the sense of Definition 1.1.4 below. So, construct the truth table for $P \Rightarrow Q$.

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

Definition 1.1.4 Compound statements are **equivalent** if they have identical truth tables.

Definition 1.1.5 A compound statement is a **tautology** if it is true regardless of the truth values of its parts. (e.g., $P \vee \neg P$)

Problem 1.1.5 Show that the following statements are equivalent using truth tables.

1. $\neg(\neg P)$ and P
2. $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$
3. $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$
4. $P \Rightarrow Q$ and $\neg P \vee Q$

By Problem 1.1.4, $P \Rightarrow Q$ is equivalent to $\neg(P \wedge \neg Q)$. So, using Problem 1.1.5, part 1, what is $\neg(P \Rightarrow Q)$ equivalent to?

Problem 1.1.6 Write what you think would be negations of the two statements below.

1. John plays basketball and John is a math major.
2. Either Jane is a math major or Jane is an English major.

Do your negations agree with parts 2 and 3 of Problem 1.1.5?

Problem 1.1.7 Show that the following statement is a tautology. $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$

Problem 1.1.7 above allows us to use “deductive reasoning” to prove that conditional statements (implications) are true. As we will see in Chapter 2 (Proving Things), many mathematical theorems are of the form $P \Rightarrow Q$. To establish the truth of such a theorem we wish to verify that $P \Rightarrow Q$ is true. From our truth tables above, we see that there is only one way for a conditional statement to be false, namely, if the hypothesis is true and the conclusion is false. So, we must show that if we assume the hypothesis to be true, then the conclusion must be true also. Let’s see how the tautology in Prob 1.1.7 above can help us.

Say we wish to show that $P \Rightarrow R$ is true. We assume that P is true. Perhaps we can’t see how “in one step” to show that R is true, but we can show that some other statement Q is true. So $P \Rightarrow Q$ is true. And, in turn, we see that knowing Q is true gives us that R is true. So, $Q \Rightarrow R$ is true. Since both of these implications are true, their conjunction $(P \Rightarrow Q) \wedge (Q \Rightarrow$

R) is true. Since Problem 1.1.7 is a tautology (always true), it can't have a true hypothesis and a false conclusion. Thus, $P \Rightarrow R$ is true and we are done. This type of “step-by-step” verification of the truth of implications is essentially what we call deductive reasoning.

Problem 1.1.8 Use Problem 1.1.7 to show that $((P \Rightarrow Q) \wedge (Q \Rightarrow R) \wedge (R \Rightarrow S)) \Rightarrow (P \Rightarrow S)$ is true. Can you now prove more “extended finite versions” of this tautology?

Note 1.1.1 Observe, using truth tables, that two statements P and Q have the same truth values exactly when the biconditional $P \Leftrightarrow Q$ is true.

Recall from Definition 1.1.4 that compound statements are equivalent if they have identical truth tables; i.e., in all cases, they have the same truth values. So, based on the note above, we will say that any two statements P and Q are **equivalent** if the biconditional $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is true, i.e., if $P \Rightarrow Q$ is true and $Q \Rightarrow P$ is true. Hence, we can verify that statements P and Q are equivalent by using deductive reasoning. We simply have two implications to verify.

Problem 1.1.9 Use deductive reasoning to prove

$P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$ (Hint: Use commutativity of \vee and Problem 1.1.5, parts 1 & 4).

Definition 1.1.6 The **contrapositive** of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$. The **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$.

Problem 1.1.10 Problem 1.1.9 above shows that each conditional statement is equivalent to its contrapositive. Is it also equivalent to its converse?

Problem 1.1.11 Consider the statements below.

P : All math majors have a 4.00 GPA.

Q : Some math majors have a 4.00 GPA.

R : There is a math major with a 4.00 GPA.

S : If a person is a math major, then he or she has a 4.00 GPA.

T : No math major has less than a 4.00 GPA.

- (1) How do these statements differ from those in the previous problems?
- (2) Try to write their negations.
- (3) Do any of the statements seem logically equivalent?

1.2 Quantifiers

A **variable** is a symbol representing something unspecified, an unknown.

If a variable appears in a sentence without previous specification, then the sentence cannot be a statement. Recall the definition of “statement”. The sentence has no logical meaning (it makes no sense to say that it is true or false) until some comment about the possible replacement values of the variable is made.

Example 1.2.1 *Here are some examples of sentences that include variables, but are not statements. That is, they are neither true nor false.*

1. $x > 10$
2. $x^2 + x - 2 = 0$
3. $\cos \theta \leq 1$
4. Δ has blue eyes.

If we modify these sentences by specifying “conditions” on the variables or by simply replacing the variables with “values”, then they may become statements. For example, looking at 1, we might write “If $x = 5$, then $x > 10$ ”, or simply “ $5 > 10$ ”. Or perhaps, “If x is an integer, then $x > 10$ ”. Looking at 4, we might write “There is a person Δ in this class such that Δ has blue eyes. Is it clear that these modified sentences are statements? Try a few yourself.

A **predicate** is a sentence containing one or more variables so that if the variables are replaced with specific “values” or if quantifiers and “sets of values” from which the variables may be chosen are specified, then the sentence becomes a statement. The sentences in Example 1.2.1 are predicates.

Here are the definitions we need to make these comments a bit more clear.

Definition 1.2.1 *The **universal set** for a variable x is the collection of all values (or objects, or things) that may be used as replacements for x in a predicate containing x .*

Definition 1.2.2 *Suppose x is a variable, U_x is its universal set, and $P(x)$ is a predicate containing only the variable x . We can make statements using quantifiers with $P(x)$ in two ways.*

(1) Adding a **universal quantifier**, as below.

For every x in U_x , $P(x)$. We write symbolically $(\forall x)P(x)$.

(2) Adding an **existential quantifier**, as below.

There is an x in U_x such that $P(x)$. We write $(\exists x)P(x)$.

Note that the reference to the universal set U_x is omitted in the symbolic notation. So, the universal set must be either stated at the outset or obvious from context. Or, one can include it in the notation; e.g., $(\exists x \text{ in } U_x)P(x)$. We will usually not include the universal set in the notation unless there is confusion by its omission.

As stated in the definition, a predicate can contain more than one variable. For example, “ x is less than y ” is a predicate with two variables. We would use the notation $P(x, y)$ to denote this predicate. And, of course, either specific values for x and y or the addition of quantifiers for both x and y are necessary to transform the predicate into a statement. Similar comments and notation apply for predicates with any finite number of variables.

Problem 1.2.1 In example 1.2.1 above, let $P(x)$ be the predicate in 1, $Q(x)$ in 2, $R(\theta)$ in 3, and $B(\Delta)$ in 4. Let U_x be the set of all real numbers, U_θ be the set of all real numbers, and U_Δ be the set of all students in this class. Consider the following quantified statements. Write them out in English. Determine if the resulting statement is true or false. And write, in English, what you think their negations should be. Notice what happens to the quantifiers when you negate a quantified statement.

1. $(\forall x)P(x)$
2. $(\exists x)Q(x)$
3. $(\exists x)(P(x) \wedge Q(x))$
4. $(\forall x)(P(x) \vee Q(x))$
5. $(\forall \theta)R(\theta)$
6. $(\forall \Delta)B(\Delta) \wedge (\exists \theta)R(\theta)$

In Problem 1.2.1(part 1) above, did you get “For every real number x , $x > 10$ ”? Could you equivalently write, “If x is a real number, then $x > 10$ ”? Notice the relationship between “If, then” terminology and universal quantifiers. In our usage of the English language, we sometimes express equivalent ideas in different ways. So, it will be important to determine precisely what kind of terminology gives rise to statements involving quantifiers. Of course, statements such as

“for every real number x , $x > 10$ ”, and

“there is a real number x such that $x^2 + x - 2 = 0$ ”

are easily seen to involve quantifiers. Let’s revisit Problem 1.1.11.

In the statement P, for example, what quantifiers are present? How many variables are involved? What is the universal set? What sort of logic connectives are involved?

