An Introduction to Mathematics

John W. Snow

Contents

1

Statements and Logical Operators

1.1 Statements: A **statement** is a declarative sentence which must be either true or false. Statements are also called **propositions**.

Examples of statements (not all of these are true):
"The grass is green."
"George W. Bush is the American president."
"The number 2 is less than the number 1."
"1+1=2"
"The sun will rise tomorrow."

Examples of things which are not statements:
"Go to bed." (an imperative or command)
"The house on the hill" (not even a sentence)
"Is this a statement?" (an interrogative or question)
"Paul is tall." (Since "tall" is relative, this might seem true to some people and false to others. It is not strictly true or false.)

1.2 Exercises: Which of the following are statements?

1.2.1 The brown and white dog ran down the long winding road.
1.2.2 True is spelled t-r-u.
1.2.3 This sentence is true.
1.2.4 This sentence is neither true nor false.
1.2.5 The old white house on the lonesome hill outside of town.
1.2.6 Feed the lazy dog on the porch once every day.
1.2.7 The clock is slow.
1.2.8 The car is slow.

1.3 Exercise: The sentence "This sentence is false" is not a statement. Explain why. Hint: What would happen if the sentence were true? What would happen if it were false?

1.4 Assumptions: There are two underlying assumptions in our definition of a statement. First, every statement must be either true or false. Second, no statement is both true and false. That any statement must be either true or false but not both is called the **law of the excluded middle**.

1.5 Truth Values: Every statement has what we call a **truth value**. If a statement is true, its truth value is true. If the statement is false, the truth value is false.

1.6 Symbols: The work of mathematicians is largely to determine what is true and what is false. The ambiguous nature of our spoken language can make this task difficult. In order to avoid ambiguity, mathematicians use symbols. As our first use of symbols we will be letting capital letters represent statements. For example, we could let the letter P be the statement "It is raining." Then whenever we see a P, we think "It is raining." Of course, there are only twenty six capital letters in our alphabet and many, many statements, so we will often use the same letter to represent different statements in different problems.

1.7 Compound Statements: A single letter representing a statement will be called an **atomic statement**. We can join atomic statements together with the words "and," "or," "not," and "implies." These words will be called **logical operators**, and the more complex statements which are formed will be called **compound statements**. To make compound statements, we will not actually use the words, but symbols for the words. This is outlined in the next few sections.

1.8 Conjunction: We will use the symbol $\wedge$ to mean "and." If P and Q are two statements, then $P \wedge Q$ is the new statement "P and Q." For example, if P is "It is raining," and Q is "The grass is green," then $P \wedge Q$ is "It is raining, and the grass is green." The statement $P \wedge Q$ is called the **conjunction** of the statements P and Q. The statement $P \wedge Q$ should be true when both of the statements P and Q are true. Otherwise, it should be false. (In fact $P \wedge Q$ can be **defined** to be the statement which is true when both P and Q are true and is false

otherwise.) We can sum this up in this **truth table**:

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

The first two columns of the table list all of the possible combinations of truth values for P and Q. The third column gives the corresponding truth value for $P \wedge Q$. As we noted above, the only time when $P \wedge Q$ is true is when P is true and Q is true.

In the English language, there are many ways of expressing $P \wedge Q$. Any statement which communicates that both P and Q are true expresses $P \wedge Q$. If P is "It is raining," and Q is "The grass is green," then each of the following communicate $P \wedge Q$:
"It is raining, and the grass is green."
"It is raining, but the grass is green."
"It is raining; however, the grass is green."
"Even though it is raining, the grass is green."
"While it is raining, the grass is green."
"The grass is green, and it is raining."
This last one is interesting; $Q \wedge P$ seems to communicate the same thing as $P \wedge Q$.

1.9 Disjunction: We will use the symbol $\vee$ to mean "or." If P and Q are two statements, then the statement $P \vee Q$ is "P or Q." This is called the **disjunction** of the statements P and Q. The statement $P \vee Q$ will be true when P is true, Q is true, or both are true. This can be expressed in a truth table:

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

Again, the first two columns of the truth table list the all possible combinations of truth values for P and Q (note that these are the same as the first two columns for $\wedge$ above). The last column gives the corresponding truth value for $P \vee Q$.

1.10 Negation: We will use the symbol $\neg$ to mean "It is not the case that..." If P is any statement then $\neg P$ means "It is not the case that P." For example, if P is "It is raining," then $\neg P$ is "It is not the case that it is raining." In English, there are simpler ways of expressing this. The best choice may be "It is not raining." For simplicity, we will most often read $\neg P$ as "Not P." A truth table for $\neg$ is easy to draw. If P is true, then $\neg P$ should be false. If P is false, then $\neg P$ should be true:

P	$\neg P$
T	F
F	T

The statement $\neg P$ is called the **negation of** P.

1.11 Implication (Conditional): We will use the symbol $\rightarrow$ to mean "implies." If P and Q are statements, then $P \rightarrow Q$ is "P implies Q." We will often read this as "If P, then Q." For example, if P is "I left my hat at home," and Q is "It will rain," then $P \rightarrow Q$ could be read as "If I left my hat at home, then it will rain." To determine the truth values for this new logical operator, it is useful to think of $P \rightarrow Q$ as a promise. Let P be the statement "You win," and let Q be the statement "We will go out to eat." Then $P \rightarrow Q$ is "If you win, then we will go out to eat." Think of this as a promise. The statement will be true when the promise is kept and false if it is broken. There is only one way in which the promise may be broken - if you win and we do not go out to eat. This is the case where P is true and Q is false. Thus if P is true and Q is false, then $P \rightarrow Q$ is false. Otherwise, the promise is not broken, so the statement should be true. Here is the truth table:

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

As with conjunction, there are many ways of expressing implication. Here are a few common ways of expressing $P \rightarrow Q$:
"If P, then Q."
"P implies Q."
"Q, if P."
"P only if Q."
"Q follows from P."

"Whenever P, Q."
"Q, whenever P."
"Not P unless Q."
"P is sufficient for Q."
"Q is necessary for P."
The part of an implication which comes before the arrow is called the **antecedent** or **hypothesis**. That which comes after the arrow is the **consequent** or **conclusion**. Thus in $B \to K$, B is the antecedent, and K is the consequent. Notice in the last two statements on our list that the antecedent is the sufficient part and the consequent is the necessary part.

1.12 Translations: Our logical operators can be applied repeatedly to atomic statements to form more complex compound statements. Let L be "The lights are on." Let O be "The oven is on," and let D be "The door is open." We can combine these statements with our logical operators to create a multitude of compound statements. In doing so, we will use parenthesis as punctuation to indicate order of operations.

For example, we could first form $L \wedge O$ - "The lights are on and the oven is on." Then we could negate this statement to get $\neg(L \wedge O)$ - "It is not the case that the lights are on and the oven is on." In English, the statement is not as clear as in symbols. In symbols, it is clear that the $\neg$ applies to all of $L \wedge O$. In English, it sounds as if it may just apply to the L - as in $(\neg L) \wedge O$. In order make this clear, we could translate $\neg(L \wedge O)$ as "It is not the case that both the lights are on and the oven is on." The "both...and..." act to join the two simpler statements together. Now, we could take this new statement and combine it with D with an "or" to get $(\neg(L \wedge O)) \vee D$ - "It is not the case that both the lights are on and the oven is on, or the door is open." Notice that we placed parenthesis around the $\neg(L \wedge O)$ to communicate that the $\neg$ applies only to this part of the statement.

The best strategy for translating from symbols to words is use parenthesis to locate the smallest compound statements within a statement. Form these, then combine them with the appropriate logical operators, using parenthesis as clues to punctuation and sentence structure. At each step along the way, it may be helpful to rephrase the statements so they will be more readable in English.

For example, consider the statement $(L \vee O) \rightarrow (\neg D)$. The simplest compound statements are $L \vee O$ - "The lights are on or the oven is on" - and $\neg D$ - "It is not the case that the door is open." The first of these may sound better as "The lights or the oven are on." The second may better be written as "The door is not open," or even "The door is closed." We combine these with an implication to get "If the lights or oven are on, then the door is closed."

1.13 Order of Operations: For the most part, we will always use parenthesis to indicate order of operations in compound statements. The one exception we will make to avoid too many parenthesis is to let $\neg$ take precedence over all other operations. This means that unless a set of parenthesis is in the way, we apply all $\neg$'s first. For example, rather than writing $((\neg P) \wedge (\neg Q)) \rightarrow (\neg (R \wedge S))$, we can write $(\neg P \wedge \neg Q) \rightarrow \neg (R \wedge S)$.

1.14 More Translations: Let L, O, and D be as above Here are some more examples of translations from words to symbols:

Symbols	Words
$L \rightarrow (O \vee D)$	If the lights are on then either the oven is on or the door is open.
$\neg (L \rightarrow D)$	It is not the case that if the lights are on then the door is open.
$(L \wedge D) \vee (L \wedge O)$	Either the lights are on and the door is open or the lights are on and the oven is on.
$\neg D \vee (L \rightarrow O)$	The door is closed, or if the lights are on, then the oven is on.

1.15 Bi-Implication: Sometimes we may want to express both $P \rightarrow Q$ and $Q \rightarrow P$. We could write this as $(P \rightarrow Q) \wedge (Q \rightarrow P)$, but a simpler way of expressing it is $P \leftrightarrow Q$. This is called the **bi-implication** or the **biconditional** and is usually read as "P if and only if Q" or "P is necessary and sufficient for Q." Sometimes, this is abbreviated as "P iff Q."

1.16 Exercises: Let M be "The moon is full." Let A be "The alarm is set for 4:00 AM," and let F be "Fred is going fishing in the morning."

Below are compound statement using A, F, M. Translate each into words. (Try to be creative).

1.16.1 $F \vee \neg A$

1.16.2 $\neg F \wedge \neg A$

1.16.3 $\neg(F \vee A)$

1.16.4 $F \wedge (M \vee A)$

1.16.5 $A \wedge M \wedge F$

1.16.6 $(F \wedge M) \vee (F \wedge \neg M)$

1.16.7 $(M \wedge A) \rightarrow F$

1.16.8 $\neg A \vee (M \rightarrow F)$

1.17 Translating from words to symbols: We can also translate statements from words to symbols. Let S be "The sun will rise in the morning." Let C "Candace leaves a candle in her window," and let D be "Doug passes his math test." Consider the statement " If Candace leaves a candle in her window or Doug passes his math test, then the sun will rise in the morning." We can identify the atomic statements C, D and S in the statement:

$$\text{"If } \overbrace{\text{Candace leaves a candle in her window}}^{C} \text{ or } \overbrace{\text{Doug passes his math class}}^{D} \text{ then } \overbrace{\text{the sun will rise in the morning.}}^{S}$$

We notice the "or" and the "if...then..." in the statement and can label them (notice we place the $\rightarrow$ over the "then"):

$$\text{If } \overbrace{\text{Candace leaves a candle in her window}}^{C} \overset{\vee}{\text{or}} \overbrace{\text{Doug passes his math class}}^{D} \overset{\rightarrow}{\text{then}} \overbrace{\text{the sun will rise in the morning.}}^{S}$$

Finally, we can use the structure of the sentence and punctuation to determine placement of parenthesis. This gives:

$$\text{If } \overbrace{\text{Candace leaves a candle in her window}}^{(C} \overset{\vee}{\text{or}} \overbrace{\text{Doug passes his math class}}^{D)}$$

$$\overset{\rightarrow}{\text{then}}\ \overbrace{\text{the sun will rise in the morning.}}^{S}$$

Thus our statement is $(C \vee D) \rightarrow S$. The process is not always this straightforward since there are many ways of expressing the logical operators in words. Consider "If Doug fails his math test, then in order for the sun to rise tomorrow, it is sufficient that Candace leaves a candle in her window." We notice the occurrence of $\neg D$, S, and C:

$$\text{If } \overbrace{\text{Doug fails his math test,}}^{\neg D} \text{ then in order for } \overbrace{\text{the sun to rise tomorrow,}}^{S}$$
$$\text{it is sufficient that } \overbrace{\text{Candace leaves a candle in her window.}}^{C}$$

We notice the "if...then..." and place an $\rightarrow$ over the "then" and group it by itself. The rest of the sentence seems to be a single unit, so we place it in parenthesis:

$$\text{If } \overbrace{\text{Doug fails his math test,}}^{\neg D}\ \overset{\rightarrow}{\text{then}} \text{ in order for } \overbrace{\text{the sun to rise tomorrow,}}^{(S}$$
$$\text{it is sufficient that } \overbrace{\text{Candace leaves a candle in her window.}}^{C)}$$

What we have in parenthesis - "In order for S, it is sufficient that C" - is an implication. The sufficient part is C, and we recall that the sufficient part of an implication is the antecedent - what comes before the arrow. Thus, what is in parenthesis is $C \rightarrow S$. We draw the arrow backwards here ($\leftarrow$) to maintain the sentence structure.

$$\text{If } \overbrace{\text{Doug fails his math test,}}^{\neg D}\ \overset{\rightarrow}{\text{then}} \text{ in order for } \overbrace{\text{the sun to rise tomorrow,}}^{(S}$$
$$\overset{\leftarrow}{\text{it is sufficient}} \text{ that } \overbrace{\text{Candace leaves a candle in her window.}}^{C)}$$

Our statement is $\neg D \rightarrow (C \rightarrow S)$. More examples are saved for the exercises.

1.18 Exercises: Let F be the statement "The fox is more clever than the rabbit." Let R be "The rabbit is quicker than the fox," and let C be "The fox will catch the rabbit." Write each of the following compound statements using symbols:

1.18.1 The rabbit is quicker than the fox; however, the fox is more clever than the rabbit and will catch the rabbit.
1.18.2 The fox is not more clever than the rabbit, and the rabbit is quicker than the fox.
1.18.3 The rabbit is quicker than the fox, but the fox will catch the rabbit anyway.
1.18.4 Although the fox is more clever than the rabbit, the fox will not catch the rabbit.
1.18.5 If the fox is more clever than the rabbit or the rabbit is not quicker than the fox, then the fox will catch the rabbit.
1.18.6 In order for the fox to catch the rabbit, it is sufficient that the rabbit is not quicker than the fox.
1.18.7 For the fox to catch the rabbit, it is necessary that the rabbit is not quicker than the fox.
1.18.8 While the fox is more clever than the rabbit, the rabbit is quicker than the fox; hence, the fox will not catch the rabbit.

1.19 Truth Tables: We now turn to determining if a compound statement is true or false. Our first method will be to draw truth tables for compound statements like we did for our logical operators. We illustrate the method with an example. Consider the statement $(P \vee Q) \wedge (\neg P \vee Q)$. We will construct a table. The first columns of the table will be labeled P and Q just as above. The next columns in the table will be labeled by the compound statements in our statement which are slightly more complicated than simply P or Q. These may be $\neg P$ or $P \vee Q$. The next column will be the next more complicated statement - $\neg P \vee Q$, and the next would be the next more complicate (which in this case would be the whole statement) and so on. Thus our table should have columns labeled by P, Q, $\neg P$, $P \vee Q$, $\neg P \vee Q$, and $(P \vee Q) \wedge (\neg P \vee Q)$.

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

The statements are single letters on the extreme left. They get more complicated as we move toward the right until we reach the entire statement. Now, the first two columns will list all possible combinations

of truth values for P and Q as above (notice we use the same pattern):

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

We next fill in the column for $\neg P$. The first line of the truth table for $\neg$ in section 1.10 could be read as $\neg T = F$, so anywhere we see a T under P, we should have a F under $\neg P$. The second row of $\neg$ could be read as $\neg F = T$, so when P is false, we place a T under $\neg P$. The column for $P \vee Q$ is filled out similarly. The rows of the truth table for $\vee$ could be read as $T \vee T = T$, $T \vee F = T$, and so on. Filling in these two columns gives

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

We fill in the column for $\neg P \vee Q$ the same way - applying $\vee$ to the columns for $\neg P$ and Q

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

Finally, we apply $\wedge$ to the last two columns to get the truth values for the entire statement. The truth table for $\wedge$ tells us that $T \wedge T = T$, and everything else is false.

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

As another example, we will draw a truth table for the statement $(A \wedge B) \rightarrow \neg C$. This statement has three letters, so we need a column

for each letter. We will also need columns for $A \wedge B$, $\neg C$, and the whole statement. To get every possible combination of truth values for A, B, and C, we need eight rows (it is best to memorize this pattern to make sure you get it right). We then fill in the other columns as we did above to get

A	B	C	$A \wedge B$	$\neg C$	$(A \wedge B) \rightarrow \neg C$
T	T	T	T	F	F
T	T	F	T	T	T
T	F	T	F	F	T
T	F	F	F	T	T
F	T	T	F	F	T
F	T	F	F	T	T
F	F	T	F	F	T
F	F	F	F	T	T

We can now use this truth table to determine truth values of our statement. For example, the third row says that if A and C are true but B is false, then the whole statement is true.

1.20 Exercises: Draw truth tables for each of these:

1.20.1 $\neg P \vee \neg Q$

1.20.2 $\neg(P \wedge Q)$

1.20.3 $\neg P \vee Q$

1.20.4 $\neg B \rightarrow \neg A$

1.20.5 $A \wedge (B \vee C)$

1.20.6 $(A \wedge B) \vee (A \wedge C)$

1.21 Calculating Truth Values: If we know the truth values of the letters in a compound statement and want to know the truth value of the whole statement, we could draw a truth table for the statement and read off the appropriate row. This is tedious - especially if there are more than two letters. A quicker way is to do arithmetic with the T's and F's. For example, suppose that A, C, and D are true while B is false. Consider the statement

$$(A \wedge \neg B) \rightarrow ((C \wedge B) \vee (\neg A \wedge D))$$

We want to know the truth value of this statement. First, replace all of the A's, C's, and D's by T, and replace the B's by F

$$(T \wedge \neg F) \rightarrow ((T \wedge F) \vee (\neg T \wedge T))$$

We can now do arithmetic with the T's and F's using the truth tables as guidlines. We follow the order of operations dictated by the parenthesis and negations (the operations are indicated by bold print):

$$
\begin{array}{ll}
(T\wedge\neg F)\rightarrow((T\wedge F)\vee(\neg T\wedge T)) & \\
=(T\wedge\mathbf{T})\rightarrow((T\wedge F)\vee(\mathbf{F}\wedge T)) & (\text{ since } \neg F=T \text{ and } \neg T=F)\\
=\mathbf{T}\rightarrow((T\wedge F)\vee(F\wedge T)) & \text{ since } T\wedge T=T\\
=T\rightarrow(\mathbf{F}\vee(F\wedge T)) & (\text{ since } T\wedge F=F)\\
=T\rightarrow(F\vee\mathbf{F}) & (\text{ since } F\wedge T=F)\\
=T\rightarrow\mathbf{F} & (\text{ since } F\wedge F=F)\\
=F & (\text{ since } T\rightarrow F=F)
\end{array}
$$

1.22 Exercises: Find the truth values of the following statements:

1.22.1 $(P\vee Q)\wedge(P\vee R)$ if P is false, Q is true, and R is true.

1.22.2 $\neg(\neg P\wedge(Q\vee\neg R))$ if P is false, Q is false, and R is true.

1.22.3 $(\neg P\wedge\neg Q)\vee(P\vee Q)$ if P is false and Q is true.

1.22.4 $\neg(P\vee Q)\wedge(P\vee\neg Q)$ if P is true and Q is false.

1.22.5 If the sun rises in the east, then it sets in the west.

1.22.6 In order for the sun to set in the west, it is necessary for it to rise in the east.

1.22.7 In order for the sun to set in the north, it is sufficient for it to rise in the west.

1.22.8 If I clap three times, the sun will rise tomorrow.

1.22.9 The sun rises in the east only if it sets in the north.

1.22.10 The sun rises in the south if and only if the sun rises in the north.

1.23 Exercises:

1.23.1 Suppose P and Q are statements (it does not matter what they are). Write a compound statement using P and Q which is always **true**. (You do not have to use both P and Q if you do not need to.)

1.23.2 Suppose P and Q are statements (it does not matter what they are). Write a compound statement using P and Q which is always **false**. (You do not have to use both P and Q if you do not need to.)

1.23.3 Suppose P and Q are statements. Use logical operators to write the statement: "P is true, or Q is true, but not both."

1.23.4 Suppose P, Q, and R are statements. Use logical operators to write the statement: "Exactly two of P, Q, and R are true."

2

Logical Equivalence

2.1 Tautology: A compound statement which is always true regardless of the truth values of the atomic statements involved is called a **tautology**. The standard example of a tautology is $P \vee \neg P$. Any statement P is either true or false. This means that one of P and $\neg P$ must always be true. Hence, $P \vee \neg P$ must be true. We can draw a truth table to verify this:

P	$\neg P$	$P \vee \neg P$
T	F	T
F	T	T

We see that the last column consists of only T's. This is the telltale sign of a tautology. Another less obvious example of a tautology is $(\neg A \vee B) \rightarrow (A \rightarrow B)$. To show this statement is a tautology, we can simply draw a truth table and see that the final column contains only T's.

A	B	$\neg A$	$A \rightarrow B$	$\neg A \vee B$	$(\neg A \vee B) \rightarrow (A \rightarrow B)$
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

2.2 Contradiction: A compound statement which is always false regardless of the truth values of the atomic statements involved is called a **contradiction**. The standard example of a contradiction is $P \wedge \neg P$. Since P and $\neg P$ will always have opposite truth values, they can never both be true, so $P \wedge \neg P$ must be false. Here is the truth table

P	$\neg P$	$P \wedge \neg P$
T	F	F
F	T	F

To show that any other statement is a contradiction, you may draw a truth table for the statement and see that the final column is all F's.

2.3 Logical Equivalence: We saw in the first chapter that the statements $P \wedge Q$ and $Q \wedge P$ communicate the same thing. For all practical purposes, we can identify these two statements. There are many instances in which different compound statements can be identified. Since logic in a sense only cares about truth values, we will identify two compound statements which have the same truth values. More precisely, when two compound statements always have the same truth values regardless of the truth values of the atomic statements involved, we will say that the two statements are **logically equivalent**. This means that two statements are equivalent if, when you draw their truth tables, the final columns in the two tables are identical. For example, the truth tables for $P \rightarrow Q$ and $\neg P \vee Q$ are

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

and

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

We begin the two tables with P and Q (the same order in both tables), and the final columns are identical. Therefore, these two statements are equivalent. We will denote logical equivalence using the symbol $\equiv$. For example, $P \wedge Q \equiv Q \wedge P$ or $P \rightarrow Q \equiv \neg P \vee Q$.

2.4 Basic Equivalences: There are only eight types of equivalences you need to remember. All other logical equivalences can be derived from these. They are listed below.

2.5 Commutative Laws: The english words "and" and "or" do not care about order. Saying "The grass is green, or the sky is blue" communicates the same thing as "The sky is blue, or the grass is green." The same is true with "and." Thus our first pair of equivalences should make sense:

$$P \wedge Q \equiv Q \wedge P \text{ and } P \vee Q \equiv Q \vee P$$

Notice that these resemble the commutative laws for multiplication and addition.

2.6 Associative Laws: Our next pair of equivalences resembles the associative laws for multiplication and addition. The two statements "Jill and Jane passed math, and Janet passed math" and "Jill passed math, and Jane and Janet passed math" communicate the same thing -

all three women passed. The word "and" does not care how statements are grouped together, and neither does "or." Thus

$$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R) \text{ and } (P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

Because of this equivalence, we will usually just write $P \wedge Q \wedge R$ or $P \vee Q \vee R$ and dispense with the parenthesis.

2.7 Idempotent Laws: Our next set of equivalences again reflect the English language. All three of these statements

"It is not the case that it is not raining."
"It is raining, and it is raining."
"Either it is raining, or it is raining."

communicate the same thing - "It is raining." Thus we have three equivalences called the idempotent laws

$$\neg(\neg P) \equiv P \text{ and } P \wedge P \equiv P \text{ and } P \vee P \equiv P$$

2.8 Absorption Laws: The next pair of equivalences are perhaps the least intuitive and least reflect a situation in english. For now, we will justify them by truth tables. They will become much more intuitive when we discuss switching networks. The equivalences are

$$P \wedge (P \vee Q) \equiv P \text{ and } P \vee (P \wedge Q) \equiv P$$

Here is a truth table for $P \wedge (P \vee Q)$

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

Notice that when P is true this statement is true. When P is false, this statement is false. Hence they are equivalent.

2.9 Distributive Laws: Consider the statement "It is raining, and either Hal forgot his hat or he forgot his coat." If this is true, what do we know? We know it is raining. We know that Hal forgot either his hat or his coat. In the first case, it is raining and he forgot his hat. In the second, it is raining and he forgot his coat. The statement seems

to say "It is raining and Hal forgot his coat, or it is raining and Hal forgot his hat." This reflects our next pair of equivalences:

$$P\wedge(Q\vee R) \equiv (P\wedge Q)\vee(P\wedge R)$$

and

$$P\vee(Q\wedge R) \equiv (P\vee Q)\wedge(P\vee R)$$

These resemble the way in which we distribute multiplication over addition.

2.10 DeMorgan's Laws: Consider the sentence "It is not true that Sam passed math and English." What does this mean? Let P be "Sam passed math," and let Q be "Sam passed English." The statement we are looking at is $\neg(P\wedge Q)$. In order for this to be true, $P\wedge Q$ needs to be false. This happens if at least one of P and Q is false. Thus our sentence appears to be $\neg P\vee\neg Q$ - "Either Sam did not pass math, or sam did not pass English." This is an example of one of DeMorgan's Laws:

$$\neg(P\wedge Q) \equiv \neg P\vee\neg Q \text{ and } \neg(P\vee Q) \equiv \neg P\wedge\neg Q$$

You can think of DeMorgan's Laws as distributing negation over $\wedge$ and $\vee$ - except that the negation applies to everything, even the $\wedge$ and the $\vee$.

2.11 Disjunctive Implication: We already saw this equivalence as an example earlier. Here it is

$$P\rightarrow Q \equiv \neg P\vee Q$$

This reflects what was said in the first chapter that $P\rightarrow Q$ can be phrased as "Not P unless Q."

2.12 Contrapositive: Suppose you know this statement is true "If Sam won his game, he is going to play in the championship game." If someone tells you that Sam is not going to play in the championship game, then you immediately conclude that Sam did not win his game. You are intuitively aware of this final logical equivalence

$$P\rightarrow Q \equiv \neg Q\rightarrow\neg P$$

The statement $\neg Q\rightarrow\neg P$ is called the **contrapositive** of $P\rightarrow Q$. You should be careful not to confuse it with the statement $\neg P\rightarrow\neg Q$ known

as the **inverse** of $P \to Q$ or with $Q \to P$ known as the **converse** of $P \to Q$. These statements are not equivalent to $P \to Q$. Here are all of the basic equivalences together:

$P \wedge Q \equiv Q \wedge P$	commutative law
$P \vee Q \equiv Q \vee P$	commutative law
$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$	associative law
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$	associative law
$\neg(\neg P) \equiv P$	idempotent law
$P \wedge P \equiv P$	idempotent law
$P \vee P \equiv P$	idempotent law
$P \equiv P \vee (P \wedge Q)$	absorption law
$P \equiv P \wedge (P \vee Q)$	absorption law
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	distributive law
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$	distributive law
$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$	DeMorgan's Law
$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$	DeMorgan's Law
$P \to Q \equiv \neg P \vee Q$	disjunctive implication
$P \to Q \equiv \neg Q \to \neg P$	contrapositive

2.13 Exercises: Draw truth tables to verify all of the basic equivalences above.

2.14 Special Equivalences: Suppose A is a true statement and P is any statement. A truth table for $P \wedge A$ would look like

P	A	$P \wedge A$
T	T	T
F	T	F

First of all, notice that we only need two rows since A is true. Second, notice that the truth values for $P \wedge A$ are identical to those for P. The statements P and $P \wedge A$ are equivalent if A is known to be true. We can summarize this by writing $P \wedge T \equiv P$ - where the T denotes a true statement or tautology. As an example of how to use this, consider the statement $(B \wedge D) \vee (B \wedge \neg D)$ We can use the distributive law to re-write this as $B \wedge (D \vee \neg D)$. Now, $D \vee \neg D$ is a tautology, so this statement looks like $B \wedge T$ (where T is the tautology). This is equivalent to B. Thus, $(B \wedge D) \vee (B \wedge \neg D) \equiv B$. A similar equivalence holds for disjunction with a contradiction. It can be written as $P \vee F \equiv P$ - where F represents a contradiction.

2.15 Examples: The equivalences above can be used to demonstrate more complicated equivalences. For example, the statement $\neg(A\wedge\neg B)$ is equivalent to $A\rightarrow B$. We can use the basic equivalences to show this. Notice that $\neg(A\wedge\neg B)$ is of the form of one of DeMorgan's Laws, so we will "distribute" the negation to get $\neg(A\wedge\neg B) \equiv \neg A\vee\neg(\neg B)$. Next, notice the double negation. We can use one of the idempotent laws to get $\neg A\vee\neg(\neg B) \equiv \neg A\vee B$. This last statement looks just like part of disjunctive implication, which tells us that $\neg A\vee B \equiv A\rightarrow B$. This is what we were looking for. Here is our work all together:

$$\begin{array}{rcll} \neg(A\wedge\neg B) & \equiv & \neg A\vee\neg(\neg B) & \text{DeMorgan's Law} \\ & \equiv & \neg A\vee B & \text{Idempotent Law} \\ & \equiv & A\rightarrow B & \text{Disjunctive Implication} \end{array}$$

Notice how we set up our work here. To show that $\neg(A\wedge\neg B) \equiv A\rightarrow B$, we begin with one statement on the left of an equivalence sign (here we use $\neg(A\wedge\neg B)$, but we could very well have started with the other statement). We then apply equivalences to this statement, listing the results to the right of equivalence signs until we arrive at $A\rightarrow B$. Here are more examples:

Problem: Show $A\rightarrow(P\vee R) \equiv (A\rightarrow P)\vee(A\rightarrow R)$
Solution:

$$\begin{array}{rcll} (A\rightarrow P)\vee(A\rightarrow R) & \equiv & (\neg A\vee P)\vee(\neg A\vee R) & \text{(disjunctive implication)} \\ & \equiv & \neg A\vee(P\vee(\neg A\vee R)) & \text{(associative law} \\ & \equiv & \neg A\vee((P\vee\neg A)\vee R) & \text{(associative law)} \\ & \equiv & \neg A\vee((\neg A\vee P)\vee R) & \text{(commutative law)} \\ & \equiv & \neg A\vee(\neg A\vee(P\vee R)) & \text{(associative law)} \\ & \equiv & (\neg A\vee\neg A)\vee(P\vee R) & \text{(associative law)} \\ & \equiv & \neg A\vee(P\vee R) & \text{(idempotent law)} \\ & \equiv & A\rightarrow(P\vee R) & \text{(disjunctive implication)} \end{array}$$

This looks a little confusing with all of the associative law applications. It is actually much simpler. If we abuse a little notation, the work looks like:

$$\begin{array}{rcll} (A\rightarrow P)\vee(A\rightarrow R) & \equiv & (\neg A\vee P)\vee(\neg A\vee R) & \text{(disjunctive implication)} \\ & \equiv & \neg A\vee P\vee\neg A\vee R & \text{(associative law)} \\ & \equiv & \neg A\vee\neg A\vee P\vee R & \text{(commutative law)} \\ & \equiv & \neg A\vee P\vee R & \text{(idempotent law)} \\ & \equiv & \neg A\vee(P\vee R) & \text{(associative law)} \\ & \equiv & A\rightarrow(P\vee R) & \text{(disjunctive implication)} \end{array}$$

Usually, we will abuse notation like this and ignore parenthesis when associativiy allows it.

Problem: Show $(A\vee B)\vee(A\wedge P)\vee(B\wedge P)\equiv(A\vee B)$
Solution:

$$\begin{array}{ll}(A\vee B)\vee(A\wedge P)\vee(B\wedge P) & \equiv(A\vee B)\vee(P\wedge A)\vee(P\wedge B)\\ & \text{(commutative law)}\\ & \equiv(A\vee B)\vee(P\wedge(A\vee B))\\ & \text{(distributive law)}\\ & \equiv(A\vee B)\vee((A\vee B)\wedge P)\\ & \text{(commutative law)}\\ & \equiv(A\vee B)\\ & \text{(absorption law)}\end{array}$$

The second step in this example can be thought of as "factoring" a common P from the last two terms. Commutativity actually lets us distribute from both directions, so we could shorten this just commuting and absorbing:

$$(A\vee B)\vee(A\wedge P)\vee(B\wedge P)\equiv(A\vee B)\vee((A\vee B)\wedge P)\equiv(A\vee B)$$

Problem: Show $(P\to B)\wedge(Q\to B)\equiv(P\vee Q)\to B$
Solution:

$$\begin{array}{lll}(P\to B)\wedge(Q\to B) & \equiv(\neg P\vee B)\wedge(\neg Q\vee B) & \text{(disjunctive implication)}\\ & \equiv(\neg P\wedge\neg Q)\vee B & \text{(distributive law)}\\ & \equiv\neg(P\vee Q)\vee B & \text{(DeMorgan's Law)}\\ & \equiv(P\vee Q)\to B & \text{(disjunctive implication)}\end{array}$$

2.16 Exercises: Use the basic logical equivalences to show that these statements are equivalent.

2.16.1 $(P\to R)\vee(Q\to R)\equiv(P\wedge Q)\to R$
2.16.2 $\neg(A\vee B)\vee P\equiv(A\to P)\wedge(B\to P)$
2.16.3 $(A\vee B)\wedge(C\vee D)\equiv(A\wedge C)\vee(B\wedge C)\vee(A\wedge D)\vee(B\wedge D)$
2.16.4 $A\vee(B\vee C)\equiv(A\vee B)\vee(A\vee C)$

2.17 Simplification: Logical equivalences can often be used to simplify statements. For example, The statement "It is not true that I passed and you did not." Sounds a little confusing. Let I be "I passed," and let Y be "You passed." The statement we are considering is $\neg(I\wedge\neg Y)$. Using DeMorgan's Law and then the idempotent law, we see $\neg(I\wedge\neg Y)\equiv\neg I\vee\neg\neg Y\equiv\neg I\vee Y$. Thus the original statement is equivalent to the simpler statement "Either I did not pass, or you did."

Logical equivalences can be used to simplify instructions or conditions. For example, suppose you are building a machine with a warning light and you are told that "The warning light should come on if either the temperature is high while the pressure is high and the door is open or the temperature is high while it is not the case that both the pressure is not high and the door is

closed." This is a baffling condition. Let T be "The temperature is high." Let P be "The pressure is high," and let D be "The door is open." Our condition for the warning light to come on is $(T \wedge P \wedge D) \vee (T \wedge \neg(\neg P \wedge \neg D))$. This is so confusing, the circuitry to build the warning light could be quite complicated. However, notice

$$\begin{aligned}(T \wedge P \wedge D) \vee (T \wedge \neg(\neg P \wedge \neg D)) \quad &\equiv T \wedge ((P \wedge D) \vee (P \vee D)) \\ &\text{(distributive law)} \\ &\equiv T \wedge (((P \wedge D) \vee P) \vee ((P \wedge D) \vee D)) \\ &\text{(distributive law)} \\ &\equiv T \wedge (P \vee D) \\ &\text{(absorption law)}\end{aligned}$$

so the condition is equivalent to the much simpler statement "The temperature is high and either the pressure is high or the door is open."

2.18 Exercises: Use logical equivalences to simplify the following statements. Write your answers in words.

2.18.1 It is not true that both it is not cold and it is raining or snowing.

2.18.2 The possible combinations of toppings on the sandwich are meat and pickles and cheese, or meat and onions and cheese, or meat and pickles and tomatoes.

2.18.3 You will pass if either you pass both the midterm and the final, or if you do not fail both the major project and the final.

2.18.4 If we beat the "Cats" and the "Dogs" but not the "Penguins," or if we beat the "Cats" and the "Penguins" but not the "Dogs," or if we beat all three, then we will go to the playoffs.

2.19 Disjunctive Normal Form: Consider the following list of equivalences:

$$\begin{aligned}P \wedge (A \rightarrow Q) \wedge \neg R \quad &\equiv P \wedge (\neg A \vee Q) \wedge \neg R \\ &\text{(disjunctive implication)} \\ &\equiv ((P \wedge \neg A) \vee (P \wedge Q)) \wedge \neg R \\ &\text{(distributive law)} \\ &\equiv (P \wedge \neg A \wedge \neg R) \vee (P \wedge Q \wedge \neg R) \\ &\text{(distributive law)}\end{aligned}$$

This last statement is in a special form. It is the disjunction ($\vee$) of statements which are conjunctions ($\wedge$) of atomic statements and negated atomic statements. Such a statement is said to be in **disjunctive normal form**. Every statement is equivalent to a statement in disjunctive normal form. There is a simple strategy for converting any statement to disjunctive normal form (the strategy is simple, but applying it can get messy). First, apply disjunctive implication to get rid of any implications. Second, apply DeMorgan's Laws along with the idempotent law repeatedly until the only statements which are

negated are atomic statements. Next, distribute $\wedge$s over $\vee$s repeatedly until you are in disjunctive normal form. Here is an example.

$$\begin{aligned} R\wedge\neg((A\wedge B)\rightarrow(P\wedge Q)) \quad & \equiv R\wedge\neg(\neg(A\wedge B)\vee(P\wedge Q)) \\ & \text{(disjunctive implication)} \\ & \equiv R\wedge(\neg\neg(A\wedge B)\wedge\neg(P\wedge Q)) \\ & \text{(DeMorgan's Law)} \\ & \equiv R\wedge((A\wedge B)\wedge\neg(P\wedge Q)) \\ & \text{(idempotent law)} \\ & \equiv R\wedge((A\wedge B)\wedge(\neg P\vee\neg Q)) \\ & \text{(DeMorgan's Law)} \\ & \equiv R\wedge((A\wedge B\wedge\neg P)\vee(A\wedge B\wedge\neg Q)) \\ & \text{(distributive law)} \\ & \equiv (R\wedge A\wedge B\wedge\neg P)\vee(R\wedge A\wedge B\wedge\neg Q) \\ & \text{(distributive law)} \end{aligned}$$

It is possible to end up with a disjunction of more than two statements. For example, you may have $(A\wedge B)\vee(A\wedge C)\vee(B\wedge C)$. It is also possible to end up with simply a conjunction of atomic statements and negations of atomic statements.

2.20 Exercises: Write each of the following statements in disjunctive normal form.

2.20.1 $A\rightarrow\neg(B\vee C)$

2.20.2 $(A\rightarrow B)\wedge\neg(A\rightarrow C)$

2.20.3 $A\wedge(\neg B\rightarrow(C\wedge D))$

2.20.4 $(A\rightarrow B)\wedge(\neg A\rightarrow\neg B)$

2.21 Rewriting Implications There are many cases in our natural language when an implication may be expressed without the words "if...then.." For example, the sentence

> The square of any even integer is even.

is logically the same as the implication

> If n is an even integer, then n^2 is even.

The statement

> All kittens are cute.

can be expressed as

> If it is a kitten, then it is cute.

The sentence

> When it rains, it pours.

can be expressed

If it is raining, then it is pouring.

Using disjunctive implication, the contrapositive, and varying english translations, we can rewrite these sentences in a variety of ways:

Original: When it rains, it pours.

Implication: If it is raining, then it is pouring.

Contrapositive: If it is not pouring, then it is not raining.

Disjunction: Either it is not raining, or it is pouring.

Necessary: In order for it to rain, it is necessary that it pours.

Sufficient: In order for it to pour, it is sufficient for it to rain.

2.22 Exercises: Translate each of these sentences into an implication. Then rewrite each with the contrapositive, as a disjunction, using "necessary," and using "sufficient."

2.22.1 All men are liars.

2.22.2 When the sun shines, she dances.

2.22.3 She cries when it rains.

2.22.4 All primes greater than 2 are odd. (Hint: "If n is...")

2.22.5 If you build it, he will come.

2.23 Fewer Logical Connectives Not all of our logical connectives are necessary. The biconditional can be expressed with conjunction and implication. Disjunctive implication lets us express the implication with $\neg$ and $\vee$. In fact, DeMorgan's Laws let us write $\vee$ with $\neg$ and $\wedge$:

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

We can also express $\wedge$ with $\neg$ and $\vee$:

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

We could write all of our logical statements using fewer logical connectives. However, having all of our connectives makes it easier to translate between symbols and english.

2.24 Exercises

2.24.1 Use the comments above to express every connective in terms of $\neg$ and $\wedge$.

2.24.2 Use the comments above to express every connective in terms of $\neg$ and $\vee$.

2.24.3 Express every connective in terms of $\neg$ and $\rightarrow$.

2.24.4 Define a new connective (called the **Sheffer Stroke**) by $P|Q = \neg(P \wedge Q)$. Express all of the logical connectives using $|$. For example, $\neg P = P|P$ and $P \wedge Q = (P|Q)|(P|Q)$. (Check these.) This means that we could do all of our logic with only one logical connective.

2.24.5 Is the Sheffer stroke operation associative?

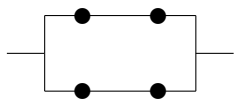
2.24.6 Is the Sheffer stroke operation commutative?

3

Switching Networks

3.1 Terminology: Switching networks were initially inspired by electronic applications; however, it is not necessary to know anything about electronics to study switching networks. The notions we employ here actually apply in any environment in which some current (such as electricity, water, or light) is flowing along a path (such as a wire, a pipe, or optic fiber) and is controlled by some type of switching mechanisms which can be turned on and off. The ultimate goal of this chapter is to gain more intuition about logic and to see an application of what we have learned so far. We will see that the design of such things as electronic circuits is tied to the rules of logic we have been studying.

3.2 Switches and Switching Networks: A **switch** is a device with two states, "on" and "off." A switch controls the flow of a current. When a switch is on, a current may flow through the switch. When a switch is off, it may not. Our currents will flow along things called paths. When switches are placed on a collection of paths to regulate the flow of the current, what results is called a **switching network**. We will assume that all of our switching networks have a single path through which the current enters the network. This will be called the **input path**. We will also assume that the network has a single path through which the current may leave. This is the **output path**. If current can flow from the input to the output path, then the network is on. Otherwise, the network is off. In this chapter, we will be drawing pictures of switching networks. In the pictures, switches will be symbolized by filled circles, and paths will be symbolized by line segments. For example



An example of a switching network.

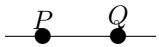
If a line segment passes through a circle it symbolizes that the corresponding switch controls the flow of the current along that path.

3.3 Switches and Logical Operators: We can draw switching networks to represent logical statements in such a way that a network is on precisely when the logical statement is true. Let P be the symbol of a logical statement. We can label switches in a switching network with the symbol P. When we do so, we assume that when P is true, then the switches labeled P are on. When P is false, they are off.
Here is a very small switching network.

A switching network for the statement P.

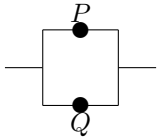
When P is true, this network is on. When P is false, this network is off.

We can draw networks for compound statements also. This is a network for $P \wedge Q$.



A network for $P \wedge Q$.

The only way that current can flow through this network is for both switches to be on. That happens when both statements are true, so $P \wedge Q$ is true. If current does not flow, one of the switches is off. This means either P or Q is false, so $P \wedge Q$ is false. The switches in the network for $P \wedge Q$ are said to be connected in **series**. We will always associate series with $\wedge$. Here is a network for $P \vee Q$.



A network for $P \vee Q$.

Current will flow through this network exactly when one of the switches is on, which is when one of the statements is true, which is exactly when $P \vee Q$ is true. The switches in the network for $P \vee Q$ are said to be connected in **parallel**. We will always associate parallel with $\vee$.

In order to draw a network for negation, we cheat. We can label switches by the negation of a symbol for a statement. For example, if P is a statement, we can label a switch as $\neg P$. This switch would be on when P is false

and off when P is true. The network would look like this.

A switching network for the statement $\neg P$.

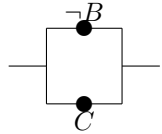
We will approach a network for $P \to Q$ later.

3.4 Multiple Switches: To be able to draw switching networks for more complicated compound statements, we will assume that we can give more than one switch the same label. For instance, a network may have many switches labeled by P. All of these switches would be on when P is true. All would be off when P is false.

3.5 Switching Networks for Compound Statements: We can draw switching networks for any statement. Here is an example of how. Consider the statement $A \wedge (B \to C)$. We have not discussed switching networks for $\to$. To handle $\to$, we will use the logical equivalence $B \to C \equiv \neg B \vee C$. Thus we will actually draw a network for $A \wedge (\neg B \vee C)$. First, we make a list of the statements inside of $A \wedge (\neg B \vee C)$ beginning with the simplest and working our way through the more complicated to the whole statement: A, B, C, $\neg B$, $\neg B \vee C$, $A \wedge (\neg B \vee C)$ (These are the statements we would employ in drawing the truth table). We will draw networks for each small statement other than the atomic statements. The network for $\neg B$ is

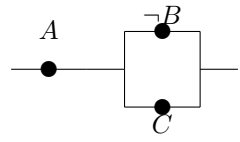
A switching network for the statement $\neg B$.

To form $\neg B \vee C$, we will take the network for $\neg B$ and place it in parallel with a network for C like so



A network for $\neg B \vee C$.

Finally, to combine this with A with an $\wedge$, we place this network in series with the network for A



A network for $A \wedge (\neg B \vee C)$

This is the strategy. First, use disjunctive implication to replace all arrows. Next, apply DeMorgan's Laws if necessary so that the only statements which are negated are atomic statements. Finally, make a list of the statements which compose the compound statement as you would for a truth table. Draw networks for each statement beginning with the simplest. To draw the conjunction ($\wedge$) of two statements, connect the networks you already have in series. To draw the disjunction ($\vee$) of two statements, connect the networks you already have in parallel.

Here is another example. We will draw a network for the statement

$$\neg(A \wedge B) \wedge (P \rightarrow (A \vee B)).$$

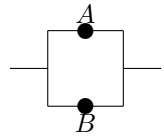
First, we must use disjunctive implication to rewrite this as

$$\neg(A \wedge B) \wedge (\neg P \vee (A \vee B)).$$

Next, DeMorgan's Law gives

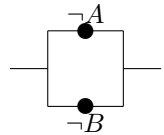
$$\neg(A \wedge B) \wedge (\neg P \vee (A \vee B)) \equiv (\neg A \vee \neg B) \wedge (\neg P \vee (A \vee B)).$$

We now make a list of statements which can be used to make this statement: A, B, P, $\neg A$, $\neg B$, $\neg P$, $A \vee B$, $\neg A \vee \neg B$, $\neg P \vee (A \vee B)$. Finally, we can start drawing. We will not draw networks for A, B, P, $\neg A$, $\neg B$, or $\neg P$. The table for $A \vee B$ looks like



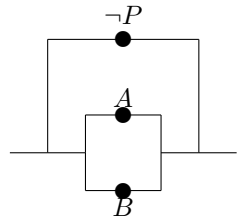
A network for $A \vee B$.

The network for $\neg A \vee \neg B$ is



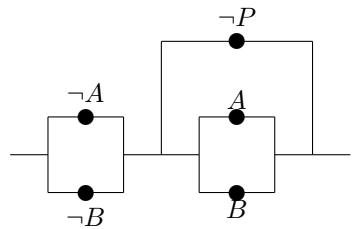
A network for $\neg A \vee \neg B$.

To form $\neg P \vee (A \vee B)$, we place the networks for $\neg P$ and $(A \vee B)$ in parallel



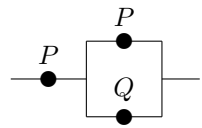
A network for $\neg P \vee (A \vee B)$.

Finally, to make $(\neg A \vee \neg B) \wedge (\neg P \vee (A \vee B))$, we place the networks above for $(\neg A \vee \neg B)$ and $(\neg P \vee (A \vee B))$ in series to get



A network for $(\neg A \vee \neg B) \wedge (\neg P \vee (A \vee B))$.

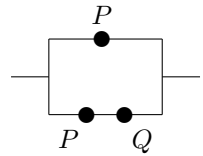
3.6 Absorption Laws: In the second chapter, we said that the absorption laws would make more sense with switching networks. The network for $P \wedge (P \vee Q)$ looks like



A network for $P \wedge (P \vee Q)$.

If P is true, then the switches labeled P are on and the current can flow through the top half of this network (regardless of Q). If P is false, then the first switch labeled P prevents the current from flowing (again, regardless of Q). The network is on precisely when P is true. It seems reasonable, then, that this statement should be equivalent to P.

The network for $P \vee (P \wedge Q)$ looks like



A network for $P \vee (P \wedge Q)$.

If P is true, current can flow through the top of the network. If P is false, it cannot flow through either half of the network. Again, the network is on exactly when P is true.

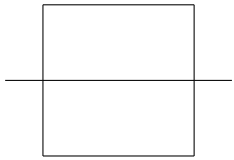
3.7 Exercises: Draw switching networks for each of the following statements.

