The Whys and Hows of Mathematical Proof

Paul Howard

December 23, 2014

Contents

Part I

The Basic Whys and Hows

Chapter 1

The Whys - The Language of Mathematics

1.1 Introduction

An essential element of understanding mathematical proof is an introduction to the language of mathematics and its meaning. After studying the language in this chapter, the methods of proof we will introduce in Chapter 2 should be easily comprehended—or even trivial.

The language of mathematics includes words and phrases from "ordinary" English together with specialized symbols. Mathematics differs from ordinary language in that every element of a sentence has a precise meaning. In this chapter, we will explore the meanings of the symbols, words, and phrases that occur most frequently in mathematical writing and we will learn how to determine the truth or falsity of statements containing them.

1.2 The Symbols

The symbols used in the language of mathematics are classified according to their use as follows:

1. Symbols representing objects-

   (a) *Standard object symbols* or symbols which (almost) always represent the same fixed object include π (representing the ratio of the circumference of a circle to the diameter $= 3.14159\ldots$); $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ (Representing the natural numbers, the integers, the rational numbers, the real numbers, and the complex numbers, respectively.); $0, 1, 2, \ldots$ (representing the individual natural numbers); $\mathbb{R}^+$ (for the positive real numbers); and so on.

(b) *Variables* are then the symbols that represent any object in a certain set. The set of allowable values for a variable is called the *domain* (or sometimes the *range*) of the variable. The domain of a variable should either be specified or be clear from the context. For example, in the phrase "x is a real number", x is a variable whose domain is the set $\mathbb{R}$ (the real numbers). Note, variables may also be referred to as *parameters*.

2. Symbols representing functions and operations- Examples of symbols in this category are the symbols $+$ and $\cdot$ for the common operations on numbers and sin for the sine function. Note that when symbols representing functions or operations are combined with symbols representing objects (as in "$2 + x$"), the result is a sequence of symbols representing an *object*.

3. Symbols representing relations- Examples include $<$, $\leq$, and $=$. Note that when symbols representing relations are combined with symbols representing objects, the result is a mathematical *sentence*. For example, "$x < 17$" is a mathematical sentence.

4. Symbols representing connectives for building more complex sentences from simpler ones- The symbols $\wedge$ (for "and"), the symbol $\rightarrow$ or $\Rightarrow$ (for "If ..., then ..."), and the symbol $\forall$ (for "for all" or "for every") are in this category.

1.3 Using the binary connectives

The connective words "and", "or", "if ..., then ...", and "if and only if" are the binary connectives. Each of these connectives is used to combine two simpler sentences to form one that is more complex. The meanings of these connective words when they are used in a mathematical setting are very close to their English counterparts. The primary difference is that when the connectives are used in English, the meanings may vary depending on the context, whereas, in mathematics, the meanings are fixed and can be described precisely.

Moreover, assume that P and Q are (mathematical) statements. Then "P and Q", "P or Q", "if P, then Q", and "P if and only if Q" are also statements where their truth or falsity is entirely determined by the truth or falsity of P and Q. This relationship can be completely described by a truth table. For example, the truth table for "P and Q" is

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

Each row of the table gives a truth value for P, a truth value for Q, and the corresponding truth value for "P and Q". For example, if P is the sentence "$0 < 7$" and Q is the sentence "$7 \leq 10$", then, since P and Q are both true, the sentence "P and Q" is true (recall the first line of the truth table).

The truth tables for the other binary connectives are

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	If P then Q
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	P if and only if Q
T	T	T
T	F	F
F	T	F
F	F	T

Note that the connective "or" described by the truth table is what is sometimes known as the "inclusive 'or' ", which might also be written as "one or the other, or both". For example, if we let P be the sentence $0 < 7$ and Q the sentence $7 \leq 10$ (as above), then the first line of the truth table for "or" yields that "P or Q" is true.

A sentence of the form "if P, then Q" is called an *implication*. The sentence P is called the *hypothesis* of the implication "if P, then Q" and the sentence Q is consequently called the *conclusion*. As a first example, consider the implication "if P, then Q" where P is the sentence $0 < 7$ and Q is the sentence $7 \leq 10$: "If $0 < 7$ then $7 \leq 10$". Since $0 < 7$ and $7 \leq 10$ are both true, we may use the first row of the the truth table to determine whether "If $0 < 7$, then $7 \leq 10$" is true.

Admittedly, the implication with hypothesis $0 < 7$ and conclusion $7 \leq 10$ sounds strange. The reason is that an implication "if P then Q" is seldom used if it is known whether or not the sentence P is true. A more reasonable example is the implication "If your score on the final exam for this course is a 100%, then your grade for the course will be an A." Whether this implication is true or false will be known after the end of the semester when the truth values of the hypothesis (your score on the final exam for this course is a 100%) and the conclusion (your grade for the course is an A) are known. Assuming that this statement is made at the beginning of the semester, under what circumstances will it turn out to have been false? Only if your grade on the final exam for this course is a 100% (the hypothesis is true) and your grade for the course is not an A (the conclusion is false). Under all other circumstances, the implication will have been true. This reasoning then justifies the truth values in the third column of the truth table "If P, then Q".

Implications are used frequently in mathematical writing and may appear in several different forms. All of the following, for example, have the same meaning as "If P then Q":

P implies Q
Q follows from P
P is sufficient for Q
Q is necessary for P
Assume P, then Q
Q if P
P only if Q
$P \to Q$
$P \Rightarrow Q$

The last two items in this list, $P \to Q$ and $P \Rightarrow Q$, are the symbolic forms of the implication "If P, then Q". The sentence "P if and only if Q" has similar symbolic forms. They are $P \leftrightarrow Q$ and $P \Leftrightarrow Q$. The symbolic forms of "P and Q" (either $P \wedge Q$ or $P\&Q$) and of "P or Q" $(P \vee Q)$ are used less frequently.

1.4 Using variables and quantifiers

The two symbols $\forall$ and $\exists$ are called *quantifiers*. The symbol $\forall$ is usually read "for all," "for every," or "for each" and the symbol $\exists$ is read "there exists". The quantifiers are used in conjunction with variables. In our examples, the domains of the variables will usually be one of the standard sets which we list below.

Definition 1.1.

1. $\mathbb{N}$ is the set of natural numbers: $0, 1, 2, \ldots$
2. $\mathbb{Z}$ is the set of integers: $\ldots -3, -2, -1, 0, 1, 2, 3, \ldots$
3. $\mathbb{Q}$ is the set of rational numbers. These are the real numbers that can be expressed as fractions $\frac{p}{q}$, where p and q are integers such that $q \neq 0$.
4. $\mathbb{R}$ is the set of real numbers.
5. $\mathbb{N}^+$ denotes the set of positive natural numbers and similarly for the other sets listed above.

It will also be convenient to have the *standard interval notation* available.

Definition 1.2. Assume that a and b are real numbers.

- (a, b) denotes the set of all real numbers x for which $a < x < b$. (a, b) is called *the open interval from a to b.*
- $[a, b]$ denotes the set of all real numbers x for which $a \leq x \leq b$ and is called *the closed interval from a to b.*
- $(a, b]$ is the set of real numbers x such that $a < x \leq b$.
- $[a, b)$ is the set of real numbers x such that $a \leq x < b$. These last two sets are usually called *half open intervals.*

For example, $(-3, 4]$ denotes the set of all real numbers between -3 and 4, not including -3, but including 4. We will follow the usual practice of extending the interval notation by allowing the symbols ∞ and $-\infty$. For example, $(-\infty, 4)$ will denote the set of all real numbers x such that $x < 4$ and $(-\infty, \infty)$ denotes the set of all real numbers in this extended notation.

Assume that $P(x)$ is a sentence in which the variable x occurs. Assume also that the domain of x is the set A. Then for each a in A, we denote $P(a)$ by the statement obtained from $P(x)$ by replacing the variable x by a. With this notation, we can give meaning to the statements "$\forall x \in A, P(x)$" and "$\exists x$ such that $P(x)$". As was the case with statements involving the binary connectives, we give meaning by stating the conditions under which each of these two statements is true:

"$\forall x \in A, P(x)$" is true if and only if for every $a \in A$, $P(a)$ is true. (1.1)

Similarly:

"$\exists x \in A$ such that $P(x)$" is true if and only if there is some a in A such that $P(a)$is true. (1.2)

For a variable x, we refer to the four expressions "$\forall x$," "$\forall x \in A$," "$\exists x$," and "$\exists x \in A$" as *quantifiers for* x. If P is a sentence in which the variable x occurs and x is in the scope of a quantifier for x in P, then x is said to be *a bound variable in* P. Otherwise, x is *a free variable in* P. Note, sometimes the word *unquantified* is used instead of the word "free" and the word *quantified* is used instead of the word "bound".

Example 1.3. Identify the free variables and the bound variables in the following sentences. Assume, unless indicated otherwise, that the range of every variable is the set of real numbers.

1. $\forall x \in \mathbb{R}$, $x^2 + 7x \geq xy$
2. $\exists x \in \mathbb{R}$ and $\exists y \in \mathbb{R}$ such that $x^2 = y^2$ and $x > y$.
3. n is a natural number and $n > 0$ and for some integer k, $0 < k < n$
4. $0 < w < 6$
5. $-3 < x^2 + w + y < 4$

In example 1, the variable x is bound because of the quantifier "$\forall x \in \mathbb{R}$". Consequently, the variable y is free since there is no quantifier for y.

In example 2, both x and y are bound because of the quantifiers "$\exists x \in \mathbb{R}$" and "$\exists y \in \mathbb{R}$".

In example 3, the variable k is bound by the quantifier "for some integer k". The variable n is free, so there is no quantifier for n in the sentence of this example. It is the case that any replacement for n that makes the sentence true must be a natural number, so in some sense the sentence puts a restriction on n. However, the word "bound" in the sense we are using it does not mean "restricted". A variable is bound *if and only if* a quantifier for it appears in the sentence.

In example 4, the variable w is free. Even though the sentence restricts w in some sense, there is no quantifier for w. Similarly, in 5, the variables x, w, and y are free.

For a second example, consider the statement

$$\forall x \in \mathbb{Z}, x \geq 17 \tag{1.3}$$

The statement (1.3) has the form "$\forall x \in \mathbb{Z}, P(x)$," where $P(x)$ is the sentence $x \geq 17$. First, we note that x is a bound variable in the statement (1.3). On the other hand, x is a free variable of the statement $P(x)$. If it's not immediately obvious whether or not (1.3) is true, we might do some exploring by replacing x in $P(x)$ by one or more elements of $\mathbb{Z}$. For example, if we replace x by 43, then we obtain the statement $P(43)$ or $43 \geq 17$ (which is true). This doesn't mean that $\forall x \in \mathbb{Z}, P(x)$ is true. That would only be the case if $P(n)$ were true for every integer n—and there are some integers n for which $P(n)$ is false. For example, $P(3)$ is the sentence $3 \geq 17$ (which is false). An element $a \in A$ (like 3 in our example) for which $P(a)$ is false is called a counter example for $\forall x \in A, P(x)$.

Definition 1.4. A *counter example* for $\forall x \in A, P(x)$ is an element $a \in A$ such that $P(a)$ is false.

and

$$\forall x \in A, P(x) \text{ is false if and only if there is a } \textit{counter example.} \tag{1.4}$$

Another example:

$$\exists n \in \mathbb{Z} \text{ such that } 6n^2 - 10n + 2 = 0$$

This is $\exists n \in \mathbb{Z}$ such that $Q(n)$, where we have abbreviated the sentence $6n^2 - 10n + 2 = 0$ by $Q(n)$. We might begin by replacing n in $Q(n)$ by some integer, say 4. The result is the statement $Q(4)$, that is, $6(4)^2 - 10(4) + 2 = 0$ (Note, in order to get the statement $Q(4)$, we had to replace each occurrence of n with (4), rather than 4.[1]). The statement $Q(4)$ is false. This doesn't necessarily

[1]In general, when $P(x)$ is a sentence with free variable x and τ is some expression representing an object, to obtain $P(\tau)$, every occurrence of x should be replaced by (τ) rather than by τ. There are several reasons for this. In the case that τ is a single symbol representing a number, $\tau = 4$ for example, the problem is caused by the standard convention of omitting the symbol for the operation of multiplication in an expression where a number is multiplied by a single letter variable.

mean that (1.4) is false, since its truth would only require one element $a \in \mathbb{Z}$ for which $Q(a)$ is true. However, solving the equation $6n^2 - 10n + 2 = 0$ using the quadratic equation shows us that there are no *integer* solutions, hence (1.4) is false. This illustrates another principle:

> "$\exists a \in A$ such that $P(a)$" is false if and only if for every $a \in A$, $P(a)$ is false.

Example 1.5. Is the statement

$$\forall x \in [-1, 1], \exists y \in \mathbb{R} \text{ such that } x < y < x^2 \tag{1.5}$$

true or false? According to what has been said above, (1.5) will be true if for every $a \in [-1, 1]$, the statement "$\exists y \in \mathbb{R}$ such that $a < y < a^2$" is true and false if there is at least one a in $[-1, 1]$ for which "$\exists y \in \mathbb{R}$ such that $a < y < a^2$" is false. Denote this latter statement by $P(a)$. We begin by trying some specific values of a. For example, if $a = -\frac{1}{2}$, then $P(a)$ is $P(-\frac{1}{2})$, which is "$\exists y \in \mathbb{R}$ such that $-\frac{1}{2} < y < (-\frac{1}{2})^2$". However, if we let $a = \frac{1}{2}$, then $P(a)$ is "$\exists y \in \mathbb{R}$ such that $\frac{1}{2} < y < (\frac{1}{2})^2$", which is false. Therefore, since we have found an a in $[-1, 1]$ for which $P(a)$ is false, we have a counter example for (1.5) and we may therefore conclude that it is false.

Example 1.6. Is the statement

$$\exists y \in \mathbb{R} \text{ such that } \forall x \in (-1, 0), \;\; x < y < x^2 \tag{1.6}$$

true or false? This statement will be true if for some real number a, the statement "$\forall x \in (-1, 0), x < a < x^2$" is true. We will abbreviate the latter statement by $Q(a)$ and try some specific values for a. For example, letting $a = 2$ we get $Q(2)$, which is "$\forall x \in (-1, 0)$, $x < 2 < x^2$". The statement $Q(2)$ has the form "$\forall x \in (-1, 0), R(x)$" where $R(x)$ is the sentence "$x < 2 < x^2$", which is an abbreviation for "$x < 2$ and $2 < x^2$". Since $2 \not< (-\frac{1}{2})^2$, $R(-\frac{1}{2})$ is false. Therefore "$\forall x \in (-1, 0), R(x)$" is false, so $Q(2)$ is false. We might try other values of a and as it turns out there is one for which $Q(a)$ is true, namely $a = 0$. The statement $Q(0)$ is "$\forall x \in (-1, 0), x < 0 < x^2$". Therefore, the original statement "$\exists y \in \mathbb{R}$ such that $\forall x \in (-1, 0), x < y < x^2$" is true.

1.5 Free and Bound Variables

1.5.1 Free and bound variables

A sentence in which all variables are bound will, in general, either be a true sentence or a false sentence. For example, the sentence

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } y^2 + xy + 2 = 0 \tag{1.7}$$

contains no free variables and is either a false sentence or a true sentence. On the other hand, the sentence

$$\exists y \in \mathbb{R} \text{ such that } y^2 + xy + 2 = 0 \tag{1.8}$$

has x as a free variable and is neither true nor false. The following facts give us some idea of the roles played by free variables (which, we recall from Section 1.2, are sometimes also referred to as parameters).

- A free variable, say x, whose domain in the set A represents a *fixed* but unspecified element of A.

- Usually a sentence $P(x)$ in which the variable x occurs free will be neither true nor false. Note, however, that if the sentence is altered by placing a quantifier for x in front or by replacing the free variable x by some specific element of A, then the resulting sentence will be either a true sentence or a false sentence. For example, equation (1.7) is the result of placing a universal quantifier $\forall x$ at the beginning of (1.8).

- There are rules which limit the introduction of free variables into a mathematical argument. These rules will be detailed later.

1.5.2 Implicit quantifiers in implications

Another important point to note is that there are some circumstances under which the universal quantifier is omitted from a sentence and must be supplied by the reader. In other words, there are sentences $P(x)$ (in which a variable x appears to be free) whose intended meaning is $\forall x, P(x)$. In this case, the quantifier $\forall x$, which is not explicitly stated, is called an *implicit quantifier*. Implicit quantifiers occur most frequently in "If ... then ..." sentences. Most people supply them automatically. For example, consider the sentence

$$\text{If } x \text{ is a real number greater than 0, then } x^2 + 1 > 0 \tag{1.9}$$

The intended meaning of this sentence is "$\forall x$, if x is a real number greater than 0, then $x^2+1 > 0$", which is true. Most people without knowing anything about quantifiers would unconsciously supply the missing $\forall x$ in (1.9) and say that the sentence is true.

1.5.3 Other instances of implicit quantification

There are other situations in which implicitly quantified variables occur. Here is a list of those situations.

1. **In identities.** If an equation or inequality with free variables is referred to as an identity, then the intended meaning is that the equation or inequality is true for all values of the free variables, where both sides of the equation or inequality are defined. For example,

Theorem. *The following equation is an identity:* $\tan^2\theta + 1 = \sec^2\theta$

means

Theorem. *For every real number* θ *for which* $\tan\theta$ *and* $\sec\theta$ *are defined,* $\tan^2\theta + 1 = \sec^2\theta$.

2. **In implications.** If $P(x)$ and $Q(x)$ are sentences in which the variable x occurs free and the range of x is the set A, then "If $P(x)$, then $Q(x)$" means "$\forall x \in A$, if $P(x)$, then $Q(x)$". Similarly, "$P(x)$ if and only if $Q(x)$" means "$\forall x \in A$, $P(x)$ if and only if $Q(x)$".

   One example is provided by 1.9 above; another is

   Theorem. *If* n^2 *is an even integer, then* n *is an even integer.*

   which has the same meaning as

   Theorem. *For every integer* n*, if* n^2 *is even, then* n *is even.*

   Similarly

   Theorem. n^2 *is an even integer if and only if* n *is an even integer.*

   has the same meaning as

   Theorem. *For every integer* n*,* n^2 *is even if and only if* n *is even.*

3. **In definitions.** In a definition, after making the quantifiers described in 2 explicit, any remaining variables that are not otherwise quantified should be quantified by adding a universal quantifier whose scope is the entire definition.

   For example, consider the sentence "Let f be the function from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x) = 7x + 3$". The variable x (with range $\mathbb{R}$) occurs in this definition and is not otherwise quantified. This means that there is an implicit universal quantifier $\forall x \in \mathbb{R}$ and this sentence has the same meaning as

   > Let f be the function from $\mathbb{R}$ to $\mathbb{R}$ defined by $\forall x \in \mathbb{R}$, $f(x) = 7x + 3$.

   Another example: The definition

   Definition 1.7. If $\langle G, * \rangle$ is a group, an element e of G is called an *identity* if $\forall x \in G$, $x * e = e * x = x$.

   has the same meaning as

   Definition 1.8. For every group $\langle G, * \rangle$ and $\forall e \in G$, e is called an *identity* if $\forall x \in G$, $x * e = e * x = x$.

Item 2 is a slight oversimplification. At the risk of making the situation seem more complicated than it actually is, we give the following more accurate version.

> If the sentence "If $P(x)$ then $Q(x)$" occurs in a mathematical work where x is a variable which is otherwise unquantified (and if the range of x is the set A) then the meaning of "If $P(x)$, then $Q(x)$" is "$\forall x \in A$, if $P(x)$, then $Q(x)$".

The idea here is that the variable x may be quantified in some larger sentence of which the implication "If $P(x)$, then $Q(x)$" is just a part and under these circumstances, it would be wrong to add the quantifier $\forall x \in A$ to the implication "If $P(x)$, then $Q(x)$". Further, this quantifier which occurs in the larger sentence may be an implicit one. As a consequence, when we make all of the quantifiers in a statement explicit, we should work from the outside in.

As an example consider the following which is a fragment of a mathematical argument taken out of context. We assume that the symbol f represents some fixed function and is, therefore, not a variable.

Example 1.9. The function f is uniformly continuous on $[0, 4]$, therefore, if ϵ is a positive real number, then there is a positive real number δ such that if x and y are in $[0, 4]$ and $|x - y| < \delta$, then $|f(x) - f(y)| < \epsilon$.

Starting with 1.9, we shall add the implicit quantifiers to the sentence step by step, working from the outside inward. The first step is to apply item 2 to the variable ϵ. This gives

> The function f is uniformly continuous on $[0, 4]$, therefore, $\forall \epsilon \in \mathbb{R}$, if $\epsilon > 0$, then there is a positive real number δ such that if x and y are in $[0, 4]$ and $|x - y| < \delta$, then $|f(x) - f(y)| < \epsilon$.

The second and final step is to apply 2 to the variables x and y in the implication "if x and y are in $[0, 4]$ and $|x - y| < \delta$, then $|f(x) - f(y)| < \epsilon$" to obtain

> The function f is uniformly continuous on $[0, 4]$, therefore, $\forall \epsilon \in \mathbb{R}$, if $\epsilon > 0$, then there is a positive real number δ such that $\forall x$ and y in $[0, 4]$, if $|x - y| < \delta$, then $|f(x) - f(y)| < \epsilon$.

1.6 Negation

The negation of a sentence P is denoted "not P" or $\neg P$. The truth table for $\neg P$ is

P	not P
T	F
F	T

The negation of P is the sentence that asserts that the sentence P is false. The negation of a sentence is seldom

Sentence	Negation
$\forall x \in S, P(x)$	$\exists x \in S$, such that not $P(x)$
$\exists x \in S$ such that $P(x)$	$\forall x \in S$, not $P(x)$
P and Q	(not P) or (not Q) If P, then (not Q) If Q, then (not P)
P or Q	(not P) and (not Q)
not P	P
If P, then Q	P and (not Q)
If $P(x)$, then $Q(x)$ (meaning "$\forall x$, If $P(x)$, then $Q(x)$" or "$\forall x \in S$, If $P(x)$, then $Q(x)$")	"$\exists x$ s.t. $P(x)$ and (not $Q(x)$)" or "$\exists x \in S$ s.t. $P(x)$ and (not $Q(x)$"

Table 1.1: Negations

obtained by placing the word "not" in front of it. For example, the negation of "$0 < 7$" might be written "0 is not less than 7" , "$0 \not< 7$", or possibly "it is not the case that $0 < 7$".