Problem 1.2.2 *Write the statements P and R from Problem 1.1.11 in symbolic notation using quantifiers. Also, write their negations in English. How close were your original attempts when you didn’t know about quantifiers?*

Problem 1.2.3 *Decide if the following statements are equivalent.*

1. *For every positive number y , there is a positive number x such that $x < y$.*
2. *There is a positive number x such that for every positive number y , $x < y$.*

We will see in the next chapter, when we begin learning how to “prove” mathematical statements, that being able to correctly interpret a statement (using quantifiers, etc.) will, in some sense, tell us exactly what we need to do to prove that the statement is true. You might want to put this comment to use when you are asked later to prove 1 and 2 of Problem 1.2.3 above.

Chapter 2

Proving Things

In this chapter, we will begin learning to prove mathematical statements. Simply stated, to prove a mathematical statement means to ascertain, somehow, that it is true. “Proving things” is what being a mathematician is all about. You will continue to develop your skills at this activity in the remainder of this course, in most of your other upper level math courses, and in your career as a mathematician and/or a teacher of mathematics. The level of skill that you develop in proving things will be directly proportional to the ease at which you learn new mathematical concepts and, in turn, to your depth of understanding and your general enjoyment of mathematics.

The techniques discussed in this chapter are basic and of a general nature. They are certainly not all-encompassing. There will be occasions when you will need to develop your own techniques to prove something; you may need to be clever or insightful. As with any endeavor that is not at once trivial, practice and hard work will eventually reward you.

Here are some important things to keep in mind when writing or presenting a proof.

1. Your audience is bright, but cannot read your mind and doesn't want to have to guess as to the meanings of undefined terms or unquantified variables.
2. You should write in complete sentences. It is OK to use notation, but when one reads the notation and surrounding words aloud, one should be reading sentences. You might observe that this is true throughout these notes.
3. The work that you do in discovering a proof is seldom written in a manner that constitutes a good presentation of your ideas. Rewrite it

so that it is clear to any reader that you have a proof.

4. As you attempt to construct a proof, talk to yourself. Figure out where you're going before you try to go there. More precisely, ask yourself questions about what eventually needs to be done and what steps will take you there. Do this before you start trying to prove anything.
5. Be sure you can explain each step of your proof once you think you have one. If someone were to ask you how you got something, would you be ready with an answer? And, if your answer takes more than one sentence to explain, write it down in your proof.

Lastly, here are some things that might help if you get stuck (which happens to all of us more often than we would like).

1. Restate, in a different way if possible, what your goal or objective is.
2. Write down the negation of the statement you're trying to prove.
3. Draw pictures if you can.
4. Look at some specific examples that illustrate the statement you are trying to prove.
5. Prove a simplified version of the statement.
6. Look for a counterexample.
7. Is there something in the hypothesis that you haven't used in your attempts? If so, how could you use it?

2.1 Quantifiers and Proofs

Almost all mathematical statements that we wish to prove will be quantified. In this section, we consider the two basic types of quantified statements. As we know, all statements are either true or false. Again, to say that we will prove a statement means that we will show that it is true.

I. Statements of the form $(\forall x)P(x)$.

To show that such a statement is true we must show that $P(x)$ holds (is true) for all x in the specified universal set. How will we do this? Two ways come to mind. We could one-by-one choose the elements of U_x and exhibit

that $P(x)$ holds for each one. Or, we could pick an “arbitrary” element of U_x and show that $P(x)$ holds. By picking an “arbitrary” element of U_x we mean that we “name” an element and assume nothing more about it than that it is in U_x .

Example 2.1.1 Prove: *All students in this class are taller than 5' 2". Recall that an equivalent way to write this statement is “If x is a student in this class, then x is taller than 5' 2".*

Discussion: Suppose we choose three students at random and measure them. And suppose each of them is over 5' 2". Have we proved the statement? Certainly not! We must, of course, measure everyone in the class.

If everyone is measured and is, indeed, taller than 5' 2", we have proved the statement. If we find one or more persons who are 5' 2" or shorter, we say that we have a **counterexample** to the statement. Thus, the statement is not true. Note that, in this case, we will have demonstrated that the negation of the statement is true. I.e., $(\exists x)(\neg P(x))$.

How would we prove a “for every” statement if the universal set is too large to test every element?

Example 2.1.2 Prove: *For all positive integers x , $x^2 + x$ is even.*

Discussion: Let's try a few positive integers.

$$1^2 + 1 = 2, \text{ which is even.}$$

$$2^2 + 2 = 6, \text{ which is even.}$$

$$3^2 + 3 = 12, \text{ which is even.}$$

$$11^2 + 11 = 132, \text{ which is even.}$$

Are we done? Is this a proof? Again, certainly not. Although the statement holds for these four positive integers, it may not hold for some others. Now, it didn't hurt anything to try a few numbers to get an idea of what's going on. In fact, sometimes it's quite helpful, in this sense, to try a few values. But the proof must go something like this.

Suppose that x is some arbitrary positive integer. We remind ourselves that for an integer to be even, it must be representable as 2 times some integer. So, we want to show that $x^2 + x$ has this property; it is representable as 2 times some integer. Notice that we focused on what we need to prove

before we concerned ourselves with “how” to prove it. So, let’s try a few things, keeping in mind what we need to prove (where we need to get to, to have a proof). Now, $x^2 + x = x(x + 1)$. Hummmm? What now? I don’t see any 2’s around. Well, since x and $x + 1$ are consecutive integers, then one of them is even. (We’ll assume that this is a fact we know.)

If x is even, then $x = 2k$ for some integer k . So, $x^2 + x = x(x + 1) = (2k)(x + 1) = 2 \cdot (k(x + 1))$, and thus is even.

If $x + 1$ is even, then $x + 1 = 2n$ for some integer n . So, $x^2 + x = x(x + 1) = x(2n) = 2 \cdot (xn)$, and thus is even. Now we’re done. Right?

II. Statements of the form $(\exists x)P(x)$.

Obviously, to prove a statement of this type, we must exhibit an element of U_x that makes $P(x)$ true. We might do this by actually picking a specific value and demonstrating that $P(x)$ holds for that value. Or, we might “somehow” show that there must be some value for which $P(x)$ holds without knowing which one it is. What can be said if we pick some x in U_x and $P(x)$ doesn’t hold?

Example 2.1.3 Prove. *There is a real number x such that*

$$x^3 - 2x^2 + 2x - \frac{5}{8} = 0 .$$

1st Proof. $\frac{1}{2}$ is a real number and

$$\left(\frac{1}{2}\right)^3 - 2\left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right) - \frac{5}{8} = \frac{1}{8} - \frac{1}{2} + 1 - \frac{5}{8} = 0 . \quad \square$$

2nd Proof. $p(x) = x^3 - 2x^2 + 2x - \frac{5}{8}$ is a polynomial. Now, $p(0) = -\frac{5}{8}$, a negative number. And $p(1) = \frac{3}{8}$, a positive number. Since polynomials are continuous everywhere, by the Intermediate Value Theorem (from Calculus), there must be a number c with $0 < c < 1$ so that $p(c) = 0$. \square

2.2 Conditional Statements

To prove that a conditional statement is true, we recall that there is only one way in which it can be false; namely, if the hypothesis is true and the conclusion is false. So, if we show that this cannot happen, then we will have our proof. Hence, we only need to show that if we assume the hypothesis to

be true, then the conclusion must be true also. There are three basic types of proof for a conditional statement,

1. a direct proof,
2. proof by contrapositive, and
3. proof by contradiction.

In a direct proof, we simply assume the hypothesis to be true, use it and any other facts we know to be true to deductively reason that the conclusion must be true.

A proof by contrapositive is based on the fact that a conditional statement is equivalent to its contrapositive. So, we simply prove the contrapositive conditional statement directly. That is, we assume that the conclusion of the original statement is false and prove that the hypothesis must be false. Here's a place where being able to negate statements comes in handy, since assuming a statement is false is equivalent to assuming its negation is true. So, what we actually do most times is assume that the negation of the conclusion is true and prove that the negation of the hypothesis must be true.