3.7.1 $(P \wedge \neg Q) \vee (\neg P \wedge Q)$
3.7.2 $((\neg P \vee Q) \wedge R) \vee \neg Q$
3.7.3 $P \rightarrow (A \wedge B)$
3.7.4 $\neg(A \vee (B \wedge C)) \wedge (P \vee Q)$
3.7.5 $A \vee (B \wedge (C \vee D))$

3.8 Networks and Disjunctive Normal Form: It is particularly easy to draw switching networks for statements in disjunctive normal form. Recall that a statement in disjunctive normal form is a disjunction ($\vee$) of statements which are conjunctions ($\wedge$) of either letters or negations of letters. We illustrate the strategy with the example

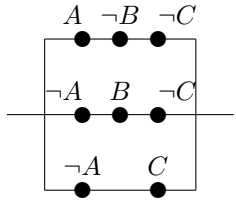
$$(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge C).$$

There are three parts to the disjunction, so our network will be made of three parallel components:



The skeleton of our network.

Networks for each conjunction replace the three horizontal lines in this picture. The first conjunction $A \wedge \neg B \wedge \neg C$ has three parts, so this line gets three dots labeled A, $\neg B$, and $\neg C$. The next conjunction $\neg A \wedge B \wedge \neg C$ again has three parts, so the middle line gets three dots labeled $\neg A$, B, and $\neg C$. Finally, the last conjunction $\neg A \wedge C$ has two parts, so the bottom line gets two dots labeled $\neg A$ and C. This gives



The skeleton of our network.

3.9 Exercises: Draw switching networks for of each these statements in disjunctive normal form.

3.9.1 $(A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$

3.9.2 $(A \wedge \neg B) \vee (B \wedge \neg C) \vee (C \wedge \neg D) \vee E$

3.9.3 $(A \wedge B) \vee (\neg A \wedge B) \vee (A \wedge \neg B) \vee (\neg A \wedge \neg B)$

3.10 Building Blocks of Statements: We can build statements which have any set of truth values we like. For example, suppose we want a statement which has a truth table that looks like

P	Q	$\cdots$	?
T	T		F
T	F		T
F	T		T
F	F		F

To construct the statement, locate the rows where we want truth. In this case, these are the middle two rows. The two rows give two conditions. The first row would require P to be true and Q to be false. A statement which would give truth here is $P \wedge \neg Q$. The second true row requires P to be false and Q to be true. A statement which has truth in this instance is $\neg P \wedge Q$. To construct the statement we need, we simply join these two statements with an $\vee$: $(P \wedge \neg Q) \vee (\neg P \wedge Q)$. This statement will have the desired truth values.

The strategy is this: For each true row in the truth table form a conjunction. Each letter involved should appear once in the conjunction. If in that row the letter is false, it will be negated in the conjunction. If in that row the letter is true, the letter appears not negated in the conjunction. Form a conjunction like this for each true row. Then join these together with $\vee$.

Here is another example. Suppose we want a statement with these truth

values

P	Q	R	$\cdots$	?
T	T	T		T
T	T	F		F
T	F	T		T
T	F	F		T
F	T	T		F
F	T	F		T
F	F	T		T
F	F	F		F

The table has five true rows, so we must first make five conjunctions. The first true row is the row where all three statements are true. The corresponding conjunction is $P \wedge Q \wedge R$. The next true row is where P and R are true and Q is false. The corresponding statement is $P \wedge \neg Q \wedge R$ (the Q is negated because Q is false on this row). The next has only P being true, so the corresponding statement is $P \wedge \neg Q \wedge \neg R$. The fourth true row has only Q being true. It gives $\neg P \wedge Q \wedge \neg R$. The last true row has only R being true, giving $\neg P \wedge \neg Q \wedge R$. To make our statement, we now take these five conjunctions and join them with $\vee$ to get

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

3.11 Exercises: Find statements which meet these conditions.

3.11.1 Find a statement which has this truth table

P	Q	R	$\cdots$	?
T	T	T		F
T	T	F		F
T	F	T		F
T	F	F		T
F	T	T		T
F	T	F		F
F	F	T		F
F	F	F		T

3.11.2 Find a statement which has this truth table

P	Q	R	$\cdots$	?
T	T	T		F
T	T	F		T
T	F	T		F
T	F	F		F
F	T	T		F
F	T	F		F
F	F	T		F
F	F	F		T

3.11.3 Find a statement which has this truth table

P	Q	R	$\cdots$	?
T	T	T		T
T	T	F		T
T	F	T		F
T	F	F		F
F	T	T		F
F	T	F		F
F	F	T		T
F	F	F		T

3.11.4 Find a compound statement using four atomic statements which is true when three or more of the atomic statements is true.

3.11.5 Find a compound statement using four atomic statements which is true when exactly two of the atomic statements is true.

3.12 Exercises:

3.12.1 There are only 16 possible final columns of a truth table with two atomic statements. Find them all and find statements which have each as the final column of their truth table. Use logical equivalences to write these as simply as possible.

3.12.2 How many possible final columns are there for a truth table of a statement with three atomic statements? Four?

3.13 Designing a Network: We want to build a switching network to control the light in a hallway. There is to be a switch at either end of the hall. The light should work this way. If the light is on and either switch is flipped, then the light should go off. If the light is off and either switch is flipped, the light should come on. We are going to construct a logical statement which mimics the behavior of the desired network, and then we will draw the network.

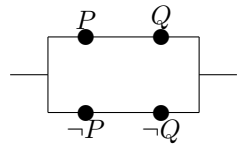
We will have two atomic statements P and Q since there are to be two physical switches in the hallway. If we decide on the desired truth values for our statement, we can use the process of the previous section to construct the statement. Suppose we begin with both switches on (P and Q are both true). In this case, we will assume the lights are on (statement is true). If we flip the switch corresponding to Q off (so P is true and Q is false), the lights should turn off (the statement if false). Similarly, if we start with both on and turn the switch for P off (so P is false and Q is true), then the lights should go off (the statement is false). At this point, if we turn the switch for Q off (P and Q are now both false), the lights should turn on (the statement is true).

This gives the desired truth table

P	Q	$\cdots$	?
T	T		T
T	F		F
F	T		F
F	F		T

Using the technique of the previous section, we construct the statement $(P \wedge Q) \vee (\neg P \wedge \neg Q)$. This should have the appropriate truth values.

We now have a logical statement which mimics the desired switching network. We need to draw the network for $(P \wedge Q) \vee (\neg P \wedge \neg Q)$. Since the statement is in disjunctive normal form, drawing it is simple.



A switching network to operate a hall light.

3.14 Exercises:

3.14.1 A light is to be operated by three switches. The light is to be on when two or more of the switches are on. Draw a switching network to control such a light.

3.14.2 A light is to be operated by three switches labeled A, E, and T. If the letters corresponding to the switches which are on can be used to spell an english word, the light should be on. Otherwise, the light is to be off. Draw a switching network to accomplish this.

4

Inference and Proof

4.1 Arguments: An **argument** is a list of statements, one of which is intended to be supported by the others. The supported statement is called the **conclusion**. The supporting statements are the **premises**. If the premises of an argument are $P_1, P_2, \ldots, P_n$, and the conclusion is C, we will write the argument in this manner

$$\begin{array}{l} P_1 \\ P_2 \\ \vdots \\ \underline{P_n} \\ \therefore C \end{array}$$

where the $\therefore$ can be read as "therefore."

4.2 Valid Arguments: The main task of logic can be viewed as deciding when the premises of an argument do support the conclusion. The argument above will be **valid** if the statement $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \rightarrow C$ is a tautology (always true). Otherwise, the argument is **invalid**. Notice the validity of an argument is independent of the actual statements in the argument and the content of those statements. Validity is a matter of form. In order to show that an argument is valid, one option is to form the statement $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \rightarrow C$, draw the truth table, and see that the final column consists of all Ts.

For example, the argument

$$\begin{array}{l} P \rightarrow Q \\ \underline{P} \\ \therefore Q \end{array}$$

is valid because the statment

$$((P \rightarrow Q) \wedge P) \rightarrow Q$$

is a tautology as can be seen in this truth table:

P	Q	$P \rightarrow Q$	$(P \rightarrow Q) \wedge P$	$((P \rightarrow Q) \wedge P) \rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

4.3 Exercises: Draw truth tables to determine if the following statements are valid or invalid.

4.3.1
$$\begin{array}{l} P \rightarrow Q \\ Q \\ \hline \therefore P \end{array}$$

4.3.2
$$\begin{array}{l} P \rightarrow Q \\ \neg P \\ \hline \therefore \neg Q \end{array}$$

4.3.3
$$\begin{array}{l} P \vee Q \\ \neg Q \\ \neg R \rightarrow \neg P \\ \hline \therefore R \end{array}$$

4.3.4
$$\begin{array}{l} P \\ Q \\ \hline \therefore P \wedge Q \end{array}$$

4.3.5
$$\begin{array}{l} P \wedge Q \\ \hline \therefore P \end{array}$$

4.3.6
$$\begin{array}{l} P \\ \hline \therefore P \vee Q \end{array}$$

4.3.7
$$\begin{array}{l} P \\ \neg P \\ \hline \therefore Q \end{array}$$

4.3.8 Is this argument valid?

If men were meant to fly, then men would have wings.
Men were meant to fly.

∴Men have wings.

4.4 Inference: Rather than drawing truth tables to establish that an argument is valid, we will make a list of short, simple arguments which we know are valid. We will be able to demonstrate the validity of complex arguments through repeated applications of these simple ones. The simple arguments will be called **rules of inference**.

4.5 Rules of Inference: We list the basic rules of inference here. Examples of their use are saved for later. Each of the letters in these rules represents any statement. They may be simple atomic statements, or they may be compound statements. This is important to remember.

4.6 Modus Ponens: Suppose as a student a professor tells you "If you pass the final, then you will pass the class." Later, you discover you did pass the final. Automatically, you conclude that you passed the class. You are instinctively applying the rule of inference known as **modus ponens**. As an argument, this is

$$\begin{array}{l} A \rightarrow B \\ A \\ \hline \therefore B \end{array}$$

which you showed to be valid in the earlier exercises. We will abreviate modus ponens as **MP**. We will usually write our rules of inference in words rather than using the argument format.
MP: From $A \rightarrow B$ and A infer B.

4.7 Tautology: It makes sense that we ought to at any time be able to deduce a tautologoy (something which is always true). This is our second rule of inference.
TAUT: If T is a tautology, we can always infer T.

4.8 Equivalence: The next rule of inference is also intuitive. If A and B are two compound statements which are equivalent, and if we know A to be true. It follows immediately that B is also true. Hence we get a rule which we will simply refer to as **equivalence**.
E: If $A \equiv B$, then from A infer B.

4.9 Addition: Since the statement $A \to (A \vee B)$ is a tautology, if we know A is true, then modus ponens tells us that $A \vee B$ is true. This gives
A: From A infer $A \vee B$.

4.10 Modus Tollens: Suppose we know $A \to B$ and $\neg B$ are true. Since $A \to B$ is true, the contrapositive $\neg B \to \neg A$ is also true (equivalence). We can now apply **MP** to the two statements $\neg B \to \neg A$ and $\neg B$ to infer that $\neg A$ must be true. This gives us a new rule of inference which we call **modus tollens**.
MT: From $A \to B$ and $\neg B$ infer $\neg A$.

4.11 Disjunctive Syllogism: The statement $A \vee B$ is equivalent to $\neg A \to B$. Thus if we know $A \vee B$ and $\neg A$, we could apply **E** and **MP** to conclude B. This gives another rule known as **disjunctive syllogism**. A syllogism is simply an argument. This argument uses disjunction ($\vee$), hence the name.
DS: From $A \vee B$ and $\neg A$ infer B.
Since $\vee$ is commutative, we could just as easily infer A if we knew $\neg B$.

4.12 Simplification: If we know the statement $A \wedge B$ is true, we immediately know that each of A and B is true. This is known as **simplification**.
S: From $A \wedge B$ infer A or infer B.

4.13 Conjunction: If we know the statements A and B are true, it follows immediately that $A \wedge B$ is true. This is **conjunction**.
C: From A and B infer $A \wedge B$.

4.14 Transitivity: Finally, suppose we know two facts.

"If Sam passes his math final, he will pass his math class."
"If Sam passes his math class, he will graduate."

Next, suppose we are informed that Sam did indeed pass his math final. By applying modus ponens twice, we can conclude first that Sam will pass his math class and, second, that he will graduate. Thus, if Sam passes his math final, he will graduate. This is our final rule of inference. It is known as **transitivity** and resembles the property of $\leq$ with the same name.
T: From $A \to B$ and $B \to C$ infer $A \to C$.

For convenience, here is a complete list of rules of inference.
MP: From $A \to B$ and A infer B.
TAUT: If T is a tautology, we can always infer T.
E: If $A \equiv B$, then from A infer B.
A: From A infer $A \vee B$.
MT: From $A \to B$ and $\neg B$ infer $\neg A$.
DS: From $A \vee B$ and $\neg A$ infer B.
S: From $A \wedge B$ infer A or infer B.
C: From A and B infer $A \wedge B$.
T: From $A \to B$ and $B \to C$ infer $A \to C$.

4.15 Which Rules are Necessary? We actually do not need such a long list of rules of inference. We will see later that we really only need modus ponens and tautology; however, having the longer list will allow us to accomplish much more with less work.

4.16 Applying Rules of Inference: We demonstrate how the rules of inference can be applied repeatedly to a list of premises to eventually arrive at a desired conclusion. The list we form will be in three columns. The first column will be statements. These will be numbered so that we can refer to them. The second column will be the rules of inference we applied to get those statements. The third column will be the numbers of the statements to which the rules were applied.
We begin with two premises.

1. $(P \vee Q) \to (R \wedge \neg S)$

2. $\neg R \vee S$

From these two premises we will build a chain of inferences concluding eventually with $\neg P$.
To begin with, premise (2) is logically equivalent via DeMorgan's Law to $\neg(R \wedge \neg S)$. Thus from the rule of inference **E**, we can infer $\neg(R \wedge \neg S)$. We now have a list of three statements:

	Statement	**Rule**	**Specifics**
1.	$(P \vee Q) \to (R \wedge \neg S)$	premise	
2.	$\neg R \vee S$	premise	
3.	$\neg(R \wedge \neg S)$	**E**	2

We can now apply **MT** to statements (1) and (3) on our list to infer $\neg(P \vee Q)$. This now gives us four statements:

	Statement	**Rule**	**Specifics**
1.	$(P \vee Q) \to (R \wedge \neg S)$	premise	
2.	$\neg R \vee S$	premise	
3.	$\neg(R \wedge \neg S)$	**E**	2
4.	$\neg(P \vee Q)$	**MT**	1, 3

Next, we can apply DeMorgan's Law to (4) to infer $\neg P \wedge \neg Q$ via **E**:

	Statement	**Rule**	**Specifics**
1.	$(P \vee Q) \rightarrow (R \wedge \neg S)$	premise	
2.	$\neg R \vee S$	premise	
3.	$\neg(R \wedge \neg S)$	**E**	2
4.	$\neg(P \vee Q)$	**MT**	1, 3
5.	$\neg P \wedge \neg Q$	**E**	4

Statement (5) is more than we are looking for. We only want half of the conjunction, so we apply simplification (**S**) to get the half we want.

	Statement	**Rule**	**Specifics**
1.	$(P \vee Q) \rightarrow (R \wedge \neg S)$	premise	
2.	$\neg R \vee S$	premise	
3.	$\neg(R \wedge \neg S)$	**E**	2
4.	$\neg(P \vee Q)$	**MT**	1, 3
5.	$\neg P \wedge \neg Q$	**E**	4
6.	$\neg P$	**S**	5

4.17 Exercises:
4.17.1 Apply **MT** to these premises:
$P \rightarrow (Q \wedge R)$
$\neg(Q \wedge R)$
4.17.2 Apply **S** and then **MP** to these two premises:
$P \wedge Q$
$P \rightarrow R$
4.17.3 Apply **MP** and then **DS** to these three premises:
$P \rightarrow (Q \vee R)$
P
$\neg R$
4.17.4 Apply **A** and then **MP** to these premises
$(P \vee R) \rightarrow (S \wedge T)$
P

4.18 Cautions: There are three mistakes (at least) which are commonly made when applying the rules of inference. We list them here as small arguments.

$$\frac{\begin{array}{l}P \rightarrow Q \\ Q\end{array}}{\therefore P} \qquad \frac{\begin{array}{l}P \rightarrow Q \\ \neg P\end{array}}{\therefore \neg Q} \qquad \frac{P}{\therefore P \wedge Q}$$

The first is an inappropriate application of modus ponens. Pay careful attention to the fact that to apply modus ponens, you need to know that the antecedent (what comes before the arrow) of your implication is true - not the consequent (what comes after the arrow). This error is called **affirming the consequent**. The next error is a fallacious application of modus tollens. In

order to apply modus tollens, you need to have the negation of the consequent of your implication. This error is called **denying the antecedent**. The third example is an error in applying addition. Addition works only with $\vee$, not with $\wedge$.

4.19 Formal Proofs: A **formal proof** of an argument is a list of statements so that every statement in the list is either a premise or follows from earlier statements by a rule of inference and so that the last statement in the list is the conlcusion of the argument. In section 4.16, what we constructed was a proof of the argument

$$\begin{array}{l} (P \vee Q) \rightarrow (R \wedge \neg S) \\ \neg R \vee S \\ \hline \therefore \neg P \end{array}$$

(Actually, what we constructed was the formal proof along with reasons for each statement, but this is what we will be calling a proof.)

4.20 Completeness and Soundness It is a theorem (a provable fact) that an argument is valid if and only if it has a formal proof. That every argument which has a proof is valid is called **Soundness**. Our deductive system is sound in that it draws only valid conclusions. That every valid argument has a proof is called **Completeness**. Our deductive system is complete in that it is strong enough to establish every valid implication.

4.21 Examples of Proofs: Here are a few exmaples of how to write proofs. To begin with, we write a proof for this argument:

$$\begin{array}{l} P \wedge Q \\ P \rightarrow R \\ \hline \therefore R \end{array}$$

First, we write down our premises:

	Statement	**Rule**	**Specifics**
1.	$P \wedge Q$	premise	
2.	$P \rightarrow R$	premise	

Now, how can we get R? We have $P \rightarrow R$, so if we had P, we could apply **MP** to get R. We can get P from statement (1) by simplification (**S**). Thus we first add P to our list of statements using simplification:

	Statement	**Rule**	**Specifics**
1.	$P \wedge Q$	premise	
2.	$P \rightarrow R$	premise	
3.	P	**S**	1

We can then add R by applying **MP** to statements (2) and (3):

	Statement	**Rule**	**Specifics**
1.	$P \wedge Q$	premise	
2.	$P \rightarrow R$	premise	
3.	P	**S**	1
4.	R	**MP**	2, 3

This completes our proof. Notice how we arrived at this proof. We looked at the conclusion and decided what we might need in order to infer the conclusion. We then looked at the premises and tried to build what we needed from these using rules of inferences. We worked from both ends to arrive at a proof. This process is typical of how proofs are written.
Next, we prove this argument:

$$\begin{array}{l} P \rightarrow (Q \vee R) \\ P \\ \neg R \\ \hline \therefore Q \end{array}$$

We again begin by listing our premises:

	Statement	**Rule**	**Specifics**
1.	$P \rightarrow (Q \vee R)$	premise	
2.	P	premise	
3.	$\neg R$	premise	

We want to end up at Q. The only Q is in statement (1) after the arrow. **MP** is the only rule of inference which gives us statements which appear after an arrow. The first two statements are set up for modus ponens, so we try it.

	Statement	**Rule**	**Specifics**
1.	$P \rightarrow (Q \vee R)$	premise	
2.	P	premise	
3.	$\neg R$	premise	
4.	$Q \vee R$	**MP**	1, 2

Remember that we are looking for Q. This new statement says that either Q is true or R is true. If we can exclude R, then we will be there by **DS**. Statement (3) does the trick. So:

	Statement	**Rule**	**Specifics**
1.	$P \rightarrow (Q \vee R)$	premise	
2.	P	premise	
3.	$\neg R$	premise	
4.	$Q \vee R$	**MP**	1, 2
5.	Q	**DS**	4, 3

Do not let the fact that (4) and (3) do not come in the right order for **DS** bother you. Knowing (3) and (4) is the same as knowing (4) and (3).
Here is the next argument we would like to prove:

$$\begin{array}{l}(P\vee R)\rightarrow(S\wedge T)\\ P\\ \hline \therefore T\end{array}$$

We need T. The only T is in the second half of the implication in the first premise. Thus if we can make the first half of the implication $(P\vee R)$ true we can get to the second half by **MP**. We could then apply simplification to get to T. We know that P is true from the second premise. This is enough to get $P\vee Q$ by **A**. Thus we arrive at this proof:

	Statement	**Rule**	**Specifics**
1.	$(P\vee R)\rightarrow(S\wedge T)$	premise	
2.	P	premise	
3.	$P\vee R$	**A**	2
4.	$S\wedge T$	**MP**	1, 3
5.	T	**S**	4

Again notice how we worked from both ends of the proof.
Here is yet another example. We prove

$$\begin{array}{l}P\rightarrow(Q\wedge R)\\ \neg Q\\ \hline \therefore\neg P\end{array}$$

We want $\neg P$. P shows up as the first half of an implication in the first premise. Thus we might try to use **MT**. In order to do this, we need $\neg(Q\wedge R)$. We can get this by beginning with the premise $\neg Q$, adding $\neg R$ to get $\neg Q\vee\neg R$ and then applying DeMorgan's Law. Hence we have:

	Statement	**Rule**	**Specifics**
1.	$P\rightarrow(Q\wedge R)$	premise	
2.	$\neg Q$	premise	
3.	$\neg Q\vee\neg R$	**A**	2
4.	$\neg(Q\wedge R)$	**E**	3
5.	$\neg P$	**MT**	1, 4

And another example:

$$\begin{array}{l}P\rightarrow Q\\ P\rightarrow R\\ P\\ \hline \therefore Q\wedge R\end{array}$$

It should be clear that we can get Q and R individually from **MP**. To get $Q \wedge R$, we simply need to use **C**:

	Statement	**Rule**	**Specifics**
1.	$P \rightarrow Q$	premise	
2.	$P \rightarrow R$	premise	
3.	P	premise	
4.	Q	**MP**	$1, 3$
5.	R	**MP**	$2, 4$
6.	$Q \wedge R$	**C**	$4, 5$

We prove one final statement that emphasizes the importance of beginning with premises that are true. From this we learn that if we assume a contradiction is true, anything can happen. The argument is

$$\frac{P \wedge \neg P}{\therefore Q}$$

This will make more sense if we show the proof and then discuss where it came from:

	Statement	**Rule**	**Specifics**
1.	$P \wedge \neg P$	premise	
2.	P	**S**	1
3.	$\neg P$	**S**	1
4.	$P \vee Q$	**A**	2
5.	Q	**DS**	$4, 3$

Knowing both P and $\neg P$ sets up up for using **DS** on any disjunction involving P. Thus all we need to do is create a disjunction involving P and Q. This is easily done with **A**. Premises such as the ones in this argument which either contain or can be used to prove a contradiction are called **inconsistent**. Premises which cannot prove a contradiction are called **consistent**.

4.22 Exercises: Prove the following valid arguments:

1. $(\neg P \vee R) \rightarrow \neg Q$, Q / $\therefore P \wedge \neg R$

3. $P \rightarrow (R \wedge S)$, $\neg R$ / $\therefore \neg P$

2. $\neg P \rightarrow (Q \vee R)$, $\neg P \wedge S$, $\neg R$ / $\therefore Q$

4. $P \rightarrow Q$, $\neg(Q \vee R)$ / $\therefore \neg P$

5. $P \to (Q \wedge R)$, $R \to S$, P / $\therefore S$

6. $(P \vee R) \to Q$, $S \to P$, S / $\therefore Q$

7. $(P \vee Q) \to R$, $\neg R$, $T \to Q$ / $\therefore \neg T$

8. $(P \vee \neg Q) \to R$, $S \to (T \wedge U)$, $S \wedge P$ / $\therefore R \wedge U$

9. $(P \wedge \neg Q) \to R$, $S \to P$, $Q \to \neg U$, $U \wedge S$ / $\therefore R$

10. $(P \to Q) \to R$, $\neg(Q \vee R)$ / $\therefore P$

11. $(P \to Q) \to (P \to R)$, $Q \wedge P$ / $\therefore R$

12. $P \to (Q \to R)$, Q / $\therefore P \to R$

13. $A \to B$, $C \to D$, $A \vee C$ / $\therefore B \vee D$

4.23 Invalid Arguments: An argument

$$\begin{array}{l} P_1 \\ P_2 \\ \vdots \\ \underline{P_n} \\ \therefore C \end{array}$$

is invalid if $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \to C$ is not a tautology. This means that there is an assignment of truth values to the atomic statements involved so that each of $P_1, P_2, \ldots,$ and P_n is true, but C is false. To demonstrate that an argument is not valid, you must find such truth values. For example, we said earlier that the argument

$$\begin{array}{l} P \to Q \\ \underline{Q} \\ \therefore P \end{array}$$

is invalid. This can be demonstrated by noting that if P is false and if Q is true, then both premises are true, but the conclusion is false.

4.24 Exercises: Show each of these arguments is invalid.

(a)
$$\begin{array}{l} P\to Q \\ \neg P \\ \hline \therefore \neg Q \end{array}$$

(b)
$$\begin{array}{l} P\to Q \\ P\to R \\ \hline \therefore Q\to R \end{array}$$

(c)
$$\begin{array}{l} (P\wedge Q)\to R \\ P \\ \hline \therefore R \end{array}$$

(d)
$$\begin{array}{l} (P\wedge Q)\to R \\ \neg R \\ \hline \therefore \neg P \end{array}$$

4.25 Exercises: Decide if the following arguments are valid or invalid. If valid, provide a proof. If not, give an assignment of truth values which shows this.

(a)
$$\begin{array}{l} P\to(Q\vee R) \\ \neg Q \\ \hline \therefore \neg P \end{array}$$

(b)
$$\begin{array}{l} P\to(Q\wedge R) \\ \neg Q \\ \hline \therefore \neg P \end{array}$$

(c)
$$\begin{array}{l} P\to R \\ \neg Q\to\neg R \\ \hline \therefore P\to Q \end{array}$$

(d)
$$\begin{array}{l} \neg(P\wedge Q) \\ P \\ \hline \therefore Q \end{array}$$

4.26 Deriving Rules of Inference from MP and TAUT Every rule of inference we are using can be derived from **MP** and **TAUT**. For example, here is a derivation of **MT**.

$$\begin{array}{l} P \to Q \\ \neg Q \\ \hline \therefore P \end{array}$$

	Statement	**Rule**	**Specifics**
1.	$P \to Q$	Premise	
2.	$\neg Q$	Premise	
3.	$(P \to Q) \to (\neg Q \to \neg P)$	**TAUT**	
4.	$\neg Q \to \neg P$	**MP**	$1, 3$
5.	$\neg P$	**MP**	$4, 2$

Here is a derivation of **C**.

$$\begin{array}{l} P \\ Q \\ \hline \therefore P \wedge Q \end{array}$$

	Statement	**Rule**	**Specifics**
1.	P	Premise	
2.	Q	Premise	
3.	$P \to (Q \to (P \wedge Q))$	**TAUT**	
4.	$Q \to (P \wedge Q)$	**MP**	$3, 1$
5.	$P \wedge Q$	**MP**	$2, 4$

4.27 Exercise: Use **MP** and **TAUT** to prove the other rules of implication which we have been employing.

5

Temporary Assumptions

Consider the argument

$$\begin{array}{l} A_1 \\ A_2 \\ \vdots \\ A_n \\ \hline \therefore P \to Q \end{array}$$

Let $A = A_1 \wedge A_2 \wedge \cdots \wedge A_n$. Then this argument is valid if and only if $A \to (P \to Q)$ is a tautology. The statement $A \to (P \to Q)$ is logically equivalent to $(A \wedge P) \to Q$. But $(A \wedge P) \to Q$ is a tautology if and only if the argument

$$\begin{array}{l} A_1 \\ A_2 \\ \vdots \\ A_n \\ P \\ \hline \therefore Q \end{array}$$

is valid. Thus, we have one of the most fundamental theorems about valid deductions:

Deduction Theorem:
This argument is valid: if and only if this argument is valid:

$$\left(\begin{array}{l} A_1 \\ A_2 \\ \vdots \\ A_n \\ \hline \therefore P \to Q \end{array} \right) \qquad \left(\begin{array}{l} A_1 \\ A_2 \\ \vdots \\ A_n \\ P \\ \hline \therefore Q \end{array} \right)$$

The Deduction Theorem can be exploited to give more power to our proof techniques with rules of inferences.

5.1 Direct Proof To prove an implication $\alpha \to \beta$, we can *assume* α and use this to establish β. By the Deduction Theorem, this is good enough to demonstrate that $\alpha \to \beta$ could have been proven with the usual rules of inference. In this strategy, α is called a **temporary assumption**. When we introduce a temporary assumption in this way, we will lead every line in our

proof with a vertical line to indicate a temporary assumption is "in play." We call this method of proof **Direct Proof**

Direct Proof: To prove $\alpha \to \beta$, assume α and use this to establish β. Conclude $\alpha \to \beta$.

5.2 Example Write a proof of this valid argument:

$$\begin{array}{l} P \to Q \\ P \to R \\ \hline \therefore P \to (Q \wedge R) \end{array}$$

Solution:

1.	$P \to Q$	Premise
2.	$P \to R$	Premise
3.	$\vert\ P$	Temp. Assumption
4.	$\vert\ Q$	Modus Ponens 1,3
5.	$\vert\ R$	Modus Ponens 2,3
6.	$\vert\ Q \wedge R$	Conjunction 4,5
7.	$P \to (Q \wedge R)$	Direct Proof 3-6

5.3 Example We can even nest temporary assumptions: Write a proof of this valid argument:

$$\begin{array}{l} P \to Q \\ (Q \wedge R) \to S \\ \hline \therefore P \to (R \to S) \end{array}$$

Solution:

1.	$P \to Q$	Premise
2.	$(Q \wedge R) \to S$	Premise
3.	$\vert\ P$	Temp. Assumption
4.	$\vert\ Q$	Modus Ponens 1,3
5.	$\vert\ \vert\ R$	Temp. Assumption
6.	$\vert\ \vert\ Q \wedge R$	Conjunction 4,5
7.	$\vert\ \vert\ S$	Modus Ponens 2,6
8.	$\vert\ R \to S$	Direct Proof 5-7
9.	$P \to (R \to S)$	Direct Proof 3-8

5.4 Proving a Disjunction Suppose that we want to prove a disjunction $P \vee Q$. Note that by disjunctive implication, $P \vee Q \equiv \neg P \to Q$. We can prove $\neg P \to Q$ by Direct Proof. Thus, a strategy to prove $P \vee Q$ is

Disjunction Proof: To prove $\alpha \vee \beta$, assume $\neg\alpha$. Use this to establish β. Conclude $\alpha \vee \beta$.

5.5 Example Write a proof of this valid argument:

$$\begin{array}{l} A \to B \\ C \to D \\ A \vee C \\ \hline \therefore B \vee D \end{array}$$

Solution:

1.	$A \to B$	Premise
2.	$C \to D$	Premise
3.	$A \vee C$	Premise
4.	$\neg B$	Temp. Assumption
5.	$\neg A$	Modus Tollens 1,4
6.	C	Disjunctive Syllogism 3,5
7.	D	Modus Ponens 2,6
8.	$B \vee D$	Disjunction Proof 4-8

5.6 Cases Suppose we want to prove a statement of the form $(P \vee Q) \to R$. From the equivalence $(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$, we see that it is good enough to prove that $P \to R$ and $Q \to R$. This is known as proof by cases.

Proof by Cases: To prove $(\alpha \vee \beta) \to \gamma$, Prove $\alpha \to \gamma$ and $\beta \to \gamma$. Conclude $(\alpha \vee \beta) \to \gamma$.

5.7 Example Write a proof for this valid argument:

$$\begin{array}{l} \neg R \to \neg(P \vee S) \\ Q \to (R \wedge T) \\ \hline \therefore (P \vee Q) \to R \end{array}$$

Solution:

1.	$\neg R \to \neg(P \vee S)$	Premise
2.	$Q \to (R \wedge T)$	Premise
3.	$\quad P$	Temp. Assumption
4.	$\quad P \vee S$	Addition 3
5.	$\quad R$	Modus Tollens 1, 4
6.	$P \to R$	Direct Proof 3-5
7.	$\quad Q$	Temp. Assumption
8.	$\quad R \wedge T$	Modus Ponens 2,7
9.	$\quad R$	Simplification 8
10.	$Q \to R$	Direct Proof 7-9
11.	$(P \vee Q) \to R$	Cases 6,10

5.8 Contrapositive When we are trying to prove an implication $P \to Q$, it is sometimes easier to prove the contrapositive $\neg Q \to \neg P$. For example, proving "If n^2 is even, then n is even" is difficult; however, it is easy to prove "If n is not even, then n^2 is not even." Note that we can use direct proof to establish the contrapositive.

5.9 Example Write a proof for this valid argument

$$\frac{\neg R \to \neg(P \vee S)}{\therefore P \to R}$$

Solution:

1.	$\neg R \to \neg(P \vee S)$	Premise
2.	$\quad \neg R$	Temp. Assumption
3.	$\quad \neg(P \vee S)$	Premise
4.	$\quad \neg P \wedge \neg S$	Equivalent 3
5.	$\quad \neg P$	Simplification 4
6.	$\neg R \to \neg P$	Direct Proof 2-5
7.	$P \to R$	Equivalent (Contrapositive) 6

5.10 Contradiction Suppose that we are trying to prove a statement α. Suppose further that by assuming $\neg\alpha$ we can prove a contradiction β (a statement which is false for every truth assignment). Since we have proven $\neg\alpha \to \beta$, we know the contrapositive $\neg\beta \to \alpha$ must also hold. Since $\neg\beta$ is a tautology, then it follows that α must hold. This is known as *indirect proof, reductio ad absurdum*, or *proof by contradiction.*

Proof by Contradiction: To prove α by contradiction, assume $\neg\alpha$. Use this to establish a contradiction such as $\beta \wedge \neg\beta$. Conclude α.

5.11 Example Write a proof of this valid argument:

$$\begin{array}{l} A \to B \\ C \to D \\ A \vee C \\ \hline \therefore B \vee D \end{array}$$

Solution:

1.	$A \to B$	Premise
2.	$C \to D$	Premise
3.	$A \vee C$	Premise
4.	$\neg(B \vee D)$	Temp. Assumption (BWOC)
5.	$\neg B \wedge \neg D$	Equivalent 4
6.	$\neg B$	Simplification 5
7.	$\neg D$	Simplification 5
8.	$\neg A$	Modus Tollens 1,6
9.	$\neg C$	Modus Tollens 2,7
10.	$\neg A \wedge \neg C$	Conjunction 8,9
11.	$\neg(A \vee C)$	Equivalent 10
12.	$(A \vee C) \wedge \neg(A \vee C)$	Conjunction 3,11
13.	$(B \vee D)$	Contradiction 4-12

5.12 Exercises: Write proofs for each of these valid arguments

5.12.1
$$\begin{array}{l} P \to \neg Q \\ Q \vee R \\ R \vee S \to T \\ \hline \therefore \to T \end{array}$$

5.12.2
$$\begin{array}{l} P \to S \\ Q \to T \\ (S \wedge T) \to R \\ \hline \therefore (P \wedge Q) \to R \end{array}$$

5.12.3
$$\begin{array}{l} P \\ Q \to R \\ \hline \therefore (P \to Q) \to R \end{array}$$

5.12.4
$$\begin{array}{l} P \to R \\ \neg S \to P \\ \hline \therefore R \vee S \end{array}$$

5.12.5
$$\begin{array}{l} P \to R \\ \neg T \to Q \\ (R \wedge T) \to (S \wedge U) \\ \hline \therefore (P \to Q) \vee S \end{array}$$

5.12.6
$$\begin{array}{l} A \\ (B \wedge C) \to D \\ \hline \therefore (A \wedge \neg B) \vee (C \to D) \end{array}$$

5.12.7
$$\begin{array}{l} P \vee S \\ Q \vee U \\ (S \wedge U) \to R \\ \hline \therefore P \vee Q \vee R \end{array}$$

5.12.8
$$\begin{array}{l} \neg P \vee R \\ (Q \vee S) \to R \\ \hline \therefore (P \vee Q) \to R \end{array}$$

5.12.9

$$\begin{array}{l} \neg A \vee C \\ (A \vee E) \rightarrow F \\ F \rightarrow D \\ B \rightarrow F \\ \neg B \vee A \\ \hline \therefore (A \vee B) \rightarrow (C \wedge D) \end{array}$$

5.12.10

$$\begin{array}{l} \neg D \rightarrow \neg C \\ S \rightarrow T \\ (B \vee \neg S) \rightarrow D \\ \neg T \\ (A \wedge \neg S) \rightarrow D \\ \hline \therefore (A \vee B \vee C) \rightarrow D \end{array}$$

6

Quantifiers

The propositional logic we have developed is powerful – it gives a reasonable picture of a large segment of natural reasoning and a model of many of the types of reasoning involved in doing mathematics. It has a natural deductive calculus which is complete in the sense that all logical implications can be proven from Modus Ponens and sound in the sense that proofs only establish sentences which are logical consequences of the assumptions.

However, propositional logic has a glaring weakness in that the notion of "statement" or "sentence" is a bit too vague. *Real* reasoning requires us to say a bit about what makes up a sentence, what a sentence can "say," and how sentences can be related beyond constructions with logical connectives.

This argument

Bob is a man. All men are mortal. Therefore, Bob is mortal.

Makes perfect sense, but the best propositional logic could do with this is to identify three seemingly unrelated atomic sentences. To propositional logic, this argument looks like

$$\frac{\begin{array}{c}A\\B\end{array}}{\therefore C}$$

which is *invalid*. The problem is that the idea of basic sentence symbols is a bit too coarse for many forms of actual reasoning. Sentences (such as the ones here) can be related by what they say as well as how they are put together with connectives. In this chapter, we introduce the ideas of predicates and quantifiers to address this problem.

6.1 Predicates We begin with the first sentence in the argument above, "Bob is a man." The sentences "Larry is a man," "Lola is a man," and "Glenda is a man" are all related to this sentence. They are all of the form "x is a man." Each has a different name (or person) substituted for the letter x. The sentence "x is a man" is an example of a predicate. A **predicate** or **open statement** is a sentence involving variables which takes on a truth value once specific objects are substituted for the variables.

We will use capital letters such as A, B, $C, \ldots$ to represent predicates. If a predicate has a variable x, and if we want to name the predicate P, we will usually refer to the predicate as $P(x)$ (read "P of x"). The same predicate with "Bob" substituted for x would be $P(\text{Bob})$. For example, if $P(x)$ is "x is a man" then $P(\text{Bob})$ would be "Bob is a man." $P(\text{Glenda})$ is "Glenda is a man."

Predicates can have more than one variable. If $Q(x, y)$ is "x is married to y," then $Q(\text{Bob}, \text{Glenda})$ is "Bob is married to Glenda." $Q(1, 2)$ is "1 is married to 2" (which makes no sense). Suppose that $B(x, y, z)$ is "y is between x and z." Then $B(1, 2, 3)$ is "2 is between 1 and 3." $B(\text{Bob}, \text{Frank}, \text{Hank})$ is "Frank is between Bob and Hank."

The number of variables in a quantifier will be called the **rank** of the predicate. Here, P has rank 1, Q has rank 2, and B has rank 3. We can also say that Q is a 2-place predicate or that B is a 3-place predicate.

6.2 Statements vs. Open Statements: It is important to remember that an open statement **is not** a statement. It has no truth value until substitutions are made for its variables.

6.3 Quantifiers Now that we are aware of predicates, we move on to the second sentence in the argument from above: "All men are mortal." There is clearly the predicate "x is mortal" at play here. The difference between this and the first sentence is that here we try to substitute all men for x at the same time. We can rewrite this sentence in this way to account for all men:

> For all x, if x is a man, then x is mortal.

Here there are two predicates which have been combined: "x is a man" and "x is mortal." We also have an implication in the form of "if...then..." What is new is the "For all x." This is a quantifier. We will have two quantifiers, one to mean "For all" and one to mean "For some."

The **universal quantifier** is the symbol $\forall$. The expression $\forall x$ can be read as "For all x." If $P(x)$ is any predicate, then $\forall x P(x)$ can be read "For all x, $P(x)$."

The **existential quantifier** is the symbol $\exists$. The expression $\exists x$ can be read as "For some x." If $P(x)$ is any predicate, then $\exists x P(x)$ can be read "For some x, $P(x)$." (Note: Here "some" means "at least one.")

Let us return now to "All men are mortal." We have translated this into

> For all x, if x is a man, then x is mortal.

Let $P(x)$ be "x is a man," and let $Q(x)$ be "x is mortal." We can express this symbolically as $\forall x(P(x) \to Q(x))$. The argument from the introduction to the chapter can now be expressed symbolically as

$$\begin{array}{l} P(\text{Bob}) \\ \forall x(P(x) \to Q(x)) \\ \hline \therefore Q(\text{Bob}) \end{array}.$$

6.4 Quantifiers and English As with our logical connectives, there are a variety of ways to translate quantifiers into English. Some translations of $\forall x P(x)$ are

For all x, $P(x)$.
For any x, $P(x)$.
$P(x)$, for all x.

Some translations of $\exists x P(x)$ are

For some x, $P(x)$.
For at least one x, $P(x)$.
There exists an x so that $P(x)$.
There is an x so that $P(x)$.
There is at least one x so that $P(x)$.
$P(x)$ for some x.
$P(x)$ for at least one x.

6.5 Sets: We need some very basic ideas about sets before we continue (we will spend much more time with sets in Chapter 8). Even though most of mathematics is built upon the theory of **sets**, a set is something which mathematicians never define. Any definition of a set would require the use of a word such as "collection." Of course, we would then need to define "collection." This might include a word like "gathering" or "group." These words would then need to be defined. Since we only have a finite number of synonyms for any word, we would eventually circle around again to the word "set." To avoid this, we simply do not define the word and hope everyone has some intuitive idea what a set is. The things which compose a set are called the **elements** of the set. To denote that something called x is an element of a set named S, we would use the notation $x \in S$. This can be read as "x is in S," or "x is an element of S," or simply "x in S." We will denote the set of real numbers as $\mathbb{R}$ and the set of integers as $\mathbb{Z}$.

6.6 Quantifiers with Sets: We will often use special notation to indicate that we are quantifying over the elements of a particular set.

The Universal Quantifier: The symbols $\forall x \in S$ will be used to mean "For all x in $S \ldots$" For example, if $P(x)$ is the open statement $x^2 \geq 0$ we can write "For all x in the real numbers, $x^2 > 0$" as $(\forall x \in \mathbb{R})P(x)$. The statement

$(\forall x \in S)P(x)$ is true if this statement is true, "If $s \in S$, then $P(s)$."

The Existential Quantifier: The symbols $\exists x \in S$ will mean "There is an x in S so that..." For example, if $P(x)$ is the statement $x^2 = x$, we can write "There is an x in the real numbers so that $x^2 = x$" as $(\exists x \in \mathbb{R})P(x)$. The statement $(\exists x \in S)P(x)$ is true if $P(s)$ is true for some $s \in S$.

6.7 Some translations of $\exists$ If $P(x)$ is the statement "x received an A," and if S is the set of people in class, then each of these statements communicates $(\exists x \in S)P(x)$.
"Someone in class received an A."
"There is a person in class who received an A."
"There exists a student in class who received an A."
Possession can also indicate the presence of an existential quantifier. For example, the statement "2 has a square root in the real numbers." Can be written as $(\exists x \in \mathbb{R})(x^2 = 2)$.

6.8 Notation: If the set is known, we can abbreviate $\exists x \in S$ and $\forall x \in S$ simply as $\exists x$ and $\forall x$. Sometimes, we will need to use more than one quantifier. For example, the statement "For all real numbers x, y, and z, if $x \leq y$ and $y \leq z$ then $x \leq z$" really begins with three quantifiers $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})\ldots$ We can abbreviate this as $(\forall x, y, z \in \mathbb{R})\ldots$ If necessary, we can place what comes after a quantifier in parenthesis to signify that it all follows that quantifier. For example, we may encounter statements such as $(\forall x \in S)(P(x) \wedge Q(x))$. Some mathematicians play it safe and always put what comes after the quantifier in parenthesis. Because we may run into many parenthesis in one statement, we will often use brackets instead of parenthesis to differentiate between sets of parenthesis.

6.9 Exercises: Find the truth value of each of these statements.
6.9.1 $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(y^2 = x)$
6.9.2 $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(y^2 = x)$
6.9.3 $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(y^2 = x)$
6.9.4 $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(x \leq y)$
6.9.5 $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x \leq y)$
6.9.6 $(\forall x \in \mathbb{R})([\neg(x = 7)] \rightarrow [(\exists \epsilon \in \mathbb{R})((\epsilon > 0) \wedge (|x - 7| > \epsilon))])$

6.10 Translating: Let S be the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. We show here how statements involving quantifiers can be translated into symbols. We begin with the statement "There is a number in S which is less than or equal to every number in S." The statement begins with "There is..." This is an existential quantifier, so we will have an $(\exists x \in S)$ in our translation. The rest of the statement says x is less than or equal to every number in S. The "every" is a universal quantifier, so we must have a $(\forall y \in S)$ also. We have no other quantifiers. Our statement should begin $(\exists x \in S)(\forall y \in S)$. The statement communicates that x is less than or equal to y. Thus the whole statement should be $(\exists x \in S)(\forall y \in S)(x \leq y)$.

Next, we look at "Not every element of S has a square in S." The "every element" is a $(\forall x \in S)$. The "has" symbolizes an existence, so we will need an $(\exists y \in S)$. Thus, we have so far $(\forall x \in S)(\exists y \in S)$. Next, the statement says that y (the thing that x "has") is the square of x, so we get $(\forall x \in S)(\exists y \in S)(x^2 = y)$. Finally, there is a "not" preceding everything, so we negate this statement to get $\neg((\forall x \in S)(\exists y \in S)(x^2 = y))$.

Let $P(x)$ be the open statement "x is prime." We will translate the statement "Any number in S larger than 7 is not prime." To begin, we translate "any number in S" as $(\forall x \in S)$. The statement communicates that if $x > 7$, then x is not prime. We can write this using $P(x)$: $(\forall x \in S)((x > 7) \rightarrow \neg P(x))$.

6.11 Exercises: Let S be the set of numbers $\{2, 3, 4, 6, 8\}$. Let $P(x)$ be "x is prime," and let $T(x)$ be "x is a multiple of 2." Translate each of the following statements into symbols.

6.11.1 There is a number in S which is both prime and a multiple of two.

6.11.2 Every number in S is either prime or is a multiple of two.

6.11.3 There is a number in S which is greater than or equal to every number in S.

6.11.4 There is a number in S which is prime but is not a multiple of two.

6.11.5 There is a prime number in S which is less than or equal to every number in S.

6.11.6 There is a prime number x in S so that for any number y in S, if y is prime, then $y \leq x$.

6.11.7 There is a number x in S so that for all numbers y in S, if y is not prime, then there is a z in S with $z = y/x$.

6.12 Exercises Introduce predicate symbols and translate each of these English sentences into symbolic sentences using quantifiers.

6.12.1 All dogs have fleas.

6.12.2 Some dogs have fleas.

6.12.3 Not every dog has fleas.

6.12.4 Some dogs do not have fleas.

6.12.5 No dog has fleas.

6.12.6 Every dog chases some cat.

6.12.7 Every dog chases every cat.

6.12.8 Some dog chases every cat.

6.12.9 Some dog does not chase any cat.

6.12.10 No dog chases every cat.

6.13 Equivalences: The logical equivalences we learned earlier still apply to statements involving quantifiers. There are, actually, more equivalences which apply. These equivalences can be used to show that any statement involving quantifiers is equivalent to one in a special form in which

all of the quantifiers come at the beginning of the statement. Such a statement is said to be in **prenex normal form**. For example, the statement $(\forall x \in S)(\exists y \in S)(Q(x,y) \rightarrow ((\exists z \in S)P(x,y,z)))$ is not in prenex normal form, but the statement $(\forall x \in S)(\exists y \in S)(\forall z \in S)(R(x,y) \vee T(x,y,z))$ is in prenex normal form.

For our purposes, it will be adequate to learn only two more equivalences which will allow us to negate statements involving $\forall$ or $\exists$. These two rules are

Universal Negation: ($\forall$**N**) $\neg(\forall x \in S)P(x) \equiv (\exists x \in S)\neg P(x)$.
If you are told, "It is not the case that everyone in class received an A," then you know immediately that someone did not get an A. This reasoning is $\forall$**N** at work.

Existential Negation: ($\exists$**N**) $\neg(\exists x \in S)P(x) \equiv (\forall x \in S)\neg P(x)$.
If you are told, "It is not the case that someone received an A," you are dissapointed because you know everyone scored below an A. Intuitively, you know $\exists$**N**.