For any mathematical statement P, exactly one of the statements P and "not P" will be true and in many instances we will be trying to decide which is the case. It is therefore helpful to be able to write the negation of a sentence in a more readable and positive form. In the present section we discuss some of the rules for doing this.

We have already seen that a sentence of the form $\forall x \in S, P(x)$ is false if and only if there is some element a of the set S such that $P(a)$ is false. But this happens if and only if "$\exists x \in S$ such that not $P(x)$" is true. This gives one way of rewriting the negation of $\forall x \in S, P(x)$: "not $\forall x \in S, P(x)$" is equivalent to "$\exists x \in S$ such that not $P(x)$". For example, the negation of $\forall x \in \mathbb{R}, x^2 > 0$ could be written "$\exists x \in \mathbb{R}$ such that not$(x^2 > 0)$" or, in a more positive form, "$\exists x \in \mathbb{R}$ such that $x^2 \leq 0$". Table 1.1 gives a list of sentences involving the connectives that we have discussed and one or more ways of writing the negation of each. (Notice that we have used the abbreviation "s.t". for the words "such that" in the table.)

There are several things to note. First, we usually handle the negation of an "if and only if" statement by using the fact that "P if and only if Q" is equivalent to "(If P then Q) and (if Q then P)". Secondly, we note that the first two lines of the table tell us that "not $\forall x \in S, P(x)$" is equivalent to "$\exists x \in S$ such that not $P(x)$" and "not $\exists x \in s$ such that $P(x)$" is equivalent to "$\forall x \in S$, not $P(x)$". In other words, the "not" can be moved across a quantifier if the quantifier is changed from $\forall$ to $\exists$ or from $\exists$ to $\forall$. Thirdly, to handle negations of sentences involving more than one connective, negate one connective at a time working from the outside in. For example, the negation of "$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that

$y < x$ and $x < y^2$" could be simplified in four steps:

$$\neg(\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } y < x \text{ and } x < y^2) \text{ is equivalent to}$$
$$\exists x \in \mathbb{R} \text{ such that } \neg(\exists y \in \mathbb{R} \text{ such that } y < x \text{ and } x < y^2) \text{ is equivalent to}$$
$$\exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, \neg(y < x \text{ and } x < y^2) \text{ is equivalent to}$$
$$\exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, (\neg(y < x) \text{ or } \neg(x < y^2)) \text{ is equivalent to}$$
$$\exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, (y \geq x) \text{ or } (x \geq y^2))$$

As a second example, the negation of

$$\forall \epsilon > 0, \exists d > 0 \text{ such that } \forall x, \text{ if } |x - 2| < d \text{ then } |x^2 - 4| < \epsilon$$

is (we are assuming that the range of all variable is $\mathbb{R}$)

$$\exists \epsilon > 0 \text{ such that } \forall d > 0, \exists x \text{ such that } |x - 2| < d \text{ and } |x^2 - 4| \geq \epsilon.$$

Finally, to show that a universally quantified statement "$\forall x \in S, P(x)$" is false, we show that its negation "$\exists x \in S$ such that $P(x)$" is true. That is, we find an element $a \in S$ such that $P(a)$ is false. To show that a statement " If $P(x)$ then $Q(x)$" is false (since "If $P(x)$ then $Q(x)$" means "$\forall x \in S$ if $P(x)$ then $Q(x)$"), we need to find an element $a \in S$ for which "If $P(a)$, then $Q(a)$" is false. In other words, we need to find an element $a \in S$ such that $P(a)$ is true and $Q(a)$ is false. Such an element a is called (like before) a *counter example* for "If $P(x)$, then $Q(x)$".

Example 1.10. Find a counter example for "If $x \in \mathbb{N}$, then $\exists y \in \mathbb{N}$ such that $y < x$".

A counter example is an element a for which $a \in \mathbb{N}$ is true and "$\exists y \in \mathbb{N}$ such that $y < a$" is false. $a = 0$ is such a counter example. Note that for the sentence of this example, there is no other counter example.

1.7 Exercises

1.1. What are the free variables and what are the bound variables in each of the following? Unless otherwise specified, assume that the range of all variables is the set of real numbers, $\mathbb{R}$.

(a) $\forall x \in \mathbb{R}, x^2 \geq y$

(b) $\exists x, \exists y$ such that $x < y$ and $x^2 > y^2$

(c) $n \in \mathbb{Z}$ and $n > 0$ and for some $k \in \mathbb{Z}$, $0 < k < n$

(d) $0 < x < 2$

(e) $0 < x^2 < 4$

(f) If $0 < x < 2$, then $0 < x^2 < 4$

1.2. Identify the free variables and the bound variables in each of the following:

(a) $\forall x \in \mathbb{R}, x > 26$

(b) $\exists x \in \mathbb{R}$ such that $x + y + z = 16$

(c) $0 < x < 1$

(d) $\forall x \in \mathbb{R}, 0 < w < |x|$

1.3. Do the followring:

(a) Give a replacement for the free variable in the following sentence which makes the sentence **true**: $(\exists y \in \mathbb{R})(y < x < 2y)$. (The universe of the variable is $\mathbb{R}$.)

(b) Give a replacement for the free variable in the sentence in the previous problem which makes the sentence **false**.

1.4. Let $P(y)$ be the sentence "$\exists x \in \mathbb{R}$ such that $y < x < y^2$".

(a) Give a replacement for the free variable which results in a true statement. (A *replacement* is a specific real number.)

(b) Give a replacement for the free variable which results in a false statement.

1.5. Do the following:

(a) Give a sentence $A(x)$ with one free variable x such that $(\forall x \in \mathbb{R})(A(x))$ is true.

(b) Give a sentence $P(x)$ with one free variable x such that $(\forall x \in \mathbb{R})(P(x))$ is false and $(\exists x \in \mathbb{R})(P(x))$ is true.

1.6. The following statements are implications. Identify the hypothesis and conclusion of each.

(a) If A, B, and C are sets, then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

(b) Assume that A, B, and C are sets, then $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(c) Let $\{x\}_{n=1}^{\infty}$ be a bounded sequence, then $\{x\}_{n=1}^{\infty}$ has a convergent subsequence.

(d) $A \cup B$ is a closed set if both A and B are closed.

(e) If $\{I_n : n \in \mathbb{N}\}$ is a nested sequence of closed intervals, then $\bigcap_{n \in \mathbb{N}} I_n$ is non-empty.

(f) An open set is either empty or contains one of its cluster points.

(g) The least upper bound of any set of real numbers with more than one element is greater than the greatest lower bound.

1.7. Are the following statements true or false?

(a) $\forall x \in \mathbb{R}, x^2 + 2x + 1 > 0$

(b) $\exists x \in \mathbb{R}$ such that $x^2 + 2x + 1 > 0$

(c) $\exists n \in \mathbb{Z}$ such that $n < 17$

(d) $\forall n \in \mathbb{Z}$, $n < 17$

(e) $\exists n \in \mathbb{Z}$ such that $\forall m \in \mathbb{Z}, n > m$

(f) $\forall m \in \mathbb{Z}, \exists n \in \mathbb{Z}$ such that $n > m$

(g) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$, such that $x + 2 = y$

(h) $\exists y \in \mathbb{R}$ such that $\forall x \in \mathbb{R}, x + 2 = y$

(i) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $x^2 < y$

(j) $\exists y$ such that $\forall x$, $x^2 < y$ (For this and the next five statements assume that the range of x, y, and z is $\mathbb{R}$.)

(k) $\forall x \exists y$ such that $x + y = 0$.

(l) $\exists y$ such that $\forall x$, $x + y = 0$.

(m) $\forall x \exists y$ such that $xy = 0$.

(n) $\exists y$ such that $\forall x$, $xy = 0$.

(o) $\forall x \exists y$ such that $\forall z$, $(xy = xz)$.

(p) $\forall y \in [7, 9], \exists x \in [0, 1]$ such that $2x + 7 = y$

(q) $\exists d$ such that $d > 0$ and $\forall x$, if $-d < x - 2 < d$, then $-1 < x^2 - 4 < 1$ (Assume that all variables have range $\mathbb{R}$.)

1.8. Answer **T** for true or **F** for false.

(a) $\forall x \in \mathbb{R}, 2x + 6 < 4$

(b) $\exists x \in \mathbb{R}$ such that $2x + 6 < 4$

(c) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, 2x + 6 < y$

(d) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $2x + 6 < y$

(e) $\exists y \in \mathbb{R}$ such that $\forall x \in \mathbb{R}, 2x + 6 < y$

(f) $\forall y \in \mathbb{R}, \exists x \in \mathbb{R}$ such that $0 < x < y$

(g) $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}, 0 < x < y$

1.9. Assume that m and n are variables whose range is the set $\mathbb{Z}$ of integers. Rewrite the following by making all the implicit quantifiers explicit.

(a) If n is an odd integer, then n^2 is odd.

(b) The following is an identity: $(n+1)^2 = n^2 + 2n + 1$.

(c) If n is an even integer, then there is an integer m such that $m^2+n+1 = 0$.

1.10. Write the negation of the following in readable form. It might help to put the statements in symbolic form first.

(a) For every real number $\epsilon > 0, \exists \delta > 0$ such that for every x and every y in $\mathbb{R}, |x-y| < \delta$ implies $|x^2 - y^2| < \epsilon$.

(b) If x and y are real numbers and $x < y$, then $x^2 < y^2$.

(c) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})$(If $y \geq x$, then $\frac{1}{y} \leq 1$).

(d) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $y > x^2$.

(e) $(\exists x \in \mathbb{R})(x^2 + x + 1 = 0)$.

1.11. Find counter examples. (The range of every variable is $\mathbb{Z}$.)

(a) If a, b, and c are integers and a divides bc, then a divides b or a divides c.

(b) If a, b, and c are integers and $a < b$ and $a < c$, then $a < bc$

(c) If x is even, then 6 divides x.

1.12. Assume that w is an integer and you want to prove that $w^2 - w$ is even. What will the last two lines of the proof probably be? Use the definition: An integer n is *even* if $\exists k \in \mathbb{Z}$ such that $n = 2k$.

1.13. Answer "true" or "false":

(a) The negation of "If $a \in \mathbb{Z}$ and a is a multiple of 6, then a is a multiple of 12" is "If $a \in \mathbb{Z}$ and a is a multiple of 6 then a is not a multiple of 12".

(b) $x = 5$ is a counter example for "If x is an even integer, then 4 divides x".

(c) $x^2 - 6x + 5 = 13$ is a true mathematical sentence. (Assume that the range of x is $\mathbb{R}$.)

(d) $x = 4$ is a counter example to "If 6 divides x, then 2 divides x".

Chapter 2

the Hows - Introduction to Proofs

2.1 Introduction

In the section we discuss most of the standard methods for proving (true) mathematical statements. For example after studying this chapter it should be routine for you to prove a sentence like

$$\forall n \in \mathbb{N}, \text{ if } n \text{ is odd then } n^2 + 3n - 1 \text{ is odd.}$$

The methods we shall discuss are natural consequences of the material in Chapter 1. They follow from what we have learned about the language of mathematics and its meaning.

A warning before we begin: The methods described here don't provide an algorithm which can be applied to any true mathematical statement and automatically produce a proof. What the methods will do is get you as quickly as possible to the heart of a proof. They get you past the routine part of an argument so that you can concentrate on the essential part.

2.2 Preliminaries

In this section we'll look at a typical mathematical proof and examine the most frequently used principle and techniques.

2.2.1 Mathematical facts we'll assume

For any proof there must be a body of facts that are assumed to be true and may be used without proving them. In this course we will assume all the mathematical facts that you are likely to learn in either an elementary algebra course or a course in trigonometry. Some examples are given below. Note that this list

is far from exhaustive but is intended to give you a general idea of what you may assume.

2.2.1.1 Algebraic identities

All the usual algebraic identities may be used. For example the following are true for all real numbers (which includes the natural numbers, the integers and the rational numbers: $x + y = y + x$, $xy = yx$, $x + (y + z) = (x + y) + z$, $(x+y)^2 = x^2 + 2xy + y^2$, $x(y+z) = (xy) + (xz) = xy + xz$ (this last expression uses the usual conventions for omitting parentheses).

2.2.1.2 Closure properties

We begin with one of several closure properties, namely

$$\forall x \text{ and } y \text{ in } \mathbb{R}, x + y \text{ is in } \mathbb{R} \tag{2.1}$$

This formula is usually expressed by saying that the real numbers are closed under addition. Similarly, the phrase "The real numbers are closed under multiplication" means

$$\forall x \text{ and } y \text{ in } \mathbb{R}, x \cdot y \text{ is in } \mathbb{R} \tag{2.2}$$

Here are the closure facts we will use:

1. The real numbers are closed under $+$, $\cdot$ and $-$. In addition $\forall x$ and y in $\mathbb{R}$, if $y \neq 0$ then $\frac{x}{y}$ is in $\mathbb{R}$ and if $x \geq 0$ is in $\mathbb{R}$ then $\sqrt{x}$ is in $\mathbb{R}$.
2. The rational numbers are closed under $+$, $\cdot$, $-$ and $\forall x$ and y in $\mathbb{Q}$, if $y \neq 0$ then $\frac{x}{y}$ is in $\mathbb{Q}$.
3. The integers are closed under $+$, $\cdot$ and $-$.
4. The natural numbers are closed under $+$ and $\cdot$.

2.2.1.3 Inequalities

We will assume all the usual properties of inequalities. Some examples are: For all real numbers x, y, z and w

1. If $x < y$ and $y < z$ the $x < z$.
2. If $x < y$ then $x + z < y + z$.
3. If $x < y$ and $z < w$ then $x + z < y + w$.
4. if $x > 0$ and $y < z$ then $xy < xz$.
5. If $x < 0$ and $y < z$ then $xy > xz$.
6. Exactly one of the following holds $x < y$, $y < x$ or $x = y$.
7. $|x| < y$ if and only if $-y < x < y$.
8. The corresponding properties for $>$, $\leq$ and $\geq$.

2.2.1.4 Other facts

Throughout the book as we study the different mathematical systems we will introduce properties of those systems which we will accept without proof. These properties will be referred to as *axioms*. Some may be familiar to you and others will be new. For purposes of the next section we will need the following definition and the theorem that follows it. We will assume that the theorem is true only temporarily. It's proof will be given in Section 2.4.

Definition 2.1. Assume that n is an integer.

1. n is *even* if and only if there is an integer k such that $n = 2k$.
2. n is *odd* if and only if there is an integer k such that $n = 2k + 1$.

Theorem 2.2. *Every integer is either even or odd and no integer is both even and odd.*

2.2.2 Terminology

We first discuss some terminology which is used in connection with proofs.

At any point in the proof of a mathematical statement there will be several other statements which are available to you for deriving further conclusions. These statements may be facts from elementary mathematics (See Subsection 2.2.1), theorems you have previously proved, axioms, assumptions you have made which are justified by one of the proof principles we shall discuss or they may be definitions. We will refer to these statements as the *active hypotheses*. For example, assuming that the definition of even has been given (See definition 2.1 part (1) above) then the statement "$\forall n \in \mathbb{Z}$, n is even if and only if $\exists k \in \mathbb{Z}$ such that $n = 2k$" may be used at any point in your proof and is therefore an active hypothesis.

In the same way, at any point in a proof, there may be free variables which have been introduced and are temporarily available for use. (We will see later in the chapter the circumstances under which such symbols may be introduced.) Such free variable are also called parameters and will be referred to as *active parameters* (or *active free variables*).

2.3 Some sample proofs and proof principles

Theorem 2.3. *$\forall n \in \mathbb{Z}$, if n is odd then $2n^2 + 3n + 4$ is odd.*

Proof.

(1) Assume that n is an integer and

(2) assume that n is odd.

(3) Then by the definition of "odd", $n = 2k + 1$ for some integer k.

(4) Therefore $2n^2+3n+4 = 2(2k+1)^2+3(2k+1)+4 = 2(2k+1)^2+6k+3+4 = 2(2k+1)^2+6k+6+1 = 2[(2k+1)^2+3k+3]+1$.

(5) Letting $i = (2k+1)^2+3k+3$

(6) We have $2n^2+3n+4 = 2i+1$ where i is an integer

(7) Hence $2n^2+3n+4$ is odd.

□

There are several points to be made about the proof just given

A. Line (1) illustrates the use of one of the basic proof principles, namely

Proof Principle 1. Proving Universally Quantified Statements. To prove "$\forall x \in A, P(x)$ " assume $x \in A$ and using only that fact about x, prove $P(x)$. □

When you write the line "Assume $x \in A$" the symbol x temporarily represents a fixed but unspecified element of A and becomes an active free variable or parameter. (This is one situation where the free variable is also referred to as parameter.) In addition the statement "$x \in A$" becomes an active hypothesis[1] and may therefore be used in your proof of $P(x)$. The parameter x remains active and the statement "$x \in A$" continues to be an active hypothesis up through the point where you prove $P(x)$.

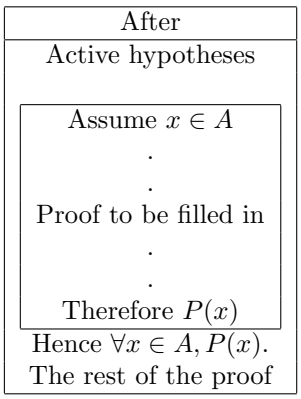
We could (and it might be better) to use a symbol different from x for the parameter introduced. For example, we might say "Assume $a \in A$" and then prove $P(a)$. However it's standard practice to use the same symbol that was used for the quantified variable. Note that using Proof Principle 1 is one instance where we are allowed to introduce a parameter or free variable into a proof.

For most of the proof principles that we introduce we will include a pair of diagrams which show graphically how the proof principle is used. The first diagram in the pair is a picture of your proof before using the proof principle and the second picture shows what the proof looks like after using it. For Proof Principle 1 the before diagram is

Before
Active hypotheses
.
.
Proof to be filled in
.
.
Hence $\forall x \in A, P(x)$.
The rest of the proof

[1] See Subsection 2.2.2 for an explanation of the terms *active hypotheses* and *active parameter*

This diagram illustrates the situation where you have several statements available for use in you proof (the active hypotheses) and you *want to prove* the statement $\forall x \in A, P(x)$. The gap between the active hypotheses and the statement you want to prove has to be filled in. Proof Principle 1 tells us what the first and last lines of the "proof to be filled in" should be. The first line will be "Assume $x \in A$." and the last line will be "Therefore (or some other word indicating that this follows from what has gone before) $P(x)$." That is, after using Proof Principle 1 the picture will be



The inner box represents the part of the proof in which x is a parameter or free variable and "$x \in S$" is an active hypothesis.

B. Line (2) illustrates another basic proof principle:

Proof Principle 2. Proving Implications. To prove an implication "If Q then R" assume Q and using this assumption prove R □

When you write the line "Assume Q" you are adding Q temporarily to the active hypotheses. The statement Q may then for be used in your proof of R. The statement Q ceases to be an active hypothesis at the point where you prove R.

The "before" and "after" diagrams for Proof Principle 2 are below.

Before using the Proof Principle:

Before
Active hypotheses . . Proof to be filled in . . Hence if P then Q. The rest of the proof

And after using Proof Principle 2 the diagram would be

After
Active hypotheses Assume P . . Proof to be filled in . . Therefore Q Hence if P then Q. The rest of the proof

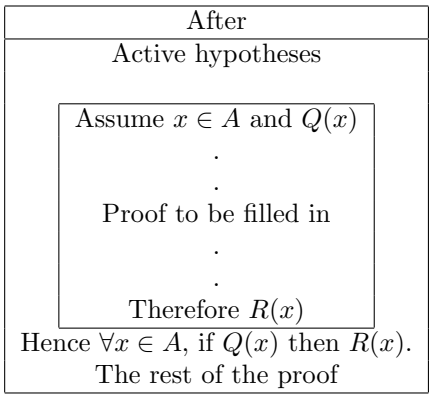
Note that P is only an active hypothesis inside the inner box.

The two proof principles above are frequently used together as they are in lines (1) and (2) of the proof just given. We state this as a proof principle.

Proof Principle 3. To prove a universally quantified implication "$\forall x \in A$ if $Q(x)$ then $R(x)$" assume $x \in A$ and $Q(x)$ and using these assumptions prove $R(x)$. □

The before and after diagrams for Proof Principle 3 are

Before
Active hypotheses . . Proof to be filled in . . Hence $\forall x \in A$, if $Q(x)$ then $R(x)$. The rest of the proof



C. Notice how the active hypotheses are introduced and used. In lines (1) and (2) the statements "n is an integer" and "n is odd" are added to the active hypotheses using Proof Principles 2 and 1 respectively. They are are then available for use later in the proof. The definition of "odd" is also available and in line (3) the assumption made in line (2) that n is odd together with the definition of "odd" is used. The definition of "odd" is used again in line (7).

D. Using Proof Principle 2 in the proof above we assumed in line (2) that n was odd and we were aiming for a proof that $2n^2+3n+4$ was odd. Using the definition of "odd", that meant that we had to prove the equality $2n^2 + 3n + 4 = 2i + 1$ for some integer i. This equality was proved by starting with its left hand side and getting its right hand side using active hypotheses including line (3) and algebraic facts. This is one valid method of proving that two objects are equal. In general we have the following proof principle.

Proof Principle 4. Proving $A = B$. There are several ways to prove an equality, for example you may begin with one side, apply legal operations and obtain the other side. Another possibility is to work with the left side A and get some expression, say C, then work with the right side B and obtain the same expression. Also note the following important points.

- **If you are proving $A = B$ by starting with A, applying legal operations and ending with B, *at a minimum* the string of equal expression you write down must begin with A and end with B. The number of expressions that occur in between A and B depends on the difficulty of obtaining each one and on the intended audience for your proof. For example, the string of equalities in line (4) in the proof of Theorem 2.3 should begin with $2n^2+3n+4$ and end with $2[(2k+1)^2+3k+3]+1$ but it might be permissible to leave out one or more if the expressions in between.**

- ***Do Not start with the equality you want to prove and derive something true. This is not a valid method of proving two things are equal.***

□

E. If there's a chance that two objects may be different they should be represented by different symbols. For example, k and i in the proof above.

F. It should be noted how a *universally quantified* active hypothesis is used. In the proof above we had the active hypothesis

$$\forall k \in \mathbb{Z}, k \text{ is odd if and only if } k = 2j + 1 \text{ for some integer } k.$$

This was an active hypothesis because it was the definition of "odd". We also had as an active hypothesis the assumption "n is odd" from line (2). Combining these two active hypotheses we concluded that "$n = 2k + 1$ for some integer k." This used the third of the following three related general principles which as a group we call Proof Principle 5.