Lastly, a proof by contradiction for a conditional statement goes like this. Suppose the statement to be proved is $P \Rightarrow Q$. Assume that $P \Rightarrow Q$ is not true. This is the same as assuming that P is true and Q is false. Using these two assumptions, we reason deductively until we get some statement to be false that we know is true. At this point, we claim to have reached a contradiction, and declare the implication $P \Rightarrow Q$ to be true. Here's what actually happened. Let's say that R is the statement that we know is true, but we reasoned it to be false. So, we showed that $\neg(P \Rightarrow Q) \Rightarrow \neg R$ is true. So, $R \Rightarrow (P \Rightarrow Q)$ is true. Since we know that R is true, it follows that $P \Rightarrow Q$ is true.

(*) The basic idea for a proof by contradiction of any statement P is to assume that P is false (which is equivalent to assuming P 's negation is true) and try to "reach a contradiction". That is, deduce from your assumption that some statement Q , which you know to be false, is true.

Let's look at some examples of these different types of proofs of conditional statements.

Example 2.2.1 Prove. *If x and y are rational numbers, then $x + y$ is a rational number.*

Direct Proof. We must recall and use the definition of rational numbers, for if we don't know precisely what rational numbers are, how can we prove anything about them?

Fact. A rational number is a real number that can be expressed as the ratio of two integers (with nonzero denominator).

So, we let x and y be arbitrary rational numbers, and we let $m, n, k,$ and r be integers so that $x = \frac{m}{n}$ and $y = \frac{k}{r}$. Then

$$x + y = \frac{m}{n} + \frac{k}{r} = \frac{mr}{nr} + \frac{nk}{nr} = \frac{mr + nk}{nr} .$$

Since $mr + nk$ and nr are integers (right?), then $x + y$ is a ratio of integers and thus is rational. \square

Example 2.2.2 Prove. *If x is rational and y is irrational, then $x + y$ is irrational.*

Proof. By way of proof by contradiction, assume that x is rational, y is irrational, and $x + y$ is rational. Since x is rational, $-x$ is rational (why?). By Example 2.2.1 above, $-x + (x + y)$ is rational. But $-x + (x + y) = y$, which is irrational, a contradiction. \square

2.3 Proving Practice

We finish this chapter with first a proof to grade, and second some proofs to do. If a problem says grade the proof, assign a letter grade of A, B, C, D, or F, and indicate what, if anything, is wrong. If something other than the original statement has been proven, state what.

Problem 2.3.1 *Grade the proof.*

Conjecture. It is not the case that for all rational numbers p and q , $p + q$ is a rational number.

Proof. Let $p = \pi$ and let $q = \frac{1}{2} - \pi$. Then $p + q = \pi + (\frac{1}{2} - \pi) = \frac{1}{2}$. Thus, p and q are irrational numbers whose sum is rational. \square

Definition 2.3.1 *If x is a real number, then the **absolute value** of x , denoted by $|x|$, is the nonnegative real number given by $|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$*

Definition 2.3.2 *If $p = (x, y)$ is a point in the Euclidean plane, then the **norm** or **modulus** of p , denoted by $\|p\|$, is the nonnegative real number given by $\|p\| = \sqrt{x^2 + y^2}$.*

Definition 2.3.3 Suppose m and n are integers. To say that n is **divisible by m** means that there is a unique integer k such that $m \cdot k = n$. We also say equivalently that m **divides n** , n is a **multiple of m** , and m is a **factor of n** . We write $m|n$.

Problem 2.3.2 In each problem below, either provide a proof or a counterexample.

1. If a, b are real numbers, then $|a + b| \leq |a| + |b|$.
2. If p and q are points in the Euclidean plane, then $\|p + q\| \leq \|p\| + \|q\|$.
3. If x is a positive real number, then $x \leq x^2$.
4. The sum of any five positive integers is divisible by 5.
5. The sum of any five consecutive positive integers is divisible by 5.
6. Suppose f is a real-valued function with domain all real numbers. If $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$, then for each $x \in \mathbb{R}$ and each rational number r , $f(r \cdot x) = r \cdot f(x)$.

Problem 2.3.3 Prove the following statements. Let $m, n, p \in \mathbb{Z}$.

1. If $m|p$ and $m|n$, then $m|(n + p)$.
2. If $m|n$, then $m|n \cdot p$.
3. If $m|n \cdot p$, then either $m|n$ or $m|p$.
4. If $m|n \cdot p$ and the greatest common divisor of m and n is 1, then $m|p$.
5. If the sum of the digits in m is divisible by 3, then $3|m$.

2.4 Mathematical Induction

Suppose the universal set for some quantified statement is the set of natural numbers \mathbb{N} , and we wish to prove a statement of the type $(\forall n)P(n)$. We can prove that such a statement is true by using the **principle of mathematical induction**(PMI). Let PMI denote the statement

$$\left[P(1) \wedge (\forall n)(P(n) \Rightarrow P(n + 1)) \right] \Rightarrow (\forall n)P(n)$$

Notice that PMI is a conditional statement whose hypothesis is a conditional statement. Assume, for the moment, that PMI is true. Then in order to prove a statement of the type $(\forall n)P(n)$, if we can prove the hypothesis of PMI is true, our statement must follow. This is exactly how we prove such statements using PMI.

Let k be a fixed natural number. To prove statements such as “ $P(n)$ is true for all natural numbers $n \geq k$ ”, we use the following modified form of PMI.

$$\left[P(k) \wedge (\forall n \geq k)(P(n) \Rightarrow P(n+1)) \right] \Rightarrow (\forall n \geq k)P(n)$$

Assume for now that PMI and its modified form are true and use them in the problems below.

Problem 2.4.1 *Prove the following statements by induction; i.e., use PMI.*

1. $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{1}{6}n(n+1)(2n+1)$ for all n in \mathbb{N} .
2. $1 + 3 + 5 + \dots + (2n-1) = n^2$ for all n in \mathbb{N} .
3. $2^n > n^2$ for all $n \geq 5$.
4. 6 divides $n^3 - n$ for all n in \mathbb{N} .

Problem 2.4.2 *For each n in \mathbb{N} , let $a_n = 4n - 3$.*

(1) Compute $\sum_{n=1}^1 a_n$, $\sum_{n=1}^2 a_n$, $\sum_{n=1}^3 a_n$, and $\sum_{n=1}^4 a_n$.

(2) Conjecture a closed form for $\sum_{n=1}^k a_n$.

(3) Prove your conjecture using induction.

Problem 2.4.3 *Suppose we remember only the following two facts from Calculus, namely*

- 1) $\frac{d}{dx}(x) = 1$, and
- 2) $\frac{d}{dx}(u \cdot v) = u \cdot \frac{dv}{dx} + \frac{du}{dx} \cdot v$.

Use induction to prove that $\frac{d}{dx}(x^n) = n \cdot x^{n-1}$ for each n in \mathbb{N} .

Problem 2.4.4 *Grade the proof.*

Conjecture. $\sum_{i=1}^{\infty} \frac{1}{i} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$ is a finite number.

Proof. We will use PMI. Since $\frac{1}{1} = 1$ is a finite number, the statement is true for 1. Assume that the statement is true for some $n \geq 1$. We look at the sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n} + \frac{1}{n+1} = \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}\right) + \frac{1}{n+1} .$$

Now, $(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n})$ is a finite number by inductive assumption and $\frac{1}{n+1}$ is certainly a finite number. The sum of two finite numbers is a finite number. \square

Axiom 2.4.1 *Every non-empty set of natural numbers has a least element.*

Problem 2.4.5 Prove that *Axiom 2.4.1* \Rightarrow *PMI*

There is another form of PMI (called the principle of complete induction) that says

$$\left[P(1) \wedge (\forall n)((P(1) \wedge P(2) \wedge \dots \wedge P(n)) \Rightarrow P(n+1)) \right] \Rightarrow (\forall n)P(n)$$

This form is actually equivalent to PMI, so we will not distinguish between them and we will use whichever one we need.