6.14 Exercises Here are eight sets of "holes." Some are filled (the dark ones). Some are not filled.

A. ○ ○ ○	D. ○ ● ●	G. ● ● ○
B. ○ ○ ●	E. ● ○ ○	
C. ○ ● ○	F. ● ○ ●	H. ● ● ●

Let $F(x)$ be "x is filled." Translate the following statements into symbols and then decide which sets of holes satisfy the statement.

6.14.1 All holes are filled.
6.14.2 Some holes are filled.
6.14.3 A hole is filled.
6.14.4 There is a hole which is filled.
6.14.5 There is a hole which is not filled.
6.14.6 All holes are not filled.
6.14.7 Some holes are not filled.
6.14.8 A hole is not filled.
6.14.9 It is not the case that all holes are filled.
6.14.10 It is not the case that some holes are filled.
6.14.11 It is not the case that all holes are not filled.
6.14.12 It is not the case that some holes are not filled.
6.14.13 Not all holes are filled.
6.14.14 Not all holes are not filled.

6.15 Negation: In writing, proving, and applying theorems, it is often necessary to negate complex statements involving quantifiers. The technique for doing this is simple. Write the statement you are negating in symbols and add a $\neg$ to the front of it. Apply equivalences from Chapter 2 along with $\forall\mathbf{N}$ and $\exists\mathbf{N}$ as necessary to move the negation into the statement until it is attached to atomic statments. Applying $\forall\mathbf{N}$ and $\exists\mathbf{N}$ amounts to this: when you encounter a $\forall$, change it to an $\exists$ and negate what comes after. When you encounter an $\exists$, change it to a $\forall$ and negate what comes after.

First, we negate $(\forall x)(\exists y)(P(x)\rightarrow R(y))$. We add a $\neg$ to the front of the statement to get $\neg(\forall x)(\exists y)(P(x)\rightarrow R(y))$. To negate the $\forall$, we change it to an $\exists$. To negate the $\exists$, we change it to a $\forall$. This brings us to $(\exists x)(\forall y)\neg(P(x)\rightarrow R(y))$. To negate the implication, we note that $P(x)\rightarrow R(y) \equiv \neg P(x)\vee R(y)$. Thus

$$\begin{array}{rcl}(\exists x)(\forall y)\neg(P(x)\rightarrow R(y)) & \equiv & (\exists x)(\forall y)\neg(\neg P(x)\vee R(y)) \\ & \equiv & (\exists x)(\forall y)(P(x)\wedge\neg R(y))\end{array}$$

Next we negate this statement given in words (we use $\mathbb{R}^+$ to denote the positive real numbers):

For every $x \in \mathbb{R}$, if $|x-7| < \epsilon$ for every $\epsilon \in \mathbb{R}^+$, then $x = 7$.

First, we translate this into symbols. In doing so, we use brackets in place of some parenthesis to help organize.

$$(\forall x \in \mathbb{R})([(\forall \epsilon \in \mathbb{R}^+)(|x-7| < \epsilon)]\rightarrow[x = 7])$$

We then add the negation and start applying equivalences:

$$\neg(\forall x \in \mathbb{R})([(\forall \epsilon \in \mathbb{R}^+)(|x-7| < \epsilon)]\rightarrow[x = 7]) \equiv$$

$$\begin{array}{rl}\equiv & (\exists x \in \mathbb{R})\neg([(\forall \epsilon \in \mathbb{R}^+)(|x-7| < \epsilon)]\rightarrow[x = 7]) \\ \equiv & (\exists x \in \mathbb{R})\neg(\neg[(\forall \epsilon \in \mathbb{R}^+)(|x-7| < \epsilon)]\vee[x = 7]) \\ \equiv & (\exists x \in \mathbb{R})([(\forall \epsilon \in \mathbb{R}^+)(|x-7| < \epsilon)]\wedge\neg[x = 7])\end{array}$$

6.16 Exercises: Negate each of these statements.

6.16.1 $[(\forall x)P(x)]\vee[(\exists x)Q(x)]$

6.16.2 $(\forall x)(P(x)\rightarrow[(\forall y)Q(x,y)])$

6.16.3 $(\exists x)(\forall y)(P(x,y)\vee(\exists z)Q(x,y,z))$

6.16.4 For every $n \in \mathbb{Z}$, there is an $x \in \mathbb{R}$ so that $x^2 = n$.

6.16.5 (Denote the positive real numbers by $\mathbb{R}^+$.) For every $\epsilon \in \mathbb{R}^+$, there is a $\delta \in \mathbb{R}^+$ so that for all $x \in \mathbb{R}$, if $|x-4| < \delta$, then $|x^2-16| < \epsilon$.

6.17 Inference: We have four rules of inference which involve quantifiers. These rules fall into two categories. The two rules of **instantiation** allow us to pass from statements involving quantifiers to statements not involving quantifiers. The two rules of **generalization** allow us to pass from statements without quantifiers to statements with quantifiers. The two rules of

instantiation are:

Universal Instantiation: (abbreviated $\forall$**I**) If $s \in S$, then from $(\forall x \in S)P(x)$ infer $P(s)$.

Existential Instantiation: (abbreviated $\exists$**I**) If s is an unused symbol for an element of S, then from $(\exists x \in S)P(x)$ infer $P(s)$.

These may be baffling at first sight, but their meanings are intuitive. The first says that if $s \in S$ and we know that $P(x)$ is true for every element of S, then it ought to be true for s. The next rule can just be thought of as naming. If we know $P(x)$ is true for some element of S we are allowed to name that element with an unused symbol for something in S. In both of these rules, we begin with quantifiers and end without. The two rules of generalization are:

Universal Generalization: (abbreviated $\forall$**G**) If s is a symbol for an arbitrary member of S, then from $P(s)$ infer $(\forall x \in S)P(x)$.

Existential Generalization: (abbreviated $\exists$**G**) If $s \in S$, from $P(s)$ infer $(\exists x \in S)P(x)$.

The first of these emphasizes that to know a statement is true for all elements of S, it suffices to know it is true for an arbitrary member of S. You may have read proofs which used words such as "Let $x \in \mathbb{R}$ be arbitrary." Whatever was proved in these proofs about x is true for all $x \in \mathbb{R}$. The second rule tells us that if we have a specific example in S where $P(x)$ is true, then we may make the general statement that there exists some element of S where $P(x)$ is true. In both of these, we begin with statements about elements of S which do not involve quantifiers, and we end with general statements involving quantifiers.

6.18 Proofs with Quantifiers: As an example of how to apply the rules of inference with quantifiers, we give two proofs employing quantifiers. First we give a proof of this argument

$$\begin{array}{l} (\forall x \in S)(P(x) \rightarrow Q(x)) \\ (\forall x \in S)(P(x) \rightarrow R(x)) \\ (\exists x \in S)P(x) \\ \hline \therefore (\exists x \in S)(Q(x) \wedge R(x)) \end{array}$$

The strategy we follow here is this: We apply $\exists$**I** to any premises beginning with $\exists$. This gives us some specific elements to work with. Next, we apply $\forall$**I** using these specific elements and any premises beginning with $\forall$. This will give us more information about our specific elements. Then we can use the rules of inference not involving quantifiers to do most of our work. Finally,

we can apply $\exists$**G** to return to a statement with quantifiers.

	Statement	**Rule**	**Specifics**
1.	$(\forall x \in S)(P(x) \to Q(x))$	premise	
2.	$(\forall x \in S)(P(x) \to R(x))$	premise	
3.	$(\exists x \in S)P(x)$	premise	
4.	$P(s)$	$\exists$**I**	3
5.	$P(s) \to Q(s)$	$\forall$**I**	1
6.	$P(s) \to R(s)$	$\forall$**I**	2
7.	$Q(s)$	**MP**	5, 4
8.	$R(s)$	**MP**	6, 4
9.	$Q(s) \wedge R(s)$	**C**	7, 8
10.	$(\exists x \in S)(Q(x) \wedge R(x))$	$\exists$**G**	9

Next we approach this argument

$$\begin{array}{l} (\forall x \in S)(P(x) \to Q(x)) \\ (\forall x \in S)(P(x) \vee T(x)) \\ (\forall x \in S)\neg T(x) \\ \hline \therefore (\forall x \in S)Q(x) \end{array}$$

Our strategy is similar to the previous example with a few differences. First, our conclusion begins with $\forall$, so we will have to eventually use $\forall$**G**. This will require a symbol for an arbitrary member of S. Also, there are no premises involving $\exists$, so we will have to use $\forall$**I** to have specific elements of S to work with. Here is the proof

	Statement	**Rule**	**Specifics**
1.	$(\forall x \in S)(P(x) \to Q(x))$	premise	
2.	$(\forall x \in S)(P(x) \vee T(x))$	premise	
3.	$(\forall x \in S)\neg T(x)$	premise	
4.	$P(s) \to Q(s)$	$\forall$**I**	1
5.	$P(s) \vee T(s)$	$\forall$**I**	2
6.	$\neg T(s)$	$\forall$**I**	3
7.	$P(s)$	**DS**	5, 6
8.	$Q(s)$	**MP**	4, 7
9.	$(\forall x \in S)Q(x)$	$\forall$**G**	8

6.19 Exercises: Prove the following valid arguments.

1. $$\begin{array}{l} (\forall x \in S)(P(x) \to Q(x)) \\ (\exists x \in S)\neg(Q(x) \vee R(x)) \\ \hline \therefore (\exists x \in S)\neg P(x) \end{array}$$

2. $$\begin{array}{l} (\forall x \in S)(P(x) \to (Q(x) \wedge R(x))) \\ (\forall x \in S)(R(x) \to T(x)) \\ (\forall x \in S)P(x) \\ \hline \therefore (\forall x \in S)T(x) \end{array}$$

3. $\dfrac{\begin{array}{l}(\forall x \in S)(P(x) \rightarrow (Q(x) \wedge R(x))) \\ (\exists x \in S) \neg Q(x)\end{array}}{\therefore (\exists x \in S) \neg P(x)}$

4. $\dfrac{\begin{array}{l}(\forall x \in S)(P(x) \rightarrow (Q(x) \vee R(x))) \\ (\forall x \in S) \neg R(x) \\ (\exists x \in S) P(x)\end{array}}{\therefore (\exists x \in S) Q(x)}$

5. $\dfrac{(\exists x \in S)(P(x) \wedge \neg P(x))}{\therefore (\exists x \in S) Q(x)}$

6. $\dfrac{(\exists x \in S)(P(x) \wedge \neg P(x))}{\therefore (\forall y \in S) Q(y)}$

7

Basic Proof Techniques

7.1 The Axiomatic Method: Mathematics begins with words called **primitives**. These are words which are undefined, but which everyone is assumed to understand. For example, the idea of a set is a primitive. From primitives, mathematicians make formal **definitions**. These definitions are usually made to make common concepts rigorous enough to be useful. Mathematicians must usually assume some knowledge about the primitives and definitions with which they work. Statements which are assumed to be true without proof are called **axioms**, **postulates**, or **premises**. From the definitions and axioms, mathematicians make conjectures which they attempt to prove to be true. These facts which they prove take on titles such as theorems, propositions, lemmas, and corollaries. In mathematical writing, **theorem** or **proposition** is usually the generic title given to a proven fact. A **lemma** is generally a fact which is proven as a stepping stone to prove a theorem. A **corollary** is a fact which usually follows quickly from a previous lemma or theorem.

7.2 Proofs: Most mathematicians rarely write formal proofs like those we wrote in Chapter 4. Instead, they write arguments which are convincing to other mathematicians. The steps in these arguments are usually combinations of rules of inference and applications of facts known already to be true. From here on, when we say "proof," we will mean these convincing arguments.

7.3 Need for Proofs: There are three basic reasons that mathematicians write proofs.

1. **To be certain:** Sometimes, a concept which appears to be true on the surface actually is not. We are not always aware of this until we attempt to rigorously show it is true and discover the error.

2. **To know why:** At times, there are ideas whose truth we are aware of, but which we do not truly understand. The process of discovering a proof can lead us to a deeper understanding of why these are true.

3. **To communicate:** Mathematics relies on communication between mathematicians to develop. Ideas propogate most quickly when they are pondered by different minds with varying experiences and intuitions.

7.4 Proof Strategies The proof techniques in Chapter 5 provide several common basic proof strategies. We give examples of these strategies here in proofs using words rather than in formal proofs using rules of inference. The strategies given here are general and will be fundamental to the rest of the text.

7.5 Working Environment: For the proofs in this section, we will be working in the **natural numbers**. This is the set $\mathbb{N} = \{0, 1, 2, \ldots\}$[1]. The natural numbers have two operations, addition and multiplication which we assume satisfy the properties below. We will have an opportunity later to discuss how $\mathbb{N}$ can be defined from a small set of axioms from which these properties can be derived.

For all $x, y, z, w \in \mathbb{N}$, the following are true
Properties of Addition:

$x + (y + z) = (x + y) + z$	associative law
$x + y = y + x$	commutative law
$y + x = z + x$ if and only if $y = z$	cancellation law
$x + 0 = 0 + x = x$	additive identity
$x \cdot 0 = 0 \cdot x = 0$	absorption law

Properties of Multiplication:

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	associative law
$x \cdot y = y \cdot x$	commutative law
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	distributive law
$x \cdot 1 = 1 \cdot x = x$	multiplicative identity
if $x \neq 0$ then $y \cdot x = z \cdot x$ iff $y = z$	cancellation law

These are the "usual" properties of arithmetic which allow us to manipulate equations and expressions involving natural numbers.

7.6 Notation: To make notation simpler, we will usually use juxtaposition to symbolize multiplication. Also, we will use an order of operations which requires us to perform multiplication prior to addition. These are typical conditions with which we should be familiar.

[1]Historically, the definition of the natural numbers did not include 0. Many, perhaps most, modern mathematicians include 0 in $\mathbb{N}$. Doing so pains me greatly. Most societies took centuries to realize the need for 0 as a number, so this number does not seem remotely natural. However, including 0 here will make the lives of my students easier, and it provides for elegant parallels between arithmetic in $\mathbb{N}$ and set theory. So, after decades of resistance, I am finally conceding and allowing 0 to be a natural number.

7.7 No Subtraction or Division: It is very important at this point in time to remember that we cannot subtract or divide. Subtraction may result in negative numbers (which are not in $\mathbb{N}$), and division may result in fractions (which may not be in $\mathbb{N}$). Our replacement for subtraction and division are the cancellation rules.

7.8 Order: We will say that a natural number n is **less than or equal** to a natural number m if $n+k=m$ for some natural number k. This is denoted by $n \leq m$. We will say that n is **less than** m if $n \leq m$ but $n \neq m$. This is denoted by $n < m$.

If $n \leq m$, we may also say that m is **greater than or equal** to n and write $m \geq n$. Similarly, we can use $m > n$ to mean that m is **greater than** n.

7.9 Divisibility: We will say that a natural number n **divides** a natural number m if there is a natural number k so that $nk = m$. This relationship will be denoted by $n|m$. If $n|m$, then we may also say that m is a **multiple** of n or that n is a **factor** of m.

7.10 Note: Note the similarity between the definitions of less than and divides. The operations addition and multiplication have the associative law, commutative law, and cancellation law in common. They are quite similar. Thus it stands to reason that these two relations might share some common properties.

7.11 Direct Proof: Most theorems in mathematics are statements of the form $P \rightarrow Q$. P is called the **hypothesis** of the theorem, and Q is the **conclusion**. One method of proving theorems such as these is to assume that P is true and use this assumption to show that Q must be true.

Theorem: If l, m, and n are natural numbers so that $l|m$ and $m|n$, then $l|n$.

Discussion: It is a good idea to do scratch work before attempting a proof. We are going to assume that l, m, and n are natural numbers, that $l|m$, and that $m|n$. We need to show that $l|n$. The first step is to consider the definition of divides and see what we know and what we need. The definition of divides tells us that there are natural numbers a and b so that $la = m$ and $mb = n$. What we need is a natural number k so that $lk = n$. By substituting la for m in $mb = n$, we see that $lab = n$, so $k = ab$ is a logical choice.

Comments: When writing a proof, there are a lot of things to consider. First, the proof should be written in complete sentences with proper English grammar. Second, one of the main purposes of the proof is to communicate, so be sure to explain to the reader what is happening. Use transitions to indicate progress through the proof. Do not assume the reader knows what you are thinking. Make sure that you define all of the appropriate variables for the reader.

Proof: Suppose that l, m, and n are natural numbers so that $l|m$ and $m|n$. We will show that $l|n$. By the definition of divides, there are natural numbers a and b so that $la = m$ and $mb = n$. Let $k = ab$. It follows that $lk = lab = mb = n$. By the definition of divides, we see that $l|n$ □

In most mathematical writing, the end of a proof is usually marked by a symbol such as the empty box above. This allows the reader to easily see where proofs end.

7.12 Exercise: Mimic the proof above to prove
Theorem: If l, m, and n are natural numbers so that $l \leq m$ and $m \leq n$, then $l \leq n$.

7.13 Hidden Implications: Not all implications are stated as clearly as that in the previous example. For example:

Theorem: For any natural numbers l, m, and n, if $m|n$ then $ml|nl$.

This theorem could be restated as, "If l, m, and n are natural numbers so that $m|n$ then $ml|nl$." Sometimes, the implication in a theorem is completely hidden. For example:

Theorem: Every natural number is divisible by 1.

This theorem could be written, "If n is a natural number, then $1|n$. (This is trivially true since $1 \cdot n = n$ by definition.)

7.14 Exercises: Prove each of the following using direct proof:
7.14.1 **Theorem:** For any natural numbers l, m, and n, if $m|n$ then $ml|nl$.
7.14.2 **Theorem:** For any natural numbers l, m, and n, if $m \leq n$, then $m + l \leq n + l$.
7.14.3 **Theorem:** For any natural numbers l, m, and n, if $m \leq n$, then $ml \leq nl$.
7.14.4 **Theorem:** If a, b, c, and d are natural numbers, $a \leq b$, and $c \leq d$, then $a + c \leq b + d$.
7.14.5 **Theorem:** If a, b, c, and d are natural numbers, $a \leq b$, and $c \leq d$, then $ac \leq bd$.

7.15 Even and Odd Numbers: A natural number n is **even** if $2|n$. A natural number n is **odd**[2] if there is a natural number k with $n = 2k + 1$.

[2]This is one place where including 0 in $\mathbb{N}$ is convenient. If we did not include 0, we would have to define a natural number n to be odd if either $n = 1$ or there is a natural number k with $n = 2k + 1$. Including 0 simplifies almost all theorems and proofs which refer to odd natural numbers.

7.16 Odd-Even Dichotomy: We will employ the following theorem repeatedly in our examples. We will have the opportunity to prove this theorem later after we have discussed the Division Algorithm 12.9.

Theorem: Every natural number is either odd or even but not both.

7.17 Example: We use a direct proof to show
Theorem: The sum of two even natural numbers is even.

Observation: Again, this is not written as an implication. We can change the theorem to an implication by writing it as "If n and m are even natural numbers, then $n + m$ is also even."

Discussion: We will assume that n and m are even integers. We must look at what we know and what we need. We know that $2|n$ and $2|m$. This means that there are natural numbers a and b so that $2a = n$ and $2b = m$. We need to show that $2|(n + m)$, so we take a look at this sum. What we know tells us that $n + m = 2a + 2b$. The distributive law tells us that $n + m = 2(a + b)$. Since $(a + b)$ is a natural number, this means $2|(n + m)$. We are ready for a proof.

Proof: Let n and m be even natural numbers. We will show that $n + m$ is even. By the definition of even, $2|n$ and $2|m$. By the definition of divides, there are natural numbers a and b so that $2a = n$ and $2b = m$. Note now that $2(a+b) = n+m$. Hence $2|(n+m)$. By the definition of even, $n+m$ is even. □

Note: In this proof, we could have let $k = a+b$ so that the final equality looked more like the definition of divisibility ($2k = n + m$). This is not necessary, but it may have helped make a complicated proof more readable.

7.18 Exercises: Prove the following.
7.18.1 **Theorem:** If n and m are odd natural numbers, then $n+m$ is even.
7.18.2 **Theorem:** If n is an even natural number, then $n \cdot n$ is an even natural number. (Hint: write $n = 2k$ and square)
7.18.3 **Theorem:** Suppose that n and m are natural numbers. If n is even, then nm is even.

7.19 If-and-only-if: Many theorems contain the words "if and only if." It is common to abbreviate "if and only if" as "iff." Recall that the statement "P if and only if Q" (called a bi-implication) is the same as "If P then Q, and if Q then P." Thus in order to prove a bi-implication, we can simply prove the two implications.

Theorem: A natural number n is even if and only if $n + 1$ is odd.

Discussion: There are two things to prove here. First, if n is even, then $n+1$ is odd. Second, we need to prove that if $n+1$ is odd, then n is even.

Proof Suppose that n is a natural number. We will prove that n is even if and only if $n+1$ is odd. First suppose that n is even. Then there exists a natural number k so that $n = 2k$. Then $n+1 = 2k+1$. By the definition of odd, $n+1$ is odd. Hence, if n is even, then $n+1$ is odd.

Now suppose that $n+1$ is odd. By the definition of odd, there is a natural number k so that $n+1 = 2k+1$. Cancelation now gives $n = 2k$, so $2|n$. Thus n is even. Hence, if $n+1$ is odd, then n is even.

We have proven that a natural number n is even if and only if $n+1$ is odd. □

7.20 Exercises: Prove the following theorems (note the "iff").

7.20.1 **Theorem:** Let m, n, and l be natural numbers. Then $m \leq n$ if and only if $m+l \leq n+l$.

7.20.2 **Theorem:** Let m and n be natural numbers. Then $m < n$ if and only if there is a natural number $k \neq 0$ so that $m+k = n$.

7.20.3 **Theorem:** A natural number n is odd if and only if $n+1$ is even.

7.21 Proofs With Cases: Recall that the statement $(P \vee Q) \rightarrow R$ is equivalent to the statement $(P \rightarrow R) \wedge (Q \rightarrow R)$. Thus, to prove $(P \vee Q) \rightarrow R$, we could prove $P \rightarrow R$ and $Q \rightarrow R$. When we do so, we are using **cases**. Consider the following theorem

Theorem: If n is a natural number then $n^2 + 3n$ is even.

Discussion: There are two cases to consider here – either n is even or n is odd. In both cases, we will invoke the definition to express n either as $2k$ or as $2k+1$ for some k. We will then substitute and follow our noses.

Proof: Suppose that n is a natural number. We will prove that $n^2 + 3n$ is even. There are two cases – either n is even or n is odd. Suppose first that n is even. Then there is a natural number k so that $n = 2k$. It follows that

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

If we let $l = 2k^2 + 3k$, then $n^2 + 3n = 2l$ is even. Thus if n is even, then $n^2 + 3n$ is also even.

Next suppose that n is odd. Then there is a natural number k so that $n = 2k + 1$. It follows that

$$\begin{aligned} n^2 + 3n &= (2k+1)^2 + 3(2k+1) \\ &= 4k^2 + 4k + 1 + 6k + 3 \\ &= 4k^2 + 10k + 4 \\ &= 2(2k^2 + 5k + 2) \end{aligned}$$

If we let $m = 2k^2 + 5k + 2$, then $n^2 + 3n = 2m$ is even. Thus if n is odd then $n^2 + 3n$ is even.

We have proven that if n is either even or odd, then $n^2 + 3n$ is even. Since every natural number is either even or odd, $n^2 + 3n$ is even for all natural numbers n. □

7.22 Exercises: Define the following notions for a natural number n:

- n is **red** if there is a natural number k with $n = 3k$.
- n is **white** if there is a natural number k with $n = 3k + 1$.
- n is **blue** if there is a natural number k with $n = 3k + 2$.

Assume the following theorem. We will be able to prove this theorem after we discuss the Division Algorithm 12.9.

Theorem: Any natural number is exactly one of red, white, or blue.

Prove the following theorems.

7.22.1 **Theorem:** The square of any natural number is either red or white.

7.22.2 **Theorem:** If n is any natural number, then $n^2 + n$ is even.

7.23 Contrapositive: We know that a statement of the form $P \rightarrow Q$ is equivalent to its contrapositive $\neg Q \rightarrow \neg P$. Often it is easier to prove the contrapositive of a theorem rather than directly proving the theorem.

Theorem: Let n be a natural number. If n^2 is even, then n is even.

Discussion: If we were to assume that n^2 is even, this would give us very little information about n. However, if we use the contrapositive, the theorem is quite easy to prove.

Proof: Let n be a natural number. We will use the contrapositive to prove that if n^2 is even then n is even. The contrapositive is "If n is not even, then n^2 is not even." Suppose then that n is not even. Since every natural number is either even or odd, n must be odd. This means that that there is a natural number k so that $n = 2k+1$. It follows that $n^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ is odd. By the theorem in 7.16, since n^2 is odd, it is not even. We have proven

that if n is not even, then n^2 is not even. This is the contrapositive of the theorem. □

7.24 Exercises: Prove the following theorems using the contrapositive.
7.24.1 **Theorem:** For any natural number n if n^2 is odd, then n is odd.
7.24.2 **Theorem:** For any natural numbers a and b, if $2|ab$, then either $2|a$ or $2|b$.
7.24.3 **Theorem:** For any natural number n, if $3n + 1$ is odd, then n is odd.

7.25 Contradiction: Suppose we want to prove a statement P is true. Suppose also that if we assume P to be false, then we can prove that a contradiction C would have to be true (recall that a contradiction is always false). This means that we can prove $\neg P \rightarrow C$ where C is false. It must follow that P is true. The statement $\neg P \rightarrow C$ is equivalent to its contrapositive $\neg C \rightarrow P$. Since C is false, $\neg C$ is true, so the implication $\neg C \rightarrow P$ would force P to be true by modus ponens.

This is the basis of proof by contradiction. To prove P by way of contradiction, assume $\neg P$ and try to prove a contradiction.

Theorem: If n is an natural number and n^2 is even, then n is even.

Discussion: We proved this above using the contrapositive. That is a better option, but we prove the same theorem by contradiction as an example. Many times, contradiction proofs can be rewritten as contrapositive proofs.

Proof: Suppose that n is a natural number and that n^2 is even. We will use contradiction to prove that n is even. Suppose by way of contradiction that n is not even. Then n is odd and there is a natural number k so that $n = 2k + 1$. It follows that

$$n^2 = (2k + 1)^2 = 2(2k^2 + 2k) + 1$$

so n^2 is odd. But then n^2 is both odd and even. This contradicts Theorem 7.16, so the assumption that n is not even must be false. It has to be the case that n is even. □

7.26 Exercises: Use contradiction to prove these theorems
7.26.1 **Theorem:** If n is a natural number so that n^2 is red, then n is red. (Use the definitions and theorem from 7.22
7.26.2 **Theorem:** If n is a natural number so that $5n + 1$ is even, then n is odd.

8

Sets

8.1 Sets: In any spoken language, at any point in time, there are only finitely many words. This has surprising consequences when you try to define words. Suppose we try to define the word "little." We may write an expression which describes what this word means. Our definition relies on the meanings of all of the words in our expression. We could then write expressions to define the words used in the definition. Then we could try to define these words, and so on. Since there are only finitely many words in the English language, one of two things must happen – either we reuse words (and end up with a circular definition) or we find words that are not defined.

An extreme example of this can be found if you look up "little." Many dictionaries will have this definition: "small in size." The same dictionaries will define "small" as "little in size." If we do not know what "little" or "small" means, these dictionaries are useless.

To avoid circular definitions, mathematicians begin with **primitives** – undefined terms. The most fundamental primitive in all of mathematics is **set**. We will not define what a set is. Presumably, *collection* is a synonym. Sets contain (another primitive) things which we call **elements**. To indicate that an element x is in a set A, we write $x \in A$. This notation can be read as "x is an element of A," or as "x is in A," or if necessary, "x in A." To express that x is not in A, we would write $x \notin A$.

If we can list the elements of a set, we will do so between braces. For example, the set containing the symbols a, b, 1, and 2 is $\{a, b, 1, 2\}$. We can even use braces to list infinite sets if there is a clear pattern. For example, the even integers are $\{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$. An element of a set can be listed within braces repeatedly without changing the set. For example, the sets $\{a, b, c\}$ and $\{a, a, b, b, c, c\}$ are the same sets. Within braces, order also does not matter. The sets $\{t, e, a\}$ and $\{a, t, e\}$ are the same set.

8.2 Special Sets of Numbers: There are certain special sets of numbers which arise in most math classes. These are sets with which we are familiar, so we feel safe naming them here. We will derive them rigorously at a later time.

The **natural numbers**[1] are the numbers $\{0, 1, 2, 3, 4, \ldots\}$. This set is denoted

[1] Again, I cannot say how much it pains my soul that we are including 0 in $\mathbb{N}$.

$\mathbb{N}$. The set $\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is called the set of **integers** and is denoted as $\mathbb{Z}$. The set of all numbers which can be expressed as an integer divided by a non-zero integer is called the set of **rational numbers** and is denoted by $\mathbb{Q}$. These are precisely those numbers in decimal form which "repeat" such as $1.456121212121212\ldots$ or which "terminate" such as 1.234. The **irrational numbers** are those numbers which cannot be expressed as a fraction of integers. These are those numbers which in decimal form do not repeat or terminate. The set of all numbers which are rational or irrational is the set of **real numbers** and is denoted $\mathbb{R}$ (that is a truly awful description, but you will have to wait for a better one).

8.3 Set Builder Notation: Sometimes we need to describe a set which is too big or complicated to simply list. In this case, we can sometimes use **set builder** notation. This notation looks like:

$$\{x : P(x)\} \text{ or } \{x \in S : P(x)\}.$$

The colon inside the braces is read as "such that." The notation on the left is defined to mean the set of all x such that $P(x)$ is true. This means that an element x is in the set if and only if the statement $P(x)$ is true. The notation on the right is similar; however, this notation lets us restrict our attention to things which are in the set S. This is the set of all x in the set S for which the statement $P(x)$ is true.

Some examples of the use of set builder notation are:

$\{2n : n \in \mathbb{Z}\}$	The set of all even integers.
$\{m : (\exists n \in \mathbb{Z})(m = 2n)\}$	The set of all even integers.
$\{x \in \mathbb{R} : x \geq 2\}$	The interval $[2, \infty)$.
$\{x \in \mathbb{R} : (\exists n, m \in \mathbb{Z})(x = n/m)\}$	The set $\mathbb{Q}$.
$\{m/n : (m, n \in \mathbb{Z}) \wedge (n \neq 0)\}$	The set $\mathbb{Q}$.
$\{x \in \mathbb{R} : x^2 - 3x + 2 = 0\}$	The solutions to the equation $x^2 - 3x + 2 = 0$.

If $H(x)$ is "x is a horse" and $B(x)$ is "x is brown" then $\{x : H(x) \wedge B(x)\}$ is the set of all brown horses.

8.4 Exercises: Use set builder notation to describe each of the following sets.

8.4.1 The set of real solutions to the equation $x^3 = x$.

8.4.2 The set of all integer multiples of 6.

8.4.3 The set of all real numbers which are less than -2 or greater than 2.

8.4.4 The set of all rational numbers which can be written as an integer divided by a positive power of 2.

8.4.5 The set of all real numbers which are larger than their squares.

Let $E(x)$ be "x is even." Let $O(x)$ be "x is odd." Let $P(x)$ be "x is prime." Recall that $\mathbb{Z}$ is the set of integers, so to say "x is an integer" you can write $x \in \mathbb{Z}$. Write the following sets in set-builder notation.

8.4.6 The set of integer multiples of 3.

8.4.7 The set of odd integers less than 10.

8.4.8 The set of all integers which are either even or greater than 10.

8.4.9 The set of all integers which are prime.

8.4.10 The set of all even prime integers.

List the elements of these sets

8.4.11 $\{x \in \mathbb{N} : x^2 < 10\}$

8.4.12 $\{x \in \mathbb{N} : (x < 20) \wedge \exists y[(y \in \mathbb{N}) \wedge ((x = 3y) \vee (x = 5y))]\}$

8.4.13 $\{n : (n \in \mathbb{N}) \wedge \exists m[(m \in \mathbb{N}) \wedge (n = m^2)] \wedge (n < 20)\}$

8.4.14 $\{x \in \mathbb{N} : \exists a \exists b[(a \in \mathbb{N}) \wedge (b \in \mathbb{N}) \wedge (a > 1) \wedge (b > 1) \wedge (a < 5) \wedge (b < 5) \wedge (x = ab)]\}$

8.5 Subsets: A set A is a **subset** of another set B if every element of A is also an element of B. We denote this relationship by $A \subseteq B$. This notation is read as "A is a subset of B." If $A \subseteq B$ but A is not the same set as B, then we say A is a **proper subset** of B. This is denoted as $A \subset B$.

8.6 Caution: It is very important not to confuse the symbols $\in$ and $\subseteq$. The notation $X \in Y$ implies that Y is a set and X is a single element of that set. The notation $X \subseteq Y$ implies that X and Y are both sets and X is a subset of Y. However, there are times when X and Y might both be sets and we still have $X \in Y$. For example, this happens if $X = \{1, 2\}$ and $Y = \{\{1, 2\}, 3\}$. Note here that Y is a set with two elements. They are $\{1, 2\}$ and 3.

8.7 Exercises: Let $A = \{a, b, c\}$, $B = \{a, b\}$, $C = \{b, c, d\}$, and $D = \{a, b, B\}$. Fill in the blank with $\in$ or $\subseteq$ or both.

8.7.1 a___A

8.7.2 B___A

8.7.3 B___D

8.7.4 $\emptyset$___C

8.8 Empty Set: The **empty set** (denoted $\emptyset$) is the set which contains no elements. The empty set is a subset of every set (including itself) since the implication "If $x \in \emptyset$ then $x \in A$" is always true because $x \in \emptyset$ is always false.

8.9 Exercise:
8.9.1 List all of the subsets of $\emptyset$
8.9.2 List all of the subsets of $\{1\}$
8.9.3 List all of the subsets of $\{1, 2\}$
8.9.4 List all of the subsets of $\{1, 2, 3\}$
8.9.5 How many subsets should $\{1, 2, 3, 4\}$ have?
8.9.6 Guess at a formula for the number of subsets of an n-element set.

8.10 Proving One Set is a Subset of Another: You will frequently need to show that one set is a subset of another. In order to show that a set A is a subset of a set B, we will usually select an arbitrary element of A and give it a name such as x. We will then use the definitions of A and B to show that $x \in B$. Since x is an arbitrary element of A, we can then conclude that every element of A is an element of B (note that this is an application of universal generalization - $\forall$**G**).

Example: Prove that the set $A = \{6n : n \in \mathbb{Z}\}$ is a subset of the set $B = \{3n : n \in \mathbb{Z}\}$.

Proof. Let $x \in A$ be arbitrary. The definition of A tells us that $x = 6n$ for some integer n. It follows that $x = 3(2n)$. Since $2n$ is an integer, x satisfies the definition of B. Thus $x \in B$. Since $x \in A$ was arbitrary, we can conclude $A \subseteq B$. □

Example: Prove that the set $S = \{x \in \mathbb{R} : x^2 - 1 = 0\}$ is a subset of the set $D = \{x \in \mathbb{R} : x^4 - 1 = 0\}$.

Proof. Suppose $x \in S$ is arbitrary. This means that $x^2 - 1 = 0$, so $x^4 - 1 = (x^2 - 1)(x^2 + 1) = 0 \cdot (x^2 + 1) = 0$. Hence, $x \in D$. Thus every element of S is an element of D. □

8.11 Exercises: Prove that $A \subseteq B$.
8.11.1 $A = \{x \in \mathbb{R} : x - 2 = 0\}$ and $B = \{x \in \mathbb{R} : x^2 - 4 = 0\}$
8.11.2 $B = \{x \in \mathbb{Z} : (\exists n \in \mathbb{Z})(x = 2n)\}$ and $A = \{4n : n \in \mathbb{Z}\}$
8.11.3 $A = \{1/2^n : n \in \mathbb{N}\}$ and $B = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$
8.11.4 $A = \{x \in \mathbb{R} : \sin(x) = 0\}$ and $B = \{x \in \mathbb{R} : \tan(x) = 0\}$

8.12 Set Operations: We can make new sets from old sets. We see five of the most important ways now.

(a) **Intersection:** If A and B are sets, then the **intersection** of A and B (denoted $A \cap B$) is the set

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\}$$

For example, if A is the set of even integers and B is the set of multiples of three, then $A \cap B$ is the set of even multiples of three. This is the set of multiples of six.

(b) **Union:** If A and B are sets, then the **union** of A and B (denoted $A \cup B$) is the set

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}$$

For example, if $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$, then $A \cup B = \{1, 2, 3, 4\}$.

(c) **Product:** The **direct product** of two sets A and B (denoted by $A \times B$) is the set of all ordered pairs (a, b) so that $a \in A$ and $b \in B$. For example, if $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

It is important to remember that in the pairs (a, b), order matters. The Cartesian plane on which we learn to graph in elementary algebra and calculus can be thought of as $\mathbb{R} \times \mathbb{R}$.

(d) **Difference:** If A and B are sets, then the difference, $A - B$, of A and B is the set

$$A - B = \{x : (x \in A) \wedge (x \notin B)\}$$

For example, if $A = \{a, b, c\}$, $B = \{b, d, f\}$ and $C = \{a, b, c, d\}$, then $A - B = \{a, c\}$ and $A - C = \emptyset$.

(e) **Powerset:** The **powerset** of a set A (denoted by $\mathcal{P}(A)$) is the set of all subsets of A. For example, if $A = \{a, b, c\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

8.13 Note: Note that the symbol for intersection resembles that for "and." This is no accident. The word "and" is important in the definition of intersection. Similarly, note that the symbol for union resembles that for "or."

8.14 Exercises: Let $A = \{a, b, c, d, e\}$, $B = \{c, d, f\}$, and $C = \{a, f\}$. Find the indicated sets.

8.14.1 $B \times C$

8.14.2 $(A \cap B) \cup C$

8.14.3 $(A \cap C) \times (B \cap C)$

8.14.4 $A - (B \cup C)$

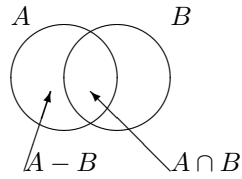
8.14.5 $A \cup ((A \cap B) \times C)$
8.14.6 $(A - B) \cup B$

8.15 Exercises: Suppose that A and B are sets. Prove each of the following.
8.15.1 $A \subseteq A \cup B$.
8.15.2 $A \cap B \subseteq A$.

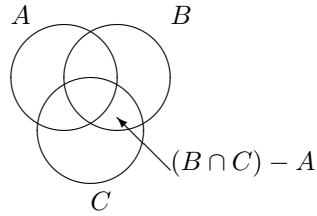
8.16 Exercises: Let $A = \{a, b, c\}$, $B = \{a, b\}$, $C = \{b, c, d\}$, and $D = \{a, b, B\}$. Fill in the blank with $\in$ or $\notin$.

8.16.1 a___A
8.16.2 b___B
8.16.3 c___B
8.16.4 B___D
8.16.5 B___A
8.16.6 (a, b)___$A \times C$
8.16.7 (a, b)___$C \times D$
8.16.8 ab___$A \times C$
8.16.9 4___$\mathbb{N} \times \mathbb{Z}$
8.16.10 4___$\mathbb{Z}$
8.16.11 -4___$\mathbb{Z}$
8.16.12 -4___$\mathbb{N}$

8.17 Venn Diagrams: Diagrams can be drawn to help visualize set operations. Each set is represented by an oval or a circle. The intersection, union, and difference of the sets can then be seen geometrically:



The union of A and B would be all of the area inside either circle. These diagrams of circles are called **Venn Diagrams**. Venn Diagrams can also be used to visualize more complicated set operations:



8.18 Exercise: Let A, B, and C be the sets

$$A = \{a, b, c, d, e\}$$

$$B = \{c, d, e, f, g\}$$

$$C = \{a, c, d, e, h, i, j\}.$$

Draw three circles as above and place the elements $\{a, b, c, d, e, f, g, h, i\}$ in the appropriate regions.

8.19 Exercises: Draw three circles as above and shade each of the following sets.

8.19.1 $(A \cap B) \cup (A \cap C)$

8.19.2 $A - (A \cap B \cap C)$

8.19.3 $(C - (A \cap B)) - (A \cap C)$

8.20 Exercises: Draw Venn diagrams to decide which of the following identities are true.

8.20.1 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

8.20.2 $A \cup (B \cap C) = (A \cup B) \cap C$

8.20.3 $A - (B \cup C) = (A - B) \cup C$

8.20.4 $A - (B \cup C) = (A - B) \cup (A - C)$

8.20.5 $A - (B \cup C) = (A - B) \cap (A - C)$

8.20.6 $A \cap (A \cup B) = A$

8.21 Set Equality: If A and B are sets, then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. To prove $A = B$, we need to prove $A \subseteq B$ and $B \subseteq A$.

8.22 Identities: Let A, B, and C be sets. We will prove that

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

First, suppose that $x \in A \cap (B \cup C)$. From the definition of intersection, this means that $x \in A$ and $x \in B \cup C$. From the definition of union, either $x \in B$ or $x \in C$. If $x \in B$, then $x \in A$ and $x \in B$, so $x \in A \cap B$. If $x \in C$, then $x \in A$ and $x \in C$, so $x \in A \cap C$. We see that either $x \in A \cap B$ or $x \in A \cap C$. This means that $x \in (A \cap B) \cup (A \cap C)$. Thus,

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

Now let $x \in (A \cap B) \cup (A \cap C)$. This means that either $x \in (A \cap B)$ or $x \in (A \cap C)$. If $x \in (A \cap B)$, then $x \in A$ and $x \in B$. Since $x \in B$, $x \in B \cup C$. Thus, $x \in A$ and $x \in B \cup C$, so $x \in A \cap (B \cup C)$. If $x \in (A \cap C)$, then $x \in A$ and $x \in C$. Since $x \in C$, $x \in B \cup C$. Thus, $x \in A$ and $x \in B \cup C$, so $x \in A \cap (B \cup C)$. In either case, $x \in A \cap (B \cup C)$. Thus

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

Since

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

and

$$(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C),$$

we know

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

The following are true for any sets A, B, and C.

$A \cap B = B \cap A$	commutative law
$A \cup B = B \cup A$	commutative law
$A \cap (B \cap C) = (A \cap B) \cap C$	associative law
$A \cup (B \cup C) = (A \cup B) \cup C$	associative law
$A \cap A = A$	idempotent law
$A \cup A = A$	idempotent law
$A \cap (A \cup B) = A$	absorption law
$A \cup (A \cap B) = A$	absorption law
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributive law
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributive law
$A - (B \cap C) = (A - B) \cup (A - C)$	DeMorgan's Law
$A - (B \cup C) = (A - B) \cap (A - C)$	DeMorgan's Law

8.23 Exercises: Suppose that A, B, and C are sets. Prove the following

8.23.1 $A \cap (A \cup B) = A$

8.23.2 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

8.23.3 $A - (B \cap C) = (A - B) \cup (A - C)$.

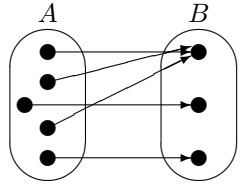
9

Functions

9.1 Transformations: Suppose A and B are sets. A **transformation** from A to B is a subset T of $A \times B$ so that for every $a \in A$, there is precisely one $b \in B$ with $(a, b) \in T$. For example, if $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4, 5\}$, then $T = \{(a, 4), (b, 2), (c, 4), (d, 5)\}$ is a transformation from A to B. A transformation from A to B is a roadmap for transforming the set A into the set B one element at a time. In our example, the transformation T says that the elements a and c of A are turned into the element 4 of B. The element b is turned into 2, and d is transformed into 5. Notice that more than one element of A can be turned into the same element of B and that not all of the elements of B are things into which elements of A are transformed.

To communicate that T is a transformation from A to B, we will use the notation $T : A \to B$. This is read "T is a transformation from A to B." In this case, the set A is called the **domain** of T. The set B is called the **codomain** of T. The set of all $b \in B$ so that there is an $a \in A$ with $(a, b) \in T$ is called the **range** or the **image** of T.

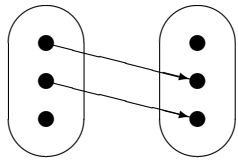
We can sometimes draw diagrams representing transformations between small sets. For example, the diagram

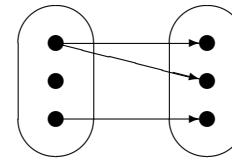


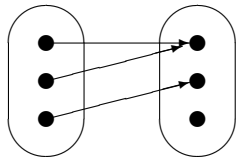
A transformation.

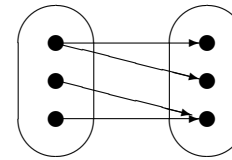
depicts a transformation from the set A with five elements on the left to the set B with three elements on the right. To determine which element of B an element of A is transformed into, you simply follow the arrows.

9.2 Exercises: Which of the following are transformations?

9.2.1 

9.2.3 

9.2.2 

9.2.4 

9.2.5 Is T a transformation from A to B if $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $T = \{(a, 1), (b, 1), (c, 1)\}$?

9.2.6 Is T a transformation from A to B if $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $T = \{(a, 2), (b, 1), (a, 3), (c, 3)\}$?

9.2.7 Is T a transformation from A to B if $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $T = \{(a, 2), (b, 1), (a, 2), (c, 3)\}$?

9.2.8 Is T a transformation from A to B if $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $T = \{(1, a), (2, b), (3, c)\}$?

9.2.9 Let $A = \emptyset$, $B = \{1, 2\}$, and $T = \emptyset$. Is T a transformation from A to B?

9.2.10 Let $B = \emptyset$, $A = \{1, 2\}$, and $T = \emptyset$. Is T a transformation from A to B?

9.3 Functions and Mappings: Transformations have many names. The most common of these are transformation, **function**, **mapping**, or simply **map**. The words mapping and transformation are perhaps the most descriptive as they communicate how one set is transformed or moved into another set. Throughout the rest of the course we will try to vary the use of these words so that we become comfortable with all of them.

9.4 Function Notation: The notation and definition of transformations given above is most useful for proving general facts about functions; however, in many environments, different notation is preferable. Often, we will use **function notation**. In this notation, to communicate that a pair (a, b) is in a transformation T we will write $T(a) = b$. This notation is intended to communicate that the mapping T moves the element a to the element b. Combining the notations, we see that as a set a transformation T is precisely the set of pairs of the form $(a, T(a))$. The set of all such ordered pairs would have been called the **graph** of T in algebra or calculus.

9.5 Matrix Notation: A convenient notation for depicting functions out of small sets is **matrix notation for functions**. In this notation, the function is displayed as a matrix with two rows. Each element of the domain of the function is listed in the first row. The image of each element is listed directly beneath that element. For example, the matrix for the function $f : \{1, 2, 3, 4, 5\} \to \mathbb{N}$ so that for each x, $f(x) = x^2$ is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 9 & 16 & 25 \end{pmatrix}$$

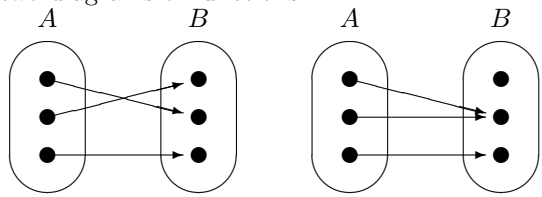
9.6 A Function as a Rule: Rather than thinking of a function $T : A \to B$ as a roadmap for transforming A into B, we can think of it as a "rule of assignment." T provides a rule for assigning to each element a of A a unique element of B. This unique element is usually called $T(a)$. This is, in fact, a naive way of defining a function. However, it is complicated by the fact that "rule" is not well defined. The set definition above uses only concepts we have already defined.

9.7 Exercises: Which of the following are functions from $\mathbb{R}$ to $\mathbb{R}$? For those that are functions, give a formula for $T(x)$.

9.7.1 $\{(a, b) \in \mathbb{R} \times \mathbb{R} : a^2 = b\}$
9.7.2 $\{(a, b) \in \mathbb{R} \times \mathbb{R} : a = b^2\}$
9.7.3 $\{(a, b) \in \mathbb{R} \times \mathbb{R} : a^2 = b^2\}$
9.7.4 $\{(a, b) \in \mathbb{R} \times \mathbb{R} : 2a + 1 = 2b + 1\}$
9.7.5 $\{(a, b) \in \mathbb{R} \times \mathbb{R} : a < b\}$
9.7.6 $\{(a, a) : a \in \mathbb{R}\}$

9.8 Injective Functions: A function (transformation) $T : A \to B$ is **injective** (or **one-to-one**) if for all x and y in A if $T(x) = T(y)$ then $x = y$. If T is injective, then different elements of A are mapped by T to different elements of B. For example, the transformation $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$ is injective. On the graph of this function, no two x-values give the same y-value. On the other hand, the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ is not one-to-one since $g(-1) = g(1)$ but $-1 \neq 1$.

Consider theses two diagrams of functions.