Proof Principle 5. Using Universally Quantified Statements.

1. **If $\forall x \in A, P(x)$ an active hypothesis and τ is an expression representing an object for which $\tau \in A$ is an active hypothesis, then you may conclude (that is, add to your active hypotheses) $P(\tau)$.**
2. **If "$\forall x \in A$, if $Q(x)$ then $R(x)$" an active hypothesis and τ is an expression representing an object for which $\tau \in A$ and $Q(\tau)$ are active hypotheses, then you may conclude (that is, add to your active hypotheses) $R(\tau)$.**
3. **If "$\forall x \in A$, $Q(x)$ if and only if $R(x)$" an active hypothesis and τ is an expression representing an object for which $\tau \in A$ and $Q(\tau)$ are active hypotheses, then you may conclude (that is, add to your active hypotheses) $R(\tau)$.**

□

Here are the before and after diagrams for this Proof Principle, part (1).

Before
Active hypotheses including $\forall x \in A, P(x)$ and $\tau \in A$
.
.
Proof to be filled in
.
.
The rest of the proof

After
Active hypotheses including $\forall x \in A, P(x)$ and $\tau \in A$ So $P(\tau)$
.
.
Proof to be filled in
.
.
The rest of the proof

G. Note that if we had applied the definition of "odd" with no change we would have concluded $n = 2j+1$ for some integer j. It's pretty clear that using the variable k instead of j is valid. The general principle involved is

> **If $P(x)$ is a sentence with free variable x and t is a variable not occurring in $P(x)$ then the two statements "$\exists x$ such that $P(x)$" and "$\exists t$ such that $P(t)$" are equivalent and may be used interchangeably. Similarly for the two statements "$\forall x, P(x)$" and "$\forall t, P(t)$".**

H. In line (3) k was the quantified variable in the statement "$n = 2k + 1$ for some integer k." (That is, in the statement "$\exists k \in \mathbb{Z}$ such that $n = 2k + 1$.") Whereas in line (4) we treated k as if it were a fixed integer for which $n = 2k + 1$. This is also valid and the proof principle we used is

Proof Principle 6. Using Existentially Quantified Statements. If "$\exists x \in A$ such that $P(x)$" is an active hypothesis then you can introduce a new active parameter or free variable (say x_0) and add "$x_0 \in A$" and "$P(x_0)$" to the active hypotheses. □

Frequently (maybe "almost always" would be more accurate) rather than introduce a new symbol, the same symbol that was used for the bound variable is used. For example, if we were to have followed the principle above strictly in line (3) we would have inserted a new line

(3.5) Let k_0 be an integer such that $n = 2k_0 + 1$

Then in the remainder of the proof we would have used the symbol k_0 in place of the symbol k. But in the actual proof we followed the usual convention of using the same symbol (k) for the parameter as was used for the bound variable.

The use of Proof Principle 6 is a second instance where a parameter may be introduced into a proof.

The before and after diagram for this Proof Principle is

Before
Active hypotheses including $\exists x \in A, P(x)$
.
.
Proof to be filled in
.
.
The rest of the proof

After
Active hypotheses including $\exists x \in A, P(x)$
Let $x \in A$ satisfy $P(x)$
.
.
Proof to be filled in
.
.
The rest of the proof

Before going on to our next example we give a sequence of diagrams showing how the proof of Theorem 2.3 might have been constructed. At the beginning of the construction we know only what the last line of the proof should be, namely "$\forall n \in \mathbb{Z}$, if n is odd then $2n^2+3n+4$ is odd" and we could picture the situation like this:

Step 1
.
.
Proof to be filled in
.
.
Therefore $\forall n \in \mathbb{Z}$, if n is odd then $2n^2 + 3n + 4$ is odd

Since we need to prove a universally quantified statement we would use Proof Principle 1. This gives us a first line and a second to last line and therefore the following diagram.

Step 2
Assume $n \in \mathbb{Z}$
.
.
Proof to be filled in
.
.
Hence if n is odd then $2n^2 + 3n + 4$ is odd.
Therefore $\forall n \in \mathbb{Z}$, if n is odd then $2n^2 + 3n + 4$ is odd

Now we need to prove an implication and therefore we use Proof Principle 2 which gives us a first and last line of the proof to be filled in.

Step 3

Assume $n \in \mathbb{Z}$

Assume n is odd.

.

.

Proof to be filled in

.

.

So $2n^2 + 3n + 4$ is odd.

Hence if n is odd then $2n^2 + 3n + 4$ is odd.

Therefore $\forall n \in \mathbb{Z}$, if n is odd then $2n^2 + 3n + 4$ is odd

But as noted earlier, when proving a universally quantified implication, the combined proof principle, Proof Principle 3, is almost always used. Therefore Steps 2 and 3 would ordinarily be combined (as they were in the actual proof) to get the following diagram.

Steps 2 and 3 combined using Proof Principle 3

Assume $n \in \mathbb{Z}$ and that n is odd

.

.

Proof to be filled in

.

.

Hence $2n^2 + 3n + 4$ is odd.

Therefore $\forall n \in \mathbb{Z}$, if n is odd then $2n^2 + 3n + 4$ is odd

Continuing from the previous diagram, since the definition of "odd" is an active hypothesis we may use it at any point in a proof. We use it to rewrite the statement "n is odd" and the statement "$2n^2 + 3n_4$ is odd". This gives us a first and last line of the part of the proof to be filled in.

Step 4

Assume $n \in \mathbb{Z}$ and that n is odd

Then $n = 2k + 1$ for some integer k.

.

.

Proof to be filled in

.

.

We have $2n^2 + 3n + 4 = 2i + 1$ where i is an integer.

Hence $2n^2 + 3n + 4$ is odd.

Therefore $\forall n \in \mathbb{Z}$, if n is odd then $2n^2 + 3n + 4$ is odd

And now since the last line of the proof to be filled in is an equality we use Proof Principle 4 by beginning with the left hand side of the equality to be proved, applying legal operations and obtaining the right hand side.

Step 5
Assume $n \in \mathbb{Z}$ and that n is odd Then $n = 2k + 1$ for some integer k. So $2n^2 + 3n + 4 =$ $2(2k + 1)^2 + 3(2k + 1) + 4 =$ $2(2k + 1)^2 + 6k + 3 + 4 =$ $2(2k + 1)^2 + 6k + 6 + 1 =$ $2[(2k + 1)^2 + 3k + 3] + 1.$ So, letting $i = (2k + 1)^2 + 3k + 3$ We have $2n^2 + 3n + 4 = 2i + 1$ where i is an integer. Hence $2n^2 + 3n + 4$ is odd.
Therefore $\forall n \in \mathbb{Z}$, if n is odd then $2n^2 + 3n + 4$ is odd

A working mathematician may not write down all these steps while constructing a proof but the steps illustrate the thought process that he or she uses to devise the proof.

Here's another example proof.

Theorem. *$\forall n \in \mathbb{Z}$, $5n^2 + 3n + 1$ is odd.*

Proof. Assume $n \in \mathbb{Z}$, then by Theorem 2.2 either n is even or n is odd.

Case 1. n is even. In this case $n = 2k$ for some integer k so that $5n^2+3n+1 = 5(2k)^2 + 3(2k) + 1 = 20k^2 + 6k + 1 = 2(10k^2 + 3k) + 1$. Letting $j = 10k^2 + 3k$ we see that in this case that $5n^2 + 3n + 1 = 2j + 1$ where j is an integer. Hence $5n^2 + 3n + 1$ is odd.

Case 2. n is odd. In this case $n = 2i + 1$ for some integer i. Hence $5n^2 + 3n + 1 = 5(2i + 1)^2 + 3(2i + 1) + 1 = 5(4i^2 + 4i + 1) + 6i + 3 + 1 = 2(10i^2 + 13i + 4) + 1 = 2r + 1$ where $r = 10i^2 + 13i + 4$ is an integer. Hence $5n^2 + 3n + 1$ is odd.

Since we have proved that $5n^2 + 3n + 1$ is odd in either possible case $5n^2 + 3n + 1$ must be odd. □

Notes: Using the Proof Principle 1 above we began the proof by assuming $n \in \mathbb{Z}$. For the remainder of the proof n represents a fixed but unspecified integer. We also use a method of proof called *Proof by Cases.*

Proof Principle 7. Proof by cases. If P and Q are two statements for which you know "P or Q" is true and you want to prove the statement R, it suffices to do two things: First assume P and prove R; second (eliminate P as an assumption and)assume Q and prove R. □

The two parts are usually referred to as case 1 and case 2, although it's not necessary to do that, especially if the proof for both parts is short. For example the proof of the theorem might be written like this:

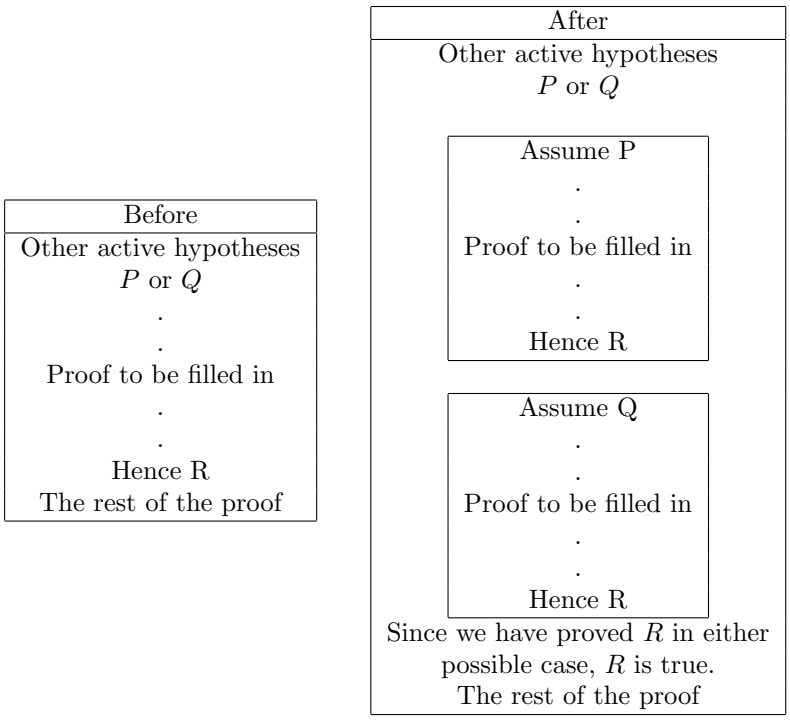
Proof. Assume $n \in \mathbb{Z}$, then by an earlier theorem either n is even or n is odd.

If n is even then $n = 2k$ for some integer k so that $5n^2 + 3n + 1 = 5(2k)^2 + 3(2k) + 1 = 20k^2 + 6k + 1 = 2(10k^2 + 3k) + 1$. Letting $j = 10k^2 + 3k$ we see that in this case that $5n^2 + 3n + 1 = 2j + 1$ where j is an integer. Hence $5n^2 + 3n + 1$ is odd.

On the other hand if n is odd then $n = 2i + 1$ for some integer i. Hence $5n^2 + 3n + 1 = 5(2i + 1)^2 + 3(2i + 1) + 1 = 5(4i^2 + 4i + 1) + 6i + 3 + 1 = 2(10i^2 + 13i + 4) + 1 = 2r + 1$ where $r = 10i^2 + 13i + 4$ is an integer. Hence $5n^2 + 3n + 1$ is odd.

Since we have proved that $5n^2 + 3n + 1$ is odd in either possible case $5n^2 + 3n + 1$ must be odd. □

The before and after diagrams for proof by cases look like this:



2.4 More proofs and proof principles

In this section we will give two more proofs which will use some new proof principles. Following the proofs we discuss the principles involved. Before starting the proofs we begin with an assumption about the natural numbers which we will assume throughout the book without proof.

Axiom 1. The well ordering property of $\mathbb{N}$. If S is any non-empty subset of the natural numbers then S has a least element, that is $\exists n \in S$ such that $\forall m \in S$, $n \leq m$.

Note that there are two important requirements for n to be the least element of S. The first is that n is in S and the second is that n is less than or equal to everything in S. Note also that the real numbers $\mathbb{R}$ do not have this property. For example the interval $(2, 7]$ is a non-empty subset of $\mathbb{R}$ with no least element.

We will use the well ordering theorem to prove

Theorem 2.4. *Every natural number is either even or odd.*

Proof. The proof will use the well ordering property of the set of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ together with the fact that if k is any natural number not equal to 0 then $k-1$ is a natural number. We will prove the theorem by assuming that it is false and showing that this assumption leads to a contradiction and is therefore impossible.

Assume the theorem is false. Then there is a natural number which is neither even nor odd and so the set S consisting of those natural numbers which are neither even nor odd is not empty. By the well ordering property of $\mathbb{N}$, S has a least element which we will call n_0. We first note that $n_0 \neq 0$ because $0 = 2 \cdot 0$ and is therefore even and not in S. Since $n_0 \neq 0$, we know that $n_0 - 1$ is a natural number and further $n_0 - 1$ is not in S since n_0 is the least element of S and $n_0 - 1 < n_0$. Since $n_0 - 1$ is not in S it is either even or odd. We now consider two cases.

Case 1. If $n_0 - 1$ is even then for some integer j, $n_0 - 1 = 2j$. It follows that $n_0 = 2j + 1$ and therefore n_0 is odd. This contradicts our assumption that n_0 is neither even nor odd.

Case 2. If $n_0 - 1$ is odd, then for some integer i, $n_0 - 1 = 2i + 1$. It follows that $n_0 = 2i + 2 = 2(i + 2) = 2k$ where k is the integer $i + 2$. Therefore n_0 is even. This also contradicts our assumption that n_0 is neither even nor odd.

Since we have arrived at a contradiction in either possible case it is impossible that there is an integer which is neither even nor odd. Therefore the theorem is proved. □

Theorem 2.5. *Every integer is either even or odd.*

Proof. Recall that the set of integers $\mathbb{Z}$ is the set $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. In symbolic form the theorem is "$\forall n \in \mathbb{Z}$, n is even or n is odd." We will therefore be using Proof Principle 1.

Assume $n \in \mathbb{Z}$, then either n is a natural number or $-n$ is a natural number. (This is one of those elementary facts about integers that we are assuming.)

Case 1. If n is a natural number then we know by Theorem 2.4 that n is either even or odd.

Case 2. If $-n$ is a natural number using Theorem 2.4 gives us that $-n$ is either even or odd. If $-n$ is even then $-n = 2j$ for some integer j so $n = 2(-j)$ so n is even since $-j$ is an integer if j is. On the other hand if $-n$ is odd then $-n = 2k+1$ for some integer k. It follows that $n = -2k-1 = 2(-k-1)+1 = 2m+1$ where m is the integer $m = -k - 1$. So n is odd. So in either case ($-n$ even or $-n$ odd) we find that n is either even or odd. This competes the proof in case 2. □

The main tool used in the proof of Theorem 2.4 is the Proof Principle called *proof by contradiction.*

Proof Principle 8. Proof by Contradiction. To prove a statement P by contradiction, assume that P is false, that is, add the negation of P to the active hypotheses and then prove any contradictory statement. □

The idea is that if the assumption that P is false leads to a contradiction then P cannot be false. Also note the following:

- The assumption that P is false is usually introduced with a sentence or two indicating that you are starting a proof by contradiction. For example, "We will prove P by contradiction. We assume therefore that P is false." or "Towards a proof by contradiction, assume that P is false."
- The contradictory statement may be a statement known to be false, for example the statement $0 = 1$. Or it may contradict one of the active hypotheses. We will see how this works in several examples.
- Note that the assumption "not P" is only an active hypothesis until you have proved a contradiction. After a contradiction has been reached you conclude that P is true and the assumption "not P" is no longer active.
- Proof by contradiction works especially well for proving negative statements since assuming that such a statement is false gives us something positive to work with.
- If P is the statement "If R then S", then the assumption "not P" is equivalent to "R and not S". (see Table 1.1 in chapter 1.)
- If from the assumption "not S" you can prove "not R", that is if you can prove "If not S then not R", then you will have shown that "R and not S" leads to a contradiction. It follows from the previous item that you will have proved "If R then S." The sentence "If not S then not R" is known as the contrapositive of the sentence "If R then S". We formulate this as a proof principle below.

Proof Principle 9. Proving the Contrapositive. In order to prove "If R then S" it suffices to prove "If not S then not R". □

Here are some more methods for doing mathematical proofs. Many of the are obvious consequences of the meanings of the connectives.

Proof Principle 10. Proving "and" Statements. To prove "P and Q" where P and Q are statements, prove P and prove Q. □

Proof Principle 11. Proving "P or Q". In order to prove a statement of the form "P or Q" it suffices to assume that one of the two sentences P or Q is false and, using this assumption, prove the other is true. Therefore there are two possibilities

1. **Add $\neg P$ to the active hypotheses and prove Q.**

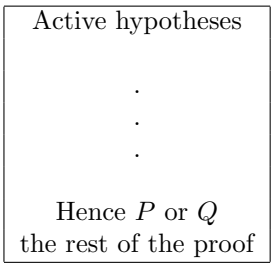
2. **Add $\neg Q$ to the active hypotheses and prove P.**

   Note that you only have to do one of these.

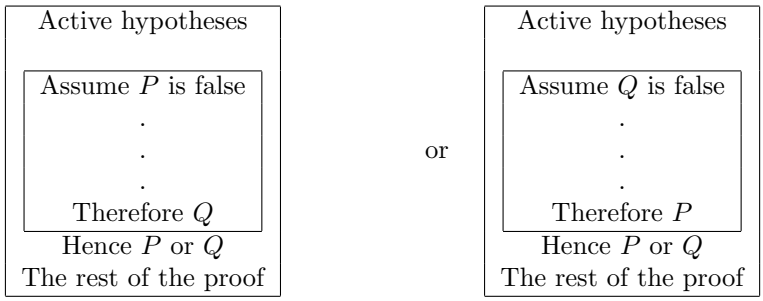
□

In the first case above $\neg P$ will be an active hypothesis only until Q is proved. At that time $\neg P$ is removed from the list of active hypotheses and "P or Q" has been proved. Similarly, in the second case $\neg Q$ will only be an active hypothesis until you prove P.

The two possible procedures described above could be diagramed as follows: The "before" diagram would be



and after using the proof principle the diagram would be one of



In the first case we might consider preceding the proof in the box with a line like "We will prove P or Q by assuming P is false and proving Q." or in the second case by a line like "We will prove P or Q by assuming Q is false and proving P."

Examples of this proof principle will occur in later chapters.

Proof Principle 12. Proofs of Existence Statements. In order to prove a statement of the form $(\exists x \in S)(P(x))$ there are ordinarily two steps the first of which will usually not appear in the finished proof

1. **Using the assumptions, you must identify, define or construct the object you want to use for x. This will ordinarily require some scratch work which will not appear in the finished proof.**

2. The first line of the proof (of $\exists x \in S$ such that $P(x)$) will be a statement of the form "Let x_0 be ..." or "define x_0 by ..." or "let $x_0 = \ldots$" or some similar statement where x_0 is a new active parameter and ... is a description of x_0 in terms of the currently active parameters and which may use the active hypotheses. The statement "$x_0 = \ldots$" is added to the active hypotheses. The word "Let" or "Define" is used to indicate that a new free variable or parameter is being introduced. The last line of the proof will be "$x_0 \in S$ and $P(x_0)$". The parameter x_0 and the assumption $x_0 = \ldots$ are only active for the proof of "$x_0 \in S$ and $P(x_0)$".

□

The situation before using this proof principle might be diagramed as follows:

Active hypotheses

.
.

Proof to be filled in

.
.

Hence $\exists x \in S$ such that $P(x)$.
The rest of the proof

After using proof principle 12 the diagram would be

Active hypotheses

Let $x_0 = \ldots$
.
.
Proof to be filled in
.
.
So $x_0 \in S$ and $P(x_0)$

Hence $\exists x \in S$ such that $P(x)$.
The rest of the proof

Here the parameter x_0 and the assumption $x_0 = \ldots$ are only active inside the inner box.

We illustrate the use of Proof Principle 12 with the following theorem.

Theorem 2.6. *For every $y \in \mathbb{R}$ if $y \neq 3$ then $\exists x \in \mathbb{R}$ such that* $\dfrac{3x-1}{x-6} = y$.

In the following proof we will put comments inside square brackets. These are explanations of what we're doing, not part of the actual proof.

Proof. [Since this is a universally quantified "if ... then" we begin with Proof Principle 3.]
Assume that $y \in \mathbb{R}$ and that $y \neq 3$. We need to show that $\exists x \in \mathbb{R}$ such that $\dfrac{3x-1}{x-6} = y$.
[We now carry out step 1 of Proof Principle 12, namely constructing an x that will work. We want a real number x for which $\dfrac{3x-1}{x-6} = y$. Since one of the conditions which x must satisfy is an equation we use that to try and find x. That is, we are going to solve the equation $\dfrac{3x-1}{x-6} = y$ for x. Multiplying both sides by $(x-6)$ gives us $3x-1 = xy-6y$. Collecting the terms involving x on the right side we obtain $3x - xy = 1 - 6y$. Finally, factoring out x on the left and dividing both sides by $(3-y)$ we end with $x = \frac{1-6y}{3-y}$. This completes step 1 (which will not appear in the proof). Now step 2:]
Let $x = \frac{1-6y}{3-y}$. Then, since $y \neq 3$, $x \in \mathbb{R}$. Further

$$\frac{3x-1}{x-6} = \frac{3\left(\frac{1-6y}{3-y}\right)-1}{\left(\frac{1-6y}{3-y}\right)-6} = \frac{3(1-6y)-(3-y)}{1-6y-6(3-y)} = \frac{-17y}{-17} = y$$

□

Note that the proof consisted (essentially) of two parts: Solving the equation $\frac{3x-1}{x-6} = y$ and then checking the solution. The process of solving the equation was the scratch work and did not appear in the proof. The second part, checking the solution, was the proof that there was a solution.[2]

To summarize: In order to prove $\exists x \in S$ such that $P(x)$, give a description of a new parameter (say x_0) and prove that x_0 works. In other words prove that $x_0 \in S$ and $P(x_0)$.

As is the case with our proof principle for proving universally quantified statements, the parameter (or free variable) that is introduced is frequently the same symbol that is used for the bound variable.