Problem 2.4.6 Prove that *PMI* \Rightarrow *Axiom 2.4.1*

So, by Problems 2.4.5 and 2.4.6, PMI and Axiom 2.4.1 are actually equivalent to each other. Since Axiom 2.4.1 is “obviously true”, we accept PMI as true also, and use it for proving statements of the type $(\forall n \text{ in } \mathbb{N})P(n)$.

Chapter 3

Naive Set Theory

You may have noticed that we have already, on occasion, mentioned words such as *set*, *function*, *domain*, etc. without having defined them. It has been presumed that you have some notion of these ideas from previous courses. However, we wish to study these ideas in greater detail now and we wish to prove quite a number of things about them. Thus, we need to define them a bit more carefully.

This chapter will deal with sets. Functions and related topics will come later.

3.1 Sets and Operations on Sets

A **set** is a collection of things. The things in the collection (or set) are called **elements** or **members** of the set. A set is completely characterized by its elements. If A is a set and 4 is an element of A , we write $4 \in A$.

How can we best describe sets that we wish to talk about or work with?

If a set has not too many elements, we can simply list the elements. We put curly brackets around the list to indicate the collection idea and we separate the elements by commas to distinguish them. For example, the set of positive integers between 1 and 5 could be written $\{2, 3, 4\}$.

If a set has “many” elements, we use **set builder notation**. The idea is to let a variable represent an arbitrary element of the set and describe what conditions the variable must satisfy in order to be a member of the set. For example, to describe the set of all points in the Cartesian plane that are between the x -axis and the line $y = 2$, we write $\{(x, y) \mid x \text{ and } y \text{ are in } \mathbb{R} \text{ and } 0 < y < 2\}$. We read this notation as “the set of all ordered pairs (x, y) of real numbers such that $0 < y < 2$ ”. Notice that since we are describing points

in the plane, we let our “variable notation” mimic the typical way that we describe points in the plane. This is sometimes helpful, but it is not necessary. We could have written $\{p \mid p \text{ is a point in the plane whose second coordinate is between } 0 \text{ and } 2\}$. Which do you prefer?

Occasionally, if the elements of a set form a “sequential pattern”, we use the dot-dot-dot notation. For example, the set of positive even integers could be written as $\{2, 4, 6, 8, \dots\}$.

Definition 3.1.1 *If A is a set, a set B is said to be a **subset** of A , written $B \subseteq A$, provided that if $x \in B$, then $x \in A$. The notation $B \subseteq A$ is referred to as a **set inclusion**.*

Definition 3.1.2 *Suppose each of A and B is a set. We say that A **equals** B , and write $A = B$, provided that $A \subseteq B$ and $B \subseteq A$.*

Definition 3.1.3 *Let \emptyset denote a set that has no elements.*

Theorem 3.1.1 *If A is any set, then $\emptyset \subseteq A$.*

Theorem 3.1.2 *The set \emptyset is unique. That is, if B is a set with no elements, then $B = \emptyset$. Thus, we will refer to \emptyset as **the empty set**.*

Definition 3.1.4 *The set B is a **proper subset** of A , written $B \subset A$, provided that $B \subseteq A$ and $B \neq A$.*

Definition 3.1.5 *Let each of A and B be a set. The **intersection** of A and B , denoted by $A \cap B$, is the set defined by*

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

*The **union** of A and B , denoted by $A \cup B$, is the set defined by*

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

If the sets that we are working with in a given problem are all subsets of some common larger set, we call this larger set the **universal set**. For example, if we are describing different sets of students at a given university, perhaps distinguishing them by major, or GPA, or whatever, we might take all students presently enrolled at that university as our universal set.

Definition 3.1.6 *Let A be a set and U a universal set. The **complement** of A (in U), denoted by A' , is the set defined by*

$$A' = \{x \in U \mid x \notin A\}.$$

Definition 3.1.7 Let each of A and B be a set. The **complement** of B in A or the **complement** of B relative to A , denoted by $A - B$, is the set defined by

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

Definition 3.1.8 Let A be a set. The **power set** of A , denoted by $\mathcal{P}(A)$, is the set of all subsets of A .

Problem 3.1.1 Let A and B be sets. In each part below, determine if TRUE or FALSE? ... and verify!

- | | |
|--|--|
| a. $\{1\} \in \{1, \{1, 2\}\}$ | f. $\mathcal{P}(A) \subseteq A$ |
| b. $\{1\} \subseteq \{1, \{1, 2\}\}$ | g. $A \subseteq A \cap B$ |
| c. $\{1, 2\} \subseteq \{1, \{1, 2\}\}$ | h. $A \subseteq A \cup B$ |
| d. $\{\{0\}\} \in \mathcal{P}(\{0\})$ | i. $A \subseteq B$ iff $B' \cap A = \emptyset$ |
| e. $\{0\} \in \mathcal{P}(\{0, \{0\}\})$ | |

Problem 3.1.2 Let A , B , and C be sets and U a universal set. Prove the following.

1. $A \cap B = B \cap A$
2. $(A \cup B) \cup C = A \cup (B \cup C)$
3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. $(A')' = A$
5. $A - B = A \cap B'$
6. $(A \cup B)' = A' \cap B'$
7. $(A \cap B)' = A' \cup B'$
8. $(A \cup B) - C = (A - C) \cup (B - C)$
9. $C - (A \cup B) = (C - A) \cap (C - B)$
10. $C - (A \cap B) = (C - A) \cup (C - B)$

Parts 6 and 7 in Problem 3.1.2 are DeMorgan's Laws for sets. What would an "extended finite version" look like?

Problem 3.1.3 We say that certain sets are "finite" and other sets are "infinite". What do we mean by this terminology? We will revisit these ideas later, but let's start thinking about them now.

1. Define **finite set** and **infinite set**.
2. What does it mean to say that the set A **has more elements than** the set B ? Is this terminology “meaningful” for infinite sets?
3. What does it mean to say that sets A and B **have the same number of elements**?

Problem 3.1.4 Let $n \in \mathbb{N}$ and let $A = \{1, 2, 3, \dots, n\}$. How many elements does $\mathcal{P}(A)$ have? Prove your conjecture!

Problem 3.1.5 Grade the proof.

Conjecture. If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.

Proof. Suppose there is an element x such that $x \in A \cap C$ and $x \notin B \cap C$. Then $x \in A$ and $x \in C$. Also, since $x \notin B \cap C$, it follows that either $x \notin B$ or $x \notin C$. But we know that $x \in C$. So, it must be the case that $x \notin B$. Hence, we have that $x \in A$ and $x \notin B$. Thus, $A \not\subseteq B$, which verifies the contrapositive of the conjecture. \square

Definition 3.1.9 Let S be a set of points in the Cartesian plane. To say that S is **convex** means that whenever p and q are points of S and $0 \leq t \leq 1$, then $t \cdot p + (1 - t) \cdot q$ is also in S .

Problem 3.1.6 Prove that $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 3\}$ is convex.
Hint. Recall Definition 2.3.2, and use Problem 2.3.2, part 2.

3.2 Indexed Families of Sets

If G is a set, each element of which is a set, it is customary to call G a family (or collection) of sets.

Definition 3.2.1 Let I be any set, and, for each $\alpha \in I$, let A_α be a set. Then $\{A_\alpha \mid \alpha \in I\}$ is called an **indexed family of sets** and I is called the **indexing set**.

Theorem 3.2.1 Every family of sets can be indexed.

Definition 3.2.2 Let $\{A_\alpha \mid \alpha \in I\}$ be an indexed family of sets. We define

$$\bigcup_{\alpha \in I} A_\alpha = \{a \mid \text{there is a } \gamma \in I \text{ such that } a \in A_\gamma\}$$

and

$$\bigcap_{\alpha \in I} A_\alpha = \{a \mid a \in A_\alpha \text{ for every } \alpha \in I\}.$$

Observation 3.2.1 Let $I = \{1, 2\}$. Observe that

(a) $A_1 \cup A_2 = \bigcup_{\alpha \in I} A_\alpha$, and (b) $A_1 \cap A_2 = \bigcap_{\alpha \in I} A_\alpha$.