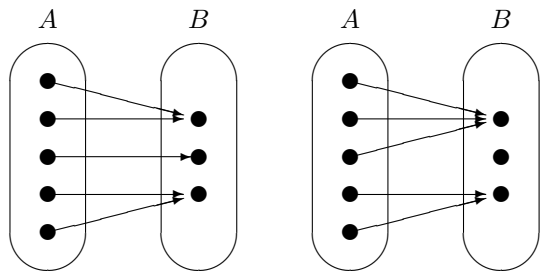


Injective Not Injective

The first function is injective. You can see this because each element of B has at most one arrow pointing at it. The second function is not injective, because one element of B has more than one arrow pointing at it.

9.9 Surjective Functions: A transformation $T : A \to B$ is **surjective** (or **onto**) if for every $b \in B$ there is an $a \in A$ so that $T(a) = b$. For example, the function $f(x) = 3x + 1$ mapping $\mathbb{R}$ to $\mathbb{R}$ is onto because if $b \in \mathbb{R}$ and $a = \dfrac{b-1}{3}$, then $f(a) = 3a + 1 = 3(\dfrac{b-1}{3}) + 1 = (b-1) + 1 = b$. On the other hand, the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2 + 1$ is not onto because there is no $x \in \mathbb{R}$ with $x^2 + 1 = 0$.

Consider these two diagrams of functions.



Surjective Not Surjective

The first function is surjective because every element of B has an arrow pointing at it. The second is not surjective since there is an element of B without an arrow pointing at it.

9.10 Exercises: Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $C = \{x, y, z, w\}$, and $D = \{u, v\}$.

9.10.1 Use matrix notation to give two examples each of injective functions from A to B and A to C.

9.10.2 Explain why there can be no injective function from A to D.

9.10.3 Use matrix notation to give two examples each of surjective functions from C to B and C to A.

9.10.4 Explain why there can be no surjective function from D to A.

9.10.5 Use matrix notation to give an injective function from A to A. Is this function surjective?

9.10.6 Use matrix notation to give an surjective function from A to A. Is this function injective?

9.11 Exercises: Suppose that $f : A \to B$ is any function. Let $X, Y \subseteq A$. Let $f(X) = \{f(x) : x \in X\}$. Similarly, let $f(Y) = \{f(y) : y \in Y\}$, $f(X \cup Y) = \{f(x) : x \in X \cup Y\}$, and $f(X \cap Y) = \{f(x) : x \in X \cap Y\}$.

9.11.1 Prove that $f(X) \cup f(Y) = f(X \cup Y)$.

9.11.2 Find an example to demonstrate that $f(X) \cap f(Y) = f(X \cap Y)$ may not hold.

9.12 Exercises: Suppose that $f : A \to B$ is any function. Let $X, Y \subseteq B$. Let $C = \{a \in A : f(a) \in X\}$. Let $D = \{a \in A : f(a) \in Y\}$. Let $E = \{a \in A : f(a) \in X \cap Y\}$. Let $F = \{a \in A : f(a) \in X \cup Y\}$.
9.12.1 Prove that $C \cap D = E$.
9.12.2 Prove that $C \cup D = F$.

9.13 Showing a Function is Injective: To show that a function $T : A \to B$ is injective, you should first select two arbitrary elements x and y in A and assume that $T(x) = T(y)$. You would then use the definition of T to conclude that $x = y$. This may involve solving the equation $T(x) = T(y)$ for x. For example

Fact: The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x^3 - 1$ is injective.

Proof: Let $x, y \in \mathbb{R}$ and assume that $f(x) = f(y)$. We will show that $x = y$. Since $f(x) = f(y)$, it follows that $3x^3 - 1 = 3y^3 - 1$. Adding 1 to both sides of this equation yields $3x^3 = 3y^3$. Dividing by 3 gives $x^3 = y^3$. Finally, taking cube roots gives $x = y$. We have shown that if $f(x) = f(y)$ then $x = y$. It follows that f is injective. □

9.14 Showing a Function is Not Injective: To show a function $T : A \to B$ is not injective, you can find two elements x and y in A so that $x \neq y$ but $f(x) = f(y)$. For example.

Fact: The function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x^3 - x$ is not one-to-one.

Proof: Let $f : \mathbb{Z} \to \mathbb{Z}$ be given by $f(x) = x^3 - x$. Note that $f(0) = 0 = f(1)$. Since $0 \neq 1$, f is not injective. □

9.15 Role of the Domain: The domain of a function can affect whether or not a function is one-to-one. For example, denote the positive real numbers by $\mathbb{R}^+$. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not injective, but the function $f : \mathbb{R}^+ \to \mathbb{R}$ is injective.

9.16 Exercises: Decide if each of these functions is one-to-one or not. Support each answer with a proof.
9.16.1 $f : \mathbb{R}^- \to \mathbb{R}$ given by $f(x) = x^2$
9.16.2 $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 9x - 9$
9.16.3 $f : \mathbb{R}^+ \to \mathbb{R}^-$ given by $f(x) = -(x^2 + 1)$
9.16.4 $f : [-1, 1] \to \mathbb{R}$ given by $f(x) = x^3 - x$

9.17 Showing a Function is Surjective: To show that a function $T : A \to B$ is surjective, pick an arbitrary element b in B. Then use the definition of T to find an element a of A so that $T(a) = b$. This may involve solving the equation $T(a) = b$ for a. For example

Fact: The function $T : \mathbb{R} \to \mathbb{R}$ given by $T(x) = 2x^5 + 1$ is surjective.

Discussion: If we set up the equation $T(a) = b$ and solve for a, we get $a = \left(\frac{b-1}{2}\right)^{1/5}$.

Proof: We prove that the function $T(x) = 2x^5 + 1$ from $\mathbb{R}$ to $\mathbb{R}$ is surjective. Let $b \in \mathbb{R}$, and let $a = \left(\frac{b-1}{2}\right)^{1/5}$. Note that

$$\begin{aligned} T(a) &= 2\left(\left(\frac{b-1}{2}\right)^{1/5}\right)^5 + 1 \\ &= 2\left(\frac{b-1}{2}\right) + 1 \\ &= (b-1) + 1 \\ &= b \end{aligned}$$

Thus for every $b \in \mathbb{R}$, there is an $a \in \mathbb{R}$ with $T(a) = b$. T is surjective. □

9.18 Showing a Function is Not Surjective: To show that a transformation $T : A \to B$ is not surjective, you should find an element b of B so that there can be no $a \in A$ with $T(a) = b$. For example
Fact: The function $f(x) = 2x^2 + 1$ from $\mathbb{R}$ to $\mathbb{R}$ is not surjective.

Proof: Notice that for all $x \in \mathbb{R}$, $f(x) = 2x^2 + 1 \geq 1$. Therefore, there can be no $x \in \mathbb{R}$ with $f(x) = 0$. Hence f is not surjective. □

9.19 The Role of the Codomain: The codomain of a function can affect if a function is surjective. For example, the function $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$ is not surjective. However, it is surjective from $\mathbb{R}$ to $\{x \in \mathbb{R} : x \geq 0\}$.

9.20 Exercises: Decide if each of the following functions is surjective or not. Support each answer with a proof.
9.20.1 $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 4x - 3$
9.20.2 $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 4x - 3$
9.20.3 $f : \mathbb{R} \to \mathbb{R}^+$ given by $f(x) = x^2 + 1$
9.20.4 $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \sin x$
9.20.5 $f : \mathbb{R}^+ \to \mathbb{R}$ given by $f(x) = \ln x$

9.21 Bijective Functions: A function which is both injective (one-to-one) and surjective (onto) is called **bijective**. To show that a function is bijective, you must show that it is both injective and surjective.

9.22 Exercises: Which of the following functions are injective, surjective, or bijective?
9.22.1 $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$
9.22.2 $f : \mathbb{R}^+ \to \mathbb{R}$ given by $f(x) = x^2$

9.22.3 $f : \mathbb{R}^+ \to \mathbb{R}^+$ given by $f(x) = x^2$
9.22.4 $f : \mathbb{R}^- \to \mathbb{R}^+$ given by $f(x) = x^2$

9.23 Composition of Functions: If $f : A \to B$ and $g : B \to C$ are functions, we can create a new function which maps A to C by first applying f and then applying g. The **composition** of f followed by g is a function $g \circ f : A \to C$ given by $g \circ f(a) = g(f(a))$ for all $a \in A$. For example, suppose $f : \mathbb{R} \to \mathbb{R}^+$ is the function $f(x) = x^2 + 1$ and $g : \mathbb{R}^+ \to \mathbb{R}^-$ is the function $g(x) = -\sqrt{x}$, then $g \circ f(x) = -\sqrt{x^2 + 1}$.

9.24 Note: Notice that $g \circ f$ is only defined if the codomain of f is the same as the domain of g.

9.25 Proving Two Functions are Equal: To prove that two functions $f : A \to B$ and $g : A \to B$ are actually equal, we need to prove that $f(a) = g(a)$ for all $a \in A$. To do so, let $a \in A$ be arbitrary and show that $f(a) = g(a)$. We follow this outline in the next example.

9.26 Associativity of Composition: Function composition is associative.

Theorem: Suppose $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Proof: To show that $h \circ (g \circ f) = (h \circ g) \circ f$, we must show that the two functions agree for every $a \in A$. Let $a \in A$. Then

$$\begin{aligned} h \circ (g \circ f)(a) &= h(g \circ f(a)) \\ &= h(g(f(a))) \\ &= h \circ g(f(a)) \\ &= (h \circ g) \circ f(a) \end{aligned}$$

□

9.27 Exercises: Suppose $f : A \to B$ and $g : B \to C$ are functions.
9.27.1 Prove that if f and g are injective, then $g \circ f$ is injective. (Hint: Suppose that $g \circ f(x) = g \circ f(y)$. This means that $g(f(x)) = g(f(y))$. Apply the fact that g is injective. Then apply the fact that f is injective.)
9.27.2 Prove that if f and g are surjective, then $g \circ f$ is surjective. (Hint: Let $c \in C$. Since g is surjective, there is a $b \in B$ with $g(b) = c$. Since f is surjective, there is an $a \in A$ with $f(a) = b$. You are almost there.)
9.27.3 Prove that if $g \circ f$ is injective, then f is injective. (Hint: Suppose $f(x) = f(y)$. Then $g(f(x)) = g(f(y))$. You can now use the fact that $g \circ f$ is injective.)
9.27.4 Prove that if $g \circ f$ is surjective, then g is surjective. (Hint: Let $c \in C$. There is an $a \in A$ with $g \circ f(a) = c$. This means $g(f(a)) = c$. You are very close now.)

9.28 Identity Function: Let A be any set. The **identity function** on A is the function $1_A : A \to A$ given by $1_A(x) = x$.

9.29 Inverse Functions: Suppose $f : A \to B$ is a function. A function $g : B \to A$ is an **inverse** of f if $g \circ f = 1_A$ and $f \circ g = 1_B$. This is equivalent to saying that for all $a \in A$ $g(f(a)) = a$ and for all $b \in B$ $f(g(b)) = b$. (You can imagine that the functions g and f "unwrap" each other.)

9.30 Theorem: Inverse functions are unique.

Discussion: What this theorem says is that a function can have at most one inverse. To prove it, we will assume that a function f has two inverses g and h. We will then show that $g = h$.

Proof: Suppose $f : A \to B$ is a function and that $g : B \to A$ and $h : B \to A$ are inverses of f. We will show that $h = g$. To do so, we must show that $h(b) = g(b)$ for all $b \in B$. Let b be an element of B. Since g is an inverse of f, $b = f(g(b))$. Therefore, $h(b) = h(f(g(b))$. On the other hand, since h is an inverse of f, $g(b) = h(f(g(b))$. Hence, $h(b) = h(f(g(b)) = g(b)$. This is true for all $b \in B$, so $h = g$. □

9.31 Notation: If a function $f : A \to B$ has an inverse, we will denote the inverse by f^{-1} (read "f inverse"). Then, f^{-1} is a function from B to A so that $f(f^{-1}(b)) = b$ for all $b \in B$ and $f^{-1}(f(a)) = a$ for all $a \in A$.

9.32 Showing One Function is the Inverse of Another: To show that a function $g : B \to A$ is the inverse of a function $f : A \to B$, you must calculate $g(f(a))$ and show this is equal to a, and you must calculate $f(g(b))$ and show this is equal to b. For example

Fact: The function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = \dfrac{x-1}{2}$ is the inverse of the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x + 1$.

Proof: Let $a \in \mathbb{R}$. We calculate $g(f(a))$.

$$g(f(a)) = g(2a+1) = \frac{(2a+1)-1}{2} = \frac{2a}{2} = a.$$

Next, let $b \in \mathbb{R}$. We calculate $f(g(b))$.

$$f(g(b)) = f(\frac{b-1}{2}) = 2\frac{b-1}{2} + 1 = (b-1) + 1 = b.$$

Since $g(f(a)) = a$ and $f(g(b)) = b$ for all a and b in $\mathbb{R}$, g is the inverse of f. □

9.33 Exercises: In each problem, show that g is the inverse of f.

9.33.1 $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = 4x - 7$. $g : \mathbb{R} \to \mathbb{R}$ is given by $g(x) = \dfrac{1}{4}(x + 7)$.

9.33.2 $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^3 - 1$. $g : \mathbb{R} \to \mathbb{R}$ is given by $g(x) = (x+1)^{1/3}$

9.33.3 $f : [\frac{3}{2}, \infty) \to [0, \infty)$ is given by $f(x) = \sqrt{2x-3}$ and $g : [0, \infty) \to [\frac{3}{2}, \infty)$ is given by $g(x) = \dfrac{x^2+3}{2}$.

9.34 Finding Inverses: To find the inverse of a function $f : A \to B$, you can attempt to solve the equation $b = f(a)$ for a. This will yield an equation $a = g(b)$. If $g(b) \in A$ for all b, and if $g(f(a)) = a$ for all $a \in A$, then g is the inverse of f. For example, let $f(x) = 3x - 6$. Consider f first as a function from $\mathbb{R}$ to $\mathbb{R}$. We will find an inverse function for f. First, we set up the equation $b = f(a)$ and solve. The equation is $b = 3a - 6$. When we solve, we get $a = \frac{1}{3}b + 2$. Thus it appears our inverse should be $g(b) = \frac{1}{3}b + 2$. We must check two things. First, note that for any real number b, $g(b) \in \mathbb{R}$. Second, we must see if $g(f(a)) = a$ for all real numbers a. We check:

$$g(f(a)) = g(3a - 6) = \frac{1}{3}(3a - 6) + 2 = a - 2 + 2 = a$$

Hence, we have found the inverse of f.

Things do not work out quite so smoothly for f if we consider f as a function from $\mathbb{Z}$ to $\mathbb{R}$. If we set up the equation above, we still get the same g, and we still get that $g(f(a)) = a$ for all $a \in \mathbb{Z}$. However, notice that $g(1) = 7/3$, so g is not even a function from $\mathbb{R}$ to $\mathbb{Z}$, so it cannot be an inverse for f if we consider f to be a function from $\mathbb{Z}$ to $\mathbb{R}$. In this form, f has no inverse.

9.35 Exercises: Find inverses for each of the following functions if possible. If not possible, explain why.

9.35.1 $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = (x+1)^3$

9.35.2 $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = (x+1)^2$

9.35.3 $f : [0, 1] \to [0, 1]$ given by $f(x) = x^2$

9.36 Inverses and Bijectivity: The existence of inverses is related to bijectivity.

Theorem: A function $f : A \to B$ has an inverse if and only if f is bijective.

Proof: This is a bi-conditional, so we must prove two statements. First, we must show that if a function has an inverse, then the function is bijective. Also, we must show that if a function is bijective, then it has an inverse.

Suppose that $f : A \to B$ has an inverse $f^{-1} : B \to A$. We show first that f is injective. Let $x, y \in A$ and suppose that $f(x) = f(y)$. Then also $f^{-1}(f(x)) = f^{-1}(f(y))$. But $f^{-1}(f(x)) = x$ and $f^{-1}(f(y)) = y$, so we have $x = y$. Hence f is injective. Next, we show that f is surjective. Let $b \in B$.

We need an $a \in A$ with $f(a) = b$. Let $a = f^{-1}(b)$. Then $f(a) = f(f^{-1}(b)) = b$ as desired. Thus f is surjective. We have shown that if f has an inverse, then f is both injective and surjective.

Next suppose that $f : A \to B$ is a bijection. We will define a function $g : B \to A$ and then show that g is the inverse of f. Let $b \in B$. Since, f is surjective, there is at least one $a \in A$ with $f(a) = b$. Define $g(b)$ to be any such a. Do this for every $b \in B$ (Note that we just used the surjectivity of f). This gives a function $g : B \to A$. We will show that this function is the inverse of f. First, note that by the choice of $g(b)$, we automatically have that $f(g(b)) = b$ for all $b \in B$. We need only that $g(f(a)) = a$ for all $a \in A$. From what we already know $f(g(f(a))) = f(a)$. Since f is injective, this requires that $g(f(a)) = a$ as desired (Note we just used the injectivity of f). Thus we have both $f(g(b)) = b$ for all $b \in B$ and $g(f(a)) = a$ for all $a \in A$. The function g is the inverse of f. We have now shown that if f is bijective, then f has an inverse. □

9.37 Checking for Bijectivity: Sometimes, we wish to prove that a function is bijective. By the previous theorem, it is enough to simply show the function has an inverse.

9.38 Exercises: Decide which of these are bijective by trying to find inverses.

9.38.1 $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 5x - 9$

9.38.2 $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 5x - 9$

9.38.3 $f : [0, 1] \to [0, 1]$ given by $f(x) = x - x^2$

9.38.4 $f : \{-1, 0, 1\} \to \{-1, 0, 1\}$ given by $f(x) = x^2$

9.38.5 $f : \{0, 1\} \to \{0, 1\}$ given by $f(x) = x^2$

9.39 Piecewise Defined Functions: If a set A is the union of two or more disjoint subsets, functions can be defined on A by defining functions on the disjoint subsets. For example, $\mathbb{R} = \{x \in \mathbb{R} : x < 0\} \cup \{0\} \cup \{x \in \mathbb{R} : x > 0\}$, so we can define a function on $\mathbb{R}$ by defining it on these three sets. Here is an example of how this can be done.

$$f(x) = \begin{cases} 2x - 1 & x < 0 \\ 4 & x = 0 \\ x^2 & x > 0 \end{cases}$$

Here the first line corresponds to the set $\{x \in \mathbb{R} : x < 0\}$. The second corresponds to the set $\{0\}$, and the last corresponds to $\{x \in \mathbb{R} : x > 0\}$ To evaluate this function at a number x, you would first decide which category x falls in, and then you would apply the appropriate function. For example, since $7 > 0$, $f(7) = 7^2 = 49$. Functions such as these are called **piecewise defined** functions. It is important when defining functions piecewise that the

subsets you use are actually disjoint. For example,

$$f(x) = \begin{cases} 2x - 1 & x \leq 0 \\ 4 & x = 0 \\ x^2 & x \geq 0 \end{cases}$$

makes no sense since 0 is in all three sets and would be assigned to three different values by the three different functions.

9.40 Permutations: A **permutation** of a set A is a bijection from A to A. We will denote the set of all permutations on a set A by S_A.

9.41 Exercises: Write your solutions to these exercises in matrix form.
9.41.1 Find all permutations on the set $\{1, 2\}$.
9.41.2 Find all permutations on the set $\{1, 2, 3\}$.
9.41.3 Find all permutations on the set $\{1, 2, 3, 4\}$.
9.41.4 How many permutations would you expect to find on a set with n elements?

9.42 Exercise: Show that if f and g are two permutations on a set A, then $f \circ g$ is also a permutation. (Hint: Look at exercises 9.27.)

9.43 Projections from Products: Suppose that A and B are sets. The **projection** function from $A \times B$ onto A is the function $\pi_A : A \times B \to A$ given by $\pi_A(a, b) = a$. This function just "plucks" the first coordinate off of an ordered pair. We could define the projection π_B onto B in a similar fashion.

9.44 Exercises:
9.44.1 If A and B are nonempty sets, show that the projection from $A \times B$ to A is onto (surjective).
9.44.2 Was it necessary to assume that B is nonempty in the previous exercise? What about A?

10

Relations

10.1 Relations: Predicates express properties of and relationships between the variables involved. For example

x is taller than y.

expresses a relationship between x and y. The sentence

x robbed the bank.

expresses the property that x may have of having robbed the bank. Mathematicians use the notion of a relation to describe abstract properties and relationships.

P is a **1-ary (or unary) relation** on a set A if P is a subset of A. When thinking of a subset P as a relation, we will write $P(x)$ for $x \in P$. If we let P be the set of all people who robbed the bank. Then $P(x)$ and $x \in P$ both mean the same thing as the predicate "x robbed the bank."

P is a **2-ary (or binary) relation** on a set A if P is a subset of $A \times A$ (so P is a set of ordered pairs of A such as (x, y)). When thinking of P as a relation, we will write $P(x, y)$ or xPy for $(x, y) \in P$. We will also use the words "x is P-related to y to express $(x, y) \in P$. If we let P be the set of all pairs of people (x, y) so that x is the father of y, then $P(x, y)$, xPy, and $(x, y) \in P$ all mean the same thing as the predicate "x is the father of y."

P is a **3-ary (or ternary) relation** on a set A if P is a subset of $A \times A \times A$ (so P is a set of ordered triples of A such as (x, y, z)). When thinking of P as a relation, we will write $P(x, y, z)$ for $(x, y, z) \in P$.

We can continue this process indefinitely. If n is a positive integer, then P is **an n-ary relation** on a set A if P is a subset of $A \times A \times \cdots \times A$ (with n factors) so that P is a set of n-tuples of A such as $(x_1, x_2, \ldots, x_n)$. When thinking of P as a relation, we will write $P(x_1, x_2, \ldots, x_n)$ for $(x_1, x_2, \ldots, x_n) \in P$. For emphasis, we will also say "$P(x_1, x_2, \ldots, x_n)$ is true" to mean that "$(x_1, x_2, \ldots, _n) \in P$ is true."

The notation we are using for relations is intended to match exactly the notation we have used for predicates and open formulas. The two concepts are intimately related. An open formula $P(x, y)$ can be used to define a set – the

set of all pairs (x, y) for which $P(x, y)$ is true (whatever that means). In set builder notation, this is $\{(x, y) : P(x, y)\}$. This set of ordered pairs can be treated as a set or a relation. We can call both the set and the relation P. In this case, $P(x, y)$ means exactly the same thing as $(x, y) \in P$.

10.2 Infix vs. Prefix Notation The notation $R(x, y)$ is called **prefix notation**. The notation xRy is **infix notation**. For binary relations, we will usually prefer infix notation since we commonly use this notation with relations such as $=$ and $\leq$.

10.3 Example: Suppose that $A = \{1, 2, 3, 4\}$. Define this relation on A:

$$P = \{(x, y, z) : y \text{ is strictly between } x \text{ and } z\}.$$

Then we would say that $P(1, 2, 3)$ is true but $P(2, 1, 3)$ is not. We equate $P(x, y, z)$ with the defining predicate "y is strictly between x and z."

10.4 Example: Let $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Let

$$P = \{x \in A : x \text{ is prime}\}.$$

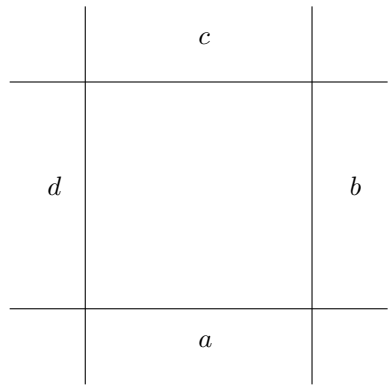
Then we equate the expression $P(x)$ with the predicate "x is prime." Thus $P(3)$ is true, but $P(4)$ is not. We can list the elements of P as $\{2, 3, 5, 7\}$.

10.5 Example: Let A be the set $\{2, 3, 4, 5, 6\}$. Define a binary relation D on A so that for all $x, y \in A$, xDy exactly when y is a multiple of x. Then $2D4$ and $3D6$, but it is not the case that $2D3$. We could write these statements also as $D(2, 4)$ and $D(3, 6)$ but not $D(2, 3)$. As a set of ordered pairs, D is

$$D = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6)\}.$$

As a predicate, xDy means "y is a multiple of x."

10.6 Example: Let A be the set of lines in this figure:



So $A = \{a, b, c, d\}$. Define a relation I on A so that xIy exactly when line x intersects line y. Then (for example) aId and aIb but it is not the case that aIc.

10.7 Exercises:
10.7.1 List two more pairs which are not in the relation I of Example 10.6 and two more pairs that are.
10.7.2 Define a relation S on $\mathbb{N}$ so that $S(x, y)$ means that $x + 1 = y$. List a few pairs in the relation S. We will see later that most of the properties of the natural numbers which we studied in arithmetic can be derived from this relation.
10.7.3 Let $A = \{1, 2, 3, 4, 5, 6\}$. Define R on A so that xRy means that $x - y \in A$. List the pairs in R.

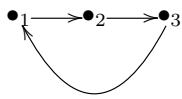
Let E and F be two unary relations on $\mathbb{N}$ so that $E(x)$ means "x is even" and $F(x)$ means "x is a multiple of 4."
10.7.4 Find an x which makes $E(x) \wedge F(x)$ true.
10.7.5 Find an x which makes $E(x) \wedge \neg F(x)$ true.
Which of these is true?
10.7.6 $\forall x(E(x) \to F(x))$
10.7.7 $\forall x(F(x) \to E(x))$
10.7.8 $\exists x(E(x) \to F(x))$
10.7.9 $\exists x(F(x) \to E(x))$

10.8 Directed Graphs: We can draw pictures of small sets with binary relations. The picture consists of one point for each element of the set. For each relation xRy, there is an arrow in the picture from x to y. Such a pictorial representation is called a **directed graph** or **digraph**.

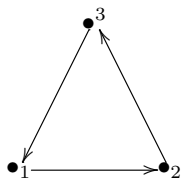
10.9 Example: The directed graph for the relation

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

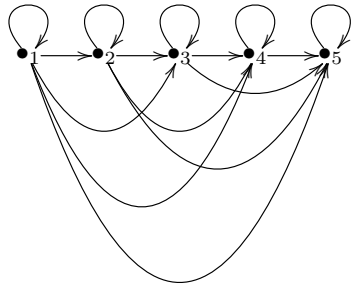
on the set $A = \{1, 2, 3\}$ is



10.10 Example: What matters in directed graphs is how the points are connected by arrows, not the physical arrangement of the points in the picture. Thus, this is another depiction of the graph from the previous example:



10.11 Example: The directed graph for the relation $\leq$ on the set $\{1, 2, 3, 4, 5\}$ is



10.12 Exercises: Draw digraphs of relations $\Rightarrow$ which satisfy each of these statements.

10.12.1 $\forall x(x \Rightarrow x)$
10.12.2 $\forall x \forall y(x \Rightarrow y)$
10.12.3 $\exists x \forall y(x \Rightarrow y)$
10.12.4 $\exists x \exists y \exists z[(x \Rightarrow y) \wedge (y \Rightarrow z)]$
10.12.5 $\forall x \forall y \neg[(x \Rightarrow y) \wedge (y \Rightarrow x)]$
10.12.6 $\forall x \forall y([(x \Rightarrow y) \vee (y \Rightarrow x)] \wedge \neg[(x \Rightarrow y) \wedge (y \Rightarrow x)])$

10.13 Some Properties of Relations: There are some properties which happened to be satisfied by many relations in different fields of mathematics. We list a few here and give examples using the set $S = \{a, b, c, d\}$ and the set $\mathbb{R}$.

10.14 Reflexive Property: A relation R on a set A is **reflexive** if aRa for every $a \in A$. This could also be written as $(a, a) \in R$ for all $a \in A$. The relation

$$R = \{(a, a), (a, c), (b, d), (b, b), (c, c), (d, d)\}$$

on S is reflexive since R contains (a, a), (b, b), (c, c), and (d, d). The relation $\leq$ on the real numbers is reflexive since $x \leq x$ is always true. The relation $<$ is not reflexive.

10.15 Symmetric Property: A relation R on a set A is **symmetric** if for all $a, b \in A$ whenever aRb, then also bRa. On the set S, the relation $R = \{(a, b), (b, a), (c, c), (d, c), (c, d)\}$ is symmetric. You can see this because if we reverse any ordered pair in R we get another ordered pair in R. The relation $\leq$ on $\mathbb{R}$ is not symmetric, since $1 \leq 2$, but it is not the case that $2 \leq 1$.

10.16 Anti-Symmetric Property: A relation R on a set A is **anti-symmetric** if for all $a, b \in A$ whenever aRb and bRa then also $a = b$. For example, the relation $\leq$ on $\mathbb{R}$ is anti-symmetric. The relation $R = \{(a, b)(b, c)(d, d)\}$ is anti-symmetric on S. If we reverse any of the ordered pairs in this relation other than (d, d), we do not get another element of R.

10.17 Transitive Property: A relation R on a set A is **transitive** if for all $a, b, c \in A$ the relations aRb and bRc together imply aRc. The relations $\leq$ and $=$ on $\mathbb{R}$ are transitive. The relation $\{(c,d),(d,a),(c,a)\}$ on S is transitive, while the relation $\{(b,d),(d,a)\}$ is not. In order to be transitive, this last relation would need to contain (b,a).

10.18 Exercises:
10.18.1 Draw one digraph of a relation on $\{a,b,c\}$ which is reflexive and one which is not reflexive. Conjecture how to decide from the digraph whether or not a relation is reflexive.
10.18.2 Draw one digraph of a relation on $\{a,b,c\}$ which is symmetric and one which is not symmetric. Conjecture how to decide from the digraph whether or not a relation is symmetric.
10.18.3 Draw one digraph of a relation on $\{a,b,c\}$ which is anti-symmetric and one which is not anti-symmetric. Conjecture how to decide from the digraph whether or not a relation is anti-symmetric.
10.18.4 Draw one digraph of a relation on $\{a,b,c\}$ which is transitive and one which is not transitive. Conjecture how to decide from the digraph whether or not a relation is transitive.

Determine if each of the following relations on the set $\{a,b,c,d\}$ is reflexive, symmetric, anti-symmetric, or transitive.
10.18.5 $R = \{(a,b),(b,c),(c,d)\}$
10.18.6 $R = \{(a,a),(c,c),(d,d)\}$
10.18.7 $R = \{(a,b),(b,a),(a,a),(c,c),(d,d)\}$
10.18.8 $R = \emptyset$
10.18.9 $R = \{(a,b),(a,a),(d,d),(b,a),(c,c),(d,c),(c,d),(b,b)\}$
10.18.10 $R = \{(a,a),(b,b),(c,c),(d,d)\}$

10.19 Equivalence Relations: A relation R on a set A is called an **equivalence relation** if it is reflexive, symmetric, and transitive.

10.20 Examples: The equality relation $(=)$ is an equivalence relation on any set. Actually, this relation is the motivation behind an equivalence relation.

The relation R on the real numbers defined by xRy if $x^2 = y^2$ is an equivalence relation.

The relation $R = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$ taken on the set $\{1,2,3\}$ is an equivalence relation.

10.21 Showing Relations are Reflexive: The proof that a relation R on a set A is reflexive usually begins with a sentence like "Let $a \in A$ be arbitrary." The proof then proceeds to use the definition of R to conclude that aRa. Since a was arbitrary, this is enough to conclude R is reflexive (note the

application of universal generalization). For example:

Fact: The relation R on $\mathbb{R}$ defined by xRy when $\sin(x) = \sin(y)$ is reflexive.

Proof: Let R be the relation on $\mathbb{R}$ given by xRy when $\sin(x) = \sin(y)$. We will prove that R is reflexive. Let $x \in \mathbb{R}$. Since $x = x$, it follows that $\sin(x) = \sin(x)$. Hence, xRx. Since $x \in \mathbb{R}$ was arbitrary, we can conclude that xRx for all $x \in \mathbb{R}$. Hence, R is reflexive. □

10.22 Showing Relations are Symmetric: The proof that a relation R on a set A is symmetric usually begins with a statement like "Let $a, b \in A$ be arbitrary." To show that R is symmetric, the proof must establish the implication "If aRb, then bRa." To do so, the proof should next assume that the antecedent (first part) of this implication is true: "Suppose aRb." The proof would then use the definition of R to somehow show that bRa. Again, since a and b were arbitrary, this will establish that R is symmetric. For example:

Fact: The relation R on $\mathbb{N}$ defined by nRm when $2|(nm)$ is symmetric.

Proof: Let R be the relation on $\mathbb{N}$ given by nRm when $2|(nm)$. We will prove that R is symmetric. Let $n, m \in \mathbb{N}$ be arbitrary and suppose that nRm. This means that $2|(nm)$, so there is a natural number k with $nm = 2k$. Since $mn = nm = 2k$, it follows that $2|(mn)$. Hence mRn. Since m and n were arbitrary, we can conclude that R is symmetric. □

10.23 Showing Relations are Transitive: A proof that a relation R on a set A is transitive usually begins by providing three arbitrary elements of A. The proof will be trying to establish the implication in the definition of transitivity, so it will then assume that the first half of the implication is true for those arbitrary elements. Such a proof might begin "Let $a, b, c \in A$ and assume that aRb and bRc." The proof must then use the definition of R to establish that aRc. Here is an example.

Fact: Let R be the relation on $\mathbb{N}$ defined by nRm when the implication "If n is even then m is even" is true. R is transitive.

Proof: Let R be the relation on $\mathbb{N}$ defined by nRm when the implication "If n is even then m is even" is true. We will prove that R is transitive. Let $a, b, c \in \mathbb{N}$ be arbitrary, and suppose aRb and bRc. We will show that aRc. In order to do so, we must prove the implication "If a is even, then c is even" is true. Suppose, then that a is even. For the implication to be true, we must show that c is even. We know that aRb and bRc. The relation aRb means that if a is even, then b is even. Since a is even, it follows that b is even also (this is a use of Modus Ponens). The relation bRc means that if b is even, then c is even. Since we know b is even, it follows that c is even. Hence, when

a is even, so is c. We have established aRc. We have shown for arbitrary $a, b, c \in \mathbb{N}$ that if aRb and bRc, then aRc. Hence, R is transitive. □

10.24 Exercises: Show that each of the following relations are equivalence relations by proving that each is reflexive, symmetric, and transitive.
10.24.1 R is the relation on $\mathbb{R}$ defined by xRy when $\sin(x) = \sin(y)$.
10.24.2 R is the relation on $\mathbb{R}$ defined by xRy if $x^2 = y^2$.
10.24.3 R is the relation on $\mathbb{N}$ defined by xRy if x and y are either both even or both odd.
10.24.4 $R = \mathbb{N} \times \mathbb{N}$ as a relation on $\mathbb{N}$.
10.24.5 $R = \{(a, a) : a \in \mathbb{N}\}$ as a relation on $\mathbb{N}$.

10.25 Equivalence Classes: Suppose R is an equivalence relation on a set A. If $a \in A$, then the **equivalence class of a modulo R** is the set $\{x \in A : aRx\}$. The equivalence class of a modulo R is denoted as $[a]_R$. If R is understood from context, we will sometimes just write $[a]$. Note that just by this definition **the statement $x \in [a]_R$ means the same thing as aRx.**

10.26 Exercises:
10.26.1 Find $[\pi]_R$ for the relation R in Exercise 10.24.1.
10.26.2 Find $[7]_R$ for the relation R in Exercise 10.24.2.
10.26.3 Find $[4]_R$ for the relation R in Exercise 10.24.3.

10.27 Exercises: Suppose R is an equivalence relation on a set A. Prove each of the following.
10.27.1 **Lemma:** For all $a \in A$, $a \in [a]_R$. (Hint: R is reflexive)
10.27.2 **Lemma:** For all $a, b \in A$ if $b \in [a]_R$, then $a \in [b]_R$. (Hint: R is symmetric)
10.27.3 **Lemma:** For all $a, b \in A$ if aRb, then $[b]_R \subseteq [a]_R$. (Hint: R is transitive)
10.27.4 **Lemma:** If $[a]_R \cap [b]_R$ is not empty, then aRb. (Hint: Let $x \in [a]_R \cap [b]_R$. This means that $x \in [a]_R$ and $x \in [b]_R$. Use the definition of this notation, symmetry, and transitivity.)
10.27.5 **Theorem:** (Important) For all $x, y \in A$, the following are equivalent:

1. xRy
2. $[x]_R = [y]_R$
3. $[x]_R \cap [y]_R \neq \emptyset$

10.27.6 **Theorem:** For all $x, y \in A$, either $[x]_R = [y]_R$ or $[x]_R \cap [y]_R = \emptyset$.

10.28 Exercises:
10.28.1 Find all equivalence relations on the set $\{1, 2\}$.
10.28.2 Find all equivalence relations on the set $\{1, 2, 3\}$.

10.29 Exercise: Suppose $f : A \to B$ is a function. Define R on A so that xRy if and only if $f(x) = f(y)$. Show that R is an equivalence relation.

10.30 Kernels: The relation R in the previous exercise is called the **kernel** of the function f. It turns out that every equivalence relation is the kernel of some function.

10.31 Factor Sets: Suppose that R is an equivalence relation on a set A. We will call the set of equivalence classes modulo R the **factor set of** A **modulo** R or the **quotient set of** A **modulo** R. This set is denoted A/R (read "A mod R"). In short $A/R = \{[a]_R : a \in A\}$.

10.32 Exercise: List the factor set of each equivalence relation in 10.28.

10.33 Quotient Maps: Suppose that R is an equivalence relation on a set A. The **quotient map** from A to A/R is the map $\pi : A \to A/R$ given by $\pi(a) = [a]_R$.

10.34 Exercise: Suppose that R is an equivalence relation on a set A and $\pi : A \to A/R$ is the quotient map just defined. Show that for all $x, y \in A$, xRy if and only if $\pi(x) = \pi(y)$. This proves that R is the kernel of π. (Hint: You may use the theorem in 10.27.)

10.35 Partitions: A partition of a set A is a set P of nonempty subsets of A so that

- If $a \in A$, then there is a set $D \in P$ so that $a \in D$.
- If $E, F \in P$ and $E \neq F$, then $E \cap F = \emptyset$.

The elements of P are called the **partition classes** of P.

10.36 Examples: Each of the following is an example of a partition on $\{1, 2, 3, 4, 5\}$.

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

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

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

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

This is a partition of $\mathbb{N}$: $\{\{n \in \mathbb{N} : n \text{ is even}\}, \{n \in \mathbb{N} : n \text{ is odd}\}\}$.

10.37 Exercises:
10.37.1 Find all partitions on the set $\{1, 2\}$.
10.37.2 Find all partitions on the set $\{1, 2, 3\}$.

10.38 Equivalence Relations Give Partitions: Suppose R is an equivalence relation on a set A. We know that if $a \in A$, then $a \in [a]_R$. We also know that if two equivalence classes $[a]_R$ and $[b]_R$ are different, then $[a]_R \cap [b]_R = \emptyset$. These two facts give us that the set of equivalence classes of R (the factor set A/R) is a partition of A.

10.39 Partitions Give Equivalence Relations: Suppose P is a partition of a set A. Define a relation $\sim_P$ on A by $a \sim_P b$ if a and b are in the same partition class. You will have the opportunity in the next exercise to show that this relation $\sim_P$ is an equivalence relation. The equivalence classes of $\sim_P$ are precisely the partition classes of P.

10.40 Exercise: Prove that the relation $\sim_P$ defined in 10.39 is an equivalence relation.

10.41 Intersections of Equivalence Relations: Suppose R and S are equivalence relations on a set A. Since R and S are merely special subsets of $A \times A$, we can intersect them. Let $a, b \in A$. Since $(a, a) \in R$ and $(a, a) \in S$, it follows that $(a, a) \in R \cap S$, thus the relation $R \cap S$ is reflexive. Suppose that $(a, b) \in R \cap S$. This means that $(a, b) \in R$ and $(a, b) \in S$. Since R and S are symmetric, we also have $(b, a) \in R$ and $(b, a) \in S$. Thus $(b, a) \in R \cap S$. The intersection thus is also symmetric. $R \cap S$ is also transitive (this is left as an exercise). Thus, the intersection of two equivalence relations is again an equivalence relation.

10.42 Exercise: Suppose R and S are equivalence relations on a set A. Fill in the details in 10.41 and finish the proof that $R \cap S$ is an equivalence relation.

10.43 Composition of Relations: Suppose R and S are relations on a set A. The **composition** of R and S is the relation

$$R \circ S = \{(a, c) : (\exists b \in A)[(aRb) \wedge (bSc)]\}$$

For example if $R = \{(1, 2), (3, 4)\}$ and $S = \{(1, 3), (2, 4), (4, 4)\}$, then $R \circ S = \{(1, 4), (3, 4)\}$ Since $1R2$, $2S4$, $3R4$, and $4S4$.

10.44 Exercises: Compute $R \circ S$ in each of the following.
10.44.1 $R = \{(1, 2), (1, 3), (2, 3)\}$ and $S = \{(3, 4), (2, 3), (3, 3), (1, 2)\}$
10.44.2 $R = \{(1, 1), (2, 2), (3, 3)\}$ and $S = \{(3, 4), (2, 3), (3, 3), (1, 2)\}$
10.44.3 $R = \{(1, 2), (1, 1), (2, 2), (3, 3), (2, 3)\}$ and
$S = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$

10.45 Associativity of Composition: Composition of relations is associative.

Proof: Suppose R, S, and T are relations on a set A. We will show that $(R \circ S) \circ T = R \circ (S \circ T)$. Since these are sets, we merely need to show they are subsets of each other. We will first show that $(R \circ S) \circ T \subseteq R \circ (S \circ T)$. Suppose $(a, d) \in (R \circ S) \circ T$. This means there is some $c \in A$ with $(a, c) \in R \circ S$ and $(c, d) \in T$. Since $(a, c) \in R \circ S$, there is some $b \in A$ with $(a, b) \in R$ and $(b, c) \in S$. Since $(b, c) \in S$ and $(c, d) \in T$, it follows that $(b, d) \in S \circ T$. Since we also know $(a, b) \in R$, this means $(a, d) \in R \circ (S \circ T)$. Thus $(R \circ S) \circ T \subseteq R \circ (S \circ T)$.

That $R \circ (S \circ T) \subseteq (R \circ S) \circ T$ is left as an exercise. When it is completed, we will have proven that $(R \circ S) \circ T = R \circ (S \circ T)$ as desired. □

10.46 Exercises:
10.46.1 Complete the proof that composition is associative.
10.46.2 Suppose R is an equivalence relation on a set A. Show that $R \circ R = R$. (Hint: Use the fact that R is transitive)
10.46.3 Find two equivalence relations R and S on $\{1, 2, 3, 4\}$ so that $R \circ S$ is not an equivalence relation. Is it true that $R \circ S = S \circ R$?
10.46.4 Suppose R is a reflexive relation on a set A. Show that R is transitive if and only if $R \circ R = R$.

10.47 Transitive Closure: Suppose R is a relation on a set A. The **transitive closure** of R is the smallest transitive relation containing R. The transitive closure of R is precisely

$$R \cup (R \circ R) \cup (R \circ R \circ R) \cup (R \circ R \circ R \circ R) \cup (R \circ R \circ R \circ R \circ R) \cup \cdots$$

To calculate the transitive closure of a relation R, you would begin calculating $R \circ R$, $R \circ R \circ R$, and so on. At each step, you get a new set. Once the new set contains no elements which are not already in earlier sets, you may stop. The transitive closure will then be the union of the sets you have calculated.

As an example, we will calculate the transitive closure of

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

(which is a relation on $\{1, 2, 3, 4, 5\}$). We proceed:

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

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

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

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

Since all of the ordered pairs in $R \circ R \circ R \circ R$ have appeared already, we can stop. The transitive closure would be the union of these sets, which is

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

10.48 Exercises: Find the transitive closures of these relations.
10.48.1 $R = \{(1, 2), (2, 3), (3, 4), (4, 5)\}$
10.48.2 $S = \{(2, 1), (1, 3), (3, 4), (2, 5), (5, 6)\}$
10.48.3 $T = \{(1, 2), (2, 3), (3, 2)\}$

10.49 Exercise: Suppose R and S are equivalence relations on a set A and that $R \circ S = S \circ R$. Show that $R \circ S$ is an equivalence relation.

10.50 Relational Converse: The **converse** of a relation R on a set A is the set $R^{\cup} = \{(a, b) : bRa\}$. To calculate the converse of a relation, you simply reverse every ordered pair in the relation.

10.51 Exercise: Prove that a relation R on a set A is symmetric if and only if $R^{\cup} = R$.

11

Natural Numbers & Induction

11.1 Natural Numbers: The natural numbers can be constructed from a small set of axioms from which the usual properties of arithmetic can be proven. We give this axiom set here and say how the operations of addition and multiplication are defined on $\mathbb{N}$. The axioms we give provide us with one of our most powerful tools for proving theorems where the natural numbers are involved.

11.2 The Peano Axioms: The **natural numbers** are a set $\mathbb{N}$ which satisfies the following five axioms called the **Peano Axioms**[1].

P1: There is a natural number which we call 0.

P2: There is a function $s : \mathbb{N} \to \mathbb{N}$ called the **successor function**. If $n \in \mathbb{N}$, then $s(n)$ is called the **successor of** n.

P3: The number 0 is not the successor of any number (0 is not in the range of s).

P4: If n and m are numbers and $s(n) = s(m)$, then $n = m$ (s is injective).

P5: If $A \subseteq \mathbb{N}$ and these two statements are true

- $0 \in A$
- If $k \in A$, then $s(k) \in A$

Then $A = \mathbb{N}$.

From this set of axioms, we are able to define the operations addition and multiplication and derive all of the familiar properties of arithmetic. Here are **recursive** (self-referential) definitions of addition and multiplication in $\mathbb{N}$.

11.3 Addition and Multiplication: Define an operation $+$ called **addition** on $\mathbb{N}$ by

- For all $n \in \mathbb{N}$, $n + 0 = n$.
- For all $n, m \in \mathbb{N}$, $n + s(m) = s(n + m)$.

Define an operation $\cdot$ on $\mathbb{N}$ called **multiplication** by

- For all $n \in \mathbb{N}$, $n \cdot 0 = 0$.

[1] Historically, $\mathbb{N}$ was defined to "begin" with 1. As I have said before, it pains me greatly to include 0 here. However, it will make the life of the student easier.

- For all $n, m \in \mathbb{N}$, $n \cdot s(m) = (n \cdot m) + n$.

Here is an example of how to use the definitions to do arithmetic (we calculate $1 \cdot 2 = 2$).

$$\begin{aligned} s(0) \cdot s(s(0)) &= [s(0) \cdot s(0)] + s(0) \\ &= [[s(0) \cdot 0] + s(0)] + s(0) \\ &= s(0) + s(0) \\ &= s(s(0) + 0) \\ &= s(s(0)) \end{aligned}$$

We can use these definitions and the axioms to prove standard properties of addition and multiplication. This derivation is a more complicated process than we are yet ready to face. Therefore, we will acknowledge that this work has been done already by those who have come before us (this is a common practice) and return to study the derivation at a later time.

11.4 Exercises: Use the definitions of addition and multiplication to calculate

11.4.1 $s(0) + s(s(0))$

11.4.2 $s(0) \cdot s(0)$

11.4.3 $s(0) \cdot (s(0) + s(0))$

11.5 Axiom 5: The oddest of the Peano Axioms is probably the fifth. This axiom is a tool for showing that certain facts are true for all natural numbers. It is the basis of mathematical induction. We give an example here of a pure application of this axiom, and then describe the general notion of induction later.

Theorem: For any natural numbers x, y, and z, the equality $(x + y) + z = x + (y + z)$ holds.

Proof: Let $x, y \in \mathbb{N}$ and let S be the set of all $z \in \mathbb{N}$ for which $x + (y + z) = (x + y) + z$. We will use Axiom 5 to show that $S = \mathbb{N}$. First, we must show that $0 \in S$. Notice that by the definition of $+$ we have[2]

$$\begin{aligned} x + (y + 0) &= x + y \\ &= (x + y) + 0 \end{aligned}$$

so $0 \in S$. Next, assume that $z \in S$. This means that $x + (y + z) = (x + y) + z$. We will show that $s(z) \in S$. That is, we must show that $x + (y + s(z)) = (x + y) + s(z)$. Again, we need only apply the definition of $+$ several times.

$$\begin{aligned} x + (y + s(z)) &= x + s(y + z) \\ &= s(x + (y + z)) \\ &= s((x + y) + z) \\ &= (x + y) + s(z) \end{aligned}$$

[2]This is again an instance where including 0 in $\mathbb{N}$ makes life easier. The arithmetic in the first step of proofs using Axiom 5 to establish properties of addition and multiplication are often simpler with 0 than with 1.

Thus if $z \in S$, then also $s(z) \in S$. By Axiom 5, we can conclude that $S = \mathbb{N}$. It follows that for all x, y, and z in $\mathbb{N}$, $(x + y) + z = x + (y + z)$. □

11.6 Example: Here is another pure application of Axiom 5.

Theorem: Every natural number either equals 0 or is the successor of a natural number.