Proof Principle 13. Proving "There is At Most One." Assume that $P(x)$ is a sentence with one free variable x. In order to prove that there is at most one object x for which $P(x)$ is true it suffices to assume that x_1 and x_2 are objects such that both $P(x_1)$ and $P(x_2)$ are true and based on this assumption prove $x_1 = x_2$. □

The usual way of introducing the new parameters x_1 and x_2 and adding $P(x_1)$ and $P(x_2)$ to the active hypotheses is to say "assume $P(x_1)$ and $P(x_2)$."

[2] In general the process of solving an equation is not a proof that the equation has a solution. For example when we solve $\sqrt{x-1} - 1 = -\sqrt{x-4}$, we assume the equation is true and carry out legal operations beginning with squaring both sides. The squaring gives $(x-1) - 2\sqrt{x-1} + 1 = x - 4$. Simplifying this equation results in $\sqrt{x-1} = 2$ then squaring both sides and adding one gives us $x = 5$. We have assumed $\sqrt{x-1} - 1 = -\sqrt{x-4}$ and proved that $x = 5$. In other words, we have proved the statement "If $\sqrt{x-1} - 1 = -\sqrt{x-4}$ then $x = 5$." To prove that $x = 5$ is a solution we would have to assume $x = 5$ and then argue that $\sqrt{x-1} - 1 = -\sqrt{x-4}$, which turns out to be false.

Note that following the procedure described in Proof Principle 13 does not prove that there is an object x for which $P(x)$ is true; it only proves that there cannot be more than one such object.

Proof Principle 14. Proofs of "There exists a unique ..." Assume that $P(x)$ is a sentence with free variable x. In order to prove "There exists a unique x such that $P(x)$" prove "$\exists x$ such that $P(x)$" and "There is at most one x such that (x)". (see Proof Principles 12 and 13). □

2.5 Exercises

2.1. For each of the following pairs a and b find integers q and r so that $a = qb+r$ and $0 \leq r < b$.

(a) $a = 752, b = 25$

(b) $a = 417, b = 11$

(c) $a = -231, b = 5$

(d) $a = 47, b = 48$

(e) $a = -47, b = 48$

(f) $a = 1000, b = 50$

2.2. Prove $\forall n \in \mathbb{Z}$, if n is odd then $n^2 + 3n + 4$ is even.

2.3. Prove $\forall n \in \mathbb{Z}$, if n is odd then $6n^2 + 5n + 4$ is odd.

2.4. Prove $\forall n \in \mathbb{Z}$, if n is even then $25n^2 + 20n + 3$ is odd.

2.5. Prove $\forall n \in \mathbb{Z}$, $9n^2 + 9n + 2$ is even.

In exercises 2.6 to 2.12 you may use any of the facts about inequalities that appear in the paragraph on inequalities of Subsection 2.2.1.

Also for each exercise from 2.6 to 2.12 you may use the results of any previous exercise.

2.6. Prove $\forall x \in \mathbb{R}^+$, (if $1 < x$ then $x < x^2$) and (if $x < 1$ then $x^2 < x$).

2.7. Prove $\forall x, y \in \mathbb{R}^+$, (if $x < y$ then $x^2 < y^2$) and (if $x \leq y$ then $x^2 \leq y^2$).

2.8. Prove $\forall x, y \in \mathbb{R}^+$, if $x < y$ then $\sqrt{x} < \sqrt{y}$. (Hint: Prove this by contradiction.)

2.9. Prove $\sqrt{\frac{9}{2}} - 2 > 0$. (Remember, you cannot begin by assuming $\sqrt{\frac{9}{2}} - 2 > 0$.)

2.10. Prove $4 < \sqrt{\frac{9}{2}} + \sqrt{\frac{7}{2}}$.

2.11. Prove $\forall \epsilon \in \mathbb{R}^+$ if $\epsilon < 4$ then $\sqrt{4+\epsilon} - 2 < 2 - \sqrt{4-\epsilon}$.

2.12. Prove $\forall \epsilon \in \mathbb{R}^+$, if $\epsilon < 4$ and $|x-2| < \sqrt{4+\epsilon} - 2$ then $|x^2 - 4| < \epsilon$.

2.13. Prove: For all sets A, B and C, $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

2.14. Prove: For all sets A, B and C, $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

2.15. Prove: For all sets A, B and C, $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

2.16. Prove that for all sets A and B, if $A \cap B = \emptyset$, then $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$.

2.17. Prove $\forall n \in \mathbb{N}$, if $n > 2$ then $\frac{1}{(n+1)^2} < \frac{1}{10}$.

2.18. Prove $\forall n \in \mathbb{N}$, if $n > 99$ then $\frac{1}{\sqrt{n+1}} < \frac{1}{10}$.

2.19. Prove: For all positive real numbers ϵ, if $\epsilon < 1$ then $\forall n \in \mathbb{N}$, if $n > \frac{1}{\sqrt{\epsilon}} - 1$ then $\frac{1}{(n+1)^2} < \epsilon$.

2.20. (a) Why is the following not a proof of $\sin^2 x \cot^2 x + \sin^2 x = 1$?

$$\begin{aligned} \sin^2 x \cot^2 x + \sin^2 x &= 1 \\ \sin^2 x(\cot^2 x + 1) &= 1 \\ \sin^2 x(\csc^2 x) &= 1 \\ \frac{\sin^2 x}{\sin^2 x} &= 1 \\ 1 &= 1 \end{aligned}$$

(b) Give a valid proof that $\sin^2 x \cot^2 x + \sin^2 x = 1$ for all x for which the left hand side is defined.

2.21. Why is the following not a proof of $\forall x \in \mathbb{R}$, if $x > 2$ then $\dfrac{1}{(x+1)^2} < \dfrac{1}{10}$?

Proof. From $\dfrac{1}{(x+1)^2} < \dfrac{1}{10}$, multiplying both sides by $10(x+1)^2$, we can conclude that $10 < (x+1)^2$. Taking the square root of both sides of this inequality give $\sqrt{10} < x + 1$ and therefore $\sqrt{10} - 1 < x$. Calculating $\sqrt{10} - 1$ gives a number larger than 2.1 therefore we have $2 < 2.1 < \sqrt{10} - 1 < x$. Hence $2 < x$. □

2.22. Prove the identity $\tan^3 \theta = \dfrac{\sec \theta}{\csc \theta} \left(\dfrac{1 - \cos^2 \theta}{1 - \sin^2 \theta} \right)$.

2.23. Prove that the following is an identity: $\dfrac{1}{\csc \theta} - \dfrac{1}{\csc^3 \theta} = \cos^2 \theta \sin \theta$.

2.24. Prove that for any real number t, $\left(\frac{t(t+1)}{2}\right)^2 + (t+1)^3 = \left(\frac{(t+1)[(t+1)+1]}{2}\right)^2$.

2.25. Prove: If x is a real number then $\frac{1}{2}(x+1)\,(3(x+1)-1) = \frac{1}{2}x(3x-1) + (3(x+1)-2))$.

2.26. Prove: For every real number y, $4(y+1)^2 - (y+1) = (4y^2 - y) + (8(y+1)-5)$.

2.27. Prove: $\forall n \in \mathbb{N}$, $2^{n+2} - 2 = 2^{n+1} - 2 + 2^{n+1}$.

2.28. Prove: For $n \in \mathbb{N}$ the following is an identity,

$$\frac{(2(n+1))!}{(n+1)!2^{n+1}} = \left(\frac{(2n)!}{n!2^n}\right)(2(n+1)-1).$$

2.29. For all real numbers a, n and r, if $r \neq 1$ then $\frac{a\left(r^{n+1}-1\right)}{r-1} = \frac{a\left(r^n-1\right)}{r-1} + ar^n$.

2.30. Prove: If a, b and c are integers and a divides b and a divides c, then a divides $b+c$. (Use the definition *a divides b* if and only if $\exists k \in \mathbb{Z}$ such that $b = ka$.)

2.31. Prove: If a, b and c are integers and a divides both b and c then a^2 divides bc.

2.32. Assume A, B and C are sets. Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. (This is sometimes called the distributive law of $\cap$ over $\cup$.)

2.33. Assume A, B and C are sets. Prove that $(A \setminus B) \cap (A \setminus C) = (A \setminus (B \cup C))$. (One of DeMorgan's laws.)

2.34. Assume A, B and C are sets. Prove that $(A \setminus B) \cup (A \setminus C) = (A \setminus (B \cap C))$. (The other of DeMorgan's laws.)

2.35. Prove by contradiction: $\forall y \in \mathbb{R}$, $\frac{3y-2}{4y-6} \neq \frac{3}{4}$.

2.36. Prove by contradiction: $\forall y \in \mathbb{R}$, $\frac{4y-2}{y-6} \neq 4$.

Part II

More Specialized Techniques

Chapter 3

Elementary Set Theory

3.1 Notation and Terminology

We begin our discussion of set theory with some of the standard notation and terminology.

A *set* is a collection of objects. The words "collection", "family" or "class" are sometimes used as synonyms for the word "set". If A is a set and x is one of the objects in A then we say x *is an element of* A and we write $x \in A$. If x is not one of the objects in A, that is, if x is not an element of A then we write $x \notin A$. There are two standard ways of specifying a set. The first works well for small finite sets and is known as the *listing method*. To specify a set by the listing method list its elements between braces, separated by commas. For example, $\{1, a, 3, 10\}$ is the set whose elements are 1, a, 3, and 10. If we denote this set by A both $1 \in A$ and $2 \notin A$ are true statements.

Specifying a very large set by the listing method may be impractical and specifying an infinite set this way is impossible. For these two kinds of sets there are two extensions of the listing method which are sometimes used. Here are two examples:

$$\{1, 2, 3, \ldots, 107\}$$

In this example the set that is specified is the set whose elements are the positive integers from 1 through 107. The three dots (... called the ellipsis) may be read "continue the pattern established until you reach". The second example is

$$\{2, 4, 6, \ldots\}$$

This denotes the infinite set consisting of the even, positive integers. The three dots mean "continue the pattern established forever".

With either of the two extensions of the listing method described above there is a potential for ambiguity if the pattern is not clear. For this reason it may be preferable to use the second standard method of specifying a set called the *rule method* or sometimes the *standard rule method*. The rule method uses braces, a variable (we'll use x in the examples given here) and a sentence with

free variable x. Suppose $P(x)$ is such a sentence, then the set whose elements are the objects a for which $P(x)$ is true when x is replaced by a is denoted:

$$\{x : P(x)\} \text{ or}$$
$$\{x \mid P(x)\}$$

For example the set of even positive integers could be written as

$$\{n : \text{ For some positive integer } k, n = 2k\}.$$

Note that the formula $P(x)$ gives the criteria for membership in the set $\{x : P(x)\}$ and that the rule method could be described by

3.1. If $P(x)$ is a sentence with free variable x and a is an expression representing an object then the statements "$P(a)$" and "$a \in \{x : P(x)\}$" are equivalent.

For example the sentence "$j \in \{n : \text{ For some positive integer } k, n = 2k\}$" is equivalent to the sentence "For some positive integer $k, j = 2k$".

We think of "$\{x : P(x)\}$" as a defined expression and when we use 3.1 to replace "$a \in \{x : P(x)\}$" with "$P(a)$" in a proof we are using the fact that definitions are always part of our active hypotheses[1] and may therefore be used at any point in a proof.

There is a variation of the rule method which we shall call *the rule and function method* for specifying a set. If $P(x)$ is a sentence with free variable x, and f is a function which is defined for all x such that $P(x)$ is true, then

$$\{f(x) : P(x)\}$$

is the set of all objects y such that for some x,

$$P(x) \text{ is true and } y = f(x).$$

To say it slightly differently, a set $\{f(x) : P(x)\}$ described by the rule and function method can be described by the standard rule method as follows:

$$\{f(x) : P(x)\} = \{y : \exists x \text{ such that } P(x) \text{ and } y = f(x)\}. \tag{3.1}$$

There is a more general version of the rule and function method in which the sentence P may have more than one free variable: If $P(x_1, x_2, \ldots, x_n)$ is a sentence with variables $x_1, x_2, \ldots, x_n$ and f is an n-place function which is defined for all n-tuples for which $P(x_1, x_2, \ldots, x_n)$ is true, then

$$\{f(x_1, x_2, \ldots, x_n) : P(x_1, x_2, \ldots, x_n)\}.$$

is the set of all objects y such that for some n-tuple $(x_1, x_2, \ldots, x_n)$,

$$P(x_1, x_2, \ldots, x_n) \text{ is true and } y = f(x_1, x_2, \ldots, x_n).$$

[1] Active hypotheses are described in Subsection 2.2.2.

That is, the set $\{f(x_1, x_2, \ldots, x_n) : P(x_1, x_2, \ldots, x_n)\}$ can be denoted using the standard rule method by

$$\{y : \text{there are objects } x_1, x_2, \ldots, x_n \text{ such that } P(x_1, x_2, \ldots, x_n) \text{ and } y = f(x_1, x_2, \ldots, x_n)\}$$

Looking back at equation (refruleandfunctiontorule) and using principle 3.1 we see that we can handle sets $\{f(x) : P(x)\}$ described by the rule and function method when they occur in proofs by a principle similar to 3.1, namely

3.2. If $P(x)$ is a sentence with free variable x and f is a function defined for all x such that $P(x)$ and if a is an expression representing an object then the statements "$a \in \{f(x) : P(x)\}$" and "$\exists x$ such that $P(x)$ and $a = f(x)$" are equivalent.

There is one more variation of the rule method: If A is a set and $P(x)$ is a sentence with variable x, then $\{x \in A : P(x)\}$ denotes the set of all elements of A for which $P(x)$ is true. In other words, translating to the standard rule method

$$\{x \in A : P(x)\} = \{x : x \in A \text{ and } P(x)\}.$$

This variation of the rule method could be written as

3.3. If $P(x)$ is a sentence with free variable x, A is a set and a is an expression representing an object then the statements "$a \in A$ and $P(a)$" and "$a \in \{x \in A : P(x)\}$" are equivalent.

which provides a way of dealing with sets $\{x \in A : P(x)\}$ when they occur in proofs.

Some sets of numbers which were mentioned in Chapter 1 and the standard symbols for these sets are given below.

$\mathbb{N}$ denotes the set of natural numbers $\{0, 1, 2, 3, \ldots\}$

$\mathbb{Z}$ is the set of integers $\{\ldots -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}$ is the set of rational numbers $\{\frac{p}{q} : p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0\}$

$\mathbb{R}$ is the set of real numbers.

We will also use $\mathbb{Z}^+$, $\mathbb{Q}^+$ and $\mathbb{R}^+$ for the set of positive integers, the set of positive rational numbers and the set of positive real numbers respectively.

One other standard symbol is $\emptyset$ for the set with no elements. We could describe $\emptyset$ by the listing method: $\emptyset = \{\}$.

3.2 The Principle of Extensionality

One of the basic principles of set theory is

Axiom 2. (The Axiom of Extensionality) If A and B are sets for which the following are true

1. Every element of A is also an element of B
2. Every element of B is also an element of A

then $A = B$.

The sentences appearing in 1 and 2 occur so often that there is a standard abbreviation for the idea expressed there.

Definition 3.4. $A \subseteq B$ means A and B are sets and every element of A is also an element of B. (Or in more symbolic form "A and B are sets and $\forall x \in A$, $x \in B$.")

Since we will frequently be interested in showing that A is not a subset of B (denoted $A \nsubseteq B$) we note that

$$A \nsubseteq B \text{ if and only if } \exists x \in A \text{ such that } x \notin B. \tag{3.2}$$

This follows from our discussion of how to negate a statement beginning with $\forall$ in section 1.6 .

Using the abbreviation $\subseteq$, the principle of extensionality could be stated

If A and B are sets and $A \subseteq B$ and $B \subseteq A$ then $A = B$.

Note that the converse of the principle of extensionality (if $A = B$ then $A \subseteq B$ and $B \subseteq A$) is a consequence of the substitution property of equality. Also note these three consequences of the principle of extensionality:

- If A and B are sets then $A \neq B$ if and only if at least one of the following happens
  1. $\exists x \in A$ such that $x \notin B$ or
  2. $\exists x \in B$ such that $x \notin A$.

  This is a consequence of (3.2) above and our discussion of how to negate an "and" statement in section 1.6.

- When a set is described by the listing method its elements may be listed in any order and any number of times. (Although, it is best to avoid listing an element more than once.) For example, the two sets $\{1, 3, 5, 7\}$ and $\{3, 1, 5, 3, 7\}$ are equal by the principle of extensionality.

- To prove that two sets A and B are equal it is sufficient to prove that $A \subseteq B$ and $B \subseteq A$. To prove that $A \subseteq B$ you assume that x is an element of A and using that assumption (and nothing else about x) prove that x is an element of B. Similarly for proving that $B \subseteq A$. (This is a consequence of Proof Principle 1 discussed in chapter 2.)

For example, we could prove that $\{2,-3\} = \{x \in \mathbb{R} : x^2 + x - 6 = 0\}$ in the following way: Assume first that $x \in \{2,-3\}$, then $x = 2$ or $x = -3$. In either case $x \in \mathbb{R}$ and $x^2 + x - 6 = 0$ hence $x \in \{x \in \mathbb{R} : x^2 + x - 6 = 0\}$. Now assume that $x \in \{x \in \mathbb{R} : x^2 + x - 6 = 0\}$. Then $x \in \mathbb{R}$ and $x^2 + x - 6 = 0$. It follows that $(x+3)(x-2) = 0$ and hence that $x+3 = 0$ or $x-2 = 0$. Therefore $x = -3$ or $x = 2$ and in either case $x \in \{2,-3\}$.

3.3 Operations on Sets

Suppose that A and B are sets (We will use the sets $A = \{1,2,3,4\}$ and $B = \{1,3,5\}$ as our first examples.) then $A \cup B$, $A \cap B$ and $A \setminus B$ are three new sets constructed from A and B and described by

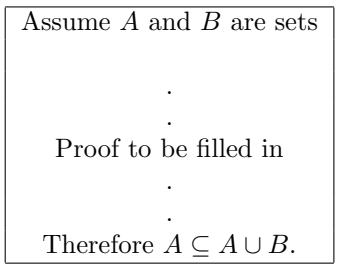
Definition 3.5. $A \cup B = \{x : x \in A \text{ or } x \in B\}$, $A \cap B = \{x : x \in A \text{ and } x \in B\}$ and $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$

The operation $\cup$ is called *union* and "$A \cup B$" is read "A union B", similarly $\cap$ is called *intersection* and "$A \cap B$" is read "A intersection B". The operation $\setminus$ is called *set difference* and "$A \setminus B$" is read "A set difference B" or "A minus B" and is sometimes denoted by $A - B$.

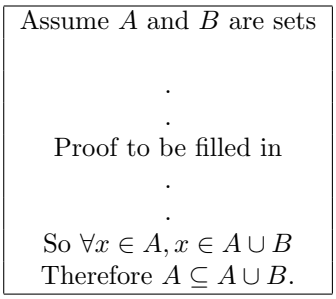
In the example $A \cup B = \{1,2,3,4,5\}$ (Note that the word "or" is used in the inclusive sense meaning *either one or the other or both.*) $A \cap B = \{1,3\}$ and $A \setminus B = \{2,4\}$.

Here are some example proofs of properties of the these three set operations. For the first two examples we picture the process used to construct the proof using diagrams.

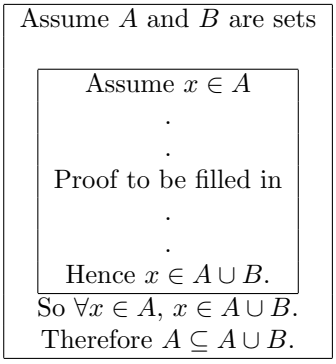
Example 3.6. Prove: For all sets A and B, $A \subseteq A \cup B$. Using Proof Principle 1 we could begin a proof whose first line is "Assume A and B are sets." and whose last line is "Therefore $A \subseteq A \cup B$." At this stage of the proof our diagram would be



Using the definition of $\subseteq$ and the fact that definitions are always active hypotheses and may be used at any point in a proof, the second to last line of the proof will probably be "$\forall x \in A$, $x \in A \cup B$". This gives us the diagram



Using Proof Principle 1 the proof of this second to last line will probably begin with "Assume $x \in A$." and end with "hence $x \in A \cup B$." If we make these additions to the diagram we obtain



And now the "proof to be filled in" would consist of a single line: "So $x \in A$ or $x \in B$." The final version of the proof would appear in paragraph form, for example:

Proof. Assume that A and B are sets and that $x \in A$. Then $x \in A$ or $x \in B$ so $x \in A \cup B$. This shows that $\forall x \in A$, $x \in A \cup B$. Therefore $A \subseteq A \cup B$. □

Example 3.7. Suppose we want to prove that for all sets A, B and C, $(A \setminus B) \cap C \subseteq (A \cap C) \setminus (B \cap C)$. We begin with a single diagram which displays the thinking that might have gone into the construction of the proof.

	Active Hypotheses		Desired Conclusion	
stage 1	(1) Assume that A, B and C are sets	A	Show that $(A - B) \cap C \subseteq (A \cap C) - (B \cap C)$.	E
stage 2	(1) A, B and C are sets (2) $x \in (A - B) \cap C$	B	$x \in (A \cap C) - (B \cap C)$	F
stage 3	(1) A, B and C are sets (2) $x \in (A - B) \cap C$ (3) $x \in (A - B)$ and $x \in C$	C	$x \in (A \cap C)$ and $x \notin (B \cap C)$	G
stage 4	(1) A, B and C are sets (2) $x \in (A - B) \cap C$ (3) $x \in (A - B)$ and $x \in C$ (4) $x \in A$ and $x \notin B$ and $x \in C$	D		

Each stage in the preliminary work is represented by a row in the table. In the left hand column are the active hypotheses that are added at each stage and in the right had column is the new conclusion.

The final version of the proof will (usually) proceed from A to E (A to B to C to D to G to F to E) therefore everything in the "Active Hypotheses" column must either be an assumption which is justified by some method of proof or follow from things above it. Everything in the "Desired Conclusion" column must follow from the thing below it.

The active hypotheses tend to increase in number while at any given point in the preliminary work "what you want to show" will usually be the last sentence in the "Desired Conclusion" column.