Problem 3.2.1 For each $n \in \mathbb{N}$, let $A_n = \{k \in \mathbb{N} \mid n \leq k\}$. Find

(a) $\bigcap_{n \geq 1} A_n$, and (b) $\bigcup_{n \geq 1} A_n$.

Problem 3.2.2 For each $n \in \mathbb{N}$, let $B_n = [-\frac{2n+1}{n+1}, \frac{2n+1}{n+1}]$ and $B_{-n} = [-\frac{1}{n+1}, \frac{1}{n+1}]$. Let $B_0 = [-1, 1]$. Find (a) $\bigcap_{n \in \mathbb{Z}} B_n$, and (b) $\bigcup_{n \in \mathbb{Z}} B_n$.

Problem 3.2.3 State and prove DeMorgan's laws for an indexed family of sets.

Problem 3.2.4 Grade the proof.

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

Proof. We will show set inclusion in both directions.

Now, for each $\alpha \in I$, $A_\alpha \subseteq B \cup A_\alpha$ and $B \subseteq B \cup A_\alpha$. So, $\bigcap_{\alpha \in I} A_\alpha \subseteq \bigcap_{\alpha \in I} (B \cup A_\alpha)$ and $B \subseteq \bigcap_{\alpha \in I} (B \cup A_\alpha)$. Therefore, $B \cup (\bigcap_{\alpha \in I} A_\alpha) \subseteq \bigcap_{\alpha \in I} (B \cup A_\alpha)$.

Suppose there is a $y \in \bigcap_{\alpha \in I} (B \cup A_\alpha)$ but $y \notin B \cup (\bigcap_{\alpha \in I} A_\alpha)$. Then either $y \notin B$ or $y \notin \bigcap_{\alpha \in I} A_\alpha$. In either case, this gives that $y \notin \bigcap_{\alpha \in I} (B \cup A_\alpha)$, a contradiction. \square

Chapter 4

Functions and Relations

4.1 Relations

Definition 4.1.1 Let each of A and B be a set. The **Cartesian product** of A and B , denoted by $A \times B$, is the set defined by $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$. The elements of $A \times B$ are called *ordered pairs* and two ordered pairs (a, b) and (c, d) are equal iff $a = c$ and $b = d$.

Problem 4.1.1 Prove or disprove. For all sets A , B , and C ,

1. $A \times B = B \times A$
2. $(A \times B) \times C = A \times (B \times C)$
3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
4. If A has m elements and B has n elements, then $A \times B$ has mn elements.
5. $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$

Definition 4.1.2 Let each of A and B be a set. A **relation** R on $A \times B$ (or a relation R from A to B) is a subset of $A \times B$. It is customary to write aRb to indicate that $(a, b) \in R$. If R is a relation from A to A , we say that R is a relation on A .

Definition 4.1.3 Let R be a relation from A to B . The **domain** of R , denoted by D_R , is the set $D_R = \{a \in A \mid (a, b) \in R \text{ for some } b \in B\}$. The **range** (or **image**) of R , denoted by I_R , is the set $I_R = \{b \in B \mid (a, b) \in R \text{ for some } a \in A\}$.

Definition 4.1.4 Let R be a relation from A to B . The **inverse relation** from B to A , denoted by R^{-1} , is the relation defined by $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.

Definition 4.1.5 Suppose that R is a relation from A to B and that S is a relation from B to C . The **composition** of S and R , denoted by $S \circ R$, is the relation from A to C defined by $S \circ R = \{(a, c) \mid \text{there is a } b \in B \text{ such that } aRb \text{ and } bSc\}$. We read $S \circ R$ as “ S after R ”.

Definition 4.1.6 Suppose that R is a relation on A .

1. R is **reflexive** if aRa for every $a \in A$.
2. R is **nonreflexive** if for no $a \in A$ does aRa hold.
3. R is **symmetric** if whenever aRb , then bRa .
4. R is **antisymmetric** if whenever aRb and bRa , then $a = b$.
5. R is **transitive** if whenever aRb and bRc , then aRc .

Problem 4.1.2 Consider the relations R and S on \mathbb{R} given below.

$R: xRy$ iff $x^2 + y^2 = 4$, and

$S: xSy$ iff $x = \tan y$.

State the domain and range of each of R and S .

Problem 4.1.3 Let $A = \{1, 2, \Delta, 5, \square, +\}$,

$R = \{(1, 2), (5, \Delta), (5, +), (\Delta, \Delta), (2, +), (1, +)\}$, and

$S = \{(1, 1), (5, \Delta), (2, 2), (\Delta, 5)\}$.

1. Find $S \circ R$ and $R \circ S$.
2. Find S^{-1} .
3. What properties of Def.4.1.6 do R and S satisfy?
4. Define a relation T on A that has all of the following properties.
 - (a) $2T5$
 - (b) $D_T = \{1, 2, \Delta, +\}$
 - (c) T is reflexive on D_T .
 - (d) T is not transitive.

Theorem 4.1.1 A relation R on A is symmetric iff $R = R^{-1}$.

Theorem 4.1.2 Suppose that R is a relation from A to B . Then $(R^{-1})^{-1} = R$.

Definition 4.1.7 A relation R on A is an **equivalence relation** if it is reflexive, symmetric, and transitive.

Definition 4.1.8 Suppose that R is an equivalence relation on A . The **equivalence class of R** determined by the element a in A , denoted by $[a]_R$ or a/R , is the subset of A given by $[a]_R = \{x \in A \mid aRx\}$. We write $[a]$ for $[a]_R$ if the reference to R is clear.

Problem 4.1.4 Define \equiv on \mathbb{Z} by $a \equiv b$ iff $5 \mid (a - b)$. Show that \equiv is an equivalence relation. Describe the equivalence classes of \equiv .

Problem 4.1.5 Define F on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ by $(a, b)F(c, d)$ iff $ad = bc$. Show that F is an equivalence relation. Describe the equivalence classes of F .

Problem 4.1.6 Define C on $\mathbb{R} \times \mathbb{R}$ by $(x, y)C(z, w)$ iff $x^2 + y^2 = z^2 + w^2$. Show that C is an equivalence relation. Describe the equivalence classes of C .

Definition 4.1.9 Let A be a set. A **partition** P of A is a collection of subsets of A such that

- i) if $a \in A$, then there is a $B \in P$ such that $a \in B$, and
- ii) if $B, C \in P$ and $B \cap C \neq \emptyset$, then $B = C$.

Problem 4.1.7 Partitions on \mathbb{N}

1. Form a partition of \mathbb{N} with three members.
2. Form a partition of \mathbb{N} with three members and so that each member is infinite.
3. Form a partition of \mathbb{N} so that each member has three elements.
4. Is there a partition of \mathbb{N} that has infinitely many members and each member has infinitely many elements?

Theorem 4.1.3 Let A be a set.

1. If \equiv is an equivalence relation on A , then the collection of equivalence classes of \equiv form a partition of A .
2. If P is a partition of A , then there is an equivalence relation on A whose equivalence classes are the members of P .

Problem 4.1.8 Grade the proof.

Conjecture. If a relation R on A is symmetric and transitive, then it must be reflexive also.

Proof. Since R is symmetric, aRb implies bRa . Since R is transitive, aRb and bRa imply aRa . Hence, R is reflexive. \square

4.2 Order Relations

Definition 4.2.1 A relation R on A is a **partial ordering** on A if it is reflexive, antisymmetric, and transitive. We write \leq for R when R is a partial ordering and we say that A is a **partially ordered set**.

Problem 4.2.1 Show that set inclusion is a partial order on the power set of a set.

Problem 4.2.2 Suppose that \leq is a partial order on A . Define $a < b$ iff $a \leq b$ and $a \neq b$. Clearly, $<$ is a relation on A . Show that $<$ is nonreflexive and transitive.

Definition 4.2.2 A relation $<$ on a set A is called an **order relation** on A if it is nonreflexive and transitive.