Discussion: Axiom 5 allows us under certain circumstances to show that a set of natural numbers is equal to all natural numbers. We first decide what our set should be. The theorem refers to the property of a number either having a successor or being equal to 0. All numbers satisfying this property will be our set. Recall that saying a natural number n is a successor means that there is a natural number m so that $n = s(m)$.

Proof: Let S be the set of all natural numbers which are either successors or which are equal to 0. Note that 0 is in S by definition. This satisfies the first requirement of Axiom 5. Next, we must show that if $k \in S$, then $s(k) \in S$. Suppose that $k \in S$. The number $s(k)$ is the successor of k. By the definition of S, $s(k) \in S$ (since $s(k)$ is a successor). Hence, if $k \in S$, then $s(k) \in S$. We have satisfied the second condition of Axiom 5. By the fifth Peano Axiom, $S = \mathbb{N}$. It follows that every natural number is either a successor or is equal to 0. □.

11.7 Principle of Mathematical Induction: Axiom 5 is the basis for mathematical induction:

Suppose $P(n)$ is an open statement about some natural number n. Let m be a natural number. If these two statements are true

- $P(m)$ is true and
- For any $k \geq m$ in $\mathbb{N}$, if $P(k)$ is true, then $P(k + 1)$ is true

then $P(n)$ is true for all n greater than or equal to m.

Theorem: For any natural number n, this equality holds

$$4 \cdot (0^3 + 1^3 + \cdots + n^3) = n^2(n + 1)^2$$

Proof: Let $P(n)$ be the open statement "$4 \cdot (0^3 + 1^3 + \cdots + n^3) = n^2(n+1)^2$." We will use induction to prove that $P(n)$ is true for all natural numbers n. First, note that $4 \cdot (0^3) = 0$ and $0^2 \cdot (0 + 1)^2 = 0$, so that $P(0)$ is true. Next, suppose that k is a natural number and that $P(k)$ is true. That is, we are assuming that

$$4 \cdot (0^3 + 1^3 + \cdots + k^3) = k^2(k + 1)^2$$

Observe that

$$\begin{aligned} 4\cdot(0^3+1^3+\cdots+k^3+(k+1)^3) &= 4\cdot(0^3+\cdots+k^3)+4(k+1)^3 \\ &= k^2(k+1)^2+4(k+1)^3 \\ &= (k+1)^2(k^2+4(k+1)) \\ &= (k+1)^2(k^2+4k+4) \\ &= (k+1)^2(k+2)^2 \\ &= (k+1)^2([k+1]+1)^2 \end{aligned}$$

Hence, $P(k+1)$ is true. We have established that $P(0)$ is true and that $P(k)$ implies $P(k+1)$. By mathematical induction, we can conclude that $P(n)$ is true for all natural numbers n. □

11.8 Example: Here is another example of proof by induction.

Theorem: For any natural number n, $4^{2n+1}+1$ is divisible by 5.

Proof: For any natural number n, let $P(n)$ be the open statement "$4^{2n+1}+1$ is divisible by 5." We will use mathematical induction to show that $P(n)$ is true for all natural numbers n. First, note that $4^{2\cdot 0+1}+1=5$ is divisible by 5, so $P(0)$ is true. Next, suppose $P(k)$ is true for some natural number k. That is, we are assuming $4^{2k+1}+1$ is divisible by 5. This means there is a natural number l so that $4^{2k+1}+1=5l$. Observe

$$\begin{aligned} 4^{2(k+1)+1}+1 &= 4^{2k+3}+1 \\ &= 4^{2k+1}4^2+1 \\ &= 4^{2k+1}\cdot 16+1 \\ &= 4^{2k+1}(3\cdot 5+1)+1 \\ &= 4^{2k+1}\cdot 3\cdot 5+4^{2k+1}+1 \\ &= 4^{2k+1}\cdot 3\cdot 5+5l \\ &= 5(4^{2k+1}\cdot 3+l) \end{aligned}$$

From the definition of divisibility, we see that 5 divides $4^{2(k+1)+1}+1$, so $P(k+1)$ is true. Thus, if $P(k)$ is true, so is $P(k+1)$. We have established that $P(0)$ is true and that $P(k)$ implies $P(k+1)$. By mathematical induction, we can conclude that $P(n)$ is true for all natural numbers n. □

11.9 Exercises: Use induction to prove the following theorems.

11.9.1 **Theorem:** For all natural numbers n, $2(0+1+\cdots+n)=n(n+1)$.

11.9.2 **Theorem:** For all natural numbers n, $6(0^2+1^2+\cdots+n^2)=n(n+1)(2n+1)$.

11.9.3 **Theorem:** $3^{2n+1}+1$ is divisible by 4 for all natural numbers n.

11.9.4 **Theorem:** For all natural numbers $n\geq 1$,

$$1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^n}=2-\frac{1}{2^n}.$$

11.9.5 Guess a formula for $1+3+\cdots+(2n+1)$ and use induction to prove that your guess is correct.
11.9.6 **Subsets:** Use induction to prove that the formula you guessed in 8.9.6 for the number of subsets of an n-element set is correct.

11.10 Divisibility and Order: The theorem in 11.6 allows us to prove this useful result which may seem obvious:

Theorem: If n and m are natural numbers with $m \neq 0$ and if $n|m$ then $n \leq m$.

Proof: Suppose that n and m are natural numbers with $m \neq 0$ and $n|m$. This means that there is some natural number k with $nk = m$. Now, by 11.6 k is either 0 or a successor. If $k = 0$, then $m = nk = n0 = 0$. Since $m \neq 0$, $k \neq 0$, and k is a successor. This means that there is some $l \in \mathbb{N}$ so that $k = l + 1$. Then

$$m = nk = n(l+1) = nl + n = n + nl.$$

Since $n + nl = m$, we have $n \leq m$. □

11.11 Well Ordering Property of $\mathbb{N}$: Peano Axiom 5 is equivalent to another property called the Well Ordering Property of $\mathbb{N}$. This is:

Well Ordering Property of $\mathbb{N}$: Every non-empty set of natural numbers has a least element.

11.12 Exercises: These exercises demonstrate the equivalence of Axiom 5 and the Well Ordering Property.
11.12.1 Assume Axiom 5 and follow these steps to prove the Well Ordering Property. Let $A \subseteq \mathbb{N}$ and suppose that A has no least element. Let $P(n)$ be the statement "The numbers 0, 1, 2, ..., n are not in A." Use induction to show this is true for all natural numbers n. Begin with the fact that if 0 were in A, then 0 would be the least element of A. This will help establish $P(0)$.
11.12.2 Now assume the Well Ordering Propery and follow these steps to prove Axiom 5. Suppose that $A \subset \mathbb{N}$ so that $0 \in A$ and so that if $k \in A$, then $k + 1 \in A$. Let $B = \mathbb{N} - A$. Suppose by way of contradiction that B is not empty. Let n be the least element of B. Since $0 \in A$, $n \neq 0$. This means that there is a natural number m so that $m + 1 = n$. Is $m \in A$?

11.13 Strong Induction: The principle of strong induction also is based on Axiom 5:

Suppose $P(n)$ is an open statement about some natural number n. Let m be a natural number. If these two statements are true

- $P(m)$ is true and

- For any $k \geq m$ in $\mathbb{N}$, if $P(m), \ldots, P(k)$ are true, then $P(k+1)$ is true

then $P(n)$ is true for all n greater than or equal to m.

11.14 Not Needed: Technically, strong induction is not needed. We can always formulate the predicate $P(n)$ in induction to accomodate the perceived need for strong induction. We did this in Exercise 11.12.1. However, some believe it is convenient to have around.

11.15 Prime Numbers: A natural number $p > 1$ is **prime** if p has no factors other than p and 1.

11.16 Prime Factors: Every natural number greater than 1 has a prime factor.

Proof: Let $P(n)$ be the open statement "n has a prime factor." We will use strong induction to prove that $P(n)$ is true for all natural numbers $n > 1$. First $P(2)$ is true because 2 is prime. Next, let $k \geq 2$ and suppose that $P(2), \ldots, P(k)$ are true. We prove that $(k+1)$ has a prime factor. There are two cases – either $(k+1)$ is prime or it is not. If $(k+1)$ is prime, then $(k+1)$ is a prime factor of itself. If $(k+1)$ is not prime, then $(k+1)$ can be expressed as a product $(k+1) = ab$ with $a \neq 1$ and $a \neq (k+1)$. Since $a|(k+1)$ and since $(k+1) \neq 0$, we know that $a \leq (k+1)$ by 11.10. Since $a \neq (k+1)$, we know that $a < (k+1)$. Thus, $1 < a < (k+1)$. Since $1 < a < (k+1)$, we know by induction that a has a prime factor p. Then $a = pm$ for some natural number m, and $n = ab = pmb$. Thus p is a prime factor of n, and $P(k+1)$ is true..

We have proven that $P(2)$ is true and that if $2 \leq k$ and $P(2), \ldots, P(k)$ are true, then so is $P(k+1)$. By strong induction, $P(n)$ is true for all natural numbers greater than 1. □

Discussion: We could have used "plain induction" on this theorem by defining the predicate $P(n)$ to be, "the natural numbers $2, \ldots, n$ all have prime factors." We will use this strategy to prove the next theorem.

11.17 Fundamental Theorem of Arithmetic: Every natural number greater than 1 is either prime or a product of primes.

Proof: Let $P(n)$ be the open statement "each natural number in $\{2, \ldots, n\}$ either prime or is a product of primes." We will use induction to prove that $P(n)$ is true for all natural numbers $n \geq 2$. First, 2 is prime, so $P(2)$ is true. Next, suppose that $k \in \mathbb{N}$ is at least 2 and that $P(k)$ is true. We will prove that $P(k+1)$ is true. We need only show that $(k+1)$ is either prime or is a product of primes. There are two cases – either $(k+1)$ is prime, or it is not. If $(k+1)$ is prime, then $P(k+1)$ is true. If $(k+1)$ is not prime, then there exist natural numbers a and b in $\{2, \ldots, k\}$ so that $(k+1) = ab$. By

induction, we know that there are primes $p_1, p_2, \ldots, p_s$ and $q_1, q_2, \ldots, q_t$ so that $a = p_1 \cdot p_2 \cdots p_s$ (if a is prime, $s = 1$) and $b = q_1 \cdot q_2 \cdots q_t$ (if b is prime, $t = 1$). But then

$$(k+1) = p_1 \cdot p_2 \cdots p_s \cdot q_1 \cdot q_2 \cdots q_t.$$

Thus $(k+1)$ is a product of primes, and $P(k+1)$ is true.

We have proven that $P(2)$ is true and that $P(k)$ implies $P(k+1)$ for any natural number $k \geq 2$. By induction $P(n)$ is true for all natural numbers $n \geq 2$. □

11.18 Binomial Coefficients: Define 0! (read as "0 factorial") to be 1. For natural numbers $n > 0$, let $n! = 1 \cdot 2 \cdot 3 \cdots n$. Define

$$\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$$

for $k = 0, 1, \ldots, n$. We will prove the following theorem in the next set of exercises.

Binomial Theorem: For any natural number $n > 0$,

$$\begin{aligned}(a+b)^n = & \left(\begin{array}{c} n \\ 0 \end{array} \right) a^n + \left(\begin{array}{c} n \\ 1 \end{array} \right) a^{n-1}b + \left(\begin{array}{c} n \\ 2 \end{array} \right) a^{n-1}b^2 + \cdots \\ & + \left(\begin{array}{c} n \\ n-1 \end{array} \right) ab^{n-1} + \left(\begin{array}{c} n \\ n \end{array} \right) b^n\end{aligned}$$

11.18.1 Show that $\left(\begin{array}{c} n \\ k \end{array} \right) + \left(\begin{array}{c} n \\ k-1 \end{array} \right) = \left(\begin{array}{c} n+1 \\ k \end{array} \right)$.

11.18.2 Use the previous exercise and induction to prove the Binomial Theorem.

11.19 Exercises: Prove the following by induction.

11.19.1 Prove that $n^2 \geq n + 1$ for all natural numbers $n \geq 2$.

11.19.2 Prove that $n! \geq n^2$ for all natural numbers $n \geq 4$.

11.19.3 Decide for which $n \in \mathbb{N}$ the inequality $2^n \geq n^2$ is true and prove it.

11.19.4 Decide for which $n \in \mathbb{N}$ the inequality $n! \geq 2^n$ is true and prove it.

11.20 Divisors of Zero: Our definitions for addition and multiplication allow us to very quickly prove one of the simplest yet most important facts about our system of arithmetic. This fact is the basis for how students are taught to solve equations and inequalities in algebra classes. It is the basis for how functions are analyzed through their derivatives in calculus. The importance of this fact for calculus and algebra cannot be over-stated. Calculus and algebra are the basis for much of the mathematics behind science and technology. Science and technology, in turn, have had far-reaching effects on the development of society. It is safe to say that without this next fact, our

very culture would be different.

Theorem:[3] If a and b are natural numbers and if $ab = 0$, then either $a = 0$ or $b = 0$.

Proof: We prove this theorem using the contrapositive. Suppose that a and b are both non-zero. This means that each of them is a successor, so there exist natural numbers m and n with $s(m) = a$ and $s(n) = b$. Then

$$ab = s(m) \cdot s(n) = (s(m) \cdot n) + s(m) = s((s(m) + n) + m).$$

Since ab is a successor, $ab \neq 0$ by axiom P3.

We have proven that if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. By the contrapositive, if $ab = 0$, then $a = 0$ or $b = 0$. □

[3]This, again, is an instance of where including 0 in $\mathbb{N}$ allows us an easily accessible proof that would normally be complicated by derivations of number systems higher than $\mathbb{N}$.

12

The Integers

12.1 Integers: The integers are the set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$. A rigorous derivation of the integers from $\mathbb{N}$ could realize each integer as a difference of natural numbers. Such a derivation would define addition, multiplication, and order on $\mathbb{Z}$ based on definitions and facts from $\mathbb{N}$. Using theorems about $\mathbb{N}$, one could then prove the "usual" properties of arithmetic in $\mathbb{Z}$. These properties would include such things as:

Properties of Addition:

$x + (y + z) = (x + y) + z$	associative law
$x + y = y + x$	commutative law
$y + x = z + x$ if and only if $y = z$	cancellation law
$x + 0 = 0 + x = x$	additive identity
$x \cdot 0 = 0 \cdot x = 0$	absorption law
For any $x \in \mathbb{Z}$, there is an integer $-x$ so that $x + (-x) = 0$	additive inverses.

Properties of Multiplication:

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	associative law
$x \cdot y = y \cdot x$	commutative law
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	distributive law
$x \cdot 1 = 1 \cdot x = x$	multiplicative identity
If $x \neq 0$ then $y \cdot x = z \cdot x$ iff $y = z$	cancellation law
$xy = 0$ if and only if $x = 0$ or $y = 0$	zero divisors

Properties of $\leq$:

For all $x, y \in \mathbb{Z}$, either $x \leq y$ or $y \leq x$	dichotomy
$x \leq x$	reflexivity
If $x \leq y$ and $y \leq x$, then $x = y$	antisymmetry
If $x \leq y$ and $y \leq z$ then $x \leq z$	transitivity
$x \leq y$ if and only if $x + z \leq y + z$	
If $z > 0$, then $x \leq y$ if and only if $xz \leq yz$	
If $z < 0$, then $x \leq y$ if and only if $yz \leq xz$	
$0 \leq x$ if and only if $-x \leq 0$	

12.2 Positive vs. Negative: An integer n is **positive** if $0 < n$. An integer n is **negative** if $n < 0$.

12.3 Subtraction: We will use the short hand notation $x - y$ to mean $x + (-y)$.

12.4 Even and Odd: We can define even and odd for integers in the same manner that we did for natural numbers. An integer n is **even** if there is an integer k so that $n = 2k$. An integer n is odd if there is an integer k so that $n = 2k + 1$.

12.5 Exercises:
12.5.1 Prove that an integer n is odd if and only if there is an integer k so that $n = 2k - 1$.
12.5.2 Prove that an integer n is even if and only if $n - 1$ is odd.

12.6 Induction: Mathematical induction can be extended from the natural numbers to the set of integers in the following way.
Let $P(n)$ be an open statement about integers and let m be any integer. If these two statements are true

- $P(m)$ is true.
- For any integer $k \geq m$, if $P(k)$ is true, then so is $P(k + 1)$

then $P(n)$ is true for integers $n \geq m$.

12.7 Exercises: Prove the following by induction.
12.7.1 For any integer $n \geq 5$, $n^2 + 15n + 50 \geq 0$.
12.7.2 For any integer $n \leq -10$, $n^2 + 15n + 50 \geq 0$. (Hint: Let $P(n)$ be "$(-n)^2 + 15(-n) + 50 \geq 0$" and prove that $P(n)$ is true for all $n \geq 10$.)

12.8 Exercises: Let $P(n)$ be the statement "$n^2 + n + 1$ is even."
12.8.1 Let $k \in \mathbb{Z}$ and suppose that $P(k)$ is true. Prove that $P(k + 1)$ is true.
12.8.2 For which $n \in \mathbb{Z}$ is $P(n)$ true? (If you have no idea, test several values of n.)
12.8.3 What is the moral?

12.9 The Division Algorithm: Suppose that n is any integer and m is a positive integer (natural number). There are integers q and r so that $0 \leq r < m$ and $n = mq + r$.

12.10 Examples: We will prove the division algorithm in a moment, but first we look at a few examples. The "algorithm" is really no algorithm at all. It tells us that we can find two special integers. It does not tell us how

to find them. Examples of the algorithm include

$$\begin{array}{rcrrcr} n & = & m & q & + & r \\ 17 & = & 5 & 3 & + & 2 \\ 121 & = & 10 & 12 & + & 1 \\ 75 & = & 2 & 37 & + & 1 \\ 30 & = & 5 & 6 & + & 0 \\ 56 & = & 1 & 56 & + & 0 \\ -17 & = & 5 & (-4) & + & 3 \\ -12 & = & 7 & (-2) & + & 2 \\ -39 & = & 4 & (-10) & + & 1 \end{array}$$

We will call the q from the division algorithm the **quotient**. We will call the r the **remainder**. Pay careful attention to the examples where n is negative. In the last example, we might be tempted to say that the quotient ought to be -9 and the remainder -3. However, we always want a positive remainder, and mq must always be less than or equal to n.

12.11 Proof of the Division Algorithm: Let m be a natural number. Let $P(n)$ be the open statement "There are integers q and r so that $0 \leq r < m$ and $n = mq+r$." We will first use mathematical induction to prove that $P(n)$ is true for all integers $n \geq 0$. Note that if $q = 0$ and $r = 0$ then $0 \leq r < m$ and $0 = mq + r$, so $P(0)$ is true.

Next, suppose that $k \geq 0$ is an integer and that $P(k)$ is true. We will prove that $P(k + 1)$ is true. Since $P(k)$ is true, there are integers q' and r' so that $0 \leq r' < m$ and $k = mq' + r'$. There are two cases to consider. Either $r' = m - 1$, or $r' < m - 1$. If $r' = m - 1$, then let $q = q' + 1$ and $r = 0$. Then it follows that $0 \leq r < m$ and

$$mq + r = m(q' + 1) = mq' + m = mq' + (m - 1) + 1 = mq' + r' + 1 = k + 1$$

so $P(k+1)$ would be true. If $r' < m-1$, then let $q = q'$ and $r = r'+1$. Then $0 \leq r < m$ and

$$mq + r = mq' + r' + 1 = k + 1$$

so $P(k+1)$ is true. In either case, $P(k+1)$ is true. Thus, we have established that $P(k)$ implies $P(k + 1)$. By mathematical induction, $P(n)$ is true for all integers $n \geq 0$.

We next show that $P(n)$ is true for all negative integers n. (We do not use induction here.) Suppose that $n < 0$. We know from above that $P(-n)$ is true, so there are integers q' and r' so that $-n = mq' + r'$. It follows that $n = m(-q') + (-r')$. If $r' = 0$, the let $q = -q'$ and let $r = 0 = -r'$. Then, $0 \leq r < m$ and

$$mq + r = m(-q') + (-r') = n$$

as desired. On the other hand, if $r' > 0$ then let $q = -q' - 1$ and let $r = m - r'$. Then $0 \leq r < m$ and

$$mq + r = m(-q' - 1) + (m - r') = m(-q') - m + m - r' = m(-q') + (-r') = n.$$

Thus in either case we can find integers q and r so that $0 \leq r < m$ and $n = mq + r$. Hence, $P(n)$ is also true for $n < 0$.

Putting both halves of our proof together, we see that if n is any integer, then there are integers q and r so that $n = mq + r$. □

12.12 Exercises: For each of the following pairs of numbers n and m find the integers q and r guaranteed by the division algorithm.

12.12.1 $n = 64$ and $m = 3$
12.12.2 $n = 43$ and $m = 7$
12.12.3 $n = -43$ and $m = 7$
12.12.4 $n = -64$ and $m = 3$
12.12.5 $n = 87$ and $m = 2$
12.12.6 $n = 88$ and $m = 1$

12.13 Divisibility: We can define a divisibility relation on the integers just like we did for natural numbers. An integer n is said to **divide** an integer m if there is an integer k so that $nk = m$. This is denoted as $n|m$.

12.14 Greatest Common Divisor: Suppose that m and n are positive integers. The **greatest common divisor** of m and n is the largest positive integer d for which $d|m$ and $d|n$. We denote the greatest common divisor of m and n as $\gcd(m, n)$.

12.15 Exercise: Suppose that $m = nq + r$ as in the Division Algorithm and that $d \in \mathbb{Z}$. Prove that d divides m and n if and only if d divides n and r.

12.16 Euclidean Algorithm: The previous exercise gives a means of finding the greatest common divisor of two positive integers. Suppose that $n < m$ are positive integers. Apply the Division Algorithm to find q_1 and r_1 so that $m = nq_1 + r_1$ and $0 \leq r_1 < n$. By the previous exercise, the set of common divisors of m and n is the same as the set of common divisors of n and r_1, so $\gcd(m, n) = \gcd(n, r_1)$. Apply the Division Algorithm again to find q_2 and r_2 so that $n = r_1 q_2 + r_2$ and $0 \leq r_1 < r_2$. Again, $\gcd(m, n) = \gcd(n, r_1) = \gcd(r_1, r_2)$. We can continue this process indefinitely to construct a decreasing sequence of remainders $n > r_1 > r_2 > \cdots \geq 0$ so that we always have $\gcd(m, n) = \gcd(r_s, r_{s+1})$. Since the positive remainders must decrease, eventually, there is some k so that $r_{k+1} = 0$. But this means that $r_{k-1} = r_k q + 0$ so $r_k | r_{k-1}$. Since $r_k | r_{k-1}$, it follows that $\gcd(m, n) = \gcd(r_{k-1}, r_k) = r_k$. The final nonzero remainder after repeated divisions is the greatest common divisor.

12.17 Example: We find $\gcd(28, 36)$. Since $36 > 28$, we divide 36 by 28 to find

$$36 = 28 \cdot 1 + 8.$$

We now divide 28 by 8 to get

$$28 = 8 \cdot 3 + 4.$$

When we divide 8 by 4 we get

$$8 = 4\dot{2} + 0.$$

Since this last remainder is 0, we are done. The greatest common divisor is the last nonzero remainder: $\gcd(28, 36) = 4$.

12.18 Exercises: Apply the Euclidean Algorithm to find the greatest common divisor of these pairs of numbers.

12.18.1 12 and 18
12.18.2 25 and 90
12.18.3 30 and 128
12.18.4 49 and 75
12.18.5 243 and 1024

12.19 Linear Combinations: Induction on the number of steps it takes to complete the Euclidean Algorithm can be used to prove this theorem:

Theorem: Suppose that m and n are positive integers. There are integers a and b so that $am + bn = \gcd(m, n)$.

12.20 Linear Combinations: Expressions of the form $am + bn$ as in this theorem are called **linear combinations** of m and n. If a and b are integers, then $am + bn$ is an **integer linear combination** of m and n.

12.21 Example: Rather than proving this theorem, we give an example. We find $\gcd(25, 34)$ and express it as a linear combination of 25 and 34. First, we divide repeatedly until we have a remainder of 0:

$$34 = 25 \cdot 1 + 9$$

$$25 = 9 \cdot 2 + 7$$

$$9 = 7 \cdot 1 + 2$$

$$7 = 2 \cdot 3 + 1$$

$$2 = 1 \cdot 2 + 0$$

We see that $\gcd(25, 34) = 1$. We now want to express 1 as a linear combination of 25 and 34. Next, we solve each of these equations except the last for the remainder:

$$9 = 34 - 25$$

$$7 = 25 - 2 \cdot 9$$

$$2 = 9 - 7$$

$$1 = 7 - 3 \cdot 2$$

Notice that the first equation expresses 9 as a linear combination of 34 and 25. The second expresses 7 as a linear combination of 25 and 9. Substituting the first into the second will give 7 as a linear combination of 34 and 25. Substituting gives:

$$7 = 25 - 2 \cdot (34 - 25).$$

Collecting like terms gives 7 as a linear combination of 34 and 25:

$$7 = -2 \cdot 34 + 3 \cdot 25.$$

We can now substitute this equation and the first equation into the third to get

$$2 = (34 - 25) - (-2 \cdot 34 + 3 \cdot 25).$$

Collecting like terms gives 2 as a linear combination of 34 and 25:

$$2 = 3 \cdot 34 - 4 \cdot 25.$$

Finally, substituting our combinations for 2 and 7 into the last equation gives:

$$1 = (-2 \cdot 34 + 3 \cdot 25) - 3(3 \cdot 34 - 4 \cdot 25).$$

Collecting like terms gives 1 as a linear combination of 34 and 25:

$$1 = -11 \cdot 34 + 15 \cdot 25.$$

12.22 Exercises: Express the greatest common divisor of each pair of integers in 12.18 as a linear combination of the pair of integers.

12.23 Primes: Recall that a natural number greater than 1 is prime if its only natural number divisors are itself and 1. Theorem 12.19 can be used to prove this theorem about primes:

Theorem: Suppose that p is a prime and that $a, b \in \mathbb{Z}$ so that $p|ab$. Then either $p|a$ or $p|b$.

Proof: We will assume that a and b are positive. Suppose that p is prime and that $p|ab$. We will prove that $p|a$ or $p|b$. To do so, suppose that p does not divide a. We must show that $p|b$. (This is an application of the method of disjunction proof from chapter 5.) Since p does not divide a, and since p is prime, $\gcd(p, a) = 1$. By 12.19 there are integers x and y so that $1 = xp + ya$. Multiplying this by b gives $b = bxp + yab$. Since $p|ab$, there is an integer k so that $pk = ab$. If we substitute this into $b = bxp + yab$, we have $b = bxp + ypk$. Factoring out a p gives $b = p(bx + yk)$, so $p|b$. If $p \not| a$, then $p|b$. It follows that either $p|a$ or $p|b$. □

12.24 Modular Congruence: Let n be a positive integer. Define a relation $\equiv_n$ called **equivalence modulo** n on $\mathbb{Z}$ so that $a \equiv_n b$ if $n|(a-b)$. The relation $a \equiv_n b$ can be read as "a is equivalent to b modulo n" or as "a is equivalent to b mod n." Sometimes, this is written as $a = b(\text{mod } n)$, but we reserve this notation for a slightly different concept below.

12.25 Examples: Here are some examples of modular equivalence:

$$\begin{array}{ll} 23 \equiv_5 88 & \text{since } 5|(23-88) \\ -1 \equiv_4 3 & \text{since } 4|(-1-3) \\ 49 \equiv_7 0 & \text{since } 7|(49-0) \end{array}$$

12.26 Exercises: Let n be any positive integer.
12.26.1 Prove that $\equiv_n$ is reflexive.
12.26.2 Prove that $\equiv_n$ is symmetric. (Hint: $(a-b) = -(b-a)$)
12.26.3 Prove that $\equiv_n$ is transitive. (Hint: If $n|x$ and $n|y$, then $n|(x+y)$. The proof of this for integers is similar to the one for natural numbers.)
12.26.4 Let k be any integer. Let q and r be the integers guaranteed by the division algorithm so that $k = nq + r$. Prove that $k \equiv_n r$

12.27 Equivalence Classes: Suppose that R is an equivalence relation on a set A and that $a \in A$. Recall that the equivalence class of a modulo R is the set $[a]_R = \{x \in A : aRx\}$.

12.28 Residue Classes: From the previous exercises, we see that $\equiv_n$ is always an equivalence relation. The equivalence classes of $\equiv_n$ are usually called **residue classes modulo** n. We can denote the residue class of an integer m modulo n as $[m]_n$. When n is understood, we will simply write $[m]$. There are precisely n residue classes modulo n. They are $[0], [1], [2], \ldots, [n-1]$. These are the equivalence classes of the possible remainders from the division algorithm (hence the name *residue*). For example

$$\begin{array}{ll} \text{The residue classes of 3 are} & [0]_3, [1]_3, [2]_3 \\ \text{The residue classes of 5 are} & [0]_5, [1]_5, [2]_5, [3]_5, [4]_5 \\ \text{The residue classes of 7 are} & [0]_7, [1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7 \end{array}$$

We will denote the set of residue classes modulo n as $\mathbb{Z}_n$. That is

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

12.29 Least Residue: Suppose n is a positive integer and m is any integer. The division algorithm guarantees a q and r so that $0 \leq r < n$ and $m = nq + r$. The remainder r is called the **least residue of** m **modulo** n. This remainder is the smallest positive integer in the residue class $[m]_n$ (hence the name least residue). We will denote the least residue of m modulo n as $m(\text{mod } n)$. For example $12(\text{mod } 5) = 2$, $17(\text{mod } 4) = 1$, and $-1(\text{mod } 26) = 25$.

12.30 Exercises: Calculate $m(\text{mod } n)$.

12.30.1 $m = 56$ and $n = 9$
12.30.2 $m = -73$ and $n = 6$
12.30.3 $m = -89$ and $n = 3$
12.30.4 $m = 24$ and $n = 13$
12.30.5 $m = 95$ and $n = 14$

12.31 Exercises: Suppose that n is a positive integer and that $a, b \in \mathbb{Z}$. In these exercises, we prove that $a \equiv_n b$ if and only if $a(\text{mod } n) = b(\text{mod } n)$.
12.31.1 Suppose that $a(\text{mod } n) = b(\text{mod } n)$. Prove that $a \equiv_n b$. Hints: Use the Division Algorithm to express $a = nq_a + r_a$ and $b = nq_b + r_b$. What is the relationship between $a(\text{mod } n)$ and q_a? What about b? Now apply 12.26.4 and transitivity.
12.31.2 Suppose that $a \equiv_n b$. Prove that $a(\text{mod } n) = b(\text{mod } n)$. Follow the same hints as the previous exercise.

12.32 Even vs. Odd The division algorithm and modular congruence give us the tools we need to prove that every integer is either even or odd but not both as in Theorem 7.16. We need a couple lemmas to prove this.

12.33 Lemma: An integer n is even if and only if $n \equiv_2 0$.

Proof: Suppose that n is even. This means that there is an integer k with $n = 2k$. It follows that $2k = (n - 0)$ so that $2|(n - 0)$ and $n \equiv_2 0$.

Now suppose that $n \equiv_2 0$. This means that $2|(n - 0)$ so there exists $k \in \mathbb{Z}$ so that $2k = (n - 0)$. But then $2k = n$, so n is even. □

12.34 Exercise: Mimic the previous proof to prove:

Lemma: An integer n is odd if and only if $n \equiv_2 1$.

12.35 Theorem: Every integer is either even or odd but not both.

Proof: Let n be an integer. Apply the division algorithm to express $n = 2q+r$ with $0 \leq r < 2$. Since $0 \leq r < 2$, we know that r is either 0 or 1. If $r = 0$, then by 12.26.4 $n \equiv_2 0$. By 12.33, n is even. On the other hand, if $r = 1$, then by 12.26.4 $n \equiv_2 1$. By 12.34, n is odd. Thus, we have proven that n is either even or odd.

Now we prove that n is not both even and odd. Suppose by way of contradiction that n is both even and odd. By 12.33 and 12.34, we know that $0 \equiv_2 n \equiv_2 1$. But then $0 \equiv_2 1$. This means that $2|(1 - 0)$, so $2|1$. This is a contradiction, so n cannot be both even and odd. □

12.36 Exercise: Prove that it is not the case that $2|1$.

12.37 Exercises: As in 7.22, define the following notions for an integer n:

- n is **red** if there is an integer k with $n = 3k$.
- n is **white** if there is an integer k with $n = 3k + 1$.
- n is **blue** if there is an integer k with $n = 3k + 2$.

Mimic the arguments above to prove:

12.37.1 An integer n is red if and only if $n \equiv_3 0$.
12.37.2 An integer n is white if and only if $n \equiv_3 1$.
12.37.3 An integer n is blue if and only if $n \equiv_3 2$.
12.37.4 Every integer is red, white, or blue.
12.37.5 No integer is both red and white.
12.37.6 No integer is both red and blue.
12.37.7 No integer is blue red and white.

12.38 Exercises: Suppose that $a \equiv_n a'$ and $b \equiv_n b'$

12.38.1 Prove that $a + b \equiv a' + b'$
12.38.2 Prove that $ab \equiv a'b'$
12.38.3 Prove that $-a \equiv -a'$

12.39 Arithmetic and Modular Congruence: What this means that that we can perform arithmetic operations and then "mod" by n or we can mod first, then perform the arithmetic, and then mod again. We will always end up in the same place.

12.40 Modular Operations: Let n be a positive integer. Define operations $+$ (addition), $\cdot$ (multiplication), and $-$ (negation) on $\mathbb{Z}_n$ (the residue classes of $\mathbb{Z}$ mod n) by

$$[a] + [b] = [a + b] \text{ and } [a] \cdot [b] = [a \cdot b] \text{ and } -[a] = [-a].$$

12.41 Note: There is no obvious reason that these operations should be well defined. That is, if $a \equiv_n a'$ and $b \equiv_n b'$, we would have $[a] = [a']$ and $[b] = [b']$, so we would need to have $[a + b] = [a' + b']$. This – and the same conditions for multiplication and negation – is the point of the previous exercises.

12.42 Examples: Here are some examples of arithmetic using the operations just defined. In each example, we write the "answer" by referring to the residue class **using the least residue**. This is typical.

$$[2]_5 + [4]_5 = [6]_5 = [1]_5$$
$$([4]_9 \cdot [3]_9) + [5]_9 = [12]_9 + [5]_9 = [17]_9 = [8]_9$$
$$(-[6]_{10}) + [5]_{10} = [-6]_{10} + [5]_{10} = [-6 + 5]_{10} = [-1]_{10} = [9]_{10}$$
$$[4]_{16} \cdot [4]_{16} = [16]_{16} = [0]_{16}$$

12.43 Notation: Often it is necessary to do modular arithmetic when we are focused on $\mathbb{Z}$ rather than on $\mathbb{Z}_n$. This introduces a variety of notations for the arithmetic we are doing. An equation such as

$$([4]_9 \cdot [3]_9) + [5]_9 = [8]_9$$

can also be expressed as

$$(4 \cdot 3) + 5 \equiv_9 8$$

or

$$(4 \cdot 3) + 5 = 8 (\text{mod } 9).$$

We will do our arithmetic in $\mathbb{Z}_n$.

12.44 Exercises: Perform the indicated operations:
12.44.1 $[4]_9 + [7]_9$
12.44.2 $([3]_{12} \cdot [7]_{12}) + [11]_{12}$
12.44.3 $([4]_4 \cdot [4]_4) + [4]_4$

12.45 Identities in $\mathbb{Z}_n$: Many of the identities which hold for addition, multiplication, and negation in the integers hold also in $\mathbb{Z}_n$. For example

Theorem: Suppose that n is a positive integer. Addition in $\mathbb{Z}_n$ is associative.

Proof: Suppose n is a positive integer. We will prove that addition in $\mathbb{Z}_n$ is associative. Let $[x], [y]$, and $[z]$ be in $\mathbb{Z}_n$. Then notice

$$\begin{aligned} ([x] + [y]) + [z] &= [x + y] + [z] \\ &= [(x + y) + z] \\ &= [x + (y + z)] \\ &= [x] + [y + z] \\ &= [x] + ([y] + [z]) \end{aligned}$$

where the third equality follows from associativity of addition in the integers. □

12.46 Exercises: Let n be a positive integer.
12.46.1 Prove that multiplication in $\mathbb{Z}_n$ is associative.
12.46.2 Prove that addition and multiplication in $\mathbb{Z}_n$ are commutative.
12.46.3 Prove that if $[a], [b], [c] \in \mathbb{Z}_n$ then $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$.
12.46.4 Prove that if $[x] \in \mathbb{Z}_n$ then there is some $[y] \in \mathbb{Z}_n$ so that $[x]+[y] = 0$. (Hint: $[n - x]$)
12.46.5 Prove that if $[x] \in \mathbb{Z}_n$ then $[0] + [x] = [x]$.
12.46.6 Prove that if $[x] \in \mathbb{Z}_n$ then $[1] \cdot [x] = [x]$.
12.46.7 Prove that if $[x] \in \mathbb{Z}_n$ then $[0] \cdot [x] = [0]$.

12.47 Zero Divisors: With integers, if $xy = 0$ then either $x = 0$ or $y = 0$. This is not the case in all of the $\mathbb{Z}_n$. For example, $[2]_6 \cdot [3]_6 = [0]_6$. Let n be a positive integer. An element $[x]$ of $\mathbb{Z}_n$ other than $[0]$ is called a 0**-divisor** if there is a non-zero element $[y]$ of $\mathbb{Z}_n$ so that $[x][y] = [0]$.

12.48 Exercises: Use trial and error to solve these exercises.
12.48.1 Find all of the 0-divisors in $\mathbb{Z}_6$.
12.48.2 Find all of the 0-divisors in $\mathbb{Z}_{12}$.
12.48.3 Find all of the 0-divisors in $\mathbb{Z}_{16}$.
12.48.4 Find all of the 0-divisors in $\mathbb{Z}_3$.
12.48.5 Find all of the 0-divisors in $\mathbb{Z}_5$.
12.48.6 Find all of the 0-divisors in $\mathbb{Z}_{13}$.
12.48.7 Make a conjecture as to which $\mathbb{Z}_n$ have zero divisors.

12.49 Exercise: Prove that if a positive integer n is not prime, then $\mathbb{Z}_n$ contains zero divisors.

12.50 Solving Equations: The lack of zero divisors in the integers plays an important role in solving equations. To see this, let's solve the equation $n^2+3n+2=0$. To solve this, we first factor the left hand side of the equation to get the equivalent equation $(n+1)(n+2)=0$. We now have two numbers $(n+1)$ and $(n+2)$ whose product is 0. This means that either $n+1=0$ or $n+2=0$, which, in turn, implies that $n=-1$ or $n=-2$. Let us now solve this equation in $\mathbb{Z}_6$. First, we have to adjust our notation. We actually find the solutions to $n^2+[3]\cdot n+[2]=[0]$. Since there are only six elements of $\mathbb{Z}_6$, we can try them all and see which ones work.

$$\begin{array}{rl}
[0]\cdot[0]+[3]\cdot[0]+[2]=[2] & \text{not a solution}\\
[1]\cdot[1]+[3]\cdot[1]+[2]=[0] & \text{a solution}\\
[2]\cdot[2]+[3]\cdot[2]+[2]=[0] & \text{a solution}\\
[3]\cdot[3]+[3]\cdot[3]+[2]=[2] & \text{not a solution}\\
[4]\cdot[4]+[3]\cdot[4]+[2]=[0] & \text{a solution}\\
[5]\cdot[5]+[3]\cdot[5]+[2]=[0] & \text{a solution}
\end{array}$$

Thus, in $\mathbb{Z}_6$, our equation has four solutions - $[1], [2], [4]$, and $[5]$.

12.51 Exercises: Use trial and error to solve these exercises.
12.51.1 Consider the equation $2x=1$. Find all solutions (if any) to this equation in $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_{10}$. What conditions should be placed on n so that this equation has a solution in $\mathbb{Z}_n$. (Notice that this equation does not have a solution in $\mathbb{Z}$.)
12.51.2 The equation $x^2+1=0$ does not have a solution in $\mathbb{Z}$. Find an n so that there is a solution in $\mathbb{Z}_n$.
12.51.3 Find all solutions to the equation $x^3=x$ in $\mathbb{Z}_3$, $\mathbb{Z}_5$, and $\mathbb{Z}_{12}$.

12.52 Multiplicative Inverses: Let n be a positive integer, and let $[m], [k] \in \mathbb{Z}_n$. Then $[m]$ and $[k]$ are **multiplicative inverses** if $[m][k]=[1]$. For example, in $\mathbb{Z}_5$, $[3][2]=[1]$, so $[2]$ and $[3]$ are multiplicative inverses. Note that the only integers with multiplicative inverses are 1 and -1.

12.53 Exercises:
12.53.1 By trial and error, find all elements of $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_7$, and $\mathbb{Z}_9$ which have multiplicative inverses.

12.53.2 For which n does it seem like every element of $\mathbb{Z}_n$ has a multiplicative inverse?
12.53.3 Can [0] ever have a multiplicative inverse?

12.54 Absolute Values: If n is an integer then the absolute value of n is

$$|n| = \begin{cases} n & 0 \leq n \\ -n & n < 0 \end{cases}$$

Proofs involving absolute values often require cases. For example:

Theorem: Suppose a and b are integers. If $|a| \leq b$, then $-b \leq a \leq b$.

Proof: Suppose that a and b are integers and that $|a| \leq b$. We will prove that $-b \leq a \leq b$. We will proceed by cases as to whether $a \geq 0$ or $a < 0$.

First, suppose that $a \geq 0$. Then $|a| = a$, so $a = |a| \leq b$. This means that $a \leq b$ and that $-a \geq -b$. Also, $-a \leq 0 \leq a$. Putting these inequalities all together gives

$$-b \leq -a \leq 0 \leq a \leq b.$$

This implies $-b \leq a \leq b$ as desired.

Next, suppose that $a < 0$. Then $|a| = -a$, so we have $-a = |a| \leq b$. This implies $-a \leq b$ and $-b \leq a$. Also, $a \leq 0 \leq -a$. Putting these inequalities all together gives

$$-b \leq a \leq 0 \leq -a \leq b.$$

This implies $-b \leq a \leq b$ as desired.

In both cases, we have $-b \leq a \leq b$. □

12.55 Exercises: Suppose that a and b are integers. Prove the following.
12.55.1 $-b \leq a \leq b$ if and only if $|a| \leq b$.
12.55.2 $|a - b| = |b - a|$
12.55.3 $|ab| = |a||b|$ (Four cases!)
12.55.4 **Triangle Inequality:** $|a + b| \leq |a| + |b|$

13

Sequences and Recursion

13.1 Sequences: A **sequence** is a function whose domain is a set of the form

$$\{m, m+1, m+2, \ldots\}$$

where $m \in \mathbb{Z}$. The most common domain for sequences is $\mathbb{N}$. We will often make comments about sequences assuming this is the domain. These comments usually refer to all sequences.

A **sequence of real numbers** is a sequence whose codomain is $\mathbb{R}$. You can think of a sequence $f : \mathbb{N} \to \mathbb{R}$ as a list of numbers

$$\langle f(0), f(1), f(2), f(3), f(4), \ldots \rangle.$$

The number $f(n)$ is refered to as the n^{th} **element** or n^{th} **term** of the sequence. It is customary to write the n^{th} element of a sequence f as f_n rather than $f(n)$. Hence a sequence looks like a list $\langle f_1, f_2, f_3, f_4, \ldots \rangle$. Often, we will list the elements of a sequence without explicitly referring to the domain of the sequence. For example, here is a sequence

$$f = \left\langle 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots \right\rangle$$

13.2 Formulas for Sequences: Sometimes, we have formulas which tell us the n^{th} term of a sequence. For example, if s is the sequence given by $s_n = \dfrac{n+1}{n}$. The terms of s would look like $\left\langle \dfrac{2}{1}, \dfrac{3}{2}, \dfrac{4}{3}, \dfrac{5}{4}, \ldots \right\rangle$. If a is the sequence given by $a_n = (-1)^n$ then the terms of a would look like $\langle -1, 1, -1, 1, -1, 1, \ldots \rangle$.

13.3 Exercises: List the first seven terms of each sequence.

13.3.1 $a_n = \dfrac{n^2 + n}{2}$

13.3.2 $b_n = \dfrac{(-1)^n}{n^2}$

13.3.3 $c_n = (-n)^2$

13.3.4 $d_n = n^2 \cos(n\pi)$

13.4 Limits: Consider the sequence s given by $s_n = \dfrac{1}{n}$. The terms of this sequence look like

$$\left\langle 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots \right\rangle$$

The terms s_n seem to get *close* to 0 as n gets larger. In this case, we would say that the **limit** of the sequence s is 0 and that the sequence **converges** to 0.

13.5 Exercise: Which of the sequences in Exercises 13.3 appear to converge?

13.6 Not All Sequences Converge: Not every sequence converges. This sequence $\langle 1, -1, 1, -1, 1, -1, \ldots \rangle$ does not converge. The terms of this sequence do not get arbitrarily close to any single number.

13.7 Recursive Definitions: Consider the sequence

$$s = \langle 1, 3, 7, 15, 31, 63, \ldots \rangle.$$

There is no clear formula for the n^{th} term of this sequence, however, if we know a term s_n, it is easy to find s_{n+1} – just double s_n and add 1. We can actually use this information to describe the sequence. The sequence s is the sequence for which

$$s_0 = 1 \text{ and}$$

$$s_{n+1} = 2s_n + 1 \text{ for all } n \in \mathbb{N}.$$

A self-referential definition such as this is called a **recursive definition**. This definition tells us that $s_0 = 1$. To find s_1, we let $n = 0$ in the recursive formula $s_{n+1} = 2s_n + 1$ to get that $s_1 = 2s_0 + 1 = 3$. To find s_2, we would let $n = 1$ in the formula. In this manner, we can build our way up to any s_n.

Consider next the recursively defined sequence r given by $r_1 = 1$ and $r_{n+1} = (n+1) \cdot r_n$. Using this definition, we can calculate:

$$\begin{array}{lcll} r_1 & = & 1 & \text{given} \\ r_2 & = & 2 \cdot r_1 = 2 & \\ r_3 & = & 3 \cdot r_2 = 6 & \\ r_4 & = & 4 \cdot r_3 = 24 & \\ & \vdots & & \end{array}$$

In this way, we can again calculate each term of the sequence. Notice that the definition of r is slightly more complicated than the definition of s. The definition of s_{n+1} depended only on s_n, but the definition of r_{n+1} depends on

both r_n and n.

Next consider the sequence t defined by $t_1 = 2$, $t_2 = 10$, and

$$t_{n+2} = n \cdot (t_{n+1} - t_n).$$

This definition is even more complicated. First, we are given two initial values of the sequence. Next, the definition of t_{n+2} is made in terms of n, t_n and t_{n+1}. The terms of this sequence would be $\langle 2, 10, 8, -4, -36, \ldots \rangle$.

13.8 Exercises: List the first six terms of each recursively defined sequence.

13.8.1 $s_1 = 0$, $s_{n+1} = (s_n)^2 + 1$

13.8.2 $s_1 = 1$, $s_2 = 1$, $s_{n+2} = s_n + s_{n+1}$

13.8.3 $s_1 = \dfrac{1}{2}$, $s_{n+1} = \left(\dfrac{1}{2^n}\right) s_n$

13.9 Exercises: Find recursive definitions for each of these sequences.

13.9.1 f is the sequence so that $f_n = n!$ (recall $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$)

13.9.2 s is the sequence $\langle 1, 2, 4, 8, 16, 32, \ldots \rangle$

13.9.3 s is the sequence $\langle 1, 1, 2, 2, 3, 3, 4, 4, \ldots \rangle$ (Hint: Define s_{n+2} in terms of s_n)

13.10 Formulas for Recursively Defined Sequences: Sometimes, we can find a formula for the n^{th} term of a recursively defined sequence. Generally, this is quite difficult. Usually, once a formula is found, an induction argument can be used to prove that it is the correct formula. For example

Theorem: Suppose s is the sequence defined by $s_1 = 1$ and $s_{n+1} = (n+1) \cdot s_n$ for all natural numbers n. Then for each $n \in \mathbb{N}$, $s_n = n!$.

Proof: Let s be the sequence defined in the statement of the theorem. Let $P(n)$ be the open statement "$s_n = n!$." We will prove that $P(n)$ is true for any natural number n. First, note that by definition $s_1 = 1$ and $1 = 1!$, so $P(1)$ is true. Next, suppose that k is a natural number and that $P(k)$ is true. That is, we are assuming that $s_k = k!$. Notice that $s_{k+1} = (k+1)s_k = (k+1)k! = (k+1)!$. Hence, $P(k+1)$ is true. We have established that $P(1)$ is true and that $P(k)$ implies $P(k+1)$. By induction, $P(n)$ is true for all natural numbers n. □

13.11 Exercises: Use induction to prove that the given formula is a formula for the n^{th} term of the recursively define sequence.