Our usual method for showing the thinking process is to give a sequence of diagrams illustrating the stages in the process. The result would be:

stage 1	Assume A, B and C are sets	active hypothesis
stage 1	Therefore $(A - B) \cap C \subseteq (A \cap C) - (B \cap C)$	to be shown

Stage 1

stage 1	Assume A, B and C are sets	active hypothesis
stage 2	Assume that $x \in (A - B) \cap C$	active hypothesis
stage 2	So $x \in (A \cap C) - (B \cap C)$	to be shown
stage 1	Therefore $(A - B) \cap C \subseteq (A \cap C) - (B \cap C)$	to be shown

Stage 2

stage 1	Assume A, B and C are sets	active hypothesis
stage 2	Assume that $x \in (A - B) \cap C$	active hypothesis
stage 3	Then $x \in A - B$ and $x \in C$	active hypothesis
stage 3	Hence $x \in (A \cap C)$ and $x \notin (B \cap C)$	to be shown
stage 2	So $x \in (A \cap C) - (B \cap C)$	to be shown
stage 1	Therefore $(A - B) \cap C \subseteq (A \cap C) - (B \cap C)$	to be shown

Stage 3

stage 1	Assume A, B and C are sets	active hypothesis
stage 2	Assume that $x \in (A - B) \cap C$	active hypothesis
stage 3	Then $x \in A - B$ and $x \in C$	active hypothesis
stage 4	So $x \in A$ and $x \notin B$ and $x \in C$	active hypothesis
stage 3	Hence $x \in (A \cap C)$ and $x \notin (B \cap C)$	to be shown
stage 2	So $x \in (A \cap C) - (B \cap C)$	to be shown
stage 1	Therefore $(A - B) \cap C \subseteq (A \cap C) - (B \cap C)$	to be shown

Stage 4

The table for the final stage, stage 4, shows the same linear structure as the first diagram but there is, in addition, the "box" structure which we have seen before and which indicates in which portion of the proof the hypotheses and parameters are active.

Once this preliminary work is done the proof might look like this

Proof. Assume A, B and C are sets and that $x \in (A - B) \cap C$. It follows that $x \in A - B$ and that $x \in C$. Therefore $x \in A$, $x \notin B$, and $x \in C$. It follows that $x \in A \cap C$ (since $x \in A$ and $x \in C$) and that $x \notin B \cap C$ (since $x \notin B$). Hence $x \in (A \cap C) - (A \cap B)$. It follows that $(A - B) \cap C \subseteq (A \cap C) - (A \cap B)$. □

Here are some elementary properties of the four set operations defined so far.

Theorem 3.8. *Assume that A, B and C are sets, then*

1. $A \cap B = B \cap A$.
2. $A \cup B = B \cup A$.
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
5. *If* $B \subseteq A$ *then* $B = A \cap B$.
6. *For all sets* X, *if* $X \subseteq A \setminus B$, *then* $X \subseteq A$ *and* $X \cap B = \emptyset$.

Proof. We will prove part 3. The proofs of some of the other parts are left for the exercises.

Assume that A, B and C are sets. We will show $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ using the principle of extensionality.

Assume first that $x \in A \cup (B \cap C)$ then either $x \in A$ or $x \in (B \cap C)$. In the first case x is in both $(A \cup B)$ and $(A \cup C)$ hence $x \in (A \cup B) \cap (A \cup C)$. Similarly, in the second case x is in both $(A \cup B)$ and $(A \cup C)$ hence $x \in (A \cup B) \cap (A \cup C)$.

Now assume that $x \in (A \cup B) \cap (A \cup C)$. Then $x \in (A \cup B)$ and $x \in (A \cup C)$. If $x \in A$, then $x \in A \cup (B \cap C)$. If $x \notin A$ then it follows from $x \in A \cup B$ that $x \in B$ and it follows from $x \in A \cup C$ that $x \in C$. Therefore if $x \notin A$, $x \in B \cap C$. In either of the two possible cases $x \in A \cup (B \cap C)$. □

Each part of the proof just given is a *proof by cases* (Proof Principle 7, discussed in detail in Chapter 2). As you will recall, the idea is that if P, Q and R are statements and you know "P or Q" and want to prove R it suffices to proof R from the assumption that P is true and then prove R for the assumption that Q is true. For example, in the first part of the proof of 3 we have assumed $x \in A \cup (B \cap C)$ from which we conclude that "$x \in A$ or $x \in (B \cap C)$". (This is the "P or Q.") Then we give a proof of $x \in (A \cup B) \cap (A \cup C)$ (this is R) from the assumption $x \in A$ and a proof of $x \in (A \cup B) \cap (A \cup C)$ from the assumption that $x \in (B \cap C)$.

There are two more operations on sets that we will encounter in later chapters. The first of these is the Cartesian product of sets.

Definition 3.9. If A and B are sets then the *Cartesian product* of A and B, denoted by $A \times B$, is the set $\{(a, b) : a \in A \text{ and } b \in B\}$ (where (a, b) denotes the ordered pair whose first component is a and whose second component is b).

At this point we will only say two things about ordered pairs. The first is that these are the ordered pairs that you used when you studied coordinates of points in a plane. The set of all ordered pairs $\mathbb{R} \times \mathbb{R}$ whose first and second components are real numbers is the set we use as coordinates for points in a plane. The second fact about ordered pairs is that if (a, b) and (c, d) are two equal ordered pairs, that is if $(a, b) = (c, d)$ then $a = c$ and $b = d$. [2]

[2] A similar statement for two element sets $\{a, b\}$ and $\{c, d\}$ is false. You cannot conclude that $a = b$ and $c = d$ from the fact that $\{a, b\} = \{c, d\}$. For example, $\{1, 2\} = \{2, 1\}$ by the extensionality principle.

The Cartesian product of two finite sets will be finite and can therefore be described by the listing method. For example,

$$\{1,3\} \times \{3,4,5\} = \{(1,3),(1,4),(1,5),(3,3),(3,4),(3,5)\}$$

As a preliminary to defining the last set operation of this chapter it should be said that it is important to think of a set as being an object different from any of its elements. In forming a set we have grouped certain objects together to form a new object. One helpful analogy in this regard is to think of a set as being a box containing its elements. This box containing elements is an object different from any of the objects in the box. With this picture in mind it is easy to see why, for most objects a, $a \neq \{a\}$. It is also easy to see that there is a set with no elements (corresponding to an empty box) which we denote by $\emptyset$ or $\{\}$. The empty set will be discussed further in section 3.4.

It will also frequently happen that we will consider sets whose elements are themselves sets. For example, we will look at sets like

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

This is a set with two elements $\{1,2,3\}$ and $\{2,4\}$ both of which happen to be sets. This provides another reason why it is important to think of a set as an object. To get a better idea of what is going on consider the following list of statements about sets, some of which are true and some of which are false.

Example 3.10. (a) $1 \in \{0,1,2,3\}$. This statement is true. The elements of a set specified by the listing method are the objects that occur in the list.

(b) $1 \subseteq \{0,1,2,3\}$. This is false. In order for $A \subseteq B$ to be true A and B must be sets (which 1 is not) and every element of A must also be an element of B.

(c) $\{1,2\} \in \{0,1,2,3\}$. False: The set on the right is described by the listing method and the objects occurring in the list are the numbers 0, 1, 2, and 3. The object $\{1,2\}$ is not one of these. However see the next example.

(d) $\{1,2\} \in \{0,2,\{1,2\}\}$. This is true. The set on the right is described by the listing method and the objects occurring in the list are the numbers 0 and 2 and the set $\{1,2\}$. These three objects are therefore the elements of the set on the right.

(e) $2 \in \{0,2,\{1,2\}\}$ is true. See the previous example.

(f) $1 \in \{0,2,\{1,2\}\}$ is false. See (d) above.

(g) $\emptyset \in \{0,1,2,3\}$ is false; $\emptyset$ is not one of the objects occurring in the list describing the set on the right. The only objects a for which $a \in \{0,1,2,3\}$ is true are the numbers 0, 1, 2, or 3.

(h) $\emptyset \subseteq \{0, 1, 2, 3\}$ is true. $\emptyset \subseteq A$ is true for every set A. We can see this by noting that for $\emptyset \subseteq A$ to be false there would have to be an element $x \in \emptyset$ such that $x \notin A$. (See equation (3.2).)

The last set operation is the power set operation, $\mathcal{P}(A)$ where A is a set. Here is the definition.

Definition 3.11. If A is a set then $\mathcal{P}(A) = \{X : X \subseteq A\}$.

So the power set of a set A is the set whose elements are the subsets of A. As an example, $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. Notice that for any set A, both $\emptyset$ and A are elements of $\mathcal{P}(A)$.

To illustrate further how the definition might be used we prove two theorems. For the first theorem we illustrate the construction of the proof with diagrams, for the second the proof is given in (the usual) paragraph form.

Theorem 3.12. *For all sets X and Y, $\mathcal{P}(X) \cup \mathcal{P}(Y) \subseteq \mathcal{P}(X \cup Y)$.*

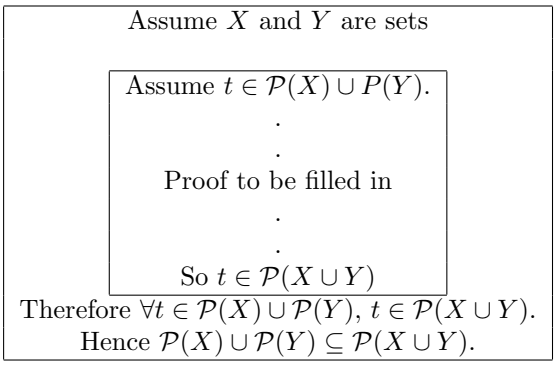
Proof. Using the generalization of Proof Principle 1 we will attempt a proof whose first line is "Assume X and Y are sets." and whose last line is "Hence $\mathcal{P}(X) \cup \mathcal{P}(Y) \subseteq \mathcal{P}(X \cup Y)$. " This would give the following diagram:

Assume X and Y are sets
.
.
Proof to be filled in
.
.
Hence $\mathcal{P}(X) \cup \mathcal{P}(Y) \subseteq \mathcal{P}(X \cup Y)$.

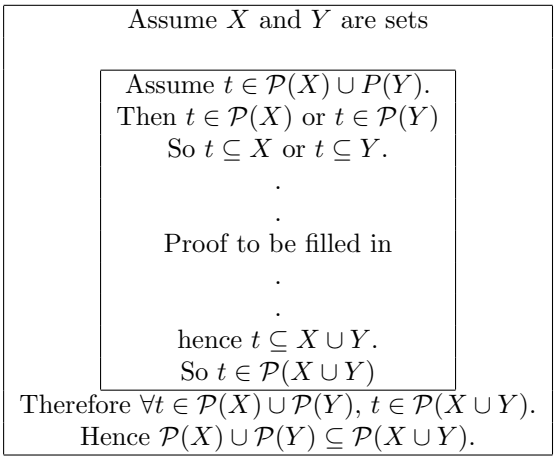
Using the definition of $\subseteq$ we can supply the second to last line of the proof, namely "$\forall t \in \mathcal{P}(X) \cup \mathcal{P}(Y)$, $t \in \mathcal{P}(X \cup Y)$." giving the diagram

Assume X and Y are sets
.
.
Proof to be filled in
.
.
Therefore $\forall t \in \mathcal{P}(X) \cup \mathcal{P}(Y)$, $t \in \mathcal{P}(X \cup Y)$.
Hence $\mathcal{P}(X) \cup \mathcal{P}(Y) \subseteq \mathcal{P}(X \cup Y)$.

Since the second to last line is a universally quantified statement, we can fill in the first and last lines of its proof using Proof Principle 1. This gives us the diagram



We can now use the definition of $\cup$ (and the fact that definitions are always active hypotheses) to replace $t \in \mathcal{P}(X) \cup \mathcal{P}(Y)$ with "$t \in \mathcal{P}(X)$ or $t \in \mathcal{P}(Y)$" and to replace $t \in \mathcal{P}(X \cup Y)$ with $t \subseteq X \cup Y$. Then we can use the same principle to replace $t \in \mathcal{P}(X)$ with $t \subseteq X$ and $t \in \mathcal{P}(Y)$ with $t \subseteq Y$. After doing this the diagram would be



The remainder of the proof can be filled in in the following way: (We will use the results of example (3.6) and problem 3.8) "If $t \subseteq X$, then since $X \subset X \cup Y$ (see Example 3.6) we can conclude that $t \subseteq X \cup Y$ by Exercise 3.8. Similarly, if $t \subseteq Y$ it follows that $t \subseteq X \cup Y$. In either of the two possible cases $t \subseteq X \cup Y$." Here is the final proof in paragraph form:

Assume X and Y are sets and assume that $t \in \mathcal{P}(X) \cup \mathcal{P}(Y)$. Then, by the definition of $\cup$, $t \in \mathcal{P}(X)$ or $t \in \mathcal{P}(Y)$. It follows, by the definition of the power set operation that $t \subseteq X$ or $t \subseteq Y$. In the first case (that is, $t \subseteq X$) it follows from $X \subseteq X \cup Y$ that $t \subseteq X \cup Y$. Similarly, in the second case (if $t \subseteq Y$) we may conclude that $t \subseteq X \cup Y$. Therefore $t \subseteq X \cup Y$. So $t \in \mathcal{P}(X \cup Y)$. Therefore $\forall t \in \mathcal{P}(X) \cup \mathcal{P}(Y), t \in \mathcal{P}(X \cup Y)$. Hence $\mathcal{P}(X) \cup \mathcal{P}(Y) \subseteq \mathcal{P}(X \cup Y)$. □

Theorem 3.13. *For all sets A and B, $\mathcal{P}(\mathcal{A} \setminus \mathcal{B}) \subseteq (\mathcal{P}(\mathcal{A}) \setminus \mathcal{P}(\mathcal{B})) \cup \{\emptyset\}$.*

Proof. Assume that $X \in \mathcal{P}(\mathcal{A} \setminus \mathcal{B})$, then by Definition 3.11 $X \subseteq A \setminus B$. This means, by Theorem 3.8, part 6, that $X \subseteq A$ and $X \cap B = \emptyset$. By the first of these conclusions $X \in \mathcal{P}(\mathcal{A})$. If it is also the case that $X \notin \mathcal{P}(\mathcal{B})$ then $X \in \mathcal{P}(\mathcal{A}) \setminus \mathcal{P}(\mathcal{B})$ so $X \in (\mathcal{P}(\mathcal{A}) \setminus \mathcal{P}(\mathcal{B})) \cup \{\emptyset\}$ and we are done. On the other hand if $X \in \mathcal{P}(\mathcal{B})$ then $X \subseteq B$. This together with the fact that $X \cap B = \emptyset$ and part 5 of theorem 3.8 give us $X = \emptyset$. Hence in this case also it is true that $X \in (\mathcal{P}(\mathcal{A}) \setminus \mathcal{P}(\mathcal{B})) \cup \{\emptyset\}$. □

3.4 The Empty Set

The empty set, denoted by $\{\}$ or $\emptyset$, was introduced in the Section 3.1. Our claim that there exists a set with no elements was based on the "box" analogy for sets. In a rigorous development of set theory the existence of such a set would follow from the basic assumptions about sets.[3] We will give an outline of a rigorous development of set theory in a later chapter. In that development we will begin with several basic assumptions which we shall call the *axioms* for set theory. One of these basic assumptions will be the axiom of extensionality (see section 3.2). There will be other axioms from which the existence of a set with no elements will follow. For the time being we shall simply assume that there is a set with no elements.

Axiom 3. Empty Set Axiom. There is a set z such that $\forall y, y \notin z$.

And we prove:

Theorem 3.14. *Let z be a set for which $\forall y, y \notin z$, then*

1. *For every sentence $Q(x)$ with one free variable x, the statement "$\exists x \in z$ such that $Q(x)$" is false.*

2. *For every sentence $P(x)$ with one free variable x, the statement "$\forall x \in z, P(x)$" is true.*

3. *For every set A, $z \subseteq A$.*

Proof. Part (1) holds by the meaning of "$\exists x \in z$ such that $Q(x)$". Part (2) is true since "$\forall x \in z, P(x)$" is the negation of "$\exists x \in z$ such that $Q(x)$" if we take $Q(x)$ to be "$\neg P(x)$". For part (3) assume that A is a set, then by definition of $\subseteq$ the statement "$z \subseteq A$" is equivalent to "$\forall x \in z, x \in A$" which is true by part (2). □

Corollary 3.15. *There is exactly one set z with the property that $\forall y, y \notin z$.*

[3] In a rigorous development of set theory we would also have to justify the existence of most of the sets we have described so far. This will be done in the chapter on axiomatic set theory.

Proof. To show that there is exactly one object of a certain property we must argue for two things: First that there is at least one object with the property and secondly that there is not more than one object. (See Proof Principle 14.) In the case of the corollary that we are proving, the Empty Set Axiom tells us that there is at least one set z such $\forall y, y \notin z$. To show that there is not more than one such object we assume that z_1 and z_2 are two objects for which $\forall y, y \notin z_1$ and $\forall y, y \notin z_2$. Based on this assumption we will prove that $z_1 = z_2$. Using Theorem 3.14 part 3 with $A = z_1$ and $z = z_2$ we conclude that $z_1 \subseteq z_2$. Similarly, $z_2 \subseteq z_1$. Therefore by the Axiom of Extensionality $z_1 = z_2$. □

Definition 3.16. The *empty set* (denoted $\emptyset$ or $\{\}$) is the unique set z such that $\forall y, y \notin z$.

Since the empty set is a possible source of confusion we will list several of its properties in this section for future use. Some of these properties have already been mentioned and all follow from the definition of the empty set or from Theorem 3.14 above.

Theorem 3.17. ***(Properties of the Empty Set)***

1. *For every object x, $x \notin \emptyset$.*
2. *For every sentence $Q(x)$ with one free variable x, the statement "$\exists x \in \emptyset$ such that $Q(x)$" is false.*
3. *For every sentence $P(x)$ with one free variable x, the statement "$\forall x \in \emptyset, P(x)$" is true.*
4. *For every set A, $\emptyset \subseteq A$.*

3.5 Exercises

3.1. Describe the following sets using the listing method or some variation of the listing method:

(a) $\{x : x \in \mathbb{Z} \text{ and } 1 \leq x < 5\}$

(b) $\{x : x \in \mathbb{R} \text{ and } x^2 - x - 6 = 0\}$

(c) The set of integers which are in the interval $[-1, 5)$

(d) $\mathcal{P}(\{1, 2\})$

(e) $\mathcal{P}(\emptyset)$

(f) The natural numbers which are multiples of three and less than 751.

(g) The natural numbers which are multiples of 5

3.2. Describe the following sets by the rule method or some variation of the rule method:

(a) The interval $[2, 4)$

(b) $\mathcal{P}(\{1, 2, 3, 4\})$

(c) $\mathcal{P}(\mathbb{R})$

(d) $\{1, 2, 3, 4, 5, 6, 7\}$

(e) The interval $[a, b]$

(f) The interval (a, b)

3.3. Describe the following sets by the *standard* rule method:

(a) $\{3n : n \in \mathbb{Z}\}$

(b) $\{x^2 - 1 : x \text{ is a real number }\}$

(c) The set of rational numbers $\mathbb{Q} = \{\frac{p}{q} : p \text{ and } q \text{ are in } \mathbb{Z} \text{ and } q \neq 0\}$

(d) $\{x \in \mathbb{Z} : x^2 = 1\}$

(e) $\{n \in \mathbb{N} : n \text{ is even}\}$

3.4. Why are the sets $\{1, 2, 3\}$ and $\{3, 1, 3, 2\}$ equal?

3.5. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 4, 6, 8, 10\}$ and $C = \{4, 5, 8\}$. Describe the following by the listing method:

(a) $A \cup B$

(b) $A \cap B$

(c) $A \setminus B$

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

(e) $C \times A$

(f) $C \times C$

3.6. Give counter examples for the following statements. Assume that all variable range over sets.

(a) If $A \setminus C = B \setminus C$ then $A = B$.

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

(c) If $A \cap C = B \cap C$ then $A = B$.

(d) If $A \cup C = B \cup C$ then $A = B$.

(e) $\forall A$ and B, $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$

(f) $\forall A$ and B, $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$.

(g) For all A and B, $A \times B = B \times A$.

(h) For all A and B, $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$.

3.7. For each of the following sentences find specific sets for which the sentence is true if possible. If there are no sets for which the sentence is true answer "not possible":

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

(b) $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$.

(c) $A \times B = B \times A$.

(d) $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$.

3.8. Prove: For all sets A, B and C, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.

3.9. Prove for all sets A, B and C that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. This is part 4 of Theorem 3.8.

3.10. Prove part 5 of Theorem 3.8.

3.11. Prove part 6 of Theorem 3.8.

3.12. Answer "true" or "false".

(a) $3 \subseteq \{1, 2, 3, 4\}$.

(b) $3 \in \{1, 2, 3, 4\}$.

(c) $\{3\} \in \{1, 2, 3, 4\}$.

(d) $\{3\} \subseteq \{1, 2, 3, 4\}$.

(e) $\emptyset \in \{1, 2, 3, 4\}$.

(f) $\emptyset \subseteq \{1, 2, 3, 4\}$.

(g) $\emptyset \in \mathcal{P}(\{1, 2, 3, 4\})$.

(h) $\emptyset \subseteq \mathcal{P}(\{1, 2, 3, 4\})$.

(i) $\{\emptyset\} \in \mathcal{P}(\{1, 2, 3, 4\})$.

(j) $\{\emptyset\} \subseteq \mathcal{P}(\{1, 2, 3, 4\})$.

3.13. Prove that for all sets A and B, $\mathcal{P}(\mathcal{A} \cap \mathcal{B}) = \mathcal{P}(\mathcal{A}) \cap \mathcal{P}(\mathcal{B})$.

3.14. Prove that there is at most one set x for which "$1 \in x$ and $\forall y \in x, y = 1$."

3.15. Prove: For all sets A, B and C, if $C \subseteq A$ then $(A \cap B) \cup C = A \cap (B \cup C)$.

3.16. Prove that for all sets A, B and C, if $(A \cap B) \cup C = A \cap (B \cup C)$ then $C \subseteq A$.

3.17. Prove: For all sets A, B and C, $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

3.18. Prove: For all sets A, B and C, $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

3.19. Prove: For all sets A, B and C, $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

3.20. Prove that for all sets A and B, if $A \cap B = \emptyset$, then $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$.

3.21. Assume A, B and C are sets. Prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. (This is sometimes called the distributive law of $\cap$ over $\cup$.)

3.22. Assume A, B and C are sets. Prove that $(A \setminus B) \cap (A \setminus C) = (A \setminus (B \cup C))$. (One of DeMorgan's laws.)

3.23. Assume A, B and C are sets. Prove that $(A \setminus B) \cup (A \setminus C) = (A \setminus (B \cap C))$. (The other of DeMorgan's laws.)