Problem 4.2.3 Suppose $<$ is an order relation on the set A . Define \leq on A by $a \leq b$ iff either $a < b$ or $a = b$. Show that \leq is a partial order on A .

Definition 4.2.3 An order relation $<$ on a set A is called a **simple order** or a **linear order** on A if for every x, y in A with $x \neq y$, either $x < y$ or $y < x$.

Theorem 4.2.1 If $<$ is an order relation on A , then so is $<^{-1}$.

Definition 4.2.4 Let $<$ be an order relation on A . The **segments** (with respect to $<$) in A are the subsets of A determined by pairs of elements a, b in A and defined by $(a, b) = \{x \in A \mid a < x < b\}$. That is, (a, b) is the notation for the set and it is called the **segment from a to b** . Let $[a, b) = \{a\} \cup (a, b)$ and define $(a, b]$ and $[a, b]$ analogously.

Problem 4.2.4 Define \prec on \mathbb{R} by $x \prec y$ iff $x^2 < y^2$, or $x^2 = y^2$ and $x < y$. Show that \prec is a linear order on \mathbb{R} . What do the segments look like?

Problem 4.2.5 Let $D = [0, 1] \times [0, 1]$ and define \prec on D by $(a, b) \prec (c, d)$ iff $a < c$, or $a = c$ and $b < d$. Show that \prec is a linear order on D . What do the segments look like?

Problem 4.2.6 Define \leq on $\mathbb{R} \times \mathbb{R}$ by $(x, y) \leq (z, w)$ iff $x \leq z$ and $y \leq w$. Show that \leq is a partial order. If $<$ is the associated order relation as in Problem 4.2.2, what do the segments of $<$ look like?

Definition 4.2.5 Let S be a partially ordered set. The element a of S is a **least (greatest) element of S** provided that $a \leq x$ ($a \geq x$) for all $x \in S$.

Definition 4.2.6 Let S be a partially ordered set. The element a of S is a **minimal (maximal) element of S** provided that whenever $x \in S$ and $x \leq a$ ($x \geq a$), then $x = a$.

Definition 4.2.7 A set S is **totally ordered** provided that it is partially ordered and if $x, y \in S$, then either $x \leq y$ or $y \leq x$.

Definition 4.2.8 Let S be partially ordered and let $T \subseteq S$. An **upper bound of T** is an element b of S such that $x \leq b$ for all $x \in T$. A **least upper bound of T** is an upper bound b such that if c is also an upper bound of T , then $b \leq c$. **Lower bounds and greatest lower bounds** are defined similarly.

Definition 4.2.9 The set D is said to be a **directed set** if D is partially ordered and each two element subset of D has an upper bound in D .

Definition 4.2.10 The subset K of the directed set D is said to be **cofinal in D** provided that whenever $d \in D$, there is an element $k \in K$ such that $d \leq k$.

Question 4.2.1 Consider \mathbb{R} with its usual linear order relation $<$. Is it true that whenever A is a nonempty set in \mathbb{R} that has an upper bound, then A has a least upper bound?

Problem 4.2.7 Answer Question 4.2.1 for each of the order relations defined in Problems 4.2.4, 4.2.5, and 4.2.6.

4.3 Functions

Definition 4.3.1 Let each of A and B be a set. A **function** f from A to B , denoted by $f: A \rightarrow B$, is a relation from A to B such that $D_f = A$, and if (a, b) and (a, c) are in f , then $b = c$. We let $f(a)$ denote the unique element of B such that $(a, f(a)) \in f$. The element $f(a)$ in B is called the **image** of a under f , or the **value** of f at a .

Definition 4.3.2 Let $f: A \rightarrow B$ and let $K \subseteq A$. The **restriction of f to K** , denoted by $f|_K$, is the function from K to B such that $f|_K(a) = f(a)$ for all $a \in K$.

Definition 4.3.3 Let X be a set. A **sequence** x in X is a function with domain the natural numbers (or some cofinal subset thereof) and range a subset of X . That is, $x: \mathbb{N} \rightarrow X$. For sequences, we denote the value of x at i by x_i rather than the usual functional notation $x(i)$. We denote the sequence by x_1, x_2, x_3, \dots or by $\{x_i\}_{i=1}^{\infty}$.

Functions are fundamental in mathematics. You probably have suspected this already from the number of encounters you have had with them in Precalculus, Calculus, Differential Equations, and, in fact, in all of your mathematics classes.

How should we describe particular functions that we wish to discuss or investigate? Since a function f is actually a subset of the Cartesian product of two sets (not necessarily different), we could specify the sets involved in the Cartesian product and then describe f as we do any set. That is, if f has not too many elements, we can simply list them. If f has many elements, we use set-builder notation. This is essentially the way we describe functions, but one must look closely to notice it. Here's an example.

Example 4.3.1 Consider the function $f: \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x^3 - 3$.

Discussion. The notation $f: \mathbb{R} \rightarrow \mathbb{R}$ (see Def.4.3.1) identifies the Cartesian product $\mathbb{R} \times \mathbb{R}$ and further indicates that \mathbb{R} is the domain of f and that \mathbb{R} contains the range of f . The equation $f(x) = x^3 - 3$ is actually our set-builder notation to describe the ordered pairs that belong to f , although we have suppressed a bit of the usual notation. It should look like $\{(x, f(x)) \in \mathbb{R} \times \mathbb{R} \mid f(x) = x^3 - 3\}$ or $\{(x, x^3 - 3) \mid x \in \mathbb{R}\}$.

Definition 4.3.4 Let X be a set. The **identity function** on X , $id: X \rightarrow X$, is defined by $id(x) = x$ for all $x \in X$.

Definition 4.3.5 Let $f: X \rightarrow Y$ be a function. We say that f is a **constant function** if there is a $y \in Y$ such that $f(x) = y$ for all $x \in X$. So, $I_f = \{y\}$.

Definition 4.3.6 Let $f: X \rightarrow Y$ be a function.

1. f is **one-to-one** (1-1), or **injective**, if whenever $f(x) = f(y)$, it follows that $x = y$.
2. f is **onto**, or **surjective**, if for each $y \in Y$, there is an $x \in X$ such that $f(x) = y$.
3. f is **bijective** if it is 1-1 and onto.

Definition 4.3.7 Let $f: X \rightarrow Y$ be a function, $H \subseteq X$, and $K \subseteq Y$. We define the **image of H under f** by $f(H) = \{f(x) \mid x \in H\}$. Observe that $f(X) = I_f$.

We define the **preimage of K under f** by $f^{-1}(K) = \{x \in X \mid f(x) \in K\}$. If $y \in Y$, we write $f^{-1}(y) = f^{-1}(\{y\})$.

Observation 4.3.1 Since a function f is a relation, in general, f^{-1} is the relation defined in Definition 4.1.4. But, if additionally, f is one-to-one, we get, from Theorem 4.3.1 below, that f^{-1} is a function.

Theorem 4.3.1 If $f: X \rightarrow Y$ is a 1-1 function, then $f^{-1}: f(X) \rightarrow X$ is a function. Furthermore, if f is a bijection, then f^{-1} is also a bijection.

Since composition of relations was defined earlier and functions are relations, it follows that the composition of functions $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ is given by $g \circ f = \{(x, z) \mid \text{there is a } y \in Y \text{ such that } (x, y) \in f \text{ and } (y, z) \in g\}$. Now, for functions, if $(x, y) \in f$, then y is the unique element of Y such that $y = f(x)$ and if $(y, z) \in g$, then z is the unique element of Z such that $z = g(y)$. So, for each $x \in X$ there can be at most one element $(x, z) \in g \circ f$, and using our functional notation $z = g(f(x))$. Thus, $g \circ f$ is a function from X into Z . With composition of functions, we usually write $g \circ f(x) = g(f(x))$ and take it as a definition, although this equality does follow from the definition of composition of relations.

Theorem 4.3.2 If $f: X \rightarrow Y$ is 1-1 and onto, then

1. $f \circ f^{-1}: Y \rightarrow Y$ is the identity function on Y , and
2. $f^{-1} \circ f: X \rightarrow X$ is the identity function on X .