13.11.1 Recursive definition: $s_1 = \dfrac{1}{2}$, $s_{n+1} = \dfrac{1}{2} s_n$; Formula: $s_n = \dfrac{1}{2^n}$

13.11.2 Recursive definition: $s_1 = 0$, $s_{n+1} = 1 - s_n$; Formula: $s_n = \dfrac{1}{2}(1 + (-1)^n)$

13.11.3 Use induction to prove the recursive formulas you guessed in 13.9 are correct.

13.12 Monotonicity: A sequence $s : \mathbb{N} \to \mathbb{R}$ is **increasing** if $s_n \leq s_{n+1}$ for all n. The sequence is decreasing if $s_n \geq s_{n+1}$ for all n. If a sequence is either increasing or decreasing, we say that the sequence is **monotonic**. Proving that a sequence is monotonic often requires induction.

Example: The sequence s given by $s_1 = 3$ and $s_{n+1} = \dfrac{2 + s_n}{2}$ is decreasing.

Proof: Let $P(n)$ be the open statement "$s_n \geq s_{n+1}$." We will use induction to prove that $P(n)$ is true for all integers $n \geq 1$. First, $s_1 = 3$ and $s_2 = \dfrac{5}{2}$, so $s_1 \geq s_2$ and $P(1)$ is true. Now suppose that $k \in \mathbb{Z}$ and $P(k)$ is true. That is, $s_k \geq s_{k+1}$. Adding 2 to this inequality gives $2 + s_k \geq 2 + s_{k+1}$. Dividing by 2 now gives $\dfrac{2 + s_k}{2} \geq \dfrac{2 + s_{k+1}}{2}$. Our recursive definition of s tells us that $s_{k+1} = \dfrac{2 + s_k}{2}$ and $s_{k+2} = \dfrac{2 + s_{k+1}}{2}$. Hence, we have $s_{k+1} \geq s_{k+2}$. Thus, $P(k + 1)$ is true.

We have proven that $P(1)$ is true and that $P(k)$ implies $P(k + 1)$ for all integers k. By induction, $P(n)$ is true for all integers $n \geq 1$. It follows that s is decreasing. □

13.13 Exercises: Prove that each of these sequences is monotonic.

13.13.1 $s_1 = 1$ and $s_{n+1} = \dfrac{s_n + 2}{3}$ for $n \geq 1$.

13.13.2 $s_1 = 2$ and $s_{n+1} = s_n^2 + s_n$.

13.13.3 $s_1 = 1$ and $s_{n+1} = \left(\dfrac{n}{n+1}\right) s_n^2$.

13.13.4 $s_1 = 1$ and $s_{n+1} = \left(1 - \dfrac{1}{n}\right) s_n$.

13.14 Decimals and the Division Algorithm: Consider the rational number $\dfrac{11}{8}$. We are going to use the division algorithm to find a representation of this rational number as a special type of sum. First, use the division algorithm to write $11 = 8 \cdot 1 + 3$. Next, multiply the remainder 3 by 10 to get 30 and apply the division algorithm to 30 and 8 to get $30 = 8 \cdot 3 + 6$. Next multiply this remainder by 10 and apply the division algorithm to get $60 = 8 \cdot 7 + 4$. Do it all once more to get $40 = 8 \cdot 5 + 0$. We have these applications of the division algorithm

$$\begin{array}{rcrcrcr} 11 & = & 8 & \cdot & 1 & + & 3 \\ 30 & = & 8 & \cdot & 3 & + & 6 \\ 60 & = & 8 & \cdot & 7 & + & 4 \\ 40 & = & 8 & \cdot & 5 & + & 0 \end{array}$$

Multiplying the first equation by $\frac{1}{8}$, the second equation by $\frac{1}{80}$, the third by $\frac{1}{800}$ and the fourth by $\frac{1}{8000}$ gives

$$\begin{aligned}
\frac{11}{8} &= 1 + \frac{3}{8} \\
\frac{3}{8} &= \frac{3}{10} + \frac{6}{80} \\
\frac{6}{80} &= \frac{7}{100} + \frac{4}{800} \\
\frac{4}{800} &= \frac{5}{1000}
\end{aligned}$$

By substituting from the second equation into the first, and then substituting into this from the third, and then the fourth, we get

$$\frac{11}{8} = 1 + \frac{3}{10} + \frac{7}{100} + \frac{5}{1000}$$

Notice that the numerators in the fractions on the right are the quotients from applying the division algorithm.

Let us attempt the same process with $\frac{56}{33}$

$$\begin{aligned}
56 &= 33 \cdot 1 + 23 \\
230 &= 33 \cdot 6 + 32 \\
320 &= 33 \cdot 9 + 23 \\
230 &= 33 \cdot 6 + 32 \\
320 &= 33 \cdot 9 + 23
\end{aligned}$$

There is a problem here. Our remainders are going to alternate between 23 and 32. We will never get a zero remainder. Let us ignore this problem and continue the process as before. We multiply by $\frac{1}{33}$, $\frac{1}{330}$, $\frac{1}{3300}$, $\frac{1}{33000}$,... to

get this unending list of equations:

$$\begin{aligned}
\frac{56}{33} &= 1 + \frac{23}{33} \\
\frac{23}{33} &= \frac{6}{10} + \frac{32}{330} \\
\frac{32}{330} &= \frac{9}{100} + \frac{23}{3300} \\
\frac{23}{3300} &= \frac{6}{1000} + \frac{32}{33000} \\
\frac{32}{33000} &= \frac{9}{10000} + \frac{23}{330000} \\
&\vdots
\end{aligned}$$

Substitution as before now yields

$$\frac{56}{33} = 1 + \frac{6}{10} + \frac{9}{100} + \frac{6}{1000} + \frac{9}{10000} + \dots$$

Notice again that the numerators are the quotients from the division algorithm.

If we perform this algorithm on any fraction $\frac{m}{n}$, then at any step of the way, the only possibilities for our remainder are $0, 1, 2, \dots, n-1$. Because of this one of two things may happen. Either a remainder will be 0 as in $\frac{11}{8}$ and the process will halt, or some nonzero remainder will repeat. In the second case, there will be a repeating pattern of remainders as in $\frac{56}{33}$.

13.15 Decimal Expansions: Suppose m and n are natural numbers. We define here two sequences q and r recursively. Let q_1 and r_1 be the quotient and remainder guaranteed by the division algorithm so that $m = nq_1 + r_1$. Assuming that q_k and r_k have been defined, let q_{k+1} and r_{k+1} be the quotient and remainder guaranteed by the division algorithm so that $10 \cdot r_k = nq_{k+1} + r_{k+1}$. The **decimal expansion** of $\frac{m}{n}$ is the expression $q_1.q_2q_3q_4\dots$. The expression $q_1.q_2q_3q_4\dots$ is shorthand for the sum $q_1 + \frac{q_2}{10} + \frac{q_3}{100} + \frac{q_4}{1000} + \cdots$.

13.16 Exercises: Find the decimal expansion of each of these fractions using the algorithm outlined above.

(1) $\frac{17}{7}$ (2) $\frac{15}{12}$ (3) $\frac{12}{99}$

13.17 Repeating and Terminating Decimals: As we said before, the algorithm for finding the decimal expansion of a rational number will always either end with a remainder of zero or will fall into a repeating pattern. This is because there are a limited number of possible remainders at each step. In the first case, we say that the decimal expansion **terminates**. In the second, we say that the decimal expansion **repeats**. It can be proven that

Theorem: The decimal expansion of any positive rational number either terminates or repeats.

Rather than prove this theorem, we leave the following exercise which gives the flavor of the proof.

13.18 Exercise: Prove that the decimal expansion of any rational number of the form $\frac{n}{3}$ either terminates or repeats. (Hint: Find q_1 and r_1 by the division algorithm so that $n = 3q_1 + r_1$. Proceed by cases as to whether $r_1 = 0$ or $r_1 = 2$ or $r_1 = 3$. If $r_1 = 0$, then the decimal terminates. If $r_1 = 1$, then the expansion will have repeating 3's. If $r_1 = 2$, then the expansion will have repeating 6's.)

13.19 Converting Decimals to Rational Numbers: The process above can be performed on any positive rational number. To find the decimal expansion of a negative rational number q, simply find the expansion of the positive number $-q$ and add a negative sign to the front. Thus, every rational number has a decimal expansion. By 13.17 this expansion either terminates or repeats. On the other hand, any terminating or repeating decimal expression is the expansion of a rational number. Rather than proving this, we give examples of how to turn a decimal into a rational number.

First, consider the terminating decimal 7.123456789. Count the digits after the decimal point. That is easy in this example – there are 9. The rational number $\frac{7123456789}{10^9}$ has 7.123456789 as its decimal expansion.

Next, we consider the repeating decimal $x = 8.12567567567567\ldots$ (the pattern 567 repeats). This example assumes we already know how to multiply decimal numbers by powers of 10 and how to subtract decimal numbers. Count the number of digits that repeat. Here, there are 3. Calculate $10^3x - x$. In this case, $1000x - x = 8117.55$ (notice how the repeating parts of the decimal cancel each other). From the previous example, this number is the decimal expansion of $\frac{811755}{100}$. Now, $1000x - x = 999x$, so we have $999x = \frac{811755}{100}$ Multiplying both sides of this equation by $\frac{1}{999}$ gives $x = \frac{811755}{99900}$.

13.20 Exercises: Convert these repeating and terminating decimals to fractional form.

13.20.1 12.34567
13.20.2 2.3434343434... (34 repeats)
13.20.3 12.123412121212... (12 repeats)

13.21 Rational Numbers: We have been working off and on with rational numbers without a formal derivation of this number system. We merely commented in Chapter 8 that the set $\mathbb{Q}$ of rational numbers is the set of all fractions of integers

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

Since different formal quotients might represent the same rational numbers – such as $\frac{2}{4}$ and $\frac{1}{2}$ – a formal derivation of $\mathbb{Q}$ would actually define an equivalence relation on these formal quotients defining when two quotients represent the same number. $\mathbb{Q}$ would then be the set of equivalence classes of this relation. Such a derivation would then define addition, multiplication, negation, and reciprocals and prove the "usual" properties of arithmetic in $\mathbb{Q}$. We have forgone this derivation, but we do want to point out that not all numbers are rational.

13.22 The square root of 2: The square root of 2 is not rational.

Theorem: Integers a and b do not exist so that $\left(\frac{a}{b}\right)^2 = 2$.

Proof: We prove the equivalent statment that there are no integers a and b so that $a^2 = 2b^2$ (thus, we get to work in $\mathbb{Z}$). We do so by contradiction. Suppose that a and b are integers and that $a^2 = 2b^2$. By the cancellation laws, we can assume that a and b are both positive (thus, we actually get to work in $\mathbb{N}$) and that (this is important)

a and b have no common divisors other than 1.

Since $a^2 = 2b^2$, it follows that a^2 is even. By 7.23, it follows that a is even, so there is some natural number k with $a = 2k$. The equation $a^2 = 2b^2$ can now be expressed as $4k^2 = 2b^2$. Cancellation gives $2k^2 = b^2$. Thus, b^2 is also even. By 7.23, it follows that b is even. We now have that a and b are both even, so

2 is a common factor of a and b.

But this contradicts the fact that a and b have no common factors. Since we have arrived at a contradiction, our original assumption must be false. It follows that 2 cannot have a rational square root. □

13.23 Exercises:
13.23.1 Use 12.23 to prove that if $n \in \mathbb{N}$ and if n^2 is a multiple of 3 then n is a multiple of 3.

13.23.2 Use the previous exercise to prove that $\sqrt{3}$ is not rational.

13.24 Sequences of Rational Numbers: Consider the sequence defined recursively by $s_1 = 1$ and $s_{n+1} = \frac{s_n}{2} + \frac{1}{s_n}$. The first few terms of this sequence are $\langle 1, \frac{3}{2}, \frac{17}{12}, \frac{577}{408}, \ldots \rangle$. It is not clear whether or not these terms converge. The decimal expansions of these terms might be more descriptive. The expansions look like

$$\langle 1, 1.5, 1.41666\ldots, 1.41421568\ldots, 1.41421356\ldots, 1.41421356\ldots, \ldots \rangle.$$

It appears that s might converge. Consider the sequence

$$\langle s_1^2, s_2^2, s_3^2, \ldots \rangle.$$

The decimal expansions of these terms look like

$$\langle 1, 2.25, 2.006944, 2.000006\ldots \rangle.$$

You can see that these terms seem to be getting close to 2. Tools from calculus can be used to show that this is actually true.

We have, then, a sequence s of positive rational numbers which converges. Since the sequence $\langle s_1^2, s_2^2, s_3^2, \ldots \rangle$ converges to 2, it follows that s should converge to $\sqrt{2}$. This means we have a sequence of rational numbers which converges to an irrational number.

13.25 Real Numbers as Limits of Sequences: One way of defining the real numbers is to consider all sequences of rational numbers which look like they ought to converge and then defining $\mathbb{R}$ essentially to be a set of limits of all such sequences.

14

Cardinality and Counting

14.1 Same Size: If two sets A and B are the same size, then it makes sense that we could pair each element of A with and element of B in such a way that each element of A is paired with exactly one element of B and each element of B is paired with exactly one element of A. This pairing would define a bijective function. This motivates the following definition.

14.2 Bijective Sets: A set A is **bijective** with a set B if there is a bijection from A to B.

14.3 Interpretation: Intuitively, we interpret the statment A is bijective with B as meaning "A and B are the same size" (whatever that means). Before we can get too involved with this notion, we need the results in the following exercises - which essentially show that bijectivity has the same properties as an equivalence relation.

14.4 Exercises: Prove the following.
14.4.1 If A is any set, then A is bijective with A (Hint: identity function).
14.4.2 If A is bijective with B, then B is bijective with A (Hint: every bijection has an inverse which is also a bijection).
14.4.3 If A is bijective with B and B is bijective with C, then A is bijective with C (Hint: the composition of bijective functions is bijective).

14.5 Size: For any set A, we would like to have a "number" which tells us how many elements are in A. Since some sets are too big to describe in this manner with conventional numbers, we need a new notion of number - a cardinal number. Here, we do not define cardinal number. We simply assume that such numbers exist and list the assumptions we make about them. This is the best that mathematicians have been able to do so far.

The assumptions below seem quite strange at first glance. We will use cardinal numbers to describe the size of sets. The first assumption is that every set has a size which is a cardinal number. This size is called the cardinality of the set. The second assumption merely says that every cardinal number is the size of some set. The third and fourth assumptions tell us the cardinality of finite sets. The final assumption is that we assume two sets have the same cardinality if and only if they are bijective.

14.6 Cardinal Numbers: We will take the idea of a **cardinal number** as a primitive (an undefined concept) relating to the size of sets, and we will assume that cardinal numbers satisfy the following properties.

1. Every set A is associated with a cardinal number, called the **cardinality** of A, which we will denote by $|A|$.
2. For any cardinal number α, there is a set A with $|A| = \alpha$.
3. $|\emptyset| = 0$, and this is the only set with cardinality 0.
4. If A is bijective with $\{1, 2, \ldots, n\}$ for some natural number n, then $|A| = n$.
5. For any two sets, $|A| = |B|$ if and only if A and B are bijective. From here on, we may use the descriptive symbols $|A| = |B|$ to indicate that A and B are bijective.

14.7 Terminology: A variety of terms are used to describe bijective sets. The terminology includes equivalent, equipotent, and equinumerous. Most text eventually progress to saying two sets "have the same cardinality."

14.8 Showing $|A| = |B|$: One way to show that two sets A and B have the same cardinality is to exhibit a bijection between the sets. For example
Example: The intervals $[0, 1]$ and $[23, 27]$ of real numbers are the same cardinality. To see this, define $f : [0, 1] \to [23, 27]$ to be the function given by $f(x) = 4x + 23$. To see that this is a bijection, note that f has an inverse $f^{-1}(x) = \frac{1}{4}(x - 23)$ (the reader should check to make sure the domains and ranges of the functions match up properly).

There is nothing special about the interval $[23, 27]$ in this example, the function $f(x) = (b - a)x + a$ is a bijection from $[0, 1]$ to $[a, b]$ for all real a and b. It follows that all closed intervals have the same cardinality.

Example: The set E of even natural numbers has the same cardinality as $\mathbb{N}$. To see this, note that $f : \mathbb{N} \to E$ given by $f(n) = 2n$ is a bijection.

14.9 Exercise:
14.9.1 Find a bijection between the even integers and the odd integers to show these two sets have the same cardinality.
14.9.2 Use a bijection to show that the sets $\{x \in \mathbb{Z} : x \leq 0\}$ and $\{x \in \mathbb{Z} : x \leq 10\}$ have the same cardinality.
14.9.3 Find a bijection between the integers and the non-negative integers.
14.9.4 Suppose that $n, m \in \mathbb{N}$, that $A = \{0, 1, 2 \ldots, n - 1\}$, that $B = \{0, 1, 2, \ldots, m - 1\}$, and that $C = \{0, 1, 2, \ldots, nm - 1\}$. Show that $|A \times B| = |C|$.

14.9.5 Suppose that $|A_n| = m_n$ for $n = 0, \ldots l$. Prove that

$$|A_0 \times A_1 \times \ldots \times A_l| = m_0 \cdot m_1 \cdot \cdots \cdot m_l.$$

(Hint: Use induction and the previous exercise.)

14.10 Fundamental Counting Principle: The last two exercises are the basis for the fundamental counting principle: If there are n ways that one event can occur and m ways that another even can occur, then there are nm ways that the two events can occur together. This is the basis for many counting problems.

14.11 Example: Find the number of different ordered sequences of three letters, assuming that letters can be reused.

Solution: Since there are 26 letters in the alphabet, there are 26 ways to pick the first letter, 26 ways to pick the second, and 26 ways to pick the third. This means that there are $26 \cdot 26 \cdot 26$ total sequences.

14.12 Example: Find the number of different ordered sequences of three letters, assuming that letters can NOT be reused.

Solution: Since there are 26 letters in the alphabet, there are 26 ways to pick the first letter. After the first letter has been picked, there are 25 ways to pick the second. After the first two letters have been picked, there are 24 ways to pick the third letter. Thus, there are $26 \cdot 25 \cdot 24$ ways to pick three letters in order without repeats.

14.13 Exercises:
14.13.1 The identification codes for students at a small college are all of the form $GLLDDD$ where G is F for females and M for males, each L is a letter of the English alphabet, and each D is a digit. How many such codes are there?
14.13.2 How many codes are possible in the previous exercise if the letters represented by L's and the digits cannot be repeated?
14.13.3 In how many ways can the letters ABC be rearranged?
14.13.4 In how many ways can the letters $ABCC$ be rearranged? (Hint: First consider ABC_1C_2.)
14.13.5 In how many ways can the letters $ABCCC$ be rearranged?
14.13.6 In how many ways can the letters $ABBBCCC$ be rearranged?

14.14 Finite vs. Infinite A set A is **finite** if $|A| \in \mathbb{N}$[1]. A set A is **infinite** if A is not finite.

[1]This is another instance where including 0 in $\mathbb{N}$ simplifies things. If we did not have $0 \in \mathbb{N}$, then we would have to define A to be finite if $|A| \in \mathbb{N}$ or $A = \emptyset$

14.15 Powersets: The natural numbers are infinite. The integers are infinite, the rational numbers and the real number are also infinite. We prove here a theorem which will show that not all infinite sets have the same cardinality. Recall that the powerset of a set A is the set of all subsets of A.

Cantor's Theorem: Let A be any set. Then $|A| \neq |\mathcal{P}(A)|$.

Proof: Suppose A is a set. If $A = \emptyset$, then $\mathcal{P}(A) = \{\emptyset\}$, so $|A| = 0 \neq 1 = |\mathcal{P}(A)|$. Suppose next that A is not empty. We will prove using contradiction that $|A| \neq |\mathcal{P}(A)|$. Suppose, then, that $|A| = |\mathcal{P}(A)|$. This means there is a bijection $f : A \to \mathcal{P}(A)$. Let $B = \{x \in A : x \notin f(x)\}$ (since $f(x)$ is a subset of A, we can ask whether or not $x \in f(x)$). Since f is a bijection, we can find $a \in A$ with $f(a) = B$. To obtain our contradiction, we ask whether or not $a \in B$. If $a \in B$, then by the definition of B, $a \notin f(a) = B$. Hence a cannot be an element of B. If $a \notin B$, then from the definition of B, it must be that $a \in f(a) = B$. Thus, it cannot be that either $a \in B$ or $a \notin B$. Since one of these must be true, we have a contradiction. Hence, the assumption that $|A| = |\mathcal{P}(A)|$ must be false. □

14.16 Countable vs. Uncountable A set A is **countable infinite** if $|A| = |\mathbb{N}|$. A set A is **countable** if A is finite or countably infinite. A set is **uncountable** if it is not countable.

14.17 An Order on Cardinalities: If A and B are sets, we say that $|A|$ is less than or equal to $|B|$ if there is an injection from A to B. This is denoted as $|A| \leq |B|$. $|A| < |B|$ will mean that $|A| \leq |B|$ and $|A| \neq |B|$.

14.18 Proving $|A| \leq |B|$: To prove that $|A| \leq |B|$, we must find an injective function from A to B.

Example: Suppose that A is any set. Then $|A| \leq |\mathcal{P}(A)|$. To see this, we need to find an injection from A to $\mathcal{P}(A)$. Define $f : A \to \mathcal{P}(A)$ by $f(a) = \{a\}$ for any $a \in A$. This is clearly an injection since if $\{a\} = \{b\}$ then $a = b$. Thus we see that $|A| \leq |\mathcal{P}(A)|$. Since Cantor's Theorem tells us that these sets do not have the same cardinality, we actually have $|A| < |\mathcal{P}(A)|$.

14.19 Exercises:

14.19.1 Let A be the set of integer multiples of 4. Prove that $|\mathbb{Z}| \leq |A|$.

14.19.2 Let $A = (0, 1)$ and $B = (1, 3)$. Prove that $|A| \leq |B|$.

14.19.3 Let $A = (0, 1)$ and $B = (1, 3)$. Prove that $|B| \leq |A|$.

14.19.4 Let $A = [-1, 1]$. Let B be the points on the top half of the unit circle. Show that $|A| \leq |B|$.

14.19.5 If A is any set, prove $|A| \leq |A|$.

14.19.6 If $|A| \leq |B|$ and $|B| \leq |C|$, prove $|A| \leq |C|$.

14.20 An Infinity of Infinities: Cantor's theorem gives us a curiosity of infinite cardinals. $|\mathbb{N}|$ is an infinite cardinal. From Cantor's theorem and the previous example, $|\mathcal{P}(\mathbb{N})|$ is a larger infinite cardinal. Again, $|\mathcal{P}(\mathcal{P}(\mathbb{N}))|$ is an even larger infinite cardinal. Likewise, $|\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))|$ is an even larger infinite cardinal. Define the following cardinal numbers

$$\aleph_0 = |\mathbb{N}|, \aleph_1 = |\mathcal{P}(\mathbb{N})|, \aleph_2 = |\mathcal{P}(\mathcal{P}(\mathbb{N}))|, \aleph_3 = |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))|, \ldots$$

($\aleph$ is the Hebrew letter "aleph"). Then we have an infinite increasing sequence of infinite cardinals

$$\aleph_0 < \aleph_1 < \aleph_2 < \aleph_3 < \aleph_4 < \ldots$$

The set $\mathcal{P}(\mathbb{N})$ is our first example of an uncountable set.

14.21 Cantor-Schroeder-Bernstein Theorem: Sometimes, it is easier to find injections between sets than it is to find bijections. Hence, this next theorem often greatly simplifies showing that two sets have the same cardinality.

Theorem: If A and B are sets, then $|A| = |B|$ if and only if both $|A| \leq |B|$ and $|B| \leq |A|$.
Before proving the theorem, we offer an example application to see its power.

Example: The cardinality of $\mathbb{N}$ is the same as the cardinality of $\mathbb{N} \times \mathbb{N}$. To show this, we will find an injection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$ and an injection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. One direction is easy. Define $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ by $f(n) = (n, 1)$. It is not difficult to show that this is injective. The other direction requires a bit more thought. Define $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $g(n, k) = 2^n 3^k$. An induction argument can be used to show that g is injective. (There are many choices for g here. Another would be $g(n, k) = 2^n(2k + 1)$.)

14.22 Exercises:
14.22.1 Find a pair of injections, one from $\mathbb{N}$ to $\mathbb{Z}$ and the other from $\mathbb{Z}$ to $\mathbb{N}$. Thus, $\mathbb{Z}$ and $\mathbb{N}$ have the same cardinality.
14.22.2 Find a pair of injections to show that the intervals $(0, 1)$ and $[0, 1]$ have the same cardinality.
14.22.3 Find a pair of injections to prove that $\mathbb{R}$ and the interval $(-1, 1)$ have the same cardinality. (Hint: You will probably need to use a piecewise defined function.)

14.23 Proof of the CSB Theorem: We outline here the proof of the Cantor-Schroeder-Bernstein Theorem with just enough detail to give you the idea of how the proof works.

Suppose that A and B are sets and that $|A| \leq |B|$ and $|B| \leq |A|$. We will prove that $|A| = |B|$. There are injections $f : A \to B$ and $g : B \to A$.

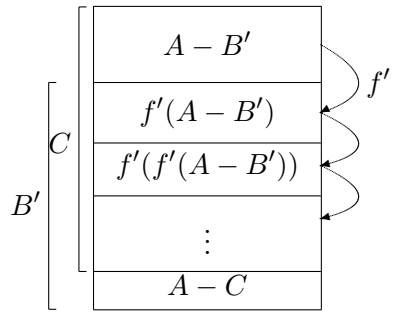


Figure 14.1:

Let $B' = g[B]$. Then $|B| = |B'|$ since the restriction of g to B' is a bijection. Also the function $f' : A \to B'$ defined by $f' = g \circ f$ is an injection. Consider the sets $A - B'$, $f'(A - B')$, $f'(f'(A - B'))$, $f'(f'(f'(A - B')))$,... These sets are all distinct, and f' maps each to the next (see figure 14.23). Define C to be $(A - B') \cup f'(A - B') \cup f'(f'(A - B')) \cup f'(f'(f'(A - B')))$ (a subset of A). Define $h : A \to B'$ by

$$h(x) = \begin{cases} f'(x) & x \in C \\ x & x \in A - C \end{cases}$$

Then h is a bijection witnessing that $|A| = |B'|$ □

14.24 Exercises:
14.24.1 Suppose that A and B are sets and that there is a surjective function $f : B \to A$. Prove that $|A| \leq |B|$ (Hint: Draw a circle diagram of the function and use it to find an injection from A to B).
14.24.2 Suppose that $|A| \leq |B|$. Prove that there is a surjection from B to A (Hint: Draw an injective function from A to B and use the picture to find a surjection from B to A).

14.25 Cardinality and Surjectivity The previous two exercises prove

Theorem: Let A and B be sets. Then $A \leq B$ if and only if there is a surjection from B to A.

14.26 Cardinalities of the Number Systems: We now address the cardinalities of the number systems. We will prove that $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are all countable while $\mathbb{R}$ and $\mathbb{C}$ are uncountable.

Theorem: $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$

Proof: We will actually prove that $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}|$. We will do so by proving $|\mathbb{N}| \leq |\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| \leq |\mathbb{N} \times \mathbb{N}| \leq \mathbb{N}$. It will then follow from 14.21 and 14.19.6 that these cardinalities are equal. To see that $|\mathbb{N}| \leq |\mathbb{Z}|$, just note that the function $f : \mathbb{N} \to \mathbb{Z}$ given by $f(n) = n$ is an injection. That $|\mathbb{Z}| \leq |\mathbb{Q}|$ is similar. To see that $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$, we must define an injection $h : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$. Let $\frac{a}{b} \in \mathbb{Q}$. There are integers n and m with no common divisors so that $\frac{a}{b} = \frac{n}{m}$. Define $h\left(\frac{a}{b}\right) = (n, m)$. This will be an injective function. Next, we show that $|\mathbb{Z} \times \mathbb{Z}| \leq |\mathbb{N} \times \mathbb{N}|$. First, recall that in Exercise 14.9.1 you proved that $|\mathbb{Z}| = |\mathbb{N}|$. This means that there is a bijection $g' : \mathbb{Z} \to \mathbb{N}$. Define $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N}$ by $g(a, b) = (g'(a), g'(b))$. This will be an injection (actually, a bijection, but we only need an injection). Finally, we must prove that $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$. This was accomplished in the example in 14.21. □

Theorem: $\mathbb{R}$ and $\mathbb{C}$ are uncountable.

Proof: We prove that no function from the natural numbers to the real numbers can be surjective. This will make it impossible for a function from the natural numbers to the real numbers to be bijective. Suppose $f : \mathbb{N} \to \mathbb{R}$ is any function. We will prove that f is not surjective. For any natural number n, let d_n be the n^{th} digit after the decimal place in $f(n)$. We are going to define a real number which is not in the image of f. Define a sequence e of real numbers by $e_n = 9 - d_n$. Let $x = 0.e_1e_2e_3\ldots$. Notice that for any $n \in \mathbb{N}$, the n^{th} digit after the decimal in x is e_n which is different from d_n - the n^{th} digit after the decimal in $f(n)$. Hence for every $n \in \mathbb{N}$, $f(n) \neq x$. The number x is not in the image of f. Thus f is not surjective.

Since no function from $\mathbb{N}$ to $\mathbb{R}$ can be surjective, $\mathbb{N}$ and $\mathbb{R}$ have different cardinalities. Since $\mathbb{R}$ is infinite, it is uncountable. Any surjective function from $\mathbb{N}$ to $\mathbb{C}$ would also map onto $\mathbb{R}$ (as a subset of $\mathbb{C}$). Since this cannot happen, there can be no surjective function from $\mathbb{N}$ to $\mathbb{C}$. Hence, $\mathbb{C}$ is also uncountable. □

14.27 The Size of $\mathbb{R}$: The set of real numbers happens to have the same cardinality as the powerset of the natural numbers, so $|\mathbb{R}| = \aleph_1$. This is proven in the next exercises.

14.28 Exercises:

14.28.1 Since $|\mathbb{N}| = |\mathbb{Q}|$, there is a bijection $f : \mathbb{N} \to \mathbb{Q}$. Define $f_1 : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{Q})$ by $f_1(X) = \{f(x) : x \in X\}$ for any $X \in \mathcal{P}(\mathbb{N})$. Prove that f_1 is bijective.

14.28.2 Define $f_2 : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ so that $f_2(X)$ is the number $0.d_1d_2d_3$ where for any n $d_n = 1$ if $n \in X$ and $d_n = 0$ otherwise. Prove that f_2 is injective.

14.28.3 Define $f_3 : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ by $f_3(x) = \{q \in \mathbb{Q} : q < x\}$. Prove that f_3 is injective. (Hint: You need to know that between any two real numbers is an irrational number.)
14.28.4 Use the previous exercises to prove that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

14.29 Continuum Hypothesis: Since $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = \aleph_1 > \aleph_0$, a logical question to ask is whether or not there is any set with a cardinality strictly between $\aleph_0$ and $\aleph_1$. A concrete version of this problem is the question of whether or not there is a subset of $\mathbb{R}$ which has a cardinality strictly larger than $\mathbb{N}$ but strictly smaller than $\mathbb{R}$. An initial guess is no. This guess is known as the **continuum hypothesis**.

Continuum Hypothesis: There is no cardinal number α so that $\aleph_0 < \alpha < \aleph_1$.

The surprising truth is that according to results of Kurt Gödel (1938) and Paul Cohen (1963) the Continuum Hypothesis can be assumed or rejected without affecting the consistency of mathematics.

14.30 The Set of All Sets: Is there such a thing as the set of all sets? Bertrand Russel argued in 1902 that there can be no set of all sets.

We can see that there can be no set of all sets perhaps most clearly by looking at cardinalities. Let U be the collection of all sets. If U were a set, then U would have to have a cardinality $|U|$. This cardinality would have to be the largest cardinal number, but Cantor's Theorem tells us that $|\mathcal{P}(U)|$ would be even larger. Thus the assumption that U is a set leads to a contradiction.

The assumption that there is a set of all sets leads to another contradiction commonly referred to as the **Russel Paradox**. Suppose that there is a set U which contains all sets. Then we can define a subset A of U in this manner

$$A = \{B \in U : B \notin B\}.$$

We now ask ourselves whether or not $A \in A$. Suppose that $A \in A$. Then A is one of the B's in the definition of A, so $A \notin A$. Hence, it cannot be that $A \in A$, so $A \notin A$. Suppose then that $A \notin A$. Then A satisfies the definition of being in A, so $A \in A$. This is a contradiction, so it cannot be that $A \notin A$. That is $A \in A$. Thus we have that both $A \notin A$ and $A \in A$ are true. This is a contradiction.

To avoid contradictions such as this, mathematicians usually restrict set builder notation to define sets of the form $\{x \in A : P(x)\}$ where A is known to be a set – in particular, A cannot be the collection of all sets.

14.31 Exercise: Suppose you are a manager of a hotel which has a countably infinite number of rooms numbered $1, 2, 3, \ldots$. One night, all of the rooms are full, but someone comes in looking for a room. If everyone is willing to move to a different room, there is a way to accomodate the guest without making any of the patrons share rooms. How?

15

The Number Systems

15.1 Numbers: Up to this point, we have only formally defined the natural numbers. In this chapter, we demonstrate why the natural numbers are not adequate, and we outline how the integers, rational numbers, real numbers, and complex numbers can be derived from the natural numbers.

15.2 Equations: There are many equations which we cannot solve employing only natural numbers. Four examples are

$$x + 2 = 1$$

$$2x = 1$$

$$x^2 = 2$$

$$x^2 + 1 = 0$$

We would like a number system in which every polynomial equation has a solution.

15.3 Natural Numbers: First, we recall some of the facts we learned about the natural numbers in Chapters 11 and 7.

The natural numbers are a set $\mathbb{N}$ endowed with two binary operations $\cdot$ and $+$ and an order relation $\leq$ which all satisfy the following properties. Each of these properties appears directly in Chapter 11 or 7 or follows from something proven there. For all $x, y, z, w \in \mathbb{N}$, the following are true

Properties of Addition:

$x + (y + z) = (x + y) + z$	associative law
$x + y = y + x$	commutative law
$y + x = z + x$ if and only if $y = z$	cancellation law
$x + 0 = 0 + x = x$	additive identity
$x \cdot 0 = 0 \cdot x = 0$	absorption law

Properties of Multiplication:

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	associative law
$x \cdot y = y \cdot x$	commutative law
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	distributive law
$x \cdot 1 = 1 \cdot x = x$	multiplicative identity
if $x \neq 0$ then $y \cdot x = z \cdot x$ iff $y = z$	cancellation law

Order Properties:
If $x \leq y$ and $y \leq z$ then $x \leq z$ $\leq$ transitive
If $x \leq y$ and $y \leq x$ then $x = y$ $\leq$ antisymmetric
$0 \leq x$
If $x \leq y$ and $z \leq w$ then $x + z \leq y + w$ and $xz \leq yw$
$x \leq y$ if and only if $x + z \leq y + z$

15.4 A relation on $\mathbb{N} \times \mathbb{N}$: Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

15.5 Exercise: Prove that $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

15.6 Interpretation: In the world of arithmetic with which we are familiar, every integer can be realized as a difference of natural numbers. For example, $13 = 63 - 50$ and $-7 = 3 - 10$. We are going to identify an ordered pair (a, b) of natural numbers with the difference $a - b$. Now, some differences are the same even though they do not look alike - for example, $4 - 6 = 40 - 42$. The equivalence relation $\sim$ tells us which ordered pairs (or differences) to identify. You can check that $a - b = c - d$ is true exactly when $a + d = b + c$. Thus this should be the condition under which we identify two ordered pairs.

Each ordered pair (a, b), represents the integer $a - b$. Every ordered pair in the equivalence class of (a, b) modulo $\sim$ represents the same difference $a - b$. Therefore, when we define the integers, we will use the whole equivalence class to represent the integer $a - b$. That is the intent of the next definition.

15.7 Integers: Define the **integers** to be the factor set $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$.

With this defintion, if a and b are natural numbers, we will identify the integer $a - b$ with the equivalence class $[(a, b)]_\sim$. To simplify notation, we will dispense with the subscripts and write only $[(a, b)]$.

15.8 Confused? Every time you see $[(a, b)]$, think $a - b$.

15.9 Addition: We must now decide how to define addition of integers. To begin, we consider that we know from previous experience that the equality $(a - b) + (c - d) = (a + c) - (b + d)$ should hold. Using the equivalence class notation, this would look like $[(a, b)] + [(c, d)] = [(a + c, b + d)]$. This is how we should define addition.

Technically, before we use this definition, we should make sure that this definition will make sense. That is, if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$, so we would need to have

$$[(a, b)] + [(c, d)] = [(a', b')] + [(c', d')]$$

To use the definition we would want to use, we must be sure that $[(a+c, b+d)] = [(a'+c', b'+d')]$, which is equivalent to $(a+c, b+d) \sim (a'+c', b'+d')$.

15.10 Exercise: Suppose $[(a,b)] = [(a',b')]$ and $[(c,d)] = [(c',d')]$. Prove that $[(a+c, b+d)] = [(a'+c', b'+d')]$.

15.11 Definition of Addition: Define an operation + called addition on $\mathbb{Z}$ by

$$[(a,b)] + [(c,d)] = [(a+c, b+d)]$$

for all integers $[(a,b)]$ and $[(c,d)]$. By the previous exercise, this operation is well defined.

15.12 Exercise: Use the definition of addition to calculate:
15.12.1 $[(2,7)] + [(26,21)]$
15.12.2 $[(1,1)] + [(45,23)]$
15.12.3 $[(2,3)] + [(3,2)]$

15.13 Multiplication: We next decide how we should define multiplication. To decide how to multiply $[(a,b)]$ and $[(c,d)]$, we multiply $(a-b)(c-d)$ as we were taught in algebra and see what we get.

$$(a-b)(c-d) = ac - ad - bc + bd = (ac+bd) - (ad+bc)$$

Thus it seems we want to define $[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$.

15.14 Definition of Multiplication: Define the operation multiplication on $\mathbb{Z}$ by

$$[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$$

for all integers $[(a,b)]$ and $[(c,d)]$.

15.15 Exercise: Prove that multiplication of integers is well defined.

15.16 Exercise: Use the definition of multiplication to calculate:
15.16.1 $[(2,7)] \cdot [(26,21)]$
15.16.2 $[(1,1)] \cdot [(45,23)]$
15.16.3 $[(2,3)] \cdot [(3,2)]$

15.17 Identities: We can now prove the operations of addition and multiplication satisfy some of the same identities as the operations on $\mathbb{N}$ with the same names.
Lemma: If a, b, c, and d are natural numbers, then $[(a,b)] \cdot [(c,d)] = [(c,d)] \cdot [(a,b)]$.

Proof: Simply note that

$$\begin{aligned} [(a,b)] \cdot [(c,d)] &= [(ac+bd, ad+bc)] \\ &= [(ca+db, da+cb)] \quad (\cdot \text{ commutative in } \mathbb{N}) \\ &= [(ca+db, cb+da)] \quad (+ \text{ commutative in } \mathbb{N}) \\ &= [(c,d)] \cdot [(a,b)]. \end{aligned}$$

□

Lemma: If a, b, c, d, e, and f are natural numbers, then

$$([(a,b)] \cdot [(c,d)]) \cdot [(e,f)] = [(a,b)] \cdot ([(c,d)] \cdot [(e,f)]).$$

Proof: Note that

$$\begin{aligned}
& ([(a,b)] \cdot [(c,d)]) \cdot [(e,f)] = \\
= \; & [(ac+bd, ad+bc)] \cdot [(e,f)] \\
= \; & [((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e)] \\
= \; & [(ace+bde+adf+bcf, acf+bdf+ade+bce)] \\
= \; & [(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df))] \\
= \; & [(a,b)] \cdot [(ce+df, cf+de)] \\
= \; & [(a,b)] \cdot ([(c,d)] \cdot [(e,f)]).
\end{aligned}$$

□

These two lemmas give us
Theorem: Multiplication of integers is commutative and associative.

15.18 Exercises: Use the definitions to prove each of these.
15.18.1 Lemma: If a, b, c, and d are natural numbers, then $[(a,b)] + [(c,d)] = [(c,d)] + [(a,b)]$.
15.18.2 Lemma: If a, b, c, d, e, and f are natural numbers, then $([(a,b)] + [(c,d)]) + [(e,f)] = [(a,b)] + ([(c,d)] + [(e,f)])$.

15.19 Additive Identities: From the previous exercises, it follows that addition of integers is commutative and associative.

15.20 Order of Operations: To simplify notation, we will follow the same conventions as we did with natural numbers and assume that multiplication takes precedence over addition. Also, we will often write multiplication simply as juxtaposition.

15.21 Distributivity: For any integers x, y, and z, $x(y+z) = xy + xz$.

Proof: Let x, y, and z be integers. This means there are natural numbers x_1, x_2, y_1, y_2, z_1, and z_2 so that $x = [(x_1, x_2)]$, $y = [(y_1, y_2)]$, and $z = [(z_1, z_2)]$. Notice that

$$
\begin{aligned}
& x(y+z) = \\
= \;& [(x_1,x_2)]([(y_1,y_2)]+[(z_1,z_2)]) \\
= \;& [(x_1,x_2)][(y_1+z_1,y_2+z_2)] \\
= \;& [(x_1(y_1+z_1)+x_2(y_2+z_2), x_1(y_2+z_2)+x_2(y_1+z_1))] \\
= \;& [(x_1y_1+x_1z_1+x_2y_2+x_2z_2, x_1y_2+x_1z_2+x_2y_1+x_2z_1)] \\
= \;& [((x_1y_1+x_2y_2)+(x_1z_1+x_2z_2), (x_1y_2+x_2y_1)+(x_1z_2+x_2z_1))] \\
= \;& [(x_1y_1+x_2y_2, x_1y_2+x_2y_1)]+[(x_1z_1+x_2z_2, x_1z_2+x_2z_1)] \\
= \;& [(x_1,x_2)][(y_1,y_2)]+[(x_1,x_2)][(z_1,z_2)] \\
= \;& xy+xz.
\end{aligned}
$$

□

15.22 1 **and** 0**:** There is an integer which behaves much like the natural number 1. We are going to abuse notation a little here and call this integer 1 also (although, technically, it is a different element of a different set). Define 1 to be the integer $[(1,0)]$. There is another natural number which has properties similar to 1. We will call it 0. Define 0 to be the integer $[(0,0)]$.

15.23 **Exercise:** Prove that for any natural number n, $(1/0) \sim (n+1,n)$, so $1 = [(n+1,n)]$.

15.24 **Exercise:** Prove that $[(a,b)] = 0$ if and only if $a = b$ (that is, prove that $(a,b) \sim (0,0)$ if and only if $a = b$).

15.25 **Identity:** For any integer x, it happens that $1 \cdot x = x \cdot 1 = x$ and $0 + x = x + 0 = x$. We describe this by saying that 1 is a **multiplicative identity** and 0 is an **additive identity**. We prove here that 1 is a multiplicative identity and leave the proof that 0 is an additive identity as an exercise. **Theorem:** 1 is a multiplicative identity.

Proof: Let x be any integer. There are natural numbers x_1 and x_2 so that $x = [(x_1,x_2)]$. Notice that

$$x \cdot 1 = 1 \cdot x = [(1,0)][(x_1,x_2)] = [(1 \cdot x_1 + 0 \cdot x_2, 1 \cdot x_2 + 0 \cdot x_1)] = [(x_1,x_2)] = x.$$

□

15.26 **Exercises:**

15.26.1 Prove that 0 is an additive identity.

15.26.2 Prove that if x is an integer, then $x \cdot 0 = 0$.

15.27 **Factors of** 0**:** If x and y are integers and $xy = 0$, then either $x = 0$ or $y = 0$.

Proof: Let x and y be integers so that $xy = 0$. We will show that either $x = 0$ or $y = 0$. If $x = 0$ there is nothing to show, so assume that $x \neq 0$ and we will show that $y = 0$. Since x and y are integers, there are natural numbers x_1, x_2, y_1, and y_2 so that $x = [(x_1,x_2)]$ and $y = [(y_1,y_2)]$. Then $0 = xy = [(x_1y_1 + x_2y_2, x_1y_2 + x_2y_1)]$. Therefore, by 15.24, we must have

$x_1y_1+x_2y_2 = x_1y_2+x_2y_1$. Since $x \neq 0$, $x_1 \neq x_2$. Since these are natural numbers, either $x_1 < x_2$ or $x_2 < x_1$. Assume that $x_1 < x_2$. By the definition of less than for natural numbers, there is a natural number k so that $x_1+k = x_2$ Substituting for x_2 in $x_1y_1 + x_2y_2 = x_1y_2 + x_2y_1$ gives $x_1y_1 + (x_1 + k)y_2 = x_1y_2 + (x_1 + k)y_1$. Distributing gives $x_1y_1 + x_1y_2 + ky_2 = x_1y_2 + x_1y_1 + ky_1$. Cancellation of addition of natural numbers yields $ky_2 = ky_1$. Finally, cancellation of multiplication of natural numbers gives $y_2 = y_1$, so $y = 0$. This concludes the case when $x_1 < x_2$. The case where $x_2 < x_1$ is similar. □

15.28 Negation: In Chapters 11 and 7, we often had a need to be able to subtract. Most of the time, cancellation filled the need, but it would still be nice to be able to subtract. We come close to that here. If $[(a, b)]$ is any integer, define the **negation** or **opposite** of $[(a, b)]$ to be the integer $[(b, a)]$. We will denote the negation of an integer x by $-x$. It should be clear from the definition that for any x, $-(-x) = x$.

15.29 Negation and Multiplication: If x and y are integers, then $-(xy) = (-x)y = x(-y)$.

Proof: Let x and y be integers. We will show that $-(xy) = (-x)y = x(-y)$. There are natural numbers x_1, x_2, y_1, and y_2 so that $x = [(x_1, x_2)]$ and $y = [(y_1, y_2)]$. We will calculate $-(xy)$, $(-x)y$, and $x(-y)$ and see that all three are equal. Observe:

$$\begin{aligned} -(xy) &= -([(x_1, x_2)][(y_1, y_2)]) \\ &= -[(x_1y_1 + x_2y_2, x_1y_2 + x_2y_1)] \\ &= [(x_1y_2 + x_2y_1, x_1y_1 + x_2y_2)] \end{aligned}$$

$$\begin{aligned} (-x)y &= (-[(x_1, x_2)])[(y_1, y_2)] \\ &= [(x_2, x_1)][(y_1, y_2)] \\ &= [(x_2y_1 + x_1y_2, x_2y_2 + x_1y_1)] \\ &= [(x_1y_2 + x_2y_1, x_1y_1 + x_2y_2)] \end{aligned}$$

$$\begin{aligned} x(-y) &= [(x_1, x_2)](-[(y_1, y_2)]) \\ &= [(x_1, x_2)][(y_2, y_1)] \\ &= [(x_1y_2 + x_2y_1, x_1y_1 + x_2y_2)] \end{aligned}$$

You can see that all three integers are equal. □

15.30 Exercises:

15.30.1 Prove that if x is any integer, then $x + (-x) = 0$.

15.30.2 Prove that if x and y are integers, then $-(x + y) = (-x) + (-y)$.

15.30.3 Prove that if x is an integer, then $-x = (-1)x$.

15.31 Cancellation: These properties of negation along with what we know about factors of 0 can be used to show that multiplication of integers is cancellative - almost.
Theorem: Suppose x, y, and z are integers and $z \neq 0$. If $xz = yz$ then $x = y$.

Proof: Suppose x, y, and z are integers, $xz = yz$, and $z \neq 0$. Adding $-(yz)$ to both sides of this equation yields $xz + (-(yz)) = yz + (-(yz))$. Exercise 15.30.1 now yields $xz + (-(yz)) = 0$. The comments in 15.29 now give $xz + (-y)z = 0$. We can now use the distributive property proved in 15.21 to factor out a z and arrive at $(x + (-y))z = 0$. Since $z \neq 0$, 15.27 now tells us that $x + (-y) = 0$. Adding y to both sides of this equation and applying Exercise 15.30.1 now gives $x = y$ as desired. □

Theorem: Suppose x, y, and z are integers. If $x + z = y + z$ then $x = y$.

Proof: This is the next exercise.

15.32 Exercise: Prove that addition of integers is cancellative.

15.33 Order: We now want to define an order on the integers. We need to decide when a difference $a - b$ is less than a difference $c - d$. From what we learned in algebra, if $a - b < c - d$ then $a + d < b + c$. Hence, we want to define $[(a, b)] < [(c, d)]$ to mean $a + d < b + c$.

15.34 Definition of Order: We will say that an integer $[(a, b)]$ is **less than** an integer $[(c, d)]$ if in the natural numbers $a+d < b+c$. We will denote this as $[(a, b)] < [(c, d)]$. We will say that an integer x is **less than or equal to** an integer y if either $x < y$ or $x = y$. This will be denoted as $x \leq y$.