Chapter 4

Functions

4.1 Introduction, Definition and Examples

In elementary algebra and in calculus if A and B are sets, a function f from A to B is sometimes defined to be a *rule* which matches elements of A with elements of B in such a way that each element of A is matched with exactly one element of B. For each element of a of A, $f(a)$ denotes the element of B which is matched with a. In an algebra course or a calculus course this definition is sufficient for most purposes, but in mathematics courses where functions are studied in more depth a more precise definition is helpful. The primary problem with the definition given above is that the word "rule" needs further explanation. The usual solution to this problem is to dispense with the word "rule" and define the word function as follows:

Definition 4.1. A *function* f is a set whose elements are ordered pairs such that for all pairs (a_1, b_1) and (a_2, b_2) in f, if $a_1 = a_2$ then $b_1 = b_2$.

This says that a function is a set of ordered pairs which cannot contain two different pairs with the same first component. The formulation of the definition as an "if ... then ... then" statement is easier to use when proving that a set of ordered pairs is a function.

The set of first components of pairs in f is known as the *domain of* f. This set is abbreviated $\text{Dom}(f)$. Using the rule method we could therefore write

$$\text{Dom}(f) = \{a : \exists b \text{ such that } (a, b) \in f\}.$$

It is a consequence of the definition that for each $a \in \text{Dom}(f)$, there is exactly one object b such that $(a, b) \in f$. This object b will be denoted by $f(a)$.

The *range of* f ($\text{Range}(f)$ for short) is the set of all second components of pairs in f. That is,

$$\text{Range}(f) = \{b : \exists a \text{ such that } (a, b) \in f\} \text{ or} \tag{4.1}$$

$$\text{Range}(f) = \{b : \exists a \in \text{Dom}(f) \text{ such that } f(a) = b\} \text{ or} \tag{4.2}$$

$$\text{Range}(f) = \{f(a) : a \in \text{Dom}(f)\}. \tag{4.3}$$

There are several ways of describing a function. One possibility for finite functions is to use the listing method. For example, $f = \{(1,2),(2,3),(3,2),(4,5)\}$ is a function with domain $\{1,2,3,4\}$ and range $\{2,3,5\}$. Note that not every set of pairs is a function. For example the set $g = \{(1,2),(2,3),(2,5)\}$ because there are two different pairs with the same first component, namely $(2,3)$ and $(2,5)$.

Another possibility is to draw a diagram. For the function f described in the preceding paragraph the diagram would be:

$$\begin{array}{ccc} & f & \\ 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 2 \\ 4 & \to & 5 \end{array}$$

In the diagram an arrow from a to b means that $f(a) = b$, that is, it means $(a,b) \in f$.

Example 4.2. As a second example consider the the set of ordered pairs $F = \left\{ \left(\frac{x-1}{2x+1}, x \right) : x \in \mathbb{R} \setminus \{-\frac{1}{2}\} \right\}$. We are going to argue that F is a function. Referring to definition 4.1 and using Proof Principles 1 and 2 we assume that (a_1,b_1) and (a_2,b_2) are two pairs in F for which $a_1 = a_2$. Using this assumption we have to show that $b_1 = b_2$. From the assumption that (a_1,b_1) and (a_2,b_2) are in F it follows that $a_1 = \frac{b_1-1}{2b_1+1}$ and that $a_2 = \frac{b_2-1}{2b_2+1}$. From the assumption $a_1 = a_2$ we therefore obtain $\frac{b_1-1}{2b_1+1} = \frac{b_2-1}{2b_2+1}$. Multiplying both sides by $(2b_1+1)(2b_2+1)$ gives $(2b_2+1)(b_1-1) = (2b_1+1)(b_2-1)$ or $2b_2b_1-2b_2+b_1-1 = 2b_1b_2-2b_1+b_2-1$. It follows that $b_2 = b_1$. This completes the argument that F is a function.

Example 4.3. One more example: Let $G = \{(2x+1, 3x-2) : x \in \mathbb{R}\}$ As in the previous example we want to prove that G is a function. Assume (a_1,b_1) and (a_2,b_2) are in G and that $a_1 = a_2$. (To show that G is a function we need to prove that $b_1 = b_2$.) From the first part of the assumption it follows that there are elements x_1 and x_2 of $\mathbb{R}$ such that $(a_1,b_1) = (2x_1+1, 3x_1-2)$ and $(a_2,b_2) = (2x_2+1, 3x_2-2)$. Using the fundamental property of ordered pairs we conclude that $a_1 = 2x_1+1$, $a_2 = 2x_2+1$ and

$$b_1 = 3x_1 - 2 \text{ and } b_2 = 3x_2 - 2. \tag{4.4}$$

Since $a_1 = a_2$ we get $2x_1 + 1 = 2x_2 + 1$. It follows from this that $x_1 = x_2$. Combining this with (4.4) we conclude that $b_1 = b_2$.

Example 4.4. As noted above, not all sets of ordered pairs are functions. Here are some more examples of non-functions.

1. $E_1 = \{(1,2),(3,5),(2,5),(1,6)\}$ is not a function since it contains the two ordered pairs $(1,2)$ and $(1,6)$ which are different pairs with the same first component.

2. $E_2 = \{(x^2, x) : x \in \mathbb{R}\}$ is not a function since it contains the pairs $((-1)^2, -1) = (1, -1)$ and $(1^2, 1) = (1, 1)$ which have identical first components. In fact if x is any positive real number then the two pairs (x^2, x) and $(x^2, -x)$ are in E_2.

3. $E_3 = \{(x, y^2) : x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$ is not a function. Any $x \in \mathbb{R}$ and $y \in \mathbb{R}$ gives us a pair in E_3. For example choosing $x = 2$ and $y = 3$ gives us the pair $(2, 9) \in E_3$. Or choosing $x = 2$ and $y = \frac{7}{5}$ gives us the pair $(1, \frac{49}{25}) \in E_3$.

4.2 Further Examples and Describing Functions by Formulas

A more common way of describing a function is to give the domain and a formula or rule for calculating the output for a given input. You have probably seen functions described in this way. For example, we could define a function (we'll call it g) by saying, let g be the function whose domain is $\mathbb{R}$, the set of real numbers, defined by $g(x) = x^2 + 7$.[1] We could write g as a set of ordered pairs, $g = \{(x, x^2 + 7) : x \in \mathbb{R}\}$ or (using the standard rule method) $g = \{w : \exists x \in \mathbb{R} \text{ such that } w = (x, x^2 + 7)\}$. In general any function f, whether described by a formula or not, can be written

$$f = \{(a, f(a)) : a \in \text{Dom}(f)\}$$

Another example of a function which is usually described by giving it's domain and a formula for calculating the output is the *identity function* whose definition is:

Definition 4.5. Let X be any set then the *identity function on* X is the function 1_X whose domain is X defined by $\forall x \in X$, $1_X(x) = x$.

For example, if $X = \{1, 2, 3, 4\}$ then $1_X = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$ and in general the identity function on any set X could be described by $1_X = \{(x, x) : x \in X\}$.

Since functions are frequently described by giving a formula and the domain, it will be helpful to find equivalent formulations for some of our definitions so that they are easier to use with this kind of function description. For example, it is frequently easier to use the formula $\text{Range}(f) = \{f(x) : x \in \text{Dom}(f)\}$ (see equation (4.3)) for the range of a function f than it is to use the definition of $\text{Range}(f)$ given at the beginning of Section 4.1.

This and other useful principles are given in the following theorem. The proofs are left as exercises. (See Exercise 4.11.)

Theorem 4.6. *Assume that f and g are functions and B is a set, then*

[1] Note that since this is a definition, there is an implicit quantifier $\forall x \in \mathbb{R}$ here. That is, g is defined by $\forall x \in \mathbb{R}$, $g(x) = x^2 + 7$.

1. *To prove* $Range(f) \subseteq B$ *if suffices to prove* $\forall x \in Dom(f), f(x) \in B$.

2. *In order to prove that the functions* f *and* g *are equal it suffices to prove that* $Dom(f) = Dom(g)$ *and that for all* x *in the common domain,* $f(x) = g(x)$.

Part 1 uses the characterization of the range of a function given in equation (4.3). With regard to part 2 of the theorem we note that since a function is a set of ordered pairs it is possible to prove that two functions are equal using the Axiom of Extensionality (Axiom 2, from Chapter 3). That is, we could prove $f \subseteq g$ and $g \subseteq f$ to show that f and g are equal. However, when two functions f and g are given by specifying their domains and giving a formulas for calculating their outputs $f(x)$ and $g(x)$ for a given input x, it is usually easier to use part 2.

A frequently used abbreviation is

$$f : A \to B$$

This is read "f is a function from A to B" and it means that f is a function, that the domain of f is A and that the range of f is a subset of B. For example if g is the function defined in the preceding paragraph, then $g : \mathbb{R} \to \mathbb{R}$ is a true statement as is $g : \mathbb{R} \to \mathbb{R}^+$ where $\mathbb{R}^+$ is the set of positive real numbers. Note that B is only required to contain the range of f, it need not *be* the range of f (in the notation $f : A \to B$). The reason for this notational convention is that it makes the notation much easier to use, especially when a function is described by giving its domain and a formula for computing its output. In this case the function can be described and the notation $f : A \to B$ can be used without finding the range. It is important to realize that when you use the notation $f : A \to B$ you are asserting that $\text{Range}(f) \subseteq B$. Usually the set B is chosen so that this fact ($\text{Range}(f) \subseteq B$) is an easy application of Theorem 4.6 part 1.

Here are some examples.

Example 4.7.

1. Define $h_1 : \mathbb{R} \to \mathbb{R}$ by $h_1(x) = 7x - 2$. Here the domain is $\mathbb{R}$ and it is clear that $\forall x \in \text{Dom}(f) = \mathbb{R}$, $h_1(x) = 7x - 2 \in \mathbb{R}$. So using Theorem 4.6 part 1 it is clear that $\text{Range}(f) \subseteq \mathbb{R}$. Therefore using notation $f : \mathbb{R} \to \mathbb{R}$ is justified.

2. Let $h_2 : \mathbb{R} \to \mathbb{R}$ defined by $h_2(x) = 2x^2 + x - 1$. As for h_1, it is clear that $\text{Range}(h)_2 \subseteq \mathbb{R}$ so we may use the notation $h_2 : \mathbb{R} \to \mathbb{R}$.

3. Let h_3 be the function $h_3 : \mathbb{R} \setminus \{3\} \to \mathbb{R}$ defined by $h_3(x) = \dfrac{2x+2}{x-3}$. We first note that it is not immediately obvious what $\text{Range}(h_3)$ is but it is clear that $\text{Range}(h_3) \subseteq \mathbb{R}$ because $\forall x \in \text{Dom}(h_3) = \mathbb{R} \setminus \{3\}$, $h_3(x)$ is clearly in $\mathbb{R}$. (Since the number 3 is not in the domain, the denominator $x - 3$ is never zero for $x \in \text{Dom}(h_3)$. Using part (1) of Theorem 4.6 again we see that $\text{Dom}(h_4) \subseteq \mathbb{R}$.

4.3 Finding the Range of a Function

For many functions it is not obvious without doing some calculating what the range is. In this section we will find the range of the functions from Example 4.7 starting with h_3.

We first introduce some terminology used in connection with the range of a function.

Definition 4.8. If f is a function and C is a set f *is onto* C means that $\text{Range}(f) = C$.

As a first step in finding the range of h_3 we will try to determine if the number 7 is in the range. Using formula (4.2) above we see that this will happen if and only if $\exists a \in \mathbb{R} \setminus \{3\}$ such that $\frac{2a+2}{a-3} = 7$. If there is an a that works it will have to be a solution to this equation. If we solve the equation for a (starting by multiplying both sides by $a-3$) we obtain $a = \frac{23}{5}$. Calculating $h_3(\frac{23}{5})$ gives an answer of 7 and therefore 7 is in $\text{Range}(h)_3$.[2]

Now we try to determine the entire range of h_3 by a similar calculation. A number b is in the range of h_3 if and only if for some $a \in \mathbb{R}\setminus\{3\}$, $h_3(a) = b$. That is, if and only if $\dfrac{2a+2}{a-3} = b$. If we attempt to solve this equation for a starting by multiplying by $(a-3)$ we obtain $2a+2 = ab-3b$. Collecting the terms involving a on one side, we get $ab - 2a = 2 + 3b$. If follows by factoring and dividing that $a = \frac{2+3b}{b-2}$. It looks like this should be possible for every $b \neq 2$ so we conjecture that $\text{Range}(h_3) = \mathbb{R} \setminus \{2\}$. The ideas that will be used in the proof can be found in the calculations we have just done but the proof itself involves more than just solving an equation. Since $\text{Range}(h_3)$ and $\mathbb{R} \setminus \{2\} = \{z \in \mathbb{R} : z \neq 2\}$ are both sets we'll prove that they are equal by showing that each of these sets is a subset of the other (using the Axiom of Extensionality).

We begin with the proof that $\{z \in \mathbb{R} : z \neq 2\} \subseteq \text{Range}(h_3)$. (There will be several diagrams to show how our proof principles are use to structure the proof.) Since $\{z \in \mathbb{R} : z \neq 2\} \subseteq \text{Range}(h_3)$ means (see the definition 3.4 of $\subseteq$) "$\forall y \in \{z \in \mathbb{R} : z \neq 2\}$, $y \in \text{Range}(h_3)$" we should consider a proof with the following structure (see Proof Principle 1):

Assume $y \in \{z \in \mathbb{R} : z \neq 2\}$.
.
Proof to be filled in
.
.
Therefore $y \in \text{Range}(h_3)$

[2] Note that solving the equation $\frac{2a+2}{a-3} = 7$ for a and obtaining $a = \frac{23}{5}$ does not prove that $\frac{23}{5}$ is a solution to the equation. Consider the equation $\sqrt{x+5} = x - 1$. Squaring both sides gives $x + 5 = x^2 - 2x + 1$. If we get a zero on one side and factor we obtain $(x-4)(x+1) = 0$ which implies that $x = 4$ or $x = -1$. We haven't proved that $x = -1$ and $x = 4$ are solutions. In fact $x = -1$ is not a solution. We could prove that $x = 4$ is a solution by replacing x by 4 and noting that the resulting equation is true.

Using the fact that $a \in \{x \in S : P(x)\}$ is equivalent to $P(a)$ (see statement 3.1in Section 3.1) we get the second line of the proof, namely, "$y \in \mathbb{R}$ and $y \neq 2$.". Similarly, keeping in mind that Range$(h_3) = \{w : \exists x \in \mathbb{R} \setminus \{3\}$ such that $w = h_3(x)\}$, a reasonable second to last line would be " $\exists x \in \mathbb{R} \setminus \{3\}$ such that $y = h_3(x)$." Adding these two lines the proof has reached the stage

Assume $y \in \{z \in \mathbb{R} : z \neq 2\}$
Then $y \in \mathbb{R}$ and $y \neq 2$.
.
.
Proof to be filled in
.
.
So $\exists x \in \mathbb{R} \setminus \{3\}$ such that $y = h_3(x)$
Therefore $y \in$ Range(h)

Continuing with the proof in our example using Proof Principle 12 we would have to do some scratch work to find an object x_0 for which $x_0 \in \mathbb{R} \setminus \{3\}$ and $y = h_3(x_0)$. This has already been done in example 4.7: Looking at the condition $y = h_3(x_0)$ and using the definition of h we find that we want an x_0 for which $y = \frac{2x_0+2}{x_0-3}$. Solving for x_0 gives us $x_0 = \frac{2+3y}{y-2}$. This ends the scratch work, the result of which is that the x_0 we are looking for is probably $x_0 = \frac{2+3y}{y-2}$ which is defined in terms of the active object symbol y. Using Proof Principle 12 we add two lines to the proof "Let $x_0 = \frac{2+3y}{y-2}$" as the third line and "Hence $x_0 \in \mathbb{R} \setminus \{3\}$ and $y = h_3(x_0)$" as the third from the last line. This gives us the following diagram.

Assume $y \in \{z \in \mathbb{R} : z \neq 2\}$
Then $y \in \mathbb{R}$ and $y \neq 2$.
Let $x_0 = \frac{2+3y}{y-2}$
.
.
Proof to be filled in
.
.
Hence $x_0 \in \mathbb{R} \setminus \{3\}$ and $y = h_3(x_0)$
So $\exists x \in \mathbb{R} \setminus \{3\}$ such that $y = h_3(x)$
Therefore $y \in$ Range(h_3)

In this diagram the "Proof to be filled in" is to be a proof of "$x_0 \in \mathbb{R} \setminus \{3\}$ and $y = h_3(x_0)$". Since this is a statement of the form "P and Q" we shall use Proof Principle 10. According to this proof principle we should give two proofs: One of "$x_0 \in \mathbb{R} \setminus \{3\}$" and another of "$y = h_3(x_0)$".

The first proof has two parts both of which should be familiar by now:

Since $y \neq 2$, $x_0 \in \mathbb{R}$.
We'll show that $x_0 \neq 3$ by contradiction:

Assume that $x_0 = 3$ then $\frac{2+3y}{y-2} = 3$.
Simplifying this equation we obtain $2 = -6$, a contradiction.
By the definition of the set difference operation $\setminus$ we conclude that $x_0 \in \mathbb{R} \setminus \{3\}$.

The second proof is straight forward:

$$\begin{aligned} h_3(x_0) &= \frac{2x_0 + 2}{x_0 - 3} \\ &= \frac{2\left(\frac{2+3y}{y-2}\right) + 2}{\left(\frac{2+3y}{y-2}\right) - 3} \\ &= \frac{2(2+3y) + 2(y-2)}{(2+3y) - 3(y-2)} \end{aligned}$$

multiplying numerator and denominator by $(y-2)$ and simplifying gives

$$= y$$

Here is the complete proof (that h_3 is onto $\{z \in \mathbb{R} : z \neq 2\}$.)

Example. 4.7 Part 3 continued. Let h_3 be the function $h_3 : \mathbb{R} \setminus \{3\} \to \mathbb{R}$ defined by $h_3(x) = \frac{2x+2}{x-3}$. Prove that h is onto $\{z \in \mathbb{R} : z \neq 2\}$

Proof. We begin by proving

$$\{z \in \mathbb{R} : z \neq 2\} \subseteq \text{Range}(h_3). \tag{4.5}$$

Assume $y \in \{z \in \mathbb{R} : z \neq 2\}$. Then $y \in \mathbb{R}$ and $y \neq 2$. Let $x_0 = \frac{2+3y}{y-2}$. Since $y \neq 2$ it is clear that $x_0 \in \mathbb{R}$. We prove that $x_0 \neq 3$ by contradiction: Assume that $x_0 = 3$, then $\frac{2+3y}{y-2} = 3$. Multiplying both sides of this equation by $(y-2)$ gives us $2+3y = 3y-6$ from which it follows that $2 = -6$. This is a contradiction. We also have that $h_3(x_0) = \frac{2x_0+2}{x_0-3} = \frac{2\left(\frac{2+3y}{y-2}\right)+2}{\left(\frac{2+3y}{y-2}\right)-3} = \frac{2(2+3y)+2(y-2)}{(2+3y)-3(y-2)} = y$. Hence $x_0 \in \mathbb{R} \setminus \{3\}$ and $y = h_3(x_0)$. So $\exists x \in \mathbb{R} \setminus \{3\}$ such that $y = h_3(x)$. Therefore $y \in \text{Range}(h_3)$. (This is the proof that was diagramed above.)

Now we prove

$$\text{Range}(h_3) \subseteq \{z \in \mathbb{R} : z \neq 2\} \tag{4.6}$$

Assume $t \in \text{Range}(h_3)$, then $\exists x \in \mathbb{R} \setminus 3$ such that $h_3(x) = t$. Assume $x_0 \in \mathbb{R}$ and $h_3(x_0) = t$. Using the formula for h, this means that $t = \frac{2x_0+2}{x_0-3}$. Since $x_0 \neq 3$ it is clear that t is a real number. In addition $t \neq 2$ can be proved by contradiction, for suppose $t = 2$, then $\frac{2x_0+2}{x_0-3} = 2$. Multiplying both sides by $(x_0 - 3)$ and collecting like terms gives $2 = -6$ which is a contradiction. We have shown that $t \in \mathbb{R}$ and that $t \neq 2$ hence $t \in \{z \in \mathbb{R} : z \neq 2\}$ This completes the proof of (4.6) and it follows from this together with (4.5) that $\text{Range}(h_3) = \{z \in \mathbb{R} : z \neq 2\}$. □

One note before we leave this example. In the proof of equation 4.6, after making our assumptions we had as an active hypothesis "$\exists x \in \mathbb{R} \setminus 3$ such that $h_3(x) = t$" and we used Proof Principle 6 to introduce a new parameter x_0 with the properties "$x_0 \in \mathbb{R}$ and $h_3(x_0) = t$". In the discussion of Proof Principle 6 it was mentioned that ordinarily the parameter which is introduced is the same as the bound variable of the existential statement. It also frequently happens that no mention is made of the introduction of a new parameter. It is just assumed that the reader will know that a parameter has been introduced and assumptions made about it. To illustrate how this might happen here are two possible ways that the proof of (4.6) above might be rewritten.

Proof. (using x instead of x_0) Assume $t \in \text{Range}(h_3)$, then $\exists x \in \mathbb{R} \setminus 3$ such that $h_3(x) = t$. Assume $x \in \mathbb{R}$ and $h_3(x) = t$. Using the formula for h_3, this means that $t = \frac{2x+2}{x-3}$. Since $x \neq 3$ it is clear that t is a real number. In addition $t \neq 2$ can be proved by contradiction, for suppose $t = 2$, then $\frac{2x+2}{x-3} = 2$. Multiplying both sides by $(x-3)$ and collecting like terms gives $2 = -6$ which is a contradiction. We have shown that $t \in \mathbb{R}$ and that $t \neq 2$ hence $t \in \{z \in \mathbb{R} : z \neq 2\}$ This completes the proof of (4.6). □

Proof. (without explicitly introducing the object symbol x or the assumptions made about it) Assume $t \in \text{Range}(h_3)$, then $\exists x \in \mathbb{R} \setminus 3$ such that $h_3(x) = t$. Using the formula for h_3, this means that $t = \frac{2x+2}{x-3}$. Since $x \neq 3$ it is clear that t is a real number. In addition $t \neq 2$ can be proved by contradiction, for suppose $t = 2$, then $\frac{2x+2}{x-3} = 2$. Multiplying both sides by $(x-3)$ and collecting like terms gives $2 = -6$ which is a contradiction. We have shown that $t \in \mathbb{R}$ and that $t \neq 2$ hence $t \in \{z \in \mathbb{R} : z \neq 2\}$ This completes the proof of (4.6). □

4.4 One to One Functions

4.4.1 Definitions and Examples

Definition 4.9. If f is a function then f is *one to one* if for all a_1 and a_2 in $\text{Dom}(f)$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$.