Theorem 4.3.3 Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ are 1-1, onto functions. Then $g \circ f: X \rightarrow Z$ is 1-1 and onto.

Problem 4.3.1 Given the functions below, answer the questions. Drawing graphs might be of some help.

$f: \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = \sin x$.

$g: [0, \infty) \rightarrow [0, \infty)$ given by $g(x) = x^2$.

$h: \mathbb{R} \rightarrow \{0, 1\}$ given by $h(x) = \begin{cases} 0 & \text{if } x \text{ is rational} \\ 1 & \text{if } x \text{ is irrational} \end{cases}$

$k: (0, \frac{2}{\pi}] \rightarrow \mathbb{R}$ given by $k(x) = \sin \frac{1}{x}$.

$t: (-\frac{\pi}{2}, \frac{\pi}{2}) \rightarrow \mathbb{R}$ given by $t(x) = \tan x$.

$m: \mathbb{R} - \{0\} \rightarrow \mathbb{R} - \{0\}$ given by $m(x) = \frac{1}{x}$.

1. Which are 1-1? Which are onto? Verify!
2. Determine the range of those that are not surjective.
3. Find $f([\frac{\pi}{4}, \frac{3\pi}{4}])$ and $f^{-1}([\frac{1}{2}, 1])$.
4. Find a defining rule for g^{-1} .
5. Determine if $k \circ m|_{[\frac{\pi}{2}, \infty)} = f|_{[\frac{\pi}{2}, \infty)}$.

Problem 4.3.2 Let \mathbb{Z}/\equiv be the set of equivalence classes in Problem 4.1.4. Define $f: \mathbb{Z}/\equiv \rightarrow \mathbb{Z}/\equiv$ by $f([n]) = [2n]$, and $g: \mathbb{Z}/\equiv \rightarrow \mathbb{Z}/\equiv$ by $g([n]) = [n^2]$.

1. Is it clear that f and g are functions? If not, verify that they are.
2. Are either of them 1-1 and/or onto?
3. Determine rules for $f \circ g$ and $g \circ f$.

Problem 4.3.3 Let $f: X \rightarrow Y$ be a function, $A \subseteq X$, and $B \subseteq Y$. Prove that

1. $A \subseteq f^{-1}(f(A))$, and equality holds if f is injective.
2. $f(f^{-1}(B)) \subseteq B$, and equality holds if f is surjective.

Problem 4.3.4 Let $f: X \rightarrow Y$ be a function, A_0, A_1 be subsets of X , and B_0, B_1 be subsets of Y . Prove.

1. If $B_0 \subseteq B_1$, then $f^{-1}(B_0) \subseteq f^{-1}(B_1)$.
2. If $A_0 \subseteq A_1$, then $f(A_0) \subseteq f(A_1)$.
3. $f^{-1}(B_1 - B_0) = f^{-1}(B_1) - f^{-1}(B_0)$.
4. $f(A_1 - A_0) = f(A_1) - f(A_0)$.

Problem 4.3.5 Let $f: X \rightarrow Y$ be a function, $\{A_\alpha \mid \alpha \in I\}$ be a family of subsets of X , and $\{B_\alpha \mid \alpha \in J\}$ be a family of subsets of Y . Prove that

1. $f^{-1}(\bigcup_{\alpha \in J} B_\alpha) = \bigcup_{\alpha \in J} f^{-1}(B_\alpha)$.
2. $f^{-1}(\bigcap_{\alpha \in J} B_\alpha) = \bigcap_{\alpha \in J} f^{-1}(B_\alpha)$.
3. $f(\bigcup_{\alpha \in I} A_\alpha) = \bigcup_{\alpha \in I} f(A_\alpha)$.
4. $f(\bigcap_{\alpha \in I} A_\alpha) = \bigcap_{\alpha \in I} f(A_\alpha)$.

4.4 The Axiom of Choice

AXIOM OF CHOICE (AOC) Let $\{A_\alpha \mid \alpha \in \Gamma\}$ be a collection of nonempty sets. Then there is a function C with domain Γ such that for each $\alpha \in \Gamma$, $C(\alpha) \in A_\alpha$.

ZORN'S LEMMA Suppose that S is a nonempty partially ordered set such that each nonempty totally ordered subset has an upper bound. Then S has a maximal element.

Definition 4.4.1 A set S is **well-ordered** provided that it is totally ordered and that every nonempty subset of S has a least element.

Well-ordering Axiom (WOA) Every set can be well-ordered.

Definition 4.4.2 Let \mathcal{G} be a collection of sets. \mathcal{H} is a **monotonic subcollection** of \mathcal{G} provided that whenever H_1 and H_2 are in \mathcal{H} , either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

HAUSDORFF MAXIMALITY PRINCIPLE (HMP) If \mathcal{G} is a collection of sets, then there is a monotonic subcollection \mathcal{H} of \mathcal{G} which is not a proper subcollection of any other monotonic collection of sets from \mathcal{G} .

Theorem 4.4.1 *These are equivalent.*

1. AOC
2. Zorn's Lemma
3. WOA
4. HMP

4.5 Generalized Products of Sets

Problem 4.5.1 *We wish to extend the idea of products of sets so that we can have a product of more than two sets.*

1. Let $k \in \mathbb{N}$ and let $\{A_i\}_{i=1}^k$ be a collection of nonempty sets. Give a definition for $A_1 \times A_2 \times A_3 \times \dots \times A_k$. We will denote this set by $\prod_{i=1}^k A_i$.
2. Let A_i be a nonempty set for each $i \in \mathbb{N}$. Give a definition for $\prod_{i=1}^{\infty} A_i$.
3. Let $\{A_\alpha \mid \alpha \in I\}$ be an indexed family of nonempty sets. Give a definition for $\prod_{\alpha \in I} A_\alpha$.

Theorem 4.5.1 *Suppose that $\{A_\alpha \mid \alpha \in I\}$ is a family of sets and $\{J, K\}$ is a partition of I . Then there is a bijection from $\prod_{\alpha \in I} A_\alpha$ to $(\prod_{\alpha \in J} A_\alpha) \times (\prod_{\alpha \in K} A_\alpha)$.*

Definition 4.5.1 *Let $\prod_{\alpha \in I} A_\alpha$ be a product of sets and let $\beta \in I$. Then the function $\pi_\beta : \prod_{\alpha \in I} A_\alpha \rightarrow A_\beta$, defined by $\pi_\beta(f) = f(\beta)$, is called a **projection function**. Notice that there is a projection function π_β for each element β in I .*

Theorem 4.5.2 *Projection functions are surjective.*

Problem 4.5.2 *Let A and B be subsets of $X \times Y$. Prove or disprove that*

1. $A = \pi_1(A) \times \pi_2(A)$, where π_1 and π_2 are respectively the projection functions onto X and Y .
2. $\pi_1^{-1}(\pi_1(A)) = A$.
3. $\pi_1(A \cap B) = \pi_1(A) \cap \pi_1(B)$.

4. $\pi_1(A \cup B) = \pi_1(A) \cup \pi_1(B)$.