15.35 Exercise: Prove that if a, b, c, and d are natural numbers then $[(a, b)] \leq [(c, d)]$ if and only if $a + d \leq b + c$.

15.36 Properties of Order: The order on the integers satisfies many of the same properties as the order on the natural numbers.
Theorem: Suppose x, y, and z are integers. If $x \leq y$ and $y \leq z$, then $x \leq z$.

Proof: Let x, y, and z be integers and suppose $x \leq y$ and $y \leq z$. We will show that $x \leq z$. There are natural numbers x_1, x_2, y_1, y_2, z_1, and z_2 so that $x = [(x_1, x_2)]$, $y = [(y_1, y_2)]$, and $z = [(z_1, z_2)]$. Since $x \leq y$, we know that $x_1 + y_2 \leq x_2 + y_1$. Since $y \leq z$, we know that $y_1 + z_2 \leq y_2 + z_1$. It follows that $x_1+y_2+y_1+z_2 \leq x_2+y_1+y_2+z_2$ and that $x_1+z_2 \leq x_2+z_1$, so $x \leq z$. □

Theorem: Suppose x, y, z, and w are integers. If $x \leq y$ and $z \leq w$, then $x + z \leq y + w$.

Proof: Let x, y, z, and w be integers and suppose $x \leq y$ and $z \leq w$. We will show that $x + z \leq y + w$. There are natural numbers $x_1, x_2, y_1, y_2, z_1, z_2, w_1$,

and w_2 so that $x = [(x_1, x_2)]$, $y = [(y_1, y_2)]$, $z = [(z_1, z_2)]$ and $w = [(w_1, w_2)]$. Since $x \leq y$ and $z \leq w$, we know that $x_1 + y_2 \leq x_2 + y_1$ and $z_1 + w_2 \leq z_2 + w_1$. It follows that $x_1 + y_2 + z_1 + w_2 \leq x_2 + y_1 + z_2 + w_1$ and, in turn, that $(x_1 + z_1) + (y_2 + w_2) \leq (x_2 + z_2) + (y_1 + w_1)$. It follows that

$$x + z = [(x_1 + z_1, x_2 + z_2)] \leq [(y_1 + w_1, y_2, w_2)] = y + w$$

as desired. □

Theorem: Suppose x and y are integers. If $x \leq y$ and $y \leq x$, then $x = y$.

Proof: Suppose that x and y are integers, $x \leq y$, and $y \leq x$. We will show that $x = y$. Since $x \leq y$ and $y \leq x$, we know that $x_1 + y_2 \leq x_2 + y_1$ and $y_1 + x_2 \leq y_2 + x_1$. Since we cannot have both $x_1 + y_2 < x_2 + y_1$ and $y_1 + x_2 < y_2 + x_1$, one of these must be an equality (and hence the other is also, but we only need one). Thus, $x_1 + y_2 = x_2 + y_1$. This means that $(x_1, x_2) \sim (y_1, y_2)$, so $x = y$. □

15.37 Positive and Negative: If x is an integer and $0 < x$, we will say that x is **positive**. If $x < 0$, then we will say that x is **negative**. Note that 0 is neither positive or negative.

15.38 Exercises:

15.38.1 Let a and b be natural numbers. Prove that $[(a, b)]$ is positive if and only if $b < a$.

15.38.2 Let a and b be natural numbers. Prove that $[(a, b)]$ is negative if and only if $a < b$.

15.38.3 Use the previous exercises to prove that if z is a positive integer, then $-z$ is a negative integer.

15.38.4 Use the previous exercises to prove that if z is a negative integer, then $-z$ is a positive integer.

15.38.5 Suppose x and y are integers. Use the previous exercises to prove that if $x \leq y$ then $-y \leq -x$.

15.38.6 Use the previous exercises to prove that a positive integer times a positive integer is positive.

15.38.7 Use the previous exercises to prove that a negative integer times a negative integer is positive. (Hint: If x and y are negative, then $-x$ and $-y$ are positive. You know that $(-x)(-y) = -(-(xy))$.)

15.38.8 Use the previous exercises to prove that a negative integer times a positive integer is negative.

15.39 Exercises:

15.39.1 Prove that if n and m are natural numbers then $[(n,0)]+[(m,0)] = [(n+m,0)]$.
15.39.2 Prove that if n and m are natural numbers then $[(n,0)]\cdot[(m,0)] = [(nm,0)]$.
15.39.3 Prove that if n and m are natural numbers then $[(n,0)] = [(m,0)]$ if and only if $n = m$.
15.39.4 Prove that if n and m are natural numbers then $[(n,0)] < [(m,0)]$ if and only if $n < m$.

15.40 Inclusion of Natural Numbers: It is standard to identify a natural number n with the integer $[(n,0)]$. Every positive integer is of this form, and every integer of this form is positive. Hence, each natural number is identified to a positive integer, and each positive integer is identified to a natural number. The previous exercises show that the addition, multiplication, and order of the natural numbers exactly coincide with the addition, multiplication, and order of the positive integers. Natural numbers, then, take on two faces. They are an entity in and of themselves, but they are also identical to the positive integers. Using this convention, it is typical to think of the integers as $\mathbb{N}$ along with 0 and $\{-n : n \in \mathbb{N}\}$.

16

The Rational Numbers

16.1 Equations and Multiplicative Inverses: The equation $2 + x = 1$ has no solution if we are required only to use natural numbers. However, there is a solution (-1) if we are allowed to use integers. There are equations (for example $2x = 1$ and $x^2 = 2$ and $x^2 + 1 = 0$) which cannot be solved using only integers. We want now to enlarge our number system until we can solve all such equations.

We begin by solving the equation $2 + x = 1$ using integers. We can solve this equation by adding -2 to both sides of the equation to arrive at $(-2)+2+x = (-2) + 1$. This then becomes $0 + x = -1$, and then $x = -1$. The essential parts of this solution (other than the associativity of $+$) are the facts that $0 + x = x$ and that there is a number we can add to 2 to get 0.

Now think about the equation $2x = 1$. This is identical to the previous equation, except addition has been replaced by multiplication. We know that $1 \cdot x = x$ for all integers x. Thus if there were some number q so that $q \cdot 2 = 1$, we could multiply this equation by q to get $1 \cdot x = q1$, which would yield $x = q$. Such a number q would be called the multiplicative inverse of 2. Unfortunately, there is no such number q in $\mathbb{Z}$.

We are, however, mathematicians. When there is no solution to a problem, we can always create one. In this chapter, we will derive the rational numbers. These will allow us to solve the first of the three equations above. The process of deriving the rational numbers is similar to that we experienced with the integers, so we will move quickly through it proving very little along the way.

16.2 Properties of Integers: First, we recall some properties of the integers. The integers are a set $\mathbb{Z}$ endowed with two binary operations $\cdot$ and $+$, a unary operation "-," and an order relation $\leq$ which all satisfy the following properties. Each of these properties appears directly in Chapter 12 or follows from something proven there.

For all $x, y, z, w \in \mathbb{Z}$, the following are true

Properties of Addition:

$x + (y + z) = (x + y) + z$	associative law
$x + y = y + x$	commutative law
$y + x = z + x$ if and only if $y = z$	cancellation law
$x + 0 = 0 + x = x$	additive identitiy

Properties of Multiplication:

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	associative law
$x \cdot y = y \cdot x$	commutative law
$x \cdot 1 = 1 \cdot x = x$	multiplicative identity
$x \cdot 0 = 0 \cdot x = 0$	
If $x \neq 0$ then $y \cdot x = z \cdot x$ if and only if $y = z$	cancellation law
If xy=0 then $x = 0$ or $y = 0$	
$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$	distributive law

Order Properties:

If $x \leq y$ and $y \leq z$ then $x \leq z$	$\leq$ transitive
If $x \leq y$ and $y \leq x$ then $x = y$	$\leq$ antisymmetric
If $0 < x$ then $y \leq z$ if and only if $xy \leq xz$	
If $x < 0$ then $y \leq z$ if and only if $xz \leq xy$	
If $x \leq y$ and $z \leq w$ then $x + z \leq y + w$	
$x \leq y$ if and only if $x + z \leq y + z$	

Properties of Negation:

$-(xy) = (-x)y = x(-y)$	
$x + (-x) = 0$	additive inverse
$-(x + y) = (-x) + (-y)$	
$(-x)(-y) = xy$	
$-(-x) = x$	
$0 < x$ if and only if $(-x) < 0$	

16.3 An Equivalence Relation: Let $\mathbb{Z}^*$ be the set of all non-zero integers. Define a relation $\sim$ on the set $\mathbb{Z} \times \mathbb{Z}^*$ by $(a, b) \sim (c, d)$ if and only if $ad = bc$. (You should compare this with the relation defined in 15.4)

16.4 Exercises:

16.4.1 Find two different ordered pairs (a, b) so that $(a, b) \sim (3, 4)$

16.4.2 Find two different ordered pairs (a, b) so that $(a, b) \sim (1, 2)$

16.4.3 Prove that the relation $\sim$ is an equivalence relation.

16.5 The Rational Numbers: Define the **rational numbers** to be the set $\mathbb{Q}$ of all equivalence classes of $\sim$. It is typical to write the equivalence class of (a, b) mod $\sim$ as $\frac{a}{b}$ (rather than $[(a, b)]$). The equivalence class $\frac{a}{b}$ is called the **quotient** or **fraction** of a over b or the **ratio** of a to b. In the fraction $\frac{a}{b}$, a is called the **numerator** and b is called the **denominator**. With fraction notation, note that two equivalence classes $\frac{a}{b}$ and $\frac{c}{d}$ are the same if and only

if $(a, b) \sim (c, d)$. That is $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$ (this should be a familiar condition).

16.6 Exercises:

16.6.1 If a and b are nonzero integers, prove that $\frac{a}{a} = \frac{b}{b}$.

16.6.2 If a and b are nonzero integers, prove that $\frac{0}{a} = \frac{0}{b}$.

16.6.3 If a, $b \neq 0$, and $c \neq 0$ are integers prove $\frac{a}{b} = \frac{ac}{bc}$.

16.6.4 If a and b are integers with $b \neq 0$, prove that $\frac{-a}{b} = \frac{a}{-b}$. Because of this, we usually just write $-\frac{a}{b}$ for either $\frac{-a}{b}$ or $\frac{a}{-b}$.

16.6.5 If a and b are integers with $b \neq 0$, prove that $\frac{a}{b} = \frac{-a}{-b}$

16.7 0 and 1: $\mathbb{Q}$ has elements which behave like 0 and 1 in the integers. We will abuse notation here (like we did in the integers) and call them 0 and 1. If b is any nonzero integer, define $0 = \frac{0}{b}$ and $1 = \frac{b}{b}$ (notice the choice of b is irrelevant by Exercise 16.6.1).

16.8 Operations: Define addition and multiplication in the following ways. If $\frac{a}{b}$ and $\frac{c}{d}$ are rational numbers, let

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \text{ and } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

(Of course, we would need to show these are well defined as we did in the integers, but that is not difficult.)

16.9 Exercises:

16.9.1 Use the definition of multiplication to prove that $1 \cdot \frac{a}{b} = \frac{a}{b}$.

16.9.2 Use the definition of addition to prove that $0 + \frac{a}{b} = \frac{a}{b}$.

16.9.3 Use the definition of addition to prove that $\frac{a}{b} + \left(-\frac{a}{b}\right) = 0$.

16.9.4 Suppose a and b are nonzero integers. Use the definition of multiplication to prove that $\frac{a}{b} \cdot \frac{b}{a} = 1$.

16.9.5 Use the definition of addition to prove that $\frac{a}{b} + \frac{c}{b} = \frac{a + c}{b}$.

16.10 Multiplicative Inverses: A **multiplicative inverse** of a rational number q is a rational number r so that $qr = 1$. If q is any rational number other than 0, there are nonzero integers a and b so that $q = \frac{a}{b}$. By The previous exercise, it follows that q has a multiplicative inverse, $\frac{b}{a}$. Hence, we have

Theorem: Every nonzero rational number has a multiplicative inverse.

We will denote the multiplicative inverse of q by q^{-1}.

16.11 Positive Denominators: As a result of Exercise 16.6.4 we can state the following theorem.
Theorem: Every rational number can be expressed as $\frac{a}{b}$ where b is positive.

16.12 Order: If $q = \frac{a}{b}$ and $r = \frac{c}{d}$ with b and d positive, then q is **less than** r (denoted $q < r$) if $ad < bc$. If q is either less than or equal to r, then we will write $q \leq r$. Define a rational number q to be **positive** if $0 < q$. Define a rational number q to be **negative** if $q < 0$.

16.13 Exercise: Prove that a rational number $\frac{a}{b}$ is positive if and only if a and b are both positive or a and b are both negative. (Hint: One direction is easy. For the other, assume $0 < \frac{a}{b}$. Note that the definition of $<$ requires the denominator to be positive. If $b > 0$, things go smoothly. If $b < 0$, use the fact that $\frac{a}{b} = \frac{-a}{-b}$ along with the definition of $<$.)

16.14 Properties of the Rationals: With the definitions we have made combined with what we know about the integers, we can repeat much of what we did in Chapters 11, 7 and 12 to derive arithmetical and order properties of the rational numbers. Since the process is similar to that which we have experienced, we will dispense with the derivation of most of them. We can prove that all of the properties listed above for the integers hold along with the following.
Properties of the multiplicative inverse
For all nonzero x and y in $\mathbb{Q}$, the following are true
$x \cdot (x^{-1}) = (x^{-1})x = 1$
$(xy)^{-1} = (y^{-1})(x^{-1})$
If $0 < x \leq y$ then $0 < y^{-1} \leq x^{-1}$

16.15 Exercise: Prove that if $q \neq 0$ and r are rational numbers, then there is a rational number x so that $qx = r$. (As a result, it is not worthwhile to discuss divisibility of rational numbers.)

16.16 Density: In Chapters 11 and 7, we saw that $1 < 2$ but there is no natural number x so that $1 < x < 2$. However, this is not the case in $\mathbb{Q}$. This next theorem establishes that the rational numbers in a sense are **dense**. There are no "gaps" between rational numbers as there are between integers.
Theorem: Suppose q and r are rational numbers and $q < r$. There is some natural number x so that $q < x$ and $x < r$.

Proof: This follows immediately from the next exercise. □

16.17 Exercise: Suppose that q and r are rational numbers and $q < r$. Let $x = \frac{1}{2} \cdot (q + r)$. Prove that $q < x$ and $x < r$. (Hint: First add r to both sides of $q < r$ and multiply by $\frac{1}{2}$. Do the same with q.)

16.18 Inclusion of Integers: We want to associate the integers with rational numbers of the form $\frac{n}{1}$. To do so, we must show that the addition, multiplication, negation, and order of the integers is the same as that of rational numbers of the form $\frac{n}{1}$. Once this is done, we will identify the integers with the rational numbers of this form. We will then write n for any rational number $\frac{n}{1}$. The work is accomplished in the following exercises.

16.19 Exercises: Let n and m be integers. Prove the following.

16.19.1 $\frac{n}{1} + \frac{m}{1} = \frac{n+m}{1}$

16.19.2 $\frac{n}{1} \cdot \frac{m}{1} = \frac{nm}{1}$

16.19.3 $\frac{n}{1} < \frac{m}{1}$ if and only if $n < m$

16.19.4 $-\frac{n}{1} = \frac{-n}{1}$

16.20 Exercise: Prove that if $\frac{a}{b}$ is any rational number then $\frac{a}{b} = ab^{-1}$ (where on the right $a = \frac{a}{1}$ and $b = \frac{b}{1}$).

16.21 The Square Root of 2: The properties of the rational numbers we have defined allow us to solve "linear equations" – those equations of the form $ax + b = c$ (simply add $-b$ to both sides of the equation and then multiply by a^{-1}.). Thus, we can solve the first equation $2x = 1$ from the list in 16.1. We want now to prove that we cannot solve the second equation using rational numbers.

Theorem: There is no rational number q so that $q^2 = 2$.

Proof: We prove by contradiction that there is no rational number q so that $q^2 = 2$. Suppose that q is a rational number and that $q^2 = 2$. We can assume that q is positive. (If q were negative, then $(-q)(-q) = q^2 = 2$ also). Since q is rational, there are integers a and b (with $b \neq 0$) so that $q = \frac{a}{b}$. Since q is positive, we can apply 16.11 and 16.13 to assume that a and b are both positive. Using 16.6.3, we can assume that there is no integer n which is a factor of both a and b. Since $\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$, we have $\frac{a^2}{b^2} = \frac{2}{1}$. Using the comments in 16.5, this means that $a^2 = 2b^2$. This is an equation with only positive integers. Since the positive integers are identical to the natural numbers, we can now refer to all we know about natural numbers. We see from this equation that $2|a^2$, so a^2 is even. It follows then that a is even (by 7.23).

Since a is even $2|a$. Since no integer divides both a and b, note that we know then that 2 does not divide b (this is what we will contradict shortly). Since $2|a$, there is an integer k so that $a = 2k$. This means $a^2 = 4k^2$, so $a^2 = 2b^2$ is $4k^2 = 2b^2$. Using the cancellation law for multiplication in the natural numbers, it follows that $2k^2 = b^2$. Hence, $2|b^2$ so $2|b$. This is a contradiction, so the assumption that $q^2 = 2$ must be false. For any rational number q, it cannot be that $q^2 = 2$. □

16.22 Deficiency: Since there is no rational solution to the equation $x^2 - 2 = 0$, the rational numbers seem to have some kind of deficiency. We will develop a number system without that deficiency in Chapter 17.

17

The Real and Complex Numbers

17.1 Equations With No Solutions: In 16.21 we saw that the equation $x^2 = 2$ cannot be solved using rational numbers. We would like to eventually derive a number system in which we can solve any equation involving polynomials with natural number coefficients. Our next step after the rationals is to define the real numbers. There are a number of ways in which this can be done - most of which are more complicated (or at least more abstract) than the manner in which the integers and rationals were defined. We outline one method here and another in Chapter 13.

17.2 Upper Bounds: Suppose that S is a set of rational numbers. An **upper bound** of S is a rational number u which is greater than or equal to every element of S (that is, if $x \in S$ then $x \leq u$). A **least upper bound** of S would be an upper bound w which is less than or equal to every other upper bound (if u is another upper bound, then $w \leq u$). Upper bounds, and hence least upper bounds, do not always exist. A set which has an upper bound is called **bounded above**. Note that we could make these same definitions in any number system with an order $\leq$.

17.3 Examples: The set of all positive rational numbers is not bounded above. The set of negative rational numbers is bounded above. It has a least upper bound which is 0.

17.4 Exercises: For each set of rational numbers, give one upper bound. Then decide which sets have a least upper bound.
17.4.1 $\{x \in \mathbb{Q} : x^2 \leq 4\}$
17.4.2 $\{x \in \mathbb{Q} : x^2 \leq 2\}$
17.4.3 $\{n/(n+1) : n \in \mathbb{Z}\}$

17.5 Dedekind Cuts: A **Dedekind cut** of the rational numbers is a subset S of the rational numbers which satisfies these properties.

- S is bounded above
- If $y \in S$ and $x \leq y$, then $x \in S$
- If S has a least upper bound (in $\mathbb{Q}$), it is not an element of S.

You can imagine a Dedekind cut as being an open interval $(-\infty, u)$ (except that u may not be a rational number). Two examples of Dedekind cuts are $\{x \in \mathbb{Q} : x^2 \leq 2\}$ and $\{x \in \mathbb{Q} : x < 0\}$.

17.6 Real Numbers from Dedekind Cuts: We define the real numbers to be the set of all Dedekind cuts of the rational numbers. With this definition, each real number is a set S of rational numbers satisfying the properties in 17.5

17.7 Operations and Order: Define 0 to be the Dedekind cut $\{x \in \mathbb{Q} : x < 0\}$ and define 1 to be the Dedekind cut $\{x \in \mathbb{Q} : x < 1\}$. If R and S are real numbers, then $R < S$ if $R \subset S$ (as sets). If either $R < S$ or $R = S$, then we write $R \leq S$ (which is equivalent to $R \subseteq S$). If $R < 0$, then R is **negative**. If $0 < R$, then R is **positive**. We define addition, multiplication, and negation of real numbers in the following way. If R and S are real numbers (these special intervals of rational numbers) then

$$R + S = \{r + s : r \in R \text{ and } s \in S\}$$

$$-R = \{-x : x \notin R \text{ and } x \text{ is not the least upper bound of } R\}$$

It should be clear from these definitions that every R is either positive or negative but not both and that $R \leq 0$ if and only if $0 \leq -R$ and $0 \leq R$ if and only if $-R \leq 0$. If $0 \leq R$ and $0 \leq S$ then define $R \cdot S$ to be the set of all rational x so that either x is negative or there are positive $r \in R$ and $s \in S$ with $x \leq rs$. If $R < 0$ and $S < 0$, define $R \cdot S = -((-R) \cdot (-S))$. If $R < 0$ and $0 \leq S$, define $R \cdot S = -((-R) \cdot S)$. If $0 \leq R$ and $S < 0$, define $R \cdot S = -(R \cdot (-S))$. Using these definitions we could prove that all of the properties listed for rational numbers in Chapter 16 hold also for real numbers.

17.8 Exercise: Prove that addition on the real numbers as defined using Dedekind cuts is associative. (Hint: $(R + S) + T = \{(r + s) + t : r \in R, s \in S, t \in T\}$, and these are sets)

17.9 Inclusion of $\mathbb{Q}$: Our definition of the real numbers allows us to identify a subset of $\mathbb{R}$ with $\mathbb{Q}$, so that we can view all of the rational numbers as real numbers. Any rational number q corresponds to the Dedekind cut $\{a \in \mathbb{Q} : a < q\}$.

17.10 Irrational Numbers: Any real number which is not a rational number (not in the inclusion of the rationals in $\mathbb{R}$) is called an **irrational number**.

17.11 The Density of $\mathbb{Q}$: Not only are the rational numbers included in $\mathbb{R}$, they are scattered throughout $\mathbb{R}$ densely.
Theorem: If $x < y$ are real numbers, then there is a rational number q so that $x < q < y$.

Discussion: This simply says that between any two real numbers there is a rational number.

Proof: Suppose that x and y are real numbers and $x < y$. We will use the Dedekind cut definition of the real numbers to prove that there is a $q \in \mathbb{Q}$ with $x < q < y$. Since $x < y$ as real numbers, we know that $x \subset y$ as Dedekind cuts. In particular, $x \neq y$. Since $x, y \subseteq \mathbb{Q}$ there is a $q \in Q$ so that $q \in y$ and $q \notin x$. As a real number, q corresponds to the Dedekind cut $\{x \in \mathbb{Q} : x < q\}$. Since $x \subset \{a \in \mathbb{Q} : a < q\} \subset y$, it follows that as real numbers $x < q < y$. □

17.12 Exercise: Suppose that X is a set of real numbers which has an upper bound U (each element of X is a Dedekind cut, and each of these is a subset of the Dekind cut U). Let Y be the union of all of the sets in X. Prove the following.

17.12.1 Y is a Dedekind cut. (Hint: For the first property, show any upper bound of U is an upper bound of Y. For the second, if $y \in Y$, then $y \in S$ for some $S \in X$. For the third, show that if Y contained a least upper bound, then one of the sets in X must contain the same element as a least upper bound.)

17.12.2 Y is an upper bound of X. (Hint: Definition of union)

17.12.3 Y is the least upper bound of X (Hint: Definition of union)

17.13 Completeness: There are sets of rational numbers which have upper bounds but do not have least upper bounds (for example $\{x \in \mathbb{Q} : x^2 < 2\}$). From the previous exercise, this cannot happen in $\mathbb{R}$. This exercise proves the next theorem.

Completeness Theorem: Every set of real numbers which has an upper bound has a least upper bound.

Discussion: Some mathematicians which begin their investigations with $\mathbb{R}$ rather than $\mathbb{N}$ as we have done take this as an axiom (they simply assume it to be true). The machinery we have makes it not too difficult to actually prove.

17.14 Exponents: We have been using exponents occasionally during this course. We defined in Chapter 7 how to raise a natural number to a positive exponent. We extend that definition in the next few sections here. Let r be a real number. Define $r^0 = 1$. If r^n is defined, define $r^{n+1} = r \cdot r^n$. (This is essentially the same recursive definition given in Chapter 7 with the addition of 0 as an exponent).

17.15 Roots: Suppose that r is a non-negative real number and n is a positive integer. Let S be the set $\{x \in \mathbb{R} : x^n < r\}$. This set has an upper bound (r for example). By the completeness property of the real numbers, S has a least upper bound u. This upper bound will satisfy the property that $u^n = r$. If n is odd, it follows from the properties of negation that $(-u)^n = -r$. It also follows from the properties of negation that if n is even

then $(-u)^n$ is also equal to r and that there is no real number v with $v^n = -r$. This motivates the next definitions.

If u and r are real numbers and n is a positive integer, then u is an n^{th} **root** of r if $u^n = r$. If u and r are either both positive or both negative, then u is the **principle** n^{th} **root of** r. The principle n^{th} root of r is denoted by $r^{\frac{1}{n}}$. Note that it follows from earlier comments that if n is even and r is negative, then r has no n^{th} root.

17.16 Exercises: Find

17.16.1 $(64)^{\frac{1}{2}}$
17.16.2 $(64)^{\frac{1}{6}}$
17.16.3 $(125)^{\frac{1}{3}}$
17.16.4 $(81)^{\frac{1}{4}}$
17.16.5 $(27)^{\frac{1}{3}}$
17.16.6 $8^{\frac{1}{3}}$

17.17 Positive Rational Exponents: Suppose that m and n are positive integers with no common divisors. If r is any real number then $r^{\frac{m}{n}}$ is defined to be $(r^{\frac{1}{n}})^m$ (if $r^{\frac{1}{n}}$ exists). For example $8^{\frac{2}{3}} = (8^{\frac{1}{3}})^2 = 2^2 = 4$.

17.18 Exercises: Find
(1) $(81)^{\frac{3}{4}}$ (2) $(64)^{\frac{5}{6}}$ (3) $(27)^{\frac{4}{3}}$ (4) $(8)^{\frac{5}{3}}$

17.19 Negative Exponents: If r is not zero, then r has a multiplicative inverse r^{-1}. We will use this multiplicative inverse to allow negative exponents. Suppose $m > 0$ and $n > 0$ are positive integers and r is a non-zero real number. Define $r^{-\frac{m}{n}} = ((r^{-1})^{\frac{1}{n}})^m$.

17.20 Exercises: Recall that the multiplicative inverse of a rational number $\frac{a}{b}$ is $\frac{b}{a}$. Find
(1) $\left(\frac{81}{16}\right)^{-\frac{3}{4}}$ (2) $\left(\frac{27}{8}\right)^{-\frac{2}{3}}$

17.21 The Equation $x^2 + 1 = 0$: From the comments in 17.15, it follows that there is no real number so that $x^2 = -1$. Therefore, there is no real solution to the equation $x^2 + 1 = 0$. Our next (and last!) step in the derivation of number systems is to rectify this deficiency.

17.22 Complex Numbers as Ordered Pairs: We will first give an abstract definition of the complex numbers and then show how this is equivalent to that given in high school algebra. Define the **complex numbers** to be the set $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Define addition, multiplication, and negation on $\mathbb{C}$ by

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac + (-bd), ad + bc)$$

$$-(a, b) = (-a, -b)$$

Define 0 to be the complex number $(0, 0)$, and define 1 to be the complex number $(1, 0)$. With these definitions, all of the properties of real numbers and rational numbers listed in Chapter 16 (except for those involving $\leq$) are true for $\mathbb{C}$.

17.23 Exercises:

17.23.1 Add $(12, 43) + (-9, 4)$

17.23.2 Add $(a, 0) + (b, 0) \cdot (0, 1)$

17.23.3 Multiply $(-3, 7) \cdot (-4, -2)$

17.23.4 Multiply $(0, 1) \cdot (0, 1)$

17.23.5 Prove that $(a, 0) + (b, 0) = (a + b, 0)$ and $(a, 0)(b, 0) = (ab, 0)$.

17.24 Inclusion of the Reals: Exercise 17.23.5 lets us view the real numbers as a subset of the complex numbers by identifying any real number x with the complex number $(x, 0)$.

17.25 The Number i and Equations: Denote the complex number $(0, 1)$ by the letter i. Notice that from Exercise 17.23.4 we know that $i^2 = -1$. Thus, $\mathbb{C}$ has a solution to the equation $x^2 + 1 = 0$. In fact, every equation of the form $p(x) = 0$ where $p(x)$ is a polynomial with complex coefficients can be solved in $\mathbb{C}$.

17.26 Notation: We noticed in Exercise 17.23.2 that every complex number (a, b) can be expressed as $(a, 0) + (b, 0)(0, 1)$. If we agree to write all complex numbers of the form $(x, 0)$ simply as x, and if we write i for $(0, 1)$, then every complex number (a, b) can be written in the form $a + bi$. In the number $a + bi$, a is called the **real part** and b the **imaginary part**. With this notation, we can do arithmetic with complex numbers without trying to remember the formulas for how to multiply and add ordered pairs. Adding is simple:

$$(a + bi) + (c + di) = a + c + bi + di = (a + c) + (b + d)i$$

Negation is just as simple:

$$-(a + bi) = (-a) + (-b)i$$

Multiplication is slightly more complicated. We must use the distributive law a couple of times and then replace i^2 by -1:
$(a + bi)(c + di) = ac + adi + bci + bdi^2$

$$= ac + (ad + bc)i + (-bd) = (ac + (-bd)) + (ad + bc)i$$

A complex number of the form $a + 0i$ we will write simply as a. We will call these real. Numbers of the form $0 + bi$ will be written as bi.

17.27 Exercises: Perform the indicated operations.
(1) $(2 + 3i) \cdot (-3 + 5i) + (1 + i)$ (2) $(7 + (-2i)) \cdot (7 + 2i)$

17.28 Fractions: The fractional notation we used for rational numbers is useful when dealing with multiplicative inverses of real numbers, so we extend the definition of the notation. For real numbers x and y, define $\frac{x}{y} = xy^{-1}$. Let a, b, c, and d be real numbers. Notice

$$\frac{a}{b} \cdot \frac{c}{d} = (ab^{-1}) \cdot (cd^{-1}) = acb^{-1}d^{-1} = (ac)(bd)^{-1} = \frac{ac}{bd}$$

$$\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= (ab^{-1}) + (cd^{-1}) \\
&= (ab^{-1})1 + (cd^{-1})1 \\
&= (ab^{-1})(dd^{-1}) + (cd^{-1})(bb^{-1}) \\
&= (ad)(b^{-1}d^{-1}) + (bc)(b^{-1}d^{-1}) \\
&= (ad)(bd)^{-1} + (bc)(bd)^{-1} \\
&= (ad + bc)(bd)^{-1} \\
&= \frac{ad + bc}{bd}
\end{aligned}$$

Thus, with this notation, the rules for the addition and multiplication of fractions of real numbers are the same as the rules for multiplication and addition of rational numbers.

17.29 Exercise: Prove that the multiplicative inverse of $a+bi$ is $\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i$.

17.30 Complex Fractions: Since complex numbers also have multiplicative inverses, we can extend the fraction notation to include complex numerators and denominators. The above arguments follow through to show that the formulas for adding and multiplying fractions of complex numbers are the same as for rational numbers or real numbers. Any complex fraction of the form $\frac{a + bi}{c + di}$ can be written in the form $x + yi$. To see how this is done, we give an example. We will write the fraction $\frac{1 + 2i}{3 + 4i}$ in this form. To do so, we first multiply by $\frac{3 + (-4i)}{3 + (-4i)} = 1$. The number $3 + (-4i)$ is called the **complex**

conjugate of $3+4i$. We proceed:

$$\begin{aligned}\frac{1+2i}{3+4i} &= \frac{1+2i}{3+4i}\cdot\frac{3+(-4i)}{3+(-4i)} = \frac{(1+2i)(3+(-4i))}{(3+4i)(3+(-4i))}\\ &= \frac{3+(-4i)+6i+(-8i^2)}{9+(-12i)+12i+(-16i^2)} = \frac{3+2i+8}{9+16}\\ &= \frac{11+2i}{25} = \frac{11}{25}+\frac{2}{25}i\end{aligned}$$

17.31 **Exercises:** Write each fraction in the form $x+yi$.

(1) $\dfrac{1+i}{1+(-i)}$ (2) $\dfrac{2+3i}{3+(-i)}$ (3) $\dfrac{i}{2+2i}$

18

Special Functions and Sets

18.1 Characteristic Functions: Suppose that B is a subset of some set A. The **characteristic function** of B is the function $\chi_B : A \to \{0, 1\}$ defined by

$$\chi_B(x) = \begin{cases} 1 & x \in B \\ 0 & x \notin B \end{cases}$$

for all $x \in A$. The characteristic function of a set B distinguishes between those elements in B and those elements not in B by mapping elements of B to 1 and everything else to 0. In fact for any $x \in A$, $\chi_B(x) = 1$ **if and only if** $x \in B$. (The symbol χ is the greek letter "chi.")

18.2 Characteristic Functions Unique: A set is uniquely determined by its characteristic function, and vice-versa.
Theorem: Suppose B and C are subsets of some set A. Then $\chi_B = \chi_C$ if and only if $B = C$.

Proof: Suppose that $\chi_B = \chi_C$. We first show that $B \subseteq C$. Let $x \in B$. This means that $\chi_C(x) = \chi_B(x) = 1$. Since $\chi_C(x) = 1$, we can conclude that $x \in C$. Thus we see that $B \subseteq C$. The proof that $C \subseteq B$ is similar, so we actually have $B = C$.

Next, suppose that $B = C$. Let $x \in A$. We must show that $\chi_B(x) = \chi_C(x)$. Either $x \in B$ or $x \notin B$. If $x \in B$, then $\chi_B(x) = 1$. Since $B = C$, we also have that $x \in C$ and $\chi_C(x) = 1$. Hence, $\chi_B(x) = \chi_C(x)$ when $x \in B$. Next, suppose that $x \notin B$. Then $\chi_B(x) = 0$. Since $B = C$, $x \notin C$, so $\chi_C(x) = 0$. Hence $\chi_B(x)$ and $\chi_C(x)$ are also equal when $x \notin B$. Thus, $\chi_B = \chi_C$. □

18.3 Exercise: Suppose A is a set and $f : A \to \{0, 1\}$ is any function. Find a subset $B \subseteq A$ so that f is precisely the function χ_B. It follows that all functions from A to $\{0, 1\}$ are characteristic functions.

18.4 An Order: Suppose B and C are subsets of some set A and let $a \in A$. Since $\chi_B(a)$ and $\chi_C(a)$ are numbers, it makes sense to ask if $\chi_B(a) \leq \chi_C(a)$. If for every $a \in A$ it is the case that $\chi_B(a) \leq \chi_C(a)$, we will say that χ_B is **less than or equal** to χ_C. We will denote this by $\chi_B \leq \chi_C$.

18.5 Exercise: Suppose that B and C are subsets of a set A. Prove that $\chi_B \leq \chi_C$ if and only if $B \subseteq C$.

18.6 Unions and Maximums: Suppose B and C are subsets of some set A and let $a \in A$. We just commented that we can ask if $\chi_B(a) \leq \chi_C(a)$. We can just as well ask for the larger of the two numbers. If a is in either B or C, then one of $\chi_B(a)$ or $\chi_C(a)$ is equal to 1, so the maximum between $\chi_B(a)$ and $\chi_C(a)$ is 1. Thus, the theorem in the next exercise might seem reasonable.

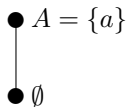
18.7 Exercise: Suppose B and C are subsets of some set A. Define a function $f : A \to \{0, 1\}$ so that $f(x)$ is the maximum between $\chi_B(x)$ and $\chi_C(x)$ for all $x \in A$. Prove that for all $x \in A$ $f(x) = \chi_{B \cup C}(x)$.

18.8 Intersections and Products: Suppose B and C are subsets of some set A and let $a \in A$. Since $\chi_B(a)$ and $\chi_C(a)$ are numbers, we can multiply them together. When we do so, $\chi_B(a) \cdot \chi_C(a)$ must be either 0 or 1. Define a function $f : A \to \{0, 1\}$ by $f(x) = \chi_B(x) \cdot \chi_C(x)$ for all $x \in A$. From 18.3, we know that f is the characteristic function of some subset of A. You get to prove in the next exercise that it is the characteristic function of $B \cap C$.

18.9 Exercise: Suppose B and C are subsets of some set A. Define a function $f : A \to \{0, 1\}$ by $f(x) = \chi_B(x) \cdot \chi_C(x)$ for all $x \in A$. Prove that for all $x \in A$, $f(x) = \chi_{B \cap C}(x)$.

18.10 Powersets: Recall that the powerset of a set A (denoted $\mathcal{P}(A)$) is the collection of all subsets of A. We can draw diagrams which depict the relationship between subsets of A. First, we draw a point for every subset of A. We then connect the points with arrows indicating the subset relation. The points are then re-arranged so that all of the arrows are pointing in an upward direction. Finally, redundant arrows are removed, and the arrows are replaced by line segments.

We begin with $A = \{a\}$. Then $\mathcal{P}(A) = \{\emptyset, \{a\}\}$ has only two elements. It is easy to draw a diagram which describes the relationship between subsets of A.

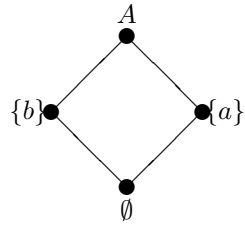


There are a few observations which we can make about this diagram.

- Every element of $\mathcal{P}(A)$ is represented by a point in the diagram.
- The lowest point in the diagram is $\emptyset$.
- The highest point in the diagram is A.
- If one subset contains another, then the larger subset is above the smaller in the picture, and there is a path of line segments connecting them.

A diagram such as this depicting an order relation such as the subset relation is called a **Hasse diagram**. We will discuss Hasse diagrams in Chapter 20.

18.11 Subsets of a Two Element Set: If $A = \{a, b\}$ is a two element set, then $\mathcal{P}(A)$ has four elements $\{\emptyset, \{a\}, \{b\}, A\}$. The Hasse diagram of $\mathcal{P}(A)$ would look like



18.12 Exercises:
18.12.1 Suppose that $A = \{a, b, c\}$. Then the powerset of A is the set

$$\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}.$$

Draw a Hasse diagram of $\mathcal{P}(A)$.
18.12.2 Suppose $A = \{a, b, c, d\}$. Then $\mathcal{P}(A)$ has 16 elements. Draw a Hasse diagram of $\mathcal{P}(A)$.
18.12.3 Select two subsets B and C on each of the diagrams you have just drawn. On each diagram, locate $B \cup C$ and $B \cap C$. Make a conjecture as to how the diagrams depict intersection and union.

18.13 Factor Sets: Recall from Chapter 10 that a relation R on a set A is an **equivalence relation** if it is reflexive, symmetric, and transitive. Also recall that if $a \in A$ then the **equivalence class** of a modulo R is the set $[a]_R = \{x \in A : aRx\}$ and that the **factor set** A/R is the set $\{[a]_R : a \in R\}$ of all equivalence classes of R. The **quotient map** from A to A/R is the map $\pi : A \to A/R$ given by $\pi(a) = [a]_R$.

18.14 Exercise: Suppose A is a set and R is an equivalence relation on A. Prove that the quotient map $\pi : A \to A/R$ is surjective.

18.15 Kernels: Suppose $f : A \to B$ is any function. Recall from Chapter 10 that the **kernel** of f is the relation $\ker f = \{(x, y) : f(x) = f(y)\}$. This is an equivalence relation on A by 10.29.

18.16 Exercise: Suppose $f : A \to B$ is any function. Define a function $\hat{f} : A/\ker f \to B$ by $\hat{f}([a]_{\ker f}) = f(a)$. If $\pi : A \to A/\ker f$ is the quotient map, prove that $\hat{f} \circ \pi = f$. Also prove that $\hat{f}$ is injective.

18.17 Exercise: Suppose that $f : A \to B$ is any injective function and that $a \in A$. How many elements can be in $[a]_{\ker f}$?

18.18 Exercise: Suppose that $f : A \to B$ is a surjective function and that $g : A \to C$ is any function. If there is a function $h : B \to C$ so that $g = h \circ f$, prove that $\ker f \subseteq \ker g$.

18.19 Exercise: Suppose that $f : A \to B$ is a surjective function and that $g : A \to C$ is any function. If $\ker f \subseteq \ker g$, prove that there is a function $h : B \to C$ so that $g = h \circ f$.

18.20 Products: If n is a natural number, then we will use A^n to denote the direct product of n copies of A (i.e. $A^1 = A$, $A^2 = A \times A$, $A^3 = A \times A \times A$, and so on). The set A^n will be called a **direct power** of A. The elements of A^n look like $(a_1, a_2, \ldots, a_n)$. If $n = 2$, these are called pairs. If $n = 3$, these are tripples. In general, elements of A^n are called **n-tuples**. It is common to use "bars" as a shorthand to refer to n-tuples. For example, we might refer to the n-tuple $(a_1, a_2, \ldots, a_n)$ as $\bar{a}$.

18.21 Functions and n-tuples: Suppose that A is a set and $\bar{a} \in A^n$. Define the function $f_{\bar{a}} : \{1, 2, \ldots, n\} \to A$ by $f_{\bar{a}}(i) = a_i$. For example, if $A = \{q, w, e, r, t\}$ and $\bar{a} = (r, w, t)$ (an element of A^3), then $f_{\bar{a}}(1) = r$, $f_{\bar{a}}(2) = w$, and $f_{\bar{a}}(3) = t$.

18.22 Exercise: Suppose that A is a set and n is natural number. Let X be the set of all functions from $\{1, 2, \ldots, n\}$ to A. Prove that the map $\bar{a} \to f_{\bar{a}}$ defined above is a bijection.

18.23 Functions and A^n: As a result of the previous exercise, there is a natural way to associate elements of A^n with functions from $\{1, 2, \ldots, n\}$ to A.

18.24 Permutations: Recall from Chapter 9 that a **permutation** on a set A is a bijective function from A to A. The collection of all permutations on a set A is denoted by S_A. The identity function 1_A is a permutation on A. In exercise 9.42, we showed that if f and g are permutations on a set A, then $f \circ g$ is also a permutation. From 9.26, we know that composition of permutations is associative. If f is a permutation, then by 9.36, f has an inverse f^{-1} which is also a permutation.

18.25 Exercise: Prove that if A is any set and $f : A \to A$ is any function, then $f \circ 1_A = 1_A \circ f = f$.

18.26 Properties of Permutations: From the previous exercise and the preceding comments, if A is any set then the collection S_A of permutations on A along with composition satisfy the following.

1. If $f, g \in S_A$, then $f \circ g \in S_A$.
2. If $f, g, h \in S_A$, then $f \circ (g \circ h) = (f \circ g) \circ h$.
3. There is an element $1_A \in S_A$ so that for all $f \in S_A$, the equality $1_A \circ f = f \circ 1_A = f$ holds.

4. If $f \in S_A$, then there is an element f^{-1} of S_A so that $f \circ f^{-1} = f^{-1} \circ f = 1_A$.

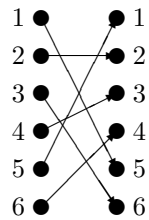
This list of properties seems a bit unusual, but they appear quite naturally in many areas of mathematics.

18.27 Exponents: Suppose that f is a permutation on a set A. Define $f^1 = f$. If k is a natural number and f^k is defined, define $f^{k+1} = f^k \circ f$. (i.e. $f^1 = f$, $f^2 = f \circ f$, $f^3 = f \circ f \circ f$, and so on). We will define $f^0 = 1_A$, and $f^{-n} = (f^{-1})^n$.

18.28 Exercise: Suppose that A is a set, and f is a permutation on A. (This exercise can be done using only the properties above and the definition of exponentiation. You do not have to use the fact that f is a function at all.) Prove that if n and m are natural numbers, then $f^m \circ f^n = f^{n+m}$ (Use induction on n).

18.29 Exponent Rules: The properties above can be used to show that the exponent rule $f^m \circ f^n = f^{n+m}$ actually holds for all integers n and m. Only the properties of permutations are necessary to prove this – not the fact that we are working with special functions.

18.30 Notation: There is a simple notation we can use to describe permutations on finite sets. To represent a permutation on the set $\{1, 2, \ldots, n\}$, we will use an array with n columns and two rows. The first row of the array is a list of the numbers $1, 2, \ldots, n$. In the second row, beneath 1 is placed the image of 1 under the permutation. Beneath 2 is placed the image of 2 under the permutation, and so on. For example, the permutation depicted here



would be represented by this matrix

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 3 & 1 & 4 \end{pmatrix}$$

18.31 Orbits: Suppose that f is a permutation on a set A and that $a \in A$. The **orbit** of a under f is the set $\{f^n(a) : n \in \mathbb{Z}\}$. (The orbit is just all of the elements of A that you get by applying f and f^{-1} repeatedly to a.)

18.32 Exercise: Find the orbit of each element of $\{1, 2, 3, 4, 5, 6\}$ under the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 3 & 1 & 4 \end{pmatrix}$.

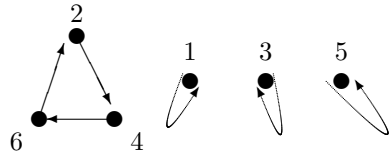
18.33 Exercises: Suppose f is a permutation on a set A.
18.33.1 Prove that if $a \in A$, then a is in the orbit of a under f. (Hint: f^0)
18.33.2 Suppose that $a, b \in A$, that X is the orbit of a under f, and that Y is the orbit of b under f. Prove that if $X \neq Y$, then $X \cap Y = \emptyset$. (Hint: Contrapositive).

18.34 Partition into Orbits: As a result of the previous exercises, the orbits of a permutation f on a set A form a partition of A. We will call this partition the **orbit partition** of f.

18.35 Cycles: A **cycle** is a permutation with only one orbit with more than one element. For example, consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$$

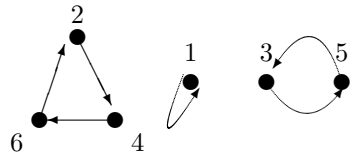
The orbits of this permutation are $\{1\}$, $\{3\}$, $\{5\}$, and $\{2, 4, 6\}$. Since only one of these orbits has more than one element, this is a cycle. A descriptive portrayal of this permutation might be something like this



The permutation rotates the numbers 2, 4, and 6 in a cycle while mapping 1, 3, and 5 to themselves. In contrast, this

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 6 & 3 & 2 \end{pmatrix}$$

which can be dipicted as



would not be a cycle since this permutation has two orbits with more than one element.

18.36 Exercises:
18.36.1 Find two different permutations on the set $\{1, 2, 3, 4, 5, 6\}$ which have the same orbit partition.
18.36.2 Suppose that P is a partition on a finite set A. Prove that P is the orbit partition of a permutation on A.
18.36.3 Can two different cycles have the same orbit partition? If your answer is yes, give and example. If your answer is no, prove it.

19

Algebras

19.1 Operations: Suppose A is a set and n is a natural number. An n-ary **operation** on A is a function from A^n to A. In particular, a **unary operation** is a function from A to A, a **binary operation** is a function from A^2 to A, and a **ternary** operation is a function from A^3 to A. The number n is the **rank** of an n-ary operation.

19.2 Notation: If f is an n-ary operation on a set A and if the n-tuple $(x_1, \ldots, x_n)$ is in A^n, we usually write $f(x_1, \ldots, x_n)$ for f applied to $(x_1, \ldots, x_n)$. This notation, in which the symbol for an operation is written before its arguments, is called **prefix notation**. Some fields of mathematics also use **postfix** notation in which the symbol for an operation is written after its arguments – such as $(x_1, \ldots, x_n)f$. We will not use this notation much; however, we note that it is useful in computer science when one is working with stack based languages. For binary operations, there is a third option. The symbol for a binary operation is often written between its arguments. For example, to express the operation of addition applied to numbers x and y, we usually write $x + y$. This is **infix** notation. Prefix notation for the same expression would look like $+(x, y)$, and postfix notation would be $(x, y)+$.

19.3 Exercises:
19.3.1 Write the expression $(x + y) + z$ with prefix notation.
19.3.2 Write the expression $x + (y + z)$ with prefix notation.
19.3.3 Write the expression $x \cdot (y + z)$ with prefix notation.

19.4 Examples: We have encountered many operations so far this semester (besides the operations of addition, multiplication, and negation of numbers). Here are a few examples.

In Chapter 1 we learned about the operations $\wedge$, $\vee$, $\neg$, and $\rightarrow$ which can be applied to the set of truth values T and F (These can also be viewed as operations on a set of statements).

Let A be a set. Then $\cap$ and $\cup$ (introduced in Chapter 8) are operations on the power set of A.

Let A be a set. Function composition (discussed in Chapters 9 and 18) is an operation on the set of all permutations on A (or of all functions from A to A).

In Chapter 12, we encoutered arithmetic operations on sets of least residues.

19.5 Exercise: Division of real numbers is often called an operation. Look at the definition of function (9.1) and the definition of operation and say why this is not strictly accurate.