There are several equivalent ways of saying that a function is one to one. The one just given is the easiest to use when proving that a function is one to one. Some other possibilities are

1. A function f is one to one if for all (a_1, b_1) and (a_2, b_2) in f, if $b_1 = b_2$ then $a_1 = a_2$.

2. A function $f : A \to B$ is one to one if for all a_1 and a_2 in A, if $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$.

Example 4.10. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 3x+8$. We will prove that f is one to one. Proof Principles 1 and 2 applies here as they usually do when proving a function is one to one. Using the definition, to show f is one to one we have to show that for all a_1 and a_2 in $\text{Dom}(f)$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$.

Proof. Assume that a_1 and a_2 are in Dom(f) and that $f(a_1) = f(a_2)$. Then $3a_1 + 8 = 3a_2 + 8$. Subtracting 8 from both sides and then dividing by 3 gives $a_1 = a_2$. We have shown that for all a_1 and a_2 in Dom(f), if $f(a_1) = f(a_2)$ then $a_1 = a_2$ and therefore f is one to one. □

Example 4.11. Define $f : \mathbb{R}\backslash\{4\} \to \mathbb{R}$ by $f(x) = \frac{2x-3}{3x-12}$. We will prove that f is one to one: *Proof.* Assume a_1 and a_2 are in Dom(f) and that $f(a_1) = f(a_2)$. By the definition of f, $\dfrac{2a_1 - 3}{3a_1 - 12} = \dfrac{2a_2 - 3}{3a_2 - 12}$. Multiplying both sides of this equation by $(3a_1 - 12)(3a_2 - 12)$ gives $6a_1a_2 - 3a_2 - 24a_1 + 36 = 6a_1a_2 - 3a_1 - 24a_2 - 36$. It follows from this (by some easy algebra) that $a_1 = a_2$. This shows that f is one to one. □

4.4.2 The Inverse of a One to One Function

For any function f we can define "the inverse of f" which we will denote by f^{-1}. [3]

Definition 4.12. If f is a function then *the inverse of* f is the set $\{(b, a) : (a, b) \in f\}$.

For example if $f = \{(1, 2), (2, 3), (3, 1), (4, 5)\}$ then $f^{-1} = \{(2, 1), (3, 2), (1, 3), (5, 4)\}$ and if $g = \{(1, 1), (-1, 1), (2, 4), (-2, 4)\}$ then $g^{-1} = \{(1, 1), (1, -1), (4, 2), (4, -2)\}$.

As can be seen from the two examples the inverse of a function may or may not be a function. In our examples f^{-1} is a function and g^{-1} is not. It can also be seen that the determining factor is whether or not the original function is one to one.

Theorem 4.13. *If f is a one to one function then*

1. *f^{-1} is a function*
2. *Dom(f^{-1}) = Range(f)*
3. *Range(f^{-1}) = Dom(f)*
4. *f^{-1} is one to one.*

The proof is left for the exercises.

Example 4.14. Let $h : [1, 3] \to \mathbb{R}$ defined by $h(x) = -2x + 3$. Prove that h is one to one and that Range$(h) = [-3, 1]$. Find a formula for the inverse of h. What are Dom(h^{-1}) and Range(h^{-1})?

To prove that h is one to one we assume that $h(x_1) = h(x_2)$. Then $-2x_1 + 3 = -2x_2 + 3$. It follows (subtracting 3 from both sides and dividing both sides by -2 that $x_1 = x_2$.

[3] The definition actually makes sense if f is any set of ordered pairs.

To prove that $\text{Range}(h) = [-3, 1]$ we prove that $\text{Range}(h) \subseteq [-3, 1]$ and that $[-3, 1] \subseteq \text{Range}(h)$. Assume first that $y \in \text{Range}(h)$. Then for some $x \in [1, 3]$, $h(x) = y$. That is $y = -2x + 3$. Since $1 \leq x \leq 3$, $-6 \leq -2x \leq -2$. Adding 3 gives us $-3 \leq -2x + 3 \leq 1$ so $-3 \leq y \leq 1$ and $y \in [-3, 1]$. Second assume that $y \in [-3, 1]$. Let $x = \frac{y-3}{-2}$. Since $-3 \leq y \leq 1$, $-6 \leq y - 3 \leq -2$. Dividing by -2 gives us $1 \leq \frac{y-3}{-2} \leq 3$, so $1 \leq x \leq 3$ and therefore $1 \in [1, 3]$. Further $h(x) = -2x + 3 = -2\left(\frac{y-3}{-2}\right) + 3 = y$. Therefore $y \in \text{Range}(f)$.

To find a formula for h^{-1} assume that $h^{-1}(y) = x$. We want to find a formula for x in terms of y. If $h^{-1}(y) = x$ then $h(x) = y$. Using the formula for h, $-2x + 3 = y$. Solving for x gives us $x = \frac{y-3}{-2}$ hence $h(y) = \frac{y-3}{-2}$.

Finally $\text{Dom}(h^{-1}) = \text{Range}(h) = [-3, 1]$ and $\text{Range}(h^{-1}) = \text{Dom}(h) = [1, 3]$.

4.5 Composition of Functions

If f and g are functions, then the *composition of g and f*, denoted by $g \circ f$ is the function from whose domain is $\{t \in \text{Dom}(f) : f(t) \in \text{Dom}(g)\}$ defined by

$$\forall t \in A, (g \circ f)(t) = g(f(t)). \tag{4.7}$$

For example, let $f = \{(1, 3), (2, 7), (3, 3), (4, 2)\}$ and let $g = \{(3, 1), (4, 3), (7, 9)\}$. We first find the domain of $g \circ f$. The domain of g is the set $\{3, 4, 7\}$ and the domain of f is $\{1, 2, 3, 4\}$. For each $t \in \text{Dom}(f)$ we check whether or not $f(t) \in \text{Dom}(g)$: $f(1) = 3 \in \text{Dom}(g)$ so $1 \in \text{Dom}(g \circ f)$. Similarly 2 and 3 are in $\text{Dom}(g \circ f)$. But $f(4) = 2 \notin \text{Dom}(g)$ so $4 \notin \text{Dom}(g \circ f)$. Therefore the domain of $g \circ f$ is $\{1, 2, 3\}$. Now we calculate $(g \circ f)(t)$ for each $t \in \{1, 2, 3\}$. For example $(g \circ f)(1) = g(f(1)) = g(3) = 1$ so $(1, 1) \in g \circ f$. Similarly $(g \circ f)(2) = g(f(2)) = g(7) = 9$ so $(2, 9) \in g \circ f$ and $(g \circ f)(3) = 1$ so $(3, 1) \in g \circ f$. Therefore writing $g \circ f$ as a set of ordered pairs we get $g \circ f = \{(1, 1), (2, 9), (3, 1)\}$.

Since a function is a set of ordered pairs, we could describe the composition of two functions g and f as a set of ordered pairs in the following way.

$$g \circ f = \{(x, z) : \exists y \text{ such that } (x, y) \in f \text{ and } (y, z) \in g\} \tag{4.8}$$

The first description of composition given in equation (4.7) is almost always easier to use.

If f and g are described by equations then it is usually possible to describe $g \circ f$ the same way using (4.7). For example if f and g are the functions from $\mathbb{R}$ to $\mathbb{R}$ defined by $f(x) = x^2 + 3x + 5$ and $g(x) = \frac{x^2+x}{2x^2+2}$ then by (4.7) $(g \circ f)(t) = g(f(t)) = g(t^2 + 3t + 5) = \frac{(t^2+3t+5)^2+(t^2+3t+5)}{2(t^2+3t+5)^2+2}$.

The following theorem will be useful in Chapter 6. The proof will be left for the exercises.

Theorem 4.15. *Assume that $f : A \to B$, $g : B \to C$ and $h : C \to D$.*

1. *If f and g are one to one then $g \circ f$ is one to one.*
2. *If f is onto B and g is onto C then $g \circ f$ is onto C.*
3. $h \circ (g \circ f) = (h \circ g) \circ g$.
4. *If f is one to one and onto B then $f^{-1} : B \to A$ and $f^{-1} \circ f = 1_A$ and $f \circ f^{-1} = 1_B$.*

Proof. We will prove part 4. The proofs of the remaining parts are left for the exercises. Assume the hypotheses of the theorem and of part 4. Since f is onto B, Range$(f) = B$. Using Theorem 4.13 this means that Dom$(f^{-1}) = B$. Similarly, since Dom$(f) = A$, Range$(f) = A$. Combining these two facts gives us $f^{-1} : B \to A$. We'll prove that $f^{-1} \circ f = 1_A$ using part 2 of Theorem 4.6. Since both $f^{-1} \circ f$ and 1_A both have domain A we have to show that $\forall x \in A$, $(f^{-1} \circ f)(x) = 1_A(x)$. Since $1_A(x) = x$ what we have to show is that $(f^{-1} \circ f)(x) = x$ for every $x \in A$. To do this assume $x \in A$. Then $(x, f(x)) \in f$. This means that $(f(x), x) \in f^{-1}$ and so $f^{-1}(f(x)) = x$. Rewriting the left hand side of this equation gives $(f^{-1} \circ f)(x) = x$.

The proof that $f \circ f^{-1} = 1_B$ is similar. □

4.6 Functions Applied to Subsets of the Domain

If $f : A \to B$ then we can define a new function from $\mathcal{P}(A)$ to $\mathcal{P}(B)$ which is closely related to f.

Definition 4.16. Assume $f : A \to B$ then the function $f^* : \mathcal{P}(A) \to \mathcal{P}(B)$ is defined by the equation $f^*(X) = \{f(x) : x \in X\}$ for all $X \in \mathcal{P}(A)$. [4]

For example, let f be the function $\{(1,3),(2,3),(3,7),(4,6),(5,7)\}$ then f^* is defined for every subset of Dom$(f) = \{1,2,3,4,5\}$ and $f^*(\{1,3,4\}) = \{f(1), f(3), f(4)\} = \{3,7,6\}$. As a second example, let $g : \mathbb{R} \to \mathbb{R}$ be defined by the equation $g(x) = 3x - 5$. Then $g^*([1,3)) = \{g(x) : x \in [1,3)\} = \{3x - 5 : 1 \leq x < 3\}$. Using y for $3x - 5$ then $x = \frac{y+5}{3}$ so we can write this set as $\{y : 1 \leq \frac{y+5}{3} < 3\} = \{y : -2 \leq y < 4\} = [-2, 4)$. That is, $g^*([1,3)) = [-2,4)$.

The next theorem gives several facts about the function f^*. The proofs are left for the exercises.

Theorem 4.17. *Assume that $f : A \to B$ and that X and Y are subsets of A then*

1. *If $X \subseteq Y$ then $f^*(X) \subseteq f^*(Y)$.*
2. *$f^*(X \cup Y) = f^*(X) \cup f^*(Y)$.*
3. *$f^*(X \cap Y) \subseteq f^*(X) \cap f^*(Y)$.*

[4] The notation f^* is not standard. If $X \subset$ Dom(f) then what we have denoted by $f^*(X)$ is also sometimes denoted by $f[X]$, $f'(X)$ or simply $f(X)$.

4.7 Functions and Infinite Set Operations

Assume that F is a function with domain I such that for all $i \in I$, $F(i)$ is a set. For such a function we will sometimes denote $F(i)$ by F_i and call F a *family of sets*. We will define the union and the intersection of the sets F_i, $i \in I$ by

Definition 4.18. 1. $\bigcup_{i\in I} F_i = \{x : \exists i \in I \text{ such that } x \in F_i\}$

2. $\bigcap_{i\in I} F_i = \{x : \forall i \in I, x \in F_i\}$

For example, $\bigcup_{i\in\mathbb{N}}[0, i+1) = [0, \infty)$. Here $I = \mathbb{N}$ and for $i \in \mathbb{N}$, $F(i) = F_i$ is the interval $[0, i+1)$. (The proof that $\bigcup_{i\in\mathbb{N}}[0, i+1) = [0, \infty)$ is left as an exercise.) Also note that $\bigcap_{i\in\mathbb{N}}[0, i+1) = [0, 1)$

As a second example, we prove that $\bigcap_{i\in\mathbb{N}}[0, \frac{1}{i+1}) = \{0\}$. Our proof will use the fact that for every positive real number x, there is a positive integer n such that $\frac{1}{n} < x$. (See exercise 4.45) [5]

We begin by proving that $\bigcap_{i\in\mathbb{N}}[0, \frac{1}{i+1}) \subseteq \{0\}$. Assume that $t \in \bigcap_{i\in\mathbb{N}}[0, \frac{1}{i+1})$ then by Definition 4.18 part 2, $\forall i \in \mathbb{N}$, $t \in [0, \frac{1}{i+1})$ and so $0 \leq t < \frac{1}{i+1}$. It follows that $0 \leq t$ and we show that $t \leq 0$ by contradiction. Assume that $t > 0$, then $\exists n \in \mathbb{N}$ such that $\frac{1}{n} < t$. Therefore, since $\frac{1}{n+1} < \frac{1}{n}$, $\frac{1}{n+1} < t$. This contradicts the fact that $t < \frac{1}{i+1}$ for all $i \in \mathbb{N}$.

To complete the proof of the equality we show that $\{0\} \subseteq \bigcap_{i\in\mathbb{N}}[0, \frac{1}{i+1})$. Assume $t \in \{0\}$, then $t = 0$. Assume $i \in \mathbb{N}$, the $i + 1 > 0$ so $\frac{1}{i+1} > 0$. It follows that $0 \leq t < \frac{1}{i+1}$ and therefore $t \in [0, \frac{1}{i+1})$. We have shown that $\forall i \in \mathbb{N}$, $t \in [0, \frac{1}{i+1})$ and therefore by Definition 4.18 part 2, $t \in \bigcap_{i\in\mathbb{N}}[0, \frac{1}{i+1})$

If $\mathcal{A}$ is a collection of sets then using the notation described in this section the union of the sets in $\mathcal{A}$ could be denoted by $\bigcup_{u\in\mathcal{A}} u$. For example, if $\mathcal{A} = \{\{1, 3, 5, \}, \{3, 7, 9\}, \{1, 6, 7\}\}$ then $\bigcup_{u\in\mathcal{A}} u = \{1, 3, 5, 6, 7, 9\}$. It should also be mentioned that the notation $\bigcup \mathcal{A}$ is sometimes used for this union. That is,

Definition 4.19. If $\mathcal{A}$ is a collection of sets, then

1. $\bigcup \mathcal{A} = \{t : \exists u \in \mathcal{A} \text{ such that } t \in u\}$

2. $\bigcup \mathcal{A} = \{t : \forall u \in \mathcal{A}, t \in u\}$

Using the example $\mathcal{A} = \{\{1, 3, 5, \}, \{3, 7, 9\}, \{1, 6, 7\}\}$ and $t = 9$ we see that $\exists u \in \mathcal{A}$ such that $9 \in u$, namely $u = \{3, 7, 9\}$ and therefore by the definition $9 \in \bigcup \mathcal{A}$. (As we asserted above $\bigcup \mathcal{A} = \bigcup_{u\in\mathcal{A}} u = \{1, 3, 5, 6, 7, 9\}$.)

NEEDS TO BE FINISHED

4.8 Exercises

4.1. Draw a diagram for the function $f = \{(2, 3), (3, 4), (4, 4), (5, 4)\}$

[5] Note that this fact is equivalent to the following: $\forall y \in \mathbb{R}$, if $y > 0$ then $\exists n \in \mathbb{N}$ such that $n > y$. This is known as the Archimedian property of the real numbers.

4.2. For the function f described in exercise 4.1 find $f(2)$, $f(3)$ and $f(4)$.

4.3. Write the function described by the diagram

$$\begin{array}{ccc} & f & \\ 1 & \to & 2 \\ 2 & \to & 3 \\ 3 & \to & 2 \\ 4 & \to & 5 \end{array}$$

as a set of ordered pairs.

4.4. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = \frac{x-1}{x^2+1}$. Write g as a set of ordered pairs.

4.5. Which of the following sets of ordered pairs are functions?

(a) $\{(1,3),(2,6),(3,1)\}$

(b) $\{(1,4),(2,4),(3,4),(4,4)\}$

(c) $\{(4,1),(4,2),(4,3),(4,4)\}$

(d) $\{(x, 2x+x^2) : x \in \mathbb{R}\}$

(e) $\{(x^2, y^2) : x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$

4.6. Prove that the following set of ordered pairs is a function: $\{(3x+9, x) : x \in \mathbb{R}\}$.

4.7. Prove that the following set of ordered pairs is a function $\{(3x+9, 2x-7) : x \in \mathbb{R}\}$

4.8. What are the domains and ranges of the functions in problems 4.6 and 4.7?

4.9. Prove that the following set of ordered pairs is a function $\{(\dfrac{3x+2}{x+7}, x) : x \in \mathbb{R} \text{ and } x \neq -7\}$.

4.10. What are the domain and range of the function in problem 4.9?

4.11. Prove parts 1 and 2 of Theorem 4.6.

4.12. Let $k : \mathbb{R} \setminus \{-4\} \to \mathbb{R}$ be defined by $k(x) = \frac{3x-2}{2x+8}$.

(a) What is Range(k)?

(b) Prove your answer to part (a).

4.13. The function $f : \mathbb{R} \setminus \{2, -2\} \to \mathbb{R}$ is defined by $f(x) = \frac{1}{x^2-4}$. Prove that f is not onto $\mathbb{R}$. (Hint: Do some scratch work to find a real number not in the range of f and then prove it's not in the range of f by contradiction.)

4.14. The function $f : \mathbb{R} \setminus \{3, -3\} \to \mathbb{R}$ is defined by $f(x) = \frac{x^2}{x^2-9}$. Prove that f is not onto $\mathbb{R}$.

4.15. Prove by contradiction: For all sets A and B, if $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$ then $A \cap B = \emptyset$ or $A \subseteq B$.

4.16. Let $k : \mathbb{R} \to \mathbb{R}$ be defined by $k(x) = x^2 - 3x + 7$

(a) What is Range(k)?

(b) Prove your answer to part (a).

4.17. Prove that Range(f) $= \{y \in \mathbb{R} : y \neq 5\}$ where $f : \{x \in \mathbb{R} : x \neq 7\} \to \mathbb{R}$ is defined by $f(x) = \frac{5x-1}{x-7}$.

4.18. Prove for all sets A, B and C that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

4.19. Prove for all sets A, B and C that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

4.20. Prove for all sets A, B and C that $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

4.21. Prove that for all sets A and B, $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

4.22. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 4x + 9$. Prove that f is one to one.

4.23. Define $f : [0, 1] \to [7, 10]$ by $f(x) = 3x + 7$. Prove that f is one to one and onto $[7, 10]$.

4.24. Define $f : \mathbb{R} \setminus \{3\} \to \mathbb{R}$ by $f(x) = \frac{2x}{x-3}$. Prove that f is one to one.

4.25. Find a one to one function f from $[3, 8]$ onto $[1, 7]$. Describe f by giving the domain of f and a formula for $f(x)$. (Hint: A function whose graph is a straight line segment joining $(3, 1)$ and $(8, 7)$ would work.)

4.26. Let $f = \{(2, 3), (3, 4), (4, 5), (5, 7), \}$. What is f^{-1}?

4.27. Find a formula for $f^{-1}(y)$ if $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = 4x + 9$.

4.28. Find a formula for $f^{-1}(y)$ if $f : \mathbb{R} \setminus \{3\} \to \mathbb{R}$ is defined by $f(x) = \frac{3x-2}{x-3}$.

4.29. Prove Theorem 4.13

4.30. Using $f = \{(2, 3), (3, 4), (4, 5), (5, 7), \}$ and $g = \{(2, 1), (3, 1), (4, 2), (5, 2), (7, 12)\}$, find $g \circ f$.

4.31. The functions $h : \mathbb{R} \to \mathbb{R}$ and $k : \mathbb{R} \to \mathbb{R}$ are defined by the equations $h(x) = 8x - 17$ and $k(x) = 3x^3 + 4x^2 + 8$. Find formulas for $(h \circ k)(t)$ and $(k \circ h)(t)$.

4.32. Prove part 1 of theorem 4.15.

4.33. Prove part 2 of theorem 4.15.

4.34. Prove part 3 of theorem 4.15.

4.35. For each of the following conditions find three sets A, B and C and two functions $f : A \to B$ and $g : B \to C$ for which the condition is true if this is possible. If it is not possible to find an example making the condition true answer "Not possible."

(a) f is one to one, g is not one to one and $g \circ f$ is one to one.

(b) f is one to one, g is not one to one and $g \circ f$ is not one to one.

(c) f is not one to one and g is one to one and $g \circ f$ is one to one.

(d) f is not onto B and $g \circ f$ is onto C.

(e) g is not onto C and $g \circ f$ is onto C.

4.36. Let $f = \{(2,3),(3,6),(4,3),(5,5),(6,6),(7,1)\}$. Find $f^*(\emptyset)$, $f^*(\{2,4,5,7\})$, $f^*(\{3\})$ and $f^*(\{4,5,6\}$.

4.37. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = \frac{2}{3}x + 4$. Find $g^*(\{1,2,3\}$, $g^*([-1,1])$, $g^*([3,\infty))$ and $g^*(\mathbb{R})$.

4.38. Define $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = x^2$. What are $h^*(\{-2,-1,0,1,3,5\})$, $h^*([2,3))$, and $h^*([-3,5])$.

4.39. Prove: If $f : A \to B$ and X and Y are subsets of A then $f^*(A \cup B) = f^*(A) \cup f^*(B)$.

4.40. Prove: If $f : A \to B$ and X and Y are subsets of A then $f^*(X \cap Y) \subseteq f^*(X) \cap f^*(Y)$.

4.41. Give two sets A and B, a function $f : A \to B$ and subsets X and Y of A such that $f^*(X \cap Y) \neq f^*(X) \cap f^*(Y)$.

4.42. Prove: If $f : A \to B$ and X and Y are subsets of A and f is one to one then $f^*(X \cap Y) = f^*(X) \cap f^*(Y)$.

4.43. Prove or disprove: If $f : A \to B$ and X and Y are subsets of A then $f^*(X \setminus Y) \subseteq f^*(X) \setminus f^*(Y)$.