Theorem 4.5.3 *Let $\{A_\alpha \mid \alpha \in I\}$ and $\{B_\alpha \mid \alpha \in I\}$ be families of sets.*

1. $(\prod_{\alpha \in I} A_\alpha) \cap (\prod_{\alpha \in I} B_\alpha) = \prod_{\alpha \in I} (A_\alpha \cap B_\alpha)$
2. $(\prod_{\alpha \in I} A_\alpha) \cup (\prod_{\alpha \in I} B_\alpha) \subseteq \prod_{\alpha \in I} (A_\alpha \cup B_\alpha)$

Problem 4.5.3 *Express each set below as a product of sets.*

1. *The set of all sequences of integers.*
2. *The set of all sequences of zeros and ones.*
3. *The set of all sequences of integers with 0 as their fifth term.*

Chapter 5

Cardinality of Sets

5.1 Finite and Infinite Sets

Definition 5.1.1 *The set A is **finite** if $A = \emptyset$, or if there is an $n \in \mathbb{N}$ and a bijection $f: A \rightarrow \{1, 2, \dots, n\}$. Otherwise, A is **infinite**.*

This definition answers (or, at least, gives one answer to) Problem 3.1.3(1). For finite sets, the answers to Problem 3.1.3(2) and 3.1.3(3) now seem easy. Right? If A and B are finite sets, then there exist natural numbers m and n and bijections $f: A \rightarrow \{1, 2, \dots, m\}$ and $g: B \rightarrow \{1, 2, \dots, n\}$. It seems reasonable to say that A and B have the same number of elements if $m = n$. Or, if $m \neq n$ and $n > m$, then it seems reasonable to say that B has more elements than A or that A has fewer elements than B . Can we mimic this terminology for infinite sets? A problem is that there are no “infinite numbers” (that we know of) to compare infinite sets to. So, let’s focus more on the bijections. For example, in the case when $m = n$, we have bijections $f: A \rightarrow \{1, 2, \dots, n\}$ and $g: B \rightarrow \{1, 2, \dots, n\}$. By Theorems 4.3.1 and 4.3.3, $g^{-1}: \{1, 2, \dots, n\} \rightarrow B$ and $g^{-1} \circ f: A \rightarrow B$ are bijections. That is, there exists a bijection from A to B . We will use this as a definition that infinite sets A and B have the same number of elements. We develop this idea and other “size” considerations of infinite sets in this chapter.

Definition 5.1.2 *Sets A and B are said to have **the same cardinality** (or the same number of elements, or to be the same size) if there exists a bijection $f: A \rightarrow B$. We write $A \sim B$.*

Problem 5.1.1 *Show that \sim is an equivalence relation.*

Definition 5.1.3 If A is a finite set and $f: A \rightarrow \{1, 2, \dots, n\}$ is a bijection, we say that the **cardinality of A** is n and we write $|A| = n$. We also say that A has n elements. Using the inverse bijection $f^{-1}: \{1, 2, \dots, n\} \rightarrow A$ we may name the elements of A and write $A = \{a_1, a_2, \dots, a_n\}$, where $a_1 = f^{-1}(1)$, $a_2 = f^{-1}(2)$, \dots , $a_n = f^{-1}(n)$. The cardinality of \emptyset is 0 and we write $|\emptyset| = 0$.

Theorem 5.1.1 If $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$ and $m < n$, then f is not 1-1.

Theorem 5.1.2 Suppose $|A| = m$, $|B| = n$, $m < n$, and $f: B \rightarrow A$, then f is not 1-1.

Theorem 5.1.3 Let A and B be finite sets with $|A| = m$ and $|B| = n$. Then $A \sim B$ iff $m = n$.

Corollary 5.1.1 The cardinality of a finite set is unique.

Notation: Based on Theorem 5.1.3 above, for finite sets we can write $|A| = |B|$ instead of $A \sim B$ to indicate that A and B have the same cardinality. Hence, we unabashedly adopt this notation for all sets A and B . I.e., we write $|A| = |B|$ as an alternative notation for $A \sim B$.

Theorem 5.1.4 If A and B are finite disjoint sets, then $A \cup B$ is finite. Furthermore, if $|A| = m$ and $|B| = n$, then $|A \cup B| = m + n$.

Theorem 5.1.5 If A is an infinite set and $n \in \mathbb{N}$, then there exists a subset B of A such that $|B| = n$.

Theorem 5.1.6 If B is a finite set and $A \subseteq B$, then A is finite.

Corollary 5.1.2 If A is infinite and $A \subseteq B$, then B is infinite.

Theorem 5.1.7 If A and B are finite sets, then $A \cup B$ is finite.

Corollary 5.1.3 If A is infinite, $B \subseteq A$, and B is finite, then $A - B$ is infinite.

Theorem 5.1.8 If A is a proper subset of the finite set B , then $|A| \neq |B|$.

Theorem 5.1.9 Let $\{A_i \mid i \in \{1, 2, \dots, k\}\}$ be a family of nonempty finite sets.

(a) $\bigcup_{i=1}^k A_i$ is finite.

(b) $\prod_{i=1}^k A_i$ is finite.

Definition 5.1.4 Let A and B be sets. We say that the **cardinality of A is less than or equal the cardinality of B** , denoted $|A| \leq |B|$, if there is an injection $f: A \rightarrow B$.

We define $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$. In this case, we say that A has **fewer elements than B** or B has **more elements than A** .

For finite sets, this notation and terminology is consistent with our previous definitions and theorems. For example, suppose that $|A| = m$, $|B| = n$, and $m < n$. Let $f: A \rightarrow \{1, 2, \dots, m\}$ and $g: B \rightarrow \{1, 2, \dots, n\}$ be bijections. Then $g^{-1}|_{\{1, 2, \dots, m\}} \circ f: A \rightarrow B$ is an injection and Theorem 5.1.2 tells us there is no bijection from A onto B . Thus, by definition we may write $|A| < |B|$, which without careful thought, we might have written at the outset simply because $m < n$.

Note: Although we have not defined “the cardinality” of an infinite set, we nevertheless will use the above terminology and notation. Each notation, in the infinite setting, is a statement about the existence or nonexistence of certain functions from A to B .

Theorem 5.1.10 (Schröder-Bernstein) If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

Theorem 5.1.11 If A is a set, then $|A| < |\mathcal{P}(A)|$.

Theorem 5.1.12 The set A is infinite iff there is a bijection from A onto a proper subset of itself.

5.2 Countable and Uncountable Sets

Definition 5.2.1 The set A is **countably infinite** if $A \sim \mathbb{N}$. If the set A is either finite or countably infinite, we say that A is **countable**. If A is not countable, we say that A is **uncountable**.

Note: If A is countably infinite, we can use the bijection from \mathbb{N} to A to “list” or “enumerate” the elements of A . We write $A = \{a_1, a_2, a_3, \dots\}$.

Theorem 5.2.1 If the set A is countably infinite, then it is infinite.

Theorem 5.2.2 Every subset of a countable set is countable.

Problem 5.2.1 Prove that

1. \mathbb{Z} is countable.
2. the interval $[0, 1]$ is uncountable.
3. $\mathbb{Z} \times \mathbb{Z}$ is countable.

Theorem 5.2.3 Every infinite set contains a countably infinite subset.

Theorem 5.2.4 If each of A_1, A_2, \dots, A_n is a countable set, then $\bigcup_{i=1}^n A_i$ is countable.

Corollary 5.2.1 If A is uncountable, $B \subseteq A$, and B is countable, then $A - B$ is uncountable.

Theorem 5.2.5 If each of A_1, A_2, A_3, \dots is a countable set, then $\bigcup_{i=1}^{\infty} A_i$ is countable.

Problem 5.2.2 Prove that

1. \mathbb{Q} is countable.
2. \mathbb{R} is uncountable.

Problem 5.2.3 Collect together, from the sets listed below, those sets that have the same cardinality. Verify by citing previous results or by exhibiting a bijection.

- | | |
|---|---|
| (1) \emptyset | (10) \mathbb{R} |
| (2) $\{1, 2, 3, 4\}$ | (11) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}$ |
| (3) \mathbb{N} | (12) \mathbb{Q} |
| (4) \mathbb{Z} | (13) \mathbb{H} |
| (5) the set of even natural numbers | (14) $\{0, 1\} \times \{2, 3\}$ |
| (6) $\{x \in \mathbb{R} \mid 4 - x^2 \geq 5\}$ | (15) $\{x \in \mathbb{R} \mid 0 < x < 1\}$ |
| (7) $\{x \in \mathbb{C} \mid x^4 = 1\}$ | (16) $\{x \in \mathbb{R} \mid -3 \leq x \leq 3\}$ |
| (8) $\{x \in \mathbb{R} \mid \sin x = 0\}$ | (17) $\{m \in \mathbb{N} \mid m = 5n \text{ for some } n \in \mathbb{N}\}$ |
| (9) $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ | (18) $\mathcal{P}(\{0, 1\})$ |