19.6 Algebras: An **algebra** is and ordered pair $\langle A, F\rangle$ where A is a set and F is a collection of operations on A. The **underlying set** or **universe** of an algebra $\langle A, F\rangle$ is the set A. The **basic operations** of the algebra $\langle A, F\rangle$ are the operations in F. If F is a set of only a few operations, such as $F = \{+, \cdot, -\}$, we can abuse notation a little and simply write $\langle A, +, \cdot, -\rangle$ for $\langle A, \{+, \cdot, -\}\rangle$. Generally, we will use plain text (A) to represent a set. When we refer to an algebra on that set, we will often use bold faced text ($\mathbf{A}$).

19.7 Examples: Throughout mathematics courses, we work with the algebras $\langle \mathbb{Z}, +, \cdot, -\rangle$ and $\langle \mathbb{R}, +, \cdot, -\rangle$.

In Chapter 1 we worked with the algebra $\langle \{T, F\}, \wedge, \vee, \neg, \rightarrow\rangle$.

Suppose A is a set. Then $\langle \mathcal{P}(A), \cap, \cup\rangle$ is an algebra.

Suppose that A is any set. Recall that S_A is the set of all permutation on A. Then $\langle S_A, \circ\rangle$ is an algebra.

Suppose that A is any set. Denote by R_A the set of all relations on A. Then $\langle R_A, \cap, \cup, \circ, ^{\cup}\rangle$ is an algebra.

19.8 Cayley Tables: We can draw "multiplication tables" which completely describe how to perform binary operations on finite sets. These tables are called **Cayley tables**. As an example, we consider the operation $\wedge$ on the set $\{T, F\}$. The table will be a matrix with two rows (labeled by T and F) and two columns (labeled also by T and F). The entry in the matrix in the row corresponding to T and the column corresponding to T will be $T \wedge T$. The entry in row T and column F will be $T \wedge F$, and so on. Usually, the row and column labels are included in the table, and the name of the operation is included in the upper left corner. Here is the table

$\wedge$	T	F
T	T	F
F	F	F

19.9 Exercises: Draw Cayley tables for each of these binary operations.

19.9.1 The operation $\vee$ on $\{T, F\}$

19.9.2 The operation $+$ on $\mathbb{Z}_6$

19.9.3 The operation $\cap$ on $\mathcal{P}(\{0, 1\})$

19.9.4 The operation $\circ$ on the set of permutations on $\{1, 2, 3\}$

19.10 Derived Operations: A **derived operation** of an algebra is an operation on the algebra obtained by composing the basic operations. For example, if an algebra has two operations called addition and multiplication, then the operation of adding two numbers and then multiplying by a third is a derived operation. An **algebraic expression** is a list of symbols for operations and variable symbols which are put together in a *sensible* manner. For example, if an algebra has two binary operations + and ·, then each of these is an algebraic expression:

$$x \cdot (y + z) \text{ and } (x + y) + z \text{ and } (x \cdot y) + (a \cdot b)$$

Each algebraic expression can be used to define a derived operation on an algebra (and vice versa). For example, on the real numbers we can define this ternary derived operation $m(x, y, z) = (x + (-y)) + z$. To evaluate the operation, we simply "plug" numbers in for x, y, and z.

19.11 Equations: An **equation** is two algebraic expressions separated by an equal sign. You can think of an equation as an open statement. The equation is almost a statement. To become one, elements of an algebra must be plugged in for the variables. An equation $m(x_1, x_2, \ldots, x_n) = t(x_1, x_2, \ldots, x_n)$ is true in an algebra **A** (or **A satisfies** the equation) if the statement

$$(\forall x_1, x_2, \ldots, x_n \in A)[m(x_1, x_2, \ldots, x_n) = t(x_1, x_2, \ldots, x_n)]$$

is true. For example, if we consider $\mathbb{R}$ with ·, then the statement

$$(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(\forall z \in \mathbb{R})[x \cdot (y \cdot z) = (x \cdot y) \cdot z]$$

is true, so $\langle \mathbb{R}, \cdot \rangle$ satisfies the equation $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

Equations are often used to define properties of operations and algebras. Let $\mathbf{A} = \langle A, \cdot \rangle$ be an algebra with a single binary operation. The operation · is **associative** if **A** satisfies the equation

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

The operation · is **idempotent** if **A** satisfies the equation

$$x \cdot x = x$$

The operation · is **commutative** if **A** satisfies the equation

$$x \cdot y = y \cdot x$$

19.12 Exercises: Which of these operations on $\{a, b, c\}$ are associative?

19.12.1

·	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

19.12.2

$\cdot$	a	b	c
a	a	b	c
b	b	b	a
c	c	a	c

19.12.3

$\cdot$	a	b	c
a	a	b	c
b	c	b	b
c	a	b	a

19.13 Exercises: Which of these operations on $\{a, b, c\}$ are idempotent?

19.13.1

$\cdot$	a	b	c
a	a	b	c
b	c	b	a
c	b	a	c

19.13.2

$\cdot$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

19.13.3

$\cdot$	a	b	c
a	a	a	b
b	b	b	b
c	c	c	b

19.13.4 How can you tell from glancing at a Cayley table if the operation presented is idempotent?

19.14 Exercises: Which of these operations on $\{a, b, c\}$ are commutative?

19.14.1

$\cdot$	a	b	c
a	a	a	b
b	a	b	a
c	b	a	c

19.14.2

$\cdot$	a	b	c
a	a	b	b
b	c	b	c
c	a	b	c

19.14.3

$\cdot$	a	b	c
a	a	b	a
b	b	b	b
c	a	c	c

19.14.4 How can you tell from glancing at a Cayley table if the operation presented is commutative.

19.15 Exercise: Find the Cayley table of each of the sixteen different binary operations on the set $\{0, 1\}$.

19.16 Semigroups: A **semigroup** is an algebra with one operation which is an associative binary operation.

19.17 Examples: These are all example of semigroups: $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{R}, \cdot \rangle$, $\langle \{T, F\}, \wedge \rangle$, $\langle \{T, F\}, \vee \rangle$, $\langle \mathcal{P}(A), \cap \rangle$, and $\langle \mathcal{P}(A), \cup \rangle$. Subtraction of real numbers is *not* associative.

19.18 Exercise: Find all of the operations from 19.15 which are semigroup operations on the set $\{0, 1\}$.

19.19 Semilattices: A **semilattice** is a semigroup whose binary operation is commutative and idempotent.

19.20 Examples: Addition and multiplication are *not* (in general) examples of semilattice operations. The powerset of any set under intersection (or union) is a semilattice. The truth values $\{T, F\}$ under $\wedge$ (or $\vee$) is a semilattice. The algebra on $\{a, b, c\}$ with the operation

$\cdot$	a	b	c
a	a	b	b
b	b	b	b
c	b	b	c

is a semilattice. The numbers $\{0, 1\}$ under multiplication form a semilattice.

19.21 Exercise: Find all of the operations from 19.15 which are semilattice operations on the set $\{0, 1\}$.

19.22 Lattices: A **lattice** is an algebra $\langle A, \wedge, \vee \rangle$ with two binary operations so that $\langle A, \wedge \rangle$ and $\langle A, \vee \rangle$ are both semigroups and so that the following two **absorption** equalities hold.

$$a \vee (a \wedge b) = a \text{ for all } a, b \in A$$

$$a \wedge (a \vee b) = a \text{ for all } a, b \in A$$

19.23 Examples: The powerset of any set along with intersection and union form a lattice. The truth values $\{T, F\}$ with $\wedge$ and $\vee$ form a lattice.

19.24 Groups: A **group** is an algebra $\langle A, \cdot \rangle$ with a single binary operation so that the following three conditions are met

G1. The operation $\cdot$ is associative.

G2. There is an element $e \in A$ so that for all $x \in A$ the equalities $e \cdot x = x$ and $x \cdot e = x$ hold. The element e is called an **identity element**.

G3. For every element $a \in A$ there is an element $b \in A$ so that the equalities $a \cdot b = e$ and $b \cdot a = e$ are true.

Notice that the three properties listed here are the same as the last three properties of permutations listed in 18.26. Groups arose from the study of permutations. Mathematicians first studied permutations and discovered properties they satisfied. They then *abstracted* these special properties and studied structures which satisfied those properties. Interestingly enough, every group can (in a sense) be realized as a set of permutations under composition.

19.25 Examples: The collection of permutations on any set under composition form a group. The real numbers under addition form a group. The identity is 0, and the inverse of any x is $-x$. The real numbers under multiplication do *not* form a group. The identity would have to be 1, but the element 0 would have no inverse. $\mathbb{Z}_n$ under addition is a group.

19.26 Exercise: Find all operations from 19.15 which are group operations on $\{0, 1\}$.

19.27 Exercises:

19.27.1 Suppose that $\langle A, \cdot \rangle$ is a group. Prove that there can only be one identity element in A. (Hint: Suppose that there are two identities e and e'. Calculate $e \cdot e'$ two ways – once assuming e is an identity and once assuming that e' is an identity. Use this to prove that $e = e'$.)

19.27.2 Suppose that $\langle A, \cdot \rangle$ is a group and that $a \in A$. Prove that if b and c are both inverses of a, then $b = c$. (Hint: Look at 9.30.)

19.28 Subalgebras: Suppose f is an n-ary operation on a set A and that B is a subset of A. B is **closed** under f if whenever $x_1, \ldots, x_n \in B$ then also $f(x_1, \ldots x_n) \in B$. If $\langle A, F \rangle$ is an algebra and B is a subset of A which is closed under the operations in F, then B is a **subuniverse** of $\langle A, F \rangle$. The algebra $\langle B, F \rangle$ is called a **subalgebra** of $\langle A, F \rangle$.

19.29 Examples: If $\langle A, F \rangle$ is any algebra, then A is a subuniverse (not a very interesting one though). In $\langle \mathbb{Z}, + \rangle$, the even integers form a subuniverse since the sum of any two even integers is even. The subuniverses of $\mathbb{Z}_8$ are $\{0\}$, $\{0, 4\}$, $\{0, 2, 4, 6\}$, and $\mathbb{Z}_8$.

19.30 Exercises: Find all subuniverses of the following algebras.

19.30.1 The permutations on $\{1, 2, 3\}$ under $\circ$.

19.30.2 $\mathbb{Z}_6$ under $+$

19.30.3 $\{T, F\}$ under $\rightarrow$

19.31 Exercise: Suppose that $\mathbf{A} = \langle A, \cdot \rangle$ is an algebra with a single binary operation. Suppose that B and C are subuniverses of $\mathbf{A}$. Prove that $B \cap C$ is also a subuniverse.

19.32 Exercise: Suppose $\mathbf{A} = \langle A, \cdot \rangle$ is an algebra with a single binary operation which is commutative. Suppose also that B is a subuniverse of $\mathbf{A}$. Prove that the algebra $\mathbf{B} = \langle B, \cdot \rangle$ has a commutative operation. (Hint: There is practically nothing to show.)

19.33 Similar Algebras: If two algebras have the same types of operations (i.e. both have two binary operations, a ternary operation, and a unary, or some arrangement like that) then the algebras are **similar**. For example, the algebras $\langle \mathbb{R}, +, \cdot, - \rangle$ and $\langle \{T, F\}, \wedge, \vee, \neg \rangle$ are similar while $\langle \mathbb{R}, +, \cdot, - \rangle$ and $\langle \{T, F\}, \wedge, \vee, \rightarrow \rangle$ are not similar. Sometimes we will use the same symbols to represent the operations of similar algebras. For example, we may start a theorem like "Let $\langle A, F \rangle$ and $\langle B, F \rangle$ be similar algebras." This just means that the algebras have the same types of operations, and that we are using the same symbols (in F) to represent operations in both algebras.

19.34 Products: Suppose $\mathbf{A} = \langle A, F \rangle$ and $\mathbf{B} = \langle B, F \rangle$ are similar algebras. The **direct product** of these algebras is an algebra $\mathbf{A} \times \mathbf{B}$ with universe $A \times B$ whose operations are defined in the following way. If $f \in F$ is an n-ary operation and $(a_1, b_1), \ldots, (a_n, b_n) \in A \times B$ then

$$f((a_1, b_1), \ldots, (a_n, b_n)) = (f(a_1, \ldots, a_n), f(b_1, \ldots, b_n))$$

19.35 Example: Consider $\mathbb{Z}_2$ and $\mathbb{Z}_3$ under addition. In $\mathbb{Z}_2 \times \mathbb{Z}_3$, we can calculate $(1, 2) + (1, 1) = (1 + 1, 2 + 1) = (0, 0)$. Notice that in the first coordinate we add mod 2. In the second we add mod 3.

19.36 Exercises:
19.36.1 Draw a cayley table for the binary operation $+$ in $\langle \mathbb{Z}_2, + \rangle \times \langle \mathbb{Z}_3, + \rangle$.
19.36.2 Suppose $\mathbf{A} = \langle A, \cdot \rangle$ is an algebra with a single binary operation. Let $B = \{(a, a) : a \in A\}$. Prove that B is a subuniverse of $\mathbf{A} \times \mathbf{A}$.
19.36.3 Suppose $\mathbf{A} = \langle A, \cdot \rangle$ and $\mathbf{B} = \langle B, \cdot \rangle$ are similar algebras with binary operations. Prove that if the operations of $\mathbf{A}$ and $\mathbf{B}$ are commutative, then so is the operation of $\mathbf{A} \times \mathbf{B}$.

19.37 Homomorphisms: Suppose $\mathbf{A} = \langle A, F \rangle$ and $\mathbf{B} = \langle B, F \rangle$ are similar algebras. A **homomorphism** from $\mathbf{A}$ to $\mathbf{B}$ is a function $h : A \rightarrow B$ so that for all n-ary operations $f \in F$ and all $x_1, \ldots, x_n \in A$ this equality is true

$$h(f(x_1, \ldots, x_n)) = f(h(x_1), \ldots, h(x_n))$$

19.38 Example: The function $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$ given by $f(0) = f(2) = 0$ and $f(1) = f(3) = 1$ is a homomorphism (using addition). To see this, we would have to check all sixteen equations which look like this

$$f(2) + f(3) = 0 + 1 = 1 = f(1) = f(2 + 3)$$

19.39 Exercises:
19.39.1 Suppose that $\mathbf{A} = \langle A, \cdot \rangle$, $\mathbf{B} = \langle B, \cdot \rangle$, and $\mathbf{C} = \langle C, \cdot \rangle$ are similar algebras with binary operations and that $f : A \rightarrow B$ and $h : B \rightarrow C$ are homomorphisms. Prove that $h \circ f : A \rightarrow C$ is a homomorphism.
19.39.2 Suppose $\mathbf{A} = \langle A, \cdot \rangle$ and $\mathbf{B} = \langle B, \cdot \rangle$ are similar algebras with binary operations and $h : A \rightarrow B$ is a homomorphism. Prove that $\ker h$ is a subuniverse of $\mathbf{A} \times \mathbf{A}$.

19.39.3 Suppose $\mathbf{A} = \langle A, \cdot \rangle$ and $\mathbf{B} = \langle B, \cdot \rangle$ are similar algebras with binary operations and $h : A \to B$ is a homomorphism. Suppose also that h is surjective and that the operation of $\mathbf{A}$ is commutative. Prove that the operation of $\mathbf{B}$ is also commutative.

19.40 Preservation of Equations: Each of the generic types of algebras we have defined in this section (semigroups, semilattices, lattices, groups) were defined using equations. Equations are central to the study of algebra. In fact, algebra was born as the science of solving equations. Exercises 19.32, 19.36.3, and 19.39.3 hint that there is a relationship between the equations satisfied by an algebra and the equations satisfied by homomorphic images, subalgebras, and products involving that algebra. They hint at the following **Theorem:** Suppose that $\mathbf{A}$ is an algebra. If an equation is true in $\mathbf{A}$, then it is true in every subalgebra and every homomorphic image of $\mathbf{A}$. If $\mathbf{B}$ is an algebra similar to $\mathbf{A}$, then an equation is true in $\mathbf{A} \times \mathbf{B}$ if and only if it is true in both $\mathbf{A}$ and $\mathbf{B}$.

19.41 Isomorphism: A bijective homomorphism is an **isomorphism**. If there is an isomorphism between two algebras, then the algebras are said to be **isomorphic**.

19.42 Example: Consider the algebras $\langle \{T, F\}, \wedge \rangle$ and $\langle \mathbb{Z}_2, \cdot \rangle$. Let $f : \{T, F\} \to \mathbb{Z}_2$ be the function given by $f(T) = 1$ and $f(F) = 0$. This function is clearly a bijection. To see that it is a homomorphism, we check these equalities

$$f(T \wedge T) = f(T) = 1 = 1 \cdot 1 = f(T) \cdot f(T)$$

$$f(T \wedge F) = f(F) = 0 = 1 \cdot 0 = f(T) \cdot f(F)$$

$$f(F \wedge T) = f(F) = 0 = 0 \cdot 1 = f(F) \cdot f(T)$$

$$f(F \wedge F) = f(F) = 0 = 0 \cdot 0 = f(F) \cdot f(F)$$

Thus, f is an isomorphism. What does it mean that these two algebras are isomorphic? A peak at their Cayley tables will tell us. The tables are

$\wedge$	T	F
T	T	F
F	F	F

$\cdot$	1	0
1	1	0
0	0	0

Drawn in this way, it is clear that the pattern in the tables is the same. By renaming the elements in one table, we can arrive at the second table. This renaming is the function f. The tables are identical except for the names of the elements.

19.43 A Rose by Any Other Name: The previous example exposes the essence of isomorphism. Saying two algebras are isomorphic is saying that the algebras are identical except, perhaps, for the names of their elements.

19.44 Examples: The algebras $\langle\{0,1,2\},\vee\rangle$ and $\langle\{a,b,c\},\vee\rangle$ whose Cayley tables are

$\vee$	0	1	2
0	0	1	2
1	1	1	2
2	2	2	2

$\vee$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c

are isomorphic via the function which maps $0 \to a$, $1 \to b$, and $2 \to c$. The algebra $\langle\mathbb{R}^+,\cdot\rangle$ (where $\mathbb{R}^+$ means the positive reals) is isomorphic to $\langle\mathbb{R},+\rangle$ via the function $\ln(x)$ since this is a bijection and $\ln(xy) = \ln(x) + \ln(y)$.

19.45 Exercises:

19.45.1 Suppose **A** and **B** are similar algebras with a single binary operation $\cdot$ and that $f : A \to B$ is an isomorphism. Prove that $f^{-1} : B \to A$ is also an isomorphism.

19.45.2 Define an operation $+$ on the set $\{0,1\}$ by $x+y = \max(x,y)$ ($x+y$ is the larger of x and y). Find an isomorphism between $\langle\{T,F\},\vee\rangle$ and $\langle\{0,1\},+\rangle$. Find an isomorphism between $\langle\{T,F\},\wedge\rangle$ and $\langle\{0,1\},+\rangle$.

19.45.3 Find an isomorphism between $\langle\{T,F\},\vee\rangle$ and $\langle\{T,F\},\wedge\rangle$.

20

Order

20.1 Order: A binary relation $\leq$ on a set A is a **partial order** if the following three conditions hold.

1. ($\leq$ is reflexive) $a \leq a$ for all $a \in A$
2. ($\leq$ is antisymmetric) For all $a, b \in A$, if $a \leq b$ and $b \leq a$, then $a = b$.
3. ($\leq$ is transitive) For all $a, b, c \in A$, if $a \leq b$ and $b \leq c$, then $a \leq c$.

The relation $\leq$ is usually read as "less than or equal." If $\leq$ is a partial order on a set A, then the system $\langle A, \leq \rangle$ is called a **partially ordered set** or a **poset**. As with algebras, we will usually use plain text to represent sets, and we will used bold faced text to represent posets.

20.2 Examples: The relation $\leq$ is a partial order on the real numbers (or the natural numbers, integers, or rational numbers).

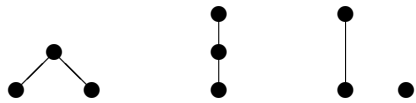
If A is any set, then $\subseteq$ is a partial order on the subsets of A.

Implication ($\rightarrow$) is a partial order on any set of statements (or on the set $\{T, F\}$).

Divisibility ($|$) is a partial order on the natural numbers (or the integers, or the non-negative integers).

20.3 Notation: Suppose that $\leq$ is a partial order on a set A. If $x, y \in A$ and $x \leq y$ but $x \neq y$, then we will write $x < y$. The relation $<$ is usually read as "less than." If $x < y$ and if there is no z between x and y (i.e. $x < z$ and $z < y$), then we say that y is a **cover** of x or that y **covers** x. This is denoted as $x \prec y$.

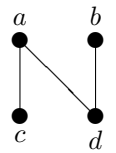
20.4 Hasse Diagrams: We can draw diagrams of finite posets which depict their partial orders. The **Hasse diagram** of a poset is a diagram of points and line segments. Each element of the poset is represented by a point in in the diagram. If one element of a poset is covered by another, then the points representing them are connected by a line segement. The points are arranged in such a manner that all line segments move upward from lesser elements to greater elements. Sometimes, the points in a Hasse diagram are labeled with the names of the elements they represent. Other times, they are not. In Packet 18 we drew the Hasse diagram of the poset of subsets of a set. These are diagrams of some (not all) posets on a three element set.



20.5 Exercises:
20.5.1 The divisibility relation is a partial order on the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Draw the Hasse diagram of this partial order.
20.5.2 Draw the Hasse diagram of every three element poset (there are 5).

20.6 Chains: Two elements x and y of a poset are **comparable** if either $x \leq y$ or $y \leq x$. If every two elements of a poset are comparable, then the poset is called a **chain**. In this case, the partial order is called a **total order**. An example of a chain would be the real numbers under the usual order. If no two elements of a poset are comparable, then the poset is an **antichain**. The Hasse diagram of an antichain consists of several points with no line segments.

20.7 Minimal and Maximal Elements: A **minimal** element of a poset $\mathbf{P}$ is an element $x \in \mathbf{P}$ which has no elements strictly less than itself (i.e. there is no $y \in \mathbf{P}$ with $y < x$). A **maximal** element of $\mathbf{P}$ would be an element z which is not strictly less than any other element (i.e. there is no element $y \in \mathbf{P}$ with $z < y$). For example, in this poset



the elements a and b are maximal, while the elements c and d are minimal. Not all posets have maximal and minimal elements. $\mathbb{R}$ (with the usual order) has neither.

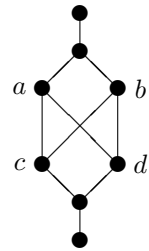
20.8 Exercises:
20.8.1 Find the minimal and maximal elements in Exercise 20.5.1.
20.8.2 Find any maximal or minimal elements of the natural numbers ordered by divisibility.

20.9 Greatest and Least: The **greatest** element of a poset (if it has one) is an element which is greater than or equal to every other element. The **least** element of a poset (if it has one) is an element which is less than or equal to every other element.

20.10 Exercises:
20.10.1 Consider the non-negative integers ($\{0, 1, 2, \ldots\}$) ordered by divisibility. Find the greatest and least elements of this poset.

20.10.2 Draw all Hasse diagrams of four element posets. In each, locate any maximal, minimal, greatest, or least elements.

20.11 Upper and Lower Bounds: Suppose $\mathbf{P}$ is a poset and $X \subseteq \mathbf{P}$. If $y \in \mathbf{P}$ and $x \leq y$ for all $x \in X$, then y is an **upper bound** of X. If $y \leq x$ for all $x \in X$, then y is a **lower bound** of X. An upper bound of X which is less than or equal to every other upper bound is called the **least upper bound** or **join** of X. A lower bound of X which is greater than or equal to every other lower bound is called the **greatest lower bound** or **meet** of X. For example, consider



In this poset, the set $\{a, b\}$ has a join. However, this set has no meet. The two candidates for a meet of this set would be c and d. Since they are not comparable, neither can be the *greatest* lower bound. Similarly, the set $\{c, d\}$ has a meet but no join.

20.12 Exercises: Suppose that $\langle A, \cdot \rangle$ is a semilattice (as defined in Packet 19). Define a relation $\leq$ on A by $x \leq y$ if and only if $x \cdot y = x$.
20.12.1 Prove that $\leq$ is reflexive, antisymmetric, and transitive, so $\leq$ is a partial order.
20.12.2 For any $x, y \in A$, prove that $x \cdot y \leq x$ and $x \cdot y \leq y$. Thus, $x \cdot y$ is a lower bound of $\{x, y\}$.
20.12.3 For any $x, y, z \in A$, prove that if $z \leq x$ and if $z \leq y$, then $z \leq x \cdot y$. Hence, $x \cdot y$ is the meet of x and y. (Note: Had we defined $x \leq y$ if and only if $x \cdot y = y$, then we would have ended up with $x \cdot y$ being the join of $\{x, y\}$.)

20.13 Semilattices: Exercises 20.12 hint that the semilattice algebras defined in Packet 19 are related to partial orders. A poset $\mathbf{P}$ is called a **meet semilattice** if every pair of elements $\{x, y\}$ has a meet (greatest lower bound). In this situation, the meet of the set $\{x, y\}$ is denoted by $x \wedge y$. A poset $\mathbf{P}$ is called a **join semilattice** if every pair of elements $\{x, y\}$ has a join (least upper bound). In this situation, the join of the set $\{x, y\}$ is denoted by $x \vee y$. The operations (they are operations) $\wedge$ and $\vee$ are associative, commutative, and idempotent, so $\langle P, \wedge \rangle$ and $\langle P, \vee \rangle$ are semilattices in the sense of Packet 19.

20.14 Exercise: Refer to the Hasse diagrams you drew in 20.5.2 and 20.10.2. Which of these are meet semilattices? Which of these are join semilattices? Are any both?

20.15 Lattices: A **lattice ordered set** or **lattice** is a poset which is both a meet semilattice and a join semilattice. That is, every pair of elements x and y has both a meet $(x \wedge y)$ and a join $(x \vee y)$. If $\mathbf{P}$ is a lattice ordered set, then $\langle P, \wedge, \vee \rangle$ is a lattice in the sense of Packet 19. On the other hand if $\langle P, \wedge, \vee \rangle$ is a lattice, then the processes of 20.12 can be used to define a natural order on P which makes P a lattice ordered set. A key step in the proof of this fact is that the two operations $\wedge$ and $\vee$ yield the same order on P. This is exercise 20.16. Since lattices and lattice ordered sets are in this way essentially the same thing, we will simply call both lattices (the same is true for semilattices).

20.16 Exercise: Suppose that $\langle P, \wedge, \vee \rangle$ is a lattice in the sense of Packet 19. Let $x, y \in P$. Prove that $x \wedge y = x$ if and only if $x \vee y = y$.

20.17 Complete Lattices: A lattice $\mathbf{L}$ is **complete** if every subset of $\mathbf{L}$ has both a join and a meet. The interval $[0, 1]$ of real numbers is a complete lattice. $\mathbb{R}$ (with the usual order) is not complete since sets such as $\{1, 2, 3, \ldots\}$ have no upper bound at all (much less a least upper bound).

20.18 Exercise: Use induction to prove that every finite lattice is complete.

20.19 Examples: We have encountered many lattices during this course. Here are a few examples.

The set of all compound statements built from two atomic statements is a complete lattice under the order $\rightarrow$. In this lattice, meets correspond to "and," and joins correspond to "or."

The powerset of a set under $\subseteq$ is a complete lattice in which meets correspond to intersection and joins correspond to unions.

The set of equivalence relations on any set under $\subseteq$ is a complete lattice. Meets are intersections. Joins are a little more complex.

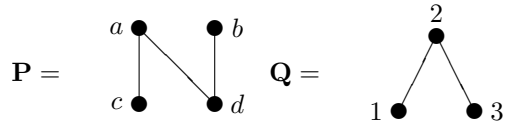
The set of subuniverses of an algebra is a complete lattice in which intersections are meets (Joins are, again, more complicated).

20.20 Order Preserving Maps: Suppose $\mathbf{P}$ and $\mathbf{Q}$ are posets and f is a function from P to Q. We say that f is **order preserving** if for all $x, y \in P$ this implication holds

$$\text{If } x \leq y \text{ then } f(x) \leq f(y).$$

20.21 Examples: Any increasing function from $\mathbb{R}$ to $\mathbb{R}$ is order preserving. The function $f(x) = x^2$ from $\mathbb{R}$ to $\mathbb{R}$ is not order preserving since $-1 \leq 0$, but $f(-1) \not\leq f(0)$.

Suppose that **P** and **Q** are these posets

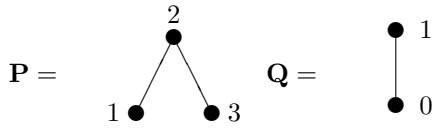


Then each of these functions is order preserving (this is not an exhaustive list)

$a \to 2$	$a \to 2$	$a \to 3$	$a \to 1$
$b \to 2$	$b \to 2$	$b \to 2$	$b \to 1$
$c \to 1$	$c \to 1$	$c \to 3$	$c \to 1$
$d \to 1$	$d \to 3$	$d \to 3$	$d \to 1$

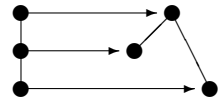
20.22 Exercises:

20.22.1 Find all order preserving functions from **P** to **Q** if



20.22.2 Suppose **P** and **Q** are meet semilattices and that f is a homomorphism from $\langle P, \wedge \rangle$ to $\langle Q, \wedge \rangle$. Prove that f is an order preserving map.

20.23 Isomorphism: Not every bijective order preserving map ought to be considered an isomorphism. For example,



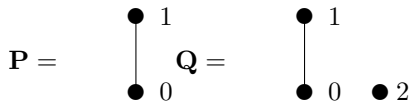
The function in this diagram is a bijective order preserving map between posets, but the posets clearly are not identical and should not be considered isomorphic. An order isomorphism ought to preserve and reflect the order of the posets involved. Hence, we make this definition. Suppose that **P** and **Q** are posets. An **order isomorphism** from **P** to **Q** is a bijection $f : \mathbf{P} \to \mathbf{Q}$ so that for all $x, y \in P$ $x \leq y$ if and only if $f(x) \leq f(y)$.

20.24 Example: The function e^x is an order isomorphism from $\mathbb{R}$ to the interval $(0, \infty)$.

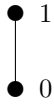
20.25 Products: Suppose that $\mathbf{P}$ and $\mathbf{Q}$ are posets. Define the **direct product** of $\mathbf{P}$ and $\mathbf{Q}$ to be a poset on the set $P \times Q$ whose order is given by $(p_1, q_1) \leq (p_2, q_2)$ if and only if both $p_1 \leq p_2$ and $q_1 \leq q_2$. We will denote this poset as $\mathbf{P} \times \mathbf{Q}$.

20.26 Exercises:

20.26.1 Draw the Hasse diagram of $\mathbf{P} \times \mathbf{Q}$ where $\mathbf{P}$ and $\mathbf{Q}$ are these posets.



20.26.2 Let $\mathbf{2}$ be this poset



Draw the Hasse diagrams of the posets $\mathbf{2} \times \mathbf{2} = \mathbf{2}^2$, $\mathbf{2} \times (\mathbf{2} \times \mathbf{2}) = \mathbf{2}^3$, and $((\mathbf{2} \times \mathbf{2}) \times \mathbf{2}) \times \mathbf{2} = \mathbf{2}^4$.

20.26.3 Suppose that $\mathbf{P}$ and $\mathbf{Q}$ are meet semilattices. Prove that $\mathbf{P} \times \mathbf{Q}$ is a meet semilattice. The same is true for joins, and hence for lattices.

20.26.4 Suppose that $\mathbf{P}$ and $\mathbf{Q}$ are posets. Let π be the projection from $\mathbf{P} \times \mathbf{Q}$ to $\mathbf{P}$. Prove that π is order preserving.

Proof Outlines

Direct Proof (7.11): The prove an implication $P \to Q$,

1. Suppose P.
2. Prove Q.

If-and-only-if (7.19): To prove a biconditional $P \leftrightarrow Q$,

1. Prove $P \to Q$.
2. Prove $Q \to P$.

Cases (7.21): To prove $(P \vee Q) \to R$,

1. Prove $P \to R$.
2. Prove $Q \to R$.

Disjunction (12.23): To prove a disjunction $P \vee Q$,

1. Suppose $\neg P$.
2. Prove Q.

Contrapositive (7.23): To prove $P \to Q$,

1. Suppose $\neg Q$.
2. Prove $\neg P$.

Contradiction (13.22): To prove P,

1. Suppose $\neg P$.
2. Prove a contradiction.
3. Conclude P.

Mathematical Induction (11.7): To prove that $P(n)$ is true for all integers $n \geq m$,

1. Prove $P(m)$.
2. Let $k \in \mathbb{Z}$ with $m \leq k$.
3. Suppose $P(k)$.
4. Prove $P(k+1)$.

Subset (8.10): To prove that a set A is a subset of a set B,

1. Let $a \in A$.
2. Prove $a \in B$.

Set Equality (8.22): To prove a set A equals a set B,

1. Prove $A \subseteq B$.
2. Prove $B \subseteq A$.

Function Equality (9.26): To prove that two functions $f : A \to B$ and $g : A \to B$ are equal,

1. Let $a \in A$.
2. Prove that $f(a) = g(a)$.

Inverse Functions (9.32): To prove that $f : A \to B$ and $g : B \to A$ are inverses,

1. Let $a \in A$.
2. Prove that $g(f(a)) = a$.
3. Let $b \in B$.
4. Prove that $f(g(b)) = b$.

Injective Functions (9.13): To prove that a function $f : A \to B$ is injective,

1. Let $x, y \in A$.
2. Suppose that $f(x) = f(y)$.
3. Prove that $x = y$.

Surjective Functions (9.17): To prove that a function $f : A \to B$ is surjective,

1. Let $b \in B$.
2. Exhibit an $a \in A$ with $f(a) = b$.

Bijective Functions: To prove that a function $f : A \to B$ is bijective,

1. Prove that f is injective.
2. Prove that f is surjective.

Reflexive Relation (10.21): To prove that a binary relation R on a set A is reflexive,

1. Let $a \in A$.
2. Prove aRa.

Symmetric Relation (10.22): To prove that a binary relation R on a set A is symmetric,

1. Let $a, b \in A$.
2. Suppose aRb.
3. Prove bRa.

Anti-Symmetric Relation: To prove that a binary relation R on a set A is anti-symmetric,

1. Let $a, b \in A$.
2. Suppose aRb and bRa.
3. Prove $a = b$.

Transitive Relation (10.23): To prove that a binary relation R on a set A is transitive,

1. Let $a, b, c \in A$.
2. Suppose aRb and bRc.
3. Prove aRc.

Equivalence Relation: To prove that a binary relation R on a set A is an equivalence relation,

1. Prove that R is reflexive.
2. Prove that R is symmetric.
3. Prove that R is transitive.

Cardinality (14.8): To prove that two sets A and B have the same cardinality, exhibit a bijection from A to B.

Cantor-Schroeder-Bernstein Theorem (14.21): To prove two sets A and B have the same cardinality,

1. Exhibit an injection from A to B.
2. Exhibit an injection from B to A.

Logical Equivalences

$P \wedge Q \equiv Q \wedge P$	commutative law
$P \vee Q \equiv Q \vee P$	commutative law
$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$	associative law
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$	associative law
$\neg(\neg P) \equiv P$	idempotent law
$P \wedge P \equiv P$	idempotent law
$P \vee P \equiv P$	idempotent law
$P \equiv P \vee (P \wedge Q)$	absorption law
$P \equiv P \wedge (P \vee Q)$	absorption law
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	distributive law
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$	distributive law
$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$	DeMorgan's Law
$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$	DeMorgan's Law
$P \to Q \equiv \neg P \vee Q$	disjunctive implication
$P \to Q \equiv \neg Q \to \neg P$	contrapositive
$\mathbf{F} \vee Q \equiv Q$	special equivalence with contradiction
$\mathbf{T} \wedge Q \equiv Q$	special equivalence with tautology
$\neg \forall x P(x) \equiv \exists x \neg P(x)$	universal negation
$\neg \exists x P(x) \equiv \forall x \neg P(x)$	existential negation

Rules of Inference

Basic Inferences
Modus Ponens MP: From $A \rightarrow B$ and A infer B.
Tautology TAUT: If T is a tautology, we can always infer T.
Equivalence E: If $A \equiv B$, then from A infer B.
Addition A: From A infer $A \vee B$.
Modus Tollens MT: From $A \rightarrow B$ and $\neg B$ infer $\neg A$.
Disjunctive Syllogism DS: From $A \vee B$ and $\neg A$ infer B.
Simplification S: From $A \wedge B$ infer A or infer B.
Conjunction C: From A and B infer $A \wedge B$.
Transitivity T: From $A \rightarrow B$ and $B \rightarrow C$ infer $A \rightarrow C$.
Universal Instantiation $\forall$I: If $s \in S$, then from $(\forall x \in S)P(x)$ infer $P(s)$.
Existential Instantiation $\exists$I: If s is an unused symbol for an element of S, then from $(\exists x \in S)P(x)$ infer $P(s)$.
Universal Generalization $\forall$G : If s is a symbol for an arbitrary member of S, then from $P(s)$ infer $(\forall x \in S)P(x)$.
Existential Generalization $\exists$G: If $s \in S$, from $P(s)$ infer $(\exists x \in S)P(x)$.

Temporary Assumptions
Direct Proof: To prove $\alpha \rightarrow \beta$, assume α and use this to establish β. Conclude $\alpha \rightarrow \beta$.
Disjunction Proof: To prove $\alpha \vee \beta$, assume $\neg\alpha$. Use this to establish β. Conclude $\alpha \vee \beta$.
Proof by Cases: To prove $(\alpha \vee \beta) \rightarrow \gamma$, Prove $\alpha \rightarrow \gamma$ and $\beta \rightarrow \gamma$. Conclude $(\alpha \vee \beta) \rightarrow \gamma$.
Proof by Contrapositive: To prove $\alpha \rightarrow \beta$, prove $\neg\beta \rightarrow \neg\alpha$.
Proof by Contradiction: To prove α by contradiction, assume $\neg\alpha$. Use this to establish a contradiction such as $\beta \wedge \neg\beta$. Conclude α.

Glossary

A

affirming the consequent Affirming the consequent is the logical fallacy

$$\begin{array}{l} P \to Q \\ \underline{Q} \\ \therefore P \end{array}.$$

.

and (logical operator) The logical operator 'and' or 'conjunction' (denoted $\wedge$) is defined so that $P \wedge Q$ is true exactly when both P and Q are true.

antecedent The antecedent of the implication $P \to Q$ is P.

anti-symmetric A binary relation $\sim$ on a set A is anti-symmetric if for all $x, y \in A$ $x \sim y$ and $y \sim x$ together imply $x = y$.

argument An argument is a list of statements, one of which (called the conclusion) is intended to be supported by the others (called the premises).

axiom An axiom is a statment which is assumed to be true (without proof).

B

bi-implication Bi-implication is the logical operator $\leftrightarrow$ defined so that

$$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P).$$

.

biconditional Biconditional is the logical operator $\leftrightarrow$ defined so that

$$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P).$$

.

bijective function A function is bijective if it is both injective and surjective.

bijective (sets) Two sets A and B are bijective if there is a bijection between them.

binary relation A binary relation on a set A is a subset of $A \times A$.

C

Cantor-Schroeder-Bernstein Theorem If A and B are sets, then $|A| = |B|$ if and only if both $|A| \leq |B|$ and $|B| \leq |A|$.

Cantor's Theorem For any set A, $|A| \neq |\mathcal{P}(A)|$.

codomain The codomain of a function $f : A \to B$ is the set B.

Completeness Theorem The Completeness Theorem says that every valid argument has a proof.

composition (function) If $f : A \to B$ and $g : B \to C$ are functions, then the composition of f and g is the function $g \circ f : A \to C$ defined by $g \circ f(x) = g(f(x))$.

composition (relation) If R and S are relations on a set A, then the composition of R and S is the relation $R \circ S = \{(x, z) : \exists y \in A(xRy \wedge ySz)\}$.

consequent The conclusion of an implication $P \to Q$ is the statement Q.

conditional (logical operator) The conditional is the logical operator $\to$ defined so that $P \to Q$ is true unless P is true and Q is false.

conjunction (logical operator) The logical operator 'and' or 'conjunction' (denoted $\wedge$) is defined so that $P \wedge Q$ is true exactly when both P and Q are true.

consequent The consequent of an implication $P \to Q$ is the statement Q.

consistent premises The premises of an argument are consistent if they are not inconsistent.

contradiction A contradiction is a statement which is always false such as $P \wedge \neg P$.

contrapositive The contrapositive of the statement $P \to Q$ is the statement $\neg Q \to \neg P$.

converse The converse of the statement $P \to Q$ is the statement $Q \to P$.

converse (of a relation) The converse of a binary relation R is the relation

$$R^{\cup} = \{(y, x) : xRy\}.$$

.

countable A set is countable if it is either countably infinite or finite.

countably infinite The set A is countably infinite if $|A| = |\mathbb{N}|$.

D

Deduction Theorem The arguments

$$\left(\begin{array}{l} A_1 \\ A_2 \\ \vdots \\ A_n \\ \hline \therefore P \to Q \end{array}\right) \text{ and } \left(\begin{array}{l} A_1 \\ A_2 \\ \vdots \\ A_n \\ P \\ \hline \therefore Q \end{array}\right)$$

are either both valid or both invalid.

denying the antecedent Denying the antecedent is the logical fallacy

$$\begin{array}{l} P \to Q \\ \neg P \\ \hline \therefore \neg Q \end{array}.$$

.

direct power For any positive integer n, the n^{th} direct power of a set A is the direct product $A \times A \times \ldots \times A$ in which there are n factors of A.

direct product The direct product of two sets A and B is the set

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

.

direct proof The method of direct proof establishes an implication $P \to Q$ by assuming P and using this assumption to establish Q.

disjunction (logical operator) The logical operator 'or' or 'disjunction' (denoted $\vee$) is defined so that $P \vee Q$ is true when at least one of P and Q is true.

disjunctive normal form A statement which is a disjunction of conjunctions or is a single conjunction or is a single atomic statement is in disjunctive normal form.

division algorithm The division algorithm states that for any integer m and any positive integer n there are unique integers q and r with $0 \leq r < n$ so that $m = nq + r$.

domain The domain of a function $f : A \to B$ is the set A.

E

element The word 'element' is a primitive (an undefined term).

empty set The empty set is the unique set which contains no elements.

equivalence class If $\sim$ is an equivalence relation on a set A and $a \in A$, then the equivalence class of a modulo $\sim$ is the set $[a]_\sim = \{x \in A : a \sim x\}$.

equivalence relation A binary relation is an equivalence relation if it is reflexive, symmetric and transitive.

F

factor set If $\sim$ is an equivalence relation on a set A, then the factor set of A modulo $\sim$ is the set $A/\sim$ of equivalence classes of $\sim$.

finite A set A is finite if $|A| \in \mathbb{N}$.

function Let A and B be sets. A function from A to B is a subset f of $A \times B$ so that for every $a \in A$ there is precisely one $b \in B$ with $(a, b) \in f$.

H

hypothesis The hypothesis of an implication $P \to Q$ is the statement P.

I

identity function The identity function on a set A is the function $1_A : A \to A$ so that $1_A(x) = x$ for all $x \in A$.

image The image of a function $f : A \to B$ is the set $\{f(a) : a \in A\}$.

implication (logical operator) The logical operator 'implication' (denoted $\to$) is defined so that $P \to Q$ is true unless P is true and Q is false.

inconsistent premises The premises of an argument are inconsistent if they can be used to prove a contradiction.

injective A function $f : A \to B$ is injective if for all $x, y \in A$ if $f(x) = f(y)$ then $x = y$.

intersection The intersection of two sets A and B is the set

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

.

invalid argument An invalid argument is an argument which is not valid.

inverse If $f : A \to B$ and $g : B \to A$ are functions, then g is the inverse of f if $f \circ g = 1_B$ and $g \circ f = 1_A$.

inverse (of an implication) The inverse of an implication $P \to Q$ is $\neg P \to \neg Q$.

irrational A real number is irrational if it is not rational.

K

kernel The kernel of a function $f : A \to B$ is the binary relation R on A defined so that xRy exactly when $f(x) = f(y)$.

L

least residue Let m and n be integers with n positive. The division algorithm guarantees integers q and r with $0 \leq r < n$ so that $m = nq + r$. The least residue of m modulo n is the integer r.

logically equivalent Two compound statements are logically equivalent if they share the same truth values regardless of the truth values of the atomic statements used to form them.

M

mapping A mapping from a set A to a set B is a subset f of $A \times B$ so that for every $a \in A$ there is precisely one $b \in B$ with $(a, b) \in f$.

modular congruence Suppose that n is a positive integer and a and b are any integers. We say that a is congruent to b modulo n (written $a \equiv_n b$) if $n|(a - b)$.

N

negation The logical operator 'negation' or 'not' (denoted $\neg$) is defined so that $\neg P$ is true exactly when P is false.

O

one-to-one A function $f : A \to B$ is one-to-one (injective) if for all $x, y \in A$ if $f(x) = f(y)$ then $x = y$.

onto A function $f : A \to B$ is onto (surjective) if the range of f is all of B.

open statement An open statement (or predicate) is a sentence with variables so that when appropriate values are substituted for the variables the sentence becomes a statement.

or (logical operator) The logical operator 'or' or 'disjunction' (denoted $\vee$) is defined so that $P \vee Q$ is true when at least one of P and Q is true.

P

partition A partition of a set A is a set $\mathcal{P}$ of nonempty subsets of A so that every element of A is in one of the sets in $\mathcal{P}$ and so that whenever $E \neq D$ in $\mathcal{P}$ then $E \cap D = \emptyset$.

Peano Axioms The Peano Axioms are the basic assumptions made about the natural numbers from which all other properties are proven. They are

P1: There is a natural number which we call 0.

P2: There is a function $s : \mathbb{N} \to \mathbb{N}$ called the **successor function**. If $n \in \mathbb{N}$, then $s(n)$ is called the **successor of** n.

P3: The number 0 is not the successor of any number.

P4: If n and m are natural numbers and $s(n) = s(m)$, then $n = m$.

P5: If $A \subseteq \mathbb{N}$ and these two statements are true

- $0 \in A$
- If $k \in A$, then $s(k) \in A$

Then $A = \mathbb{N}$.

.

permutation A permutation of a set A is a bijective function from A to A.

postulate A postulate (axiom) is a statment which is assumed to be true (without proof).

powerset The powerset of a set A is the set of all subsets of A.

predicate A predicate (or open statement) is a sentence with variables so that when appropriate values are substituted for the variables the sentence becomes a statement.

primitive A primitive is an undefined term.

proof A formal proof of an argument is a list of statements so that every statement in the list is either a premise of the argument or follows by rules of inference from previous statements and so that the final statement in the list is the conclusion of the argument.

proper subset A proper subset of a set A is a subset B of A so that $A \neq B$.

Q

quotient set If $\sim$ is an equivalence relation on a set A, then the quotient set of A modulo $\sim$ is the set $A/\sim$ of equivalence classes of $\sim$.

R

range The range of a function $f : A \to B$ is the set $\{f(a) : a \in A\}$.

recursive see recursive.

reflexive A binary relation $\sim$ on a set A is reflexive if $a \sim a$ for all $a \in A$.

relation A relation on a set A is a subset of a direct power of A.

residue class Suppose that m and n are integers with n positive. The residue class of m is the equivalence class of m modulo the equivalence relation $\equiv_n$.

S

sequence A sequence is a function whose domain is a set of the form $\{m, m+1, m+2, \ldots\}$ where m is an integer.

set The word 'set' is a primitive - an undefined term.

Sheffer stroke The Sheffer stroke operation is the logical operation $P|Q = \neg(P \wedge Q)$.

Soundness Theorem The Soundness Theorem says that every argument which has a proof is valid.

subset If A and B are sets, then B is a subset of A (denoted $B \subseteq A$) if whenever $x \in B$ it is also the case that $x \in A$.

surjective A function $f : A \to B$ is surjective if the range of f is all of B.

symmetric A binary relation $\sim$ on a set A is symmetric if for all $x, y \in A$ if $x \sim y$ then $y \sim x$.

T

tautology A tautology is a compound statment which is always true regardless of the truth values of the atomic statements involved.

transitive A relation $\sim$ on a set A is transitive if for all $x, y, z \in A$ if $x \sim y$ and $y \sim z$ then $x \sim z$.

transitive closure The transitive closure of a binary relation R on a set A is the smallest transitive relation on A containing R.

triangle inequality For any real numbers x and y $|x + y| \leq |x| + |y|$.

U

uncountable A set is uncountable if it is not countable.

uncountably infinite A set is uncountably infinite if it is not countable.

union If A and B are sets then the union of A and B is the set

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

.

V

valid argument An argument with premises $P_1, \ldots, P_n$ and conclusion C is valid if the statement

$$(P1 \wedge P_2 \wedge \ldots \wedge P_n) \to C$$

is a tautology.

W

Well Ordering Property The Well Ordering Property of $\mathbb{N}$ says that every nonempty subset of $\mathbb{N}$ has a least element.