4.44. Prove or disprove: If $f : A \to B$ and X and Y are subsets of A then $f^*(X) \setminus f^*(Y) \subseteq f^*(X \setminus Y)$.

4.45. Prove that the following two statements are equivalent:

(a) For every positive real number x there is a natural number n such that $\frac{1}{n} < x$.

(b) For every positive real number y there is a natural number n such that $n > y$.

Part (b) is known as the Archimedian property of real numbers and is one of the basic assumptions about the real numbers.

4.46. Prove that $\bigcup_{i\in\mathbb{N}}[0, i+1) = [0, \infty)$ (by showing that each set is a subset of the other.)

4.47. What is $\bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}]$? Prove your answer.

4.48. What is $\bigcap_{i\in\mathbb{N}}[1 - \frac{1}{i+1}, 1 + \frac{1}{i+1}]$?

4.49. What is $\bigcap_{i\in\mathbb{N}}[0, \frac{i}{i+1}]$?

4.50. Let $\mathcal{A} = \{\{1, 3, 5, 7, 9\}, \{2, 3, 7, 9, 11\}, \{3, 4, 9, 11\}\}$. Find $\bigcup \mathcal{A}$ and $\bigcap \mathcal{A}$.

4.51. What is $\bigcup\{[0, \frac{i}{i+1}] : i \in \mathbb{N}\}$?

Chapter 5

Mathematical Induction

5.1 Introduction

In its basic form mathematical induction is a principle which is used for proving that a sentence $P(n)$ is true for every n in the set $\mathbb{N} = \{0, 1, 2, \ldots\}$ of natural numbers. For example, as we'll see shortly, we could prove that "for every natural number n, $n^2 + n$ is even" using mathematical induction.

5.2 The Principle of Mathematical Induction

The principle of mathematical induction is one of the basic facts about the natural numbers.[1] It can be stated in several ways. We start with the version that makes an assertion about sets of natural numbers. In order to give this set theoretic version a definition is required.

Definition 5.1. A subset S of the set $\mathbb{R}$ of real numbers is called *an inductive set* if the following two conditions are met

1. $0 \in S$
2. $\forall k \in S$, $k + 1 \in S$

For example the set of all real numbers is inductive as is the set of real numbers greater than 0. Other examples of inductive sets are $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$.

The principle of mathematical induction is

5.2. (**The Principle of Mathemtaical Induction, Set Form**) If S is any inductive subset of $\mathbb{N}$ then $S = \mathbb{N}$.

[1] The Principle of Mathematical Induction can be proved using the well ordering property of the natural numbers. See Chapter 2., Axiom 1. There is an outline of the argument in Exercise 5.1. It is also possible to prove the well ordering property of $\mathbb{N}$ using the Principle of Mathematical Induction (see Exercise 5.2).

This is a precise statement of our intuitive feeling about the natural numbers that if you begin with zero and add 1 repeatedly then you will eventually obtain every natural number. Assume that S is an inductive set, then by the definition part 1, $0 \in S$. Since $0 \in S$ part 2 of the definition tells us (using Proof Principle 5) that $0 + 1 \in S$, that is, $1 \in S$. Since $1 \in S$, part 2 tells us that $1 + 1 \in S$, that is, $2 \in S$. Similarly, since $2 \in S$, $3 \in S$. If we repeatedly appeal to part 2 it seems that for every natural number n we should eventually have an argument that n is in S. This is what the Principle of Mathematical Induction says.

We could state this as a proof principle:

> If S is a subset of $\mathbb{N}$ then in order to prove $S = \mathbb{N}$ is is sufficient to prove that S is inductive. That is, it is sufficient to prove that
>
> 1. $0 \in S$ and
> 2. $\forall k \in S$, $k + 1 \in S$.

but a more useful form is stated in terms of sentences rather that sets.

Proof Principle 15. (The Principle of Mathematical Induction) Assume that $P(n)$ is a sentence with free variable n. Then in order to prove the statement "$\forall n \in \mathbb{N}$, $P(n)$" it is sufficient to prove

1. $P(0)$ **and**
2. $\forall k \in \mathbb{N}$**, If** $P(k)$ **then** $P(k + 1)$

□

Note that

1. Proof Principle 15 follows from the set form of the Principle of Mathematical Induction (5.2) by letting $S = \{n \in \mathbb{N} : P(n)\}$ for the sentence $P(n)$ with one free variable n. If you prove $P(0)$ then if follows that $0 \in S$. If you prove "$\forall k \in \mathbb{N}$, If $P(k)$ then $P(k + 1)$" it follows that "$\forall k \in S$, $k + 1 \in S$". Hence, if you have proved parts 1 and 2 of Proof Principle 15, you have shown that S is inductive. It follows from the set form of the Principle of Mathematical Induction that $S = \mathbb{N}$ and therefore $P(n)$ is true for all $n \in \mathbb{N}$.

2. A proof by mathematical induction will ordinarily have two parts: A proof of part 1 and a proof of part 2 in Proof Principle 15. The proof of part 1 will usually be easy. It may be no more than a matter of noting that $P(0)$ is true. We shall discuss the proof of part 2 more fully following the first example. For the time being we only note that it could be written (and frequently is written) without the explicit quantifier $\forall k \in N$ and with the understanding that the range of the variable k is $\mathbb{N}$. So we might see part 2 written as

$$\text{If } P(k) \text{ then } P(k + 1) \tag{5.1}$$

or

$$P(k) \text{ implies } P(k+1) \tag{5.2}$$

3. In proving $\forall n \in \mathbb{N}$, $P(n)$ by the Principle of Mathematical induction it is a common practice to use the same variable where we have used n and k.

4. Proving $\forall n \in \mathbb{N}$, $P(n)$ by mathematical induction is sometime referred to as proving the statement *by induction on* n.

5.3 Examples

Since many of our examples and exercises involve the concepts of "even" and "odd" for integers we recall the definitions.

Definition. (Definition 2.1) An integer n is *even* if there exists an integer k such that $n = 2k$. An integer n is *odd* if there exists an integer k such that $n = 2k + 1$.

We will also need the definition of "divides" given earlier as part of Exercise 2.30. We repeat it here

Definition 5.3. For all integers n and m, n *divides* m if and only if there is an integer k such that $m = nk$. "n divides m" is sometimes also expressed by saying "m is a multiple of m". The short hand notation for "n divides m" is $n \mid m$.

We begin our examples with

Example 5.4. Prove by mathematical induction that for every natural number n, $n^2 + n$ is even. In this example the sentence $P(n)$ is "$n^2 + n$ is even." Before beginning the proof we note that the three statements $P(0)$, $P(k)$ and $P(k+1)$ are respectively "$0^2 + 0$ is even", "$k^2 + k$ is even" and "$(k+1)^2 + (k+1)$ is even." Note especially that to obtain $P(k+1)$ we replaced n by $(k+1)$ (with $k+1$ enclosed in parentheses) in the statement $P(n)$.

Proof. Let $P(n)$ be the sentence "$\forall n \in \mathbb{N}$, $n^2 + n$ is even". We first note that $0^2 + 0 = 0 = 2 \cdot 0$ is even and therefore "$n^2 + n$ is even" is true when $n = 0$.

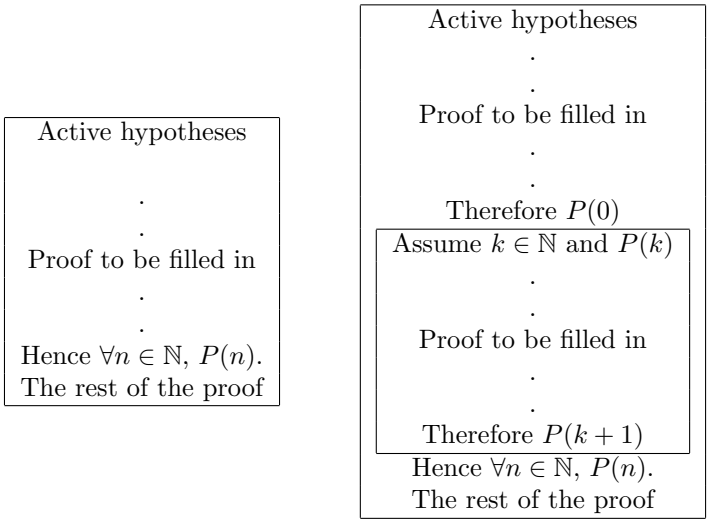
To show that $P(k)$ implies $P(k+1)$ is true (using Proof Principles 1 and 2) assume that $k \in \mathbb{N}$ and assume $P(k)$. This means that $k^2 + k$ is even so by the definition of *even*,

$$\exists t \in \mathbb{Z} \text{ such that } k^2 + k = 2t. \tag{5.3}$$

Using this to simplify $(k+1)^2 + (k+1)$ we obtain $(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = k^2 + k + 2k + 2 = 2t + 2k + 2 = 2(t + k + 1)$. Since $t + k + 1$ is an integer, this shows that $(k+1)^2 + (k+1)$ is even. Hence $P(k+1)$.

Since we have proved both $P(0)$ and "$P(k)$ implies $P(k+1)$" we conclude by the Principle of Mathematical Induction that $\forall n \in \mathbb{N}$, $P(n)$ is true. That is, $\forall n \in \mathbb{N}$, $n^2 + n$ is even. □

The "before" and "after" diagrams for a proof by mathematical induction would be



Note that a free variable (k in the diagram) is introduced using Proof Principle 1 and represents a *fixed* but unspecified natural number. Also note that the statements $k \in \mathbb{N}$ and $P(k)$ are added to the active hypotheses. The free variable k and the assumptions $k \in \mathbb{N}$ and $P(k)$ are only active for the proof of $P(k+1)$.

Example 5.5. Prove $\forall n \in \mathbb{N}$, $7^n - 13$ is a multiple of 6. (See Definition 5.3 for the meaning of the word 'multiple'.)

Proof. Let $P(n)$ be the sentence "$7^n - 13$ is a multiple of 6". For the basis step we note that $P(0)$ is the sentence "$7^0 - 13$ is a multiple of 6" which is true since $7^0 - 13 = -12 = (-2) \cdot (6)$.

For the induction step assume that $k \in \mathbb{N}$ and assume $P(k)$. Then $7^k - 13$ is a multiple of 6 and therefore

$$7^k - 13 = 6j \text{ for some integer } j \tag{5.4}$$

(We have to argue that $P(k+1)$ is true in other words that $7^{k+1} - 13$ is a multiple of 6.[2]) Note that

$$7^{k+1} - 13 = 7^k \cdot 7 - 13. \tag{5.5}$$

By equation (5.4), $7^k = 6j + 13$. Substituting $6j + 13$ for 7^k in equation (5.5) we obtain $7^{k+1} - 13 = (6j + 13) \cdot 7 - 13 = 42j + 6 \cdot 13 = 6(7j + 13) = 6i$ where i is the integer $7j + 13$. Therefore $7^{k+1} - 13$ is a multiple of 6.

By the principle of mathematical induction we conclude that $\forall n \in \mathbb{N}$, $7^n - 13$. □

[2]Recall that if any statement which still has to be proved appears in a proof then the fact that the statement still has to be proved must be clearly indicated.

Example 5.6. Prove $\forall n \in \mathbb{N}$, $2n < 3^n$.

Proof. Let $P(n)$ be the sentence $2n < 3^n$. Then $P(0)$ is "$2 \cdot 0 < 3^0$" which is true.

For the induction step assume that $k \in \mathbb{N}$ and $P(k)$, then

$$2k < 3^k \tag{5.6}$$

(We have to prove $P(k+1)$ which is the sentence $2(k+1) < 3^{k+1}$.) Note that

$$2(k+1) = 2k + 2. \tag{5.7}$$

By (5.6) we may conclude that $2k + 2 < 3^k + 2$. (We've added 2 to both sides of (5.6).) Combining this with equation (5.7) we get

$$2(k+1) < 3^k + 2 \tag{5.8}$$

Now we note that since $k \in \mathbb{N}$, $1 \leq 3^k$ so $2 \leq 2 \cdot 3^k$. Therefore (adding 3^k to both sides) we have $3^k + 2 \leq 3^k + 2 \cdot 3^k = 3 \cdot 3^k = 3^{k+1}$. Putting this together with equation (5.8) we get $2(k+1) < 3^{k+1}$.

By the principle of mathematical induction it follows that $\forall n \in \mathbb{N}$, $2n < 3^n$ □

Example 5.7. Prove $\forall n \in \mathbb{N}$, $n^2 < 3^n$.

Proof. Let $P(n)$ be the sentence $n^2 < 3^n$. Then $P(0)$ is "$0^2 < 3^0$" which is true.

For the induction step assume $k \in \mathbb{N}$ and $P(k)$ then

$$k^2 < 3^k. \tag{5.9}$$

(We have to prove $P(k+1)$ which is the sentence $(k+1)^2 < 3^{k+1}$.) Starting with the left hand side of $P(k+1)$ we have

$$(k+1)^2 = k^2 + 2k + 1. \tag{5.10}$$

By the previous example we know that $2k < 3^k$. Since $k \in \mathbb{N}$ we have that $1 \leq 3^k$. Adding these two inequalities and inequality (5.9) we obtain $k^2+2k+1 < 3^k + 3^k + 3^k = 3 \cdot 3^k = 3^{k+1}$. Therefore by (5.10), $(k+1)^2 < 3^{k+1}$.

By the principle of mathematical induction $\forall n \in \mathbb{N}$, $n^2 < 3^n$.

□

5.4 Variations of Mathematical Induction

5.4.1 Complete Induction

There are cases where the second step in a proof by mathematical induction is difficult. In these cases the following principle may be useful.

Proof Principle 16. (The Principle of Complete Induction) Assume that $P(n)$ is a sentence with free variable n. Then in order to prove the statement "$\forall n \in \mathbb{N}$, $P(n)$" it is sufficient to prove

1. $P(0)$ **and**
2. $\forall k \in \mathbb{N}$**, If** $\forall j \in \mathbb{N}$**, if** $j \leq k, P(j)$ **then** $P(k+1)$

□

Note that the difference between this and Proof Principle 15 is that in step 2, we would assume $\forall j \leq k, P(j)$ (that is, we would assume $P(0)$ and $P(1)$, and ... and $P(k)$) and using this assumption we would prove $P(k+1)$. This gives you more to work with that part 2 of The Principle of Mathematical Induction where you assume only $P(k)$.

Example 5.8. As an example, here is a proof of a theorem called the Division Algorithm using complete induction.[3]

The Division Algorithm is

> For all positive natural numbers d, $\forall x \in \mathbb{N}$, there are two natural numbers q and r such that $0 \leq r < d$ and $x = qd + r$.

Proof. Assume that d is a positive natural number. We'll prove using complete induction that "$\forall x \in \mathbb{N}$, there are two natural numbers q and r such that $0 \leq r < d$ and $x = qd + r$". Let $P(x)$ be the sentence "There are two natural numbers q and r such that $0 \leq r < d$ and $x = qd+r$". Then $P(0)$ is the sentence "there are two natural numbers q and r such that $0 \leq r < d$ and $0 = qd + r$". This is true since $q = r = 0$ fulfill the requirements.

Assume that $k \in \mathbb{N}$ and $\forall j \in \mathbb{N}$, if $j \leq x, P(j)$ (See item 2. above. We must argue that $P(x+1)$ is true). We'll consider two cases.

Case 1. $x + 1 < d$.

In this case we let $q = 0$ and $r = x + 1$. Then clearly $0 \leq r < d$ and $x + 1 = qd + r$.

Case 2. $x + 1 \geq d$.

In this case $x + 1 - d \geq 0$ so $x + 1 - d$ is a natural number. Also since $d > 0$, $x + 1 - d \leq k$. By our assumption, with $j = x + 1 - d$ we have $P(x + 1 - d)$. That is, there are two natural numbers q_0 and r_0 such that $0 \leq r_0 < d$ and $x + 1 - d = q_0 d + r_0$. Adding d to both sides of this equation gives us $x + 1 = (q_0 + 1)d + r_0$. Letting $q = q_0 + 1$ and $r = r_0$ we see that $x + 1 = qd + r$ and $0 \leq r < d$. Therefore $P(x + 1)$ is true. This completes the proof. □

Note that in proving $P(x + 1)$ we used $P(x + 1 - d)$. This was valid since our assumption was that $\forall j \in \mathbb{N}$, if $j \leq x$ then $P(j)$. Compare this with the original proof of the Division Algorithm where we had only the assumption $P(x)$ available to prove $P(x + 1)$.

[3] A (possibly) easier proof of the Division Algorithm can be given using the well ordering property of $\mathbb{N}$. See Axiom 1 in Chapter 2. See Exercise 5.18

5.4.2 Varying the starting point

It is also possible to prove a statement of the form "$\forall n \in \mathbb{Z}$, if $n \geq n_0$, then $P(n)$." where $P(n)$ is a sentence with one free variable n and n_0 is a specific integer using a variation of the Principle of Mathematical Induction.

Proof Principle 17. Assume that $P(n)$ is a sentence with free variable n and n_0 is a fixed integer. Then in order to prove the statement "$\forall n \in \mathbb{Z}$, If $n \geq n_0$, $P(n)$" it is sufficient to prove

1. $P(n_0)$ **and**
2. $\forall k \in \mathbb{Z}, k \geq n_0$**, If** $P(k)$ **then** $P(k+1)$

□

Example 5.9. We'll prove that for any integer $n \geq 7$, $5n + 7 \leq n^2$.

Proof. (We'll use Proof Principle 17. Here $n_0 = 7$ and $P(n)$ is the sentence $5n+7 \leq n^2$.) For part 1 we note that $P(7)$ is the statement $5 \cdot 7+7 \leq 7^2$ which is true.

For part 2 we assume that $k \in \mathbb{Z}$ and that $k \geq 7$ and that $5k + 7 \leq k^2$. (We have to prove $P(k+1)$, that is we have to prove $5(k+1)+7 \leq (k+1)^2$.) We first note that $5(k+1)+7 = 5k+5+7 = 5k+7+5 \leq k^2+5$, where the last inequality follows from our assumption of $P(k)$. Since $k \geq 7$, $5 < k < 2k < 2k + 1$ and therefore $k^2 + 5 \leq k^2 + 2k + 1 = (k + 1)^2$. It follows that $5(k + 1) + 7 \leq (k + 1)^2$ and we have completed part 2.

Therefore by the Principle of Mathematical Induction for every integer $n \geq 7$, $5n + 7 \leq n^2$. □

5.5 Definition by Recursion

In this section we look at a method which can sometimes be used to define a function whose domain is the set of natural numbers. Consider the three functions $\text{fac}(n) = n!$, $\exp_2(n) = 2^n$, and $\text{sumsqrs}(n) = \sum_{i=0}^{n} i^2$. These three functions are frequently defined by equations as follows: $\text{fac}(n) = n! = n(n-1)(n-2)\cdots 1$, $\exp_2(n) = 2^n = \underbrace{2 \cdot 2 \cdots 2}_{n \text{ factors}}$, and $\text{sqrsum}(n) = \sum_{i=0}^{n} i^2 = 0^2 + 1^2 + 2^2 + \cdots + n^2$ with the additional stipulations that $0! = 1$ and $2^0 = 1$. In each case the three dots $\cdots$ (called the ellipsis) have been used. Their meaning is approximately the same here as it was when they were used in Chapter 3, namely "continue the pattern that has been established until you reach". We also encounter the same problem here that we encountered there, there is a possibility that the intended pattern may be misinterpreted. Definition by recursion is an alternative to the three dots which eliminates the possibility for ambiguity.

First consider the function fac. There are two important facts about this function. The first,

$$\text{fac}(0) = 0! = 1 \tag{5.11}$$

is part of the definition given above. The second important fact gives an easy way of calculating $\text{fac}(k+1) = (k+1)!$ if $\text{fac}(k) = k!$ has been calculated:

$$\forall k \in \mathbb{N}, \text{fac}(k+1) = (k+1)\text{fac}(k) \text{ or } (k+1)! = (k+1)(k!) \tag{5.12}$$

(If fac is defined using the three dots then (5.12) would probably be considered to be an obvious property of the function fac.) The definition by recursion of the function fac simply uses (5.11) and (5.12). That is,

Definition 5.10. fac is the function from $\mathbb{N}$ to $\mathbb{N}$ defined by the formulas

1. $\text{fac}(0) = 1$ and
2. $\forall k \in \mathbb{N}, \text{fac}(k+1) = (k+1)\text{fac}(k)$

Note the following:

- We have defined the function fac without giving an explicit formula in terms of n for calculating $\text{fac}(n)$. However, $\text{fac}(n)$ can be calculated for any natural number n using 1. and 2. of definition 5.10. For example, to calculate $\text{fac}(5)$ we would start with part 1. to get $\text{fac}(0) = 1$. Then using part 2. with $k = 0$ would give us $\text{fac}(1) = \text{fac}(0+1) = 1 \cdot \text{fac}(0) = 1 \cdot 1 = 1$. Using part 2. with $k = 1$ gives $\text{fac}(2) = \text{fac}(1+1) = 2 \cdot \text{fac}(1) = 2 \cdot 1 = 2$. Then with $k = 2$, part 2. gives $\text{fac}(3) = \text{fac}(2+1) = 3 \cdot \text{fac}(2) = 3 \cdot 2$. Using part 2. with $k = 3$ in a similar way gives $\text{fac}(4) = 4 \cdot \text{fac}(3) = 24$ and finally with $k = 4$, part 2. gives $\text{fac}(5) = 5 \cdot 24 = 120$.

- The notation fac for the factorial function is our abbreviation. Definition 5.10 would ordinarily use the ! notation and would appear as

  Definition 5.11. $n!$ is defined for all natural numbers n by the two formulas

  1. $0! = 1$ and
  2. $\forall k \in \mathbb{N}$, $(k+1)! = (k+1)(k!)$

- The Recursion Theorem (given below) is what justifies defining a function by recursion. It says that there is one and only one function fac with domain $\mathbb{N}$ for which 1 and 2 are true.

We give two versions of the Recursion Theorem, one informal and the other more precise.

Theorem. ***The Recursion Theorem, Informal Version.*** *You can define a function f whose domain is $\mathbb{N}$ by giving two things:*

1. *A value for $f(0)$ and*
2. *A method for calculating $f(k+1)$ which works for every natural number k and which may us $f(k)$ and k as inputs.*

Definition 5.10 gives the two things required by the Recursion Theorem, namely a value for fac(0) and a formula for calculating fac$(k+1)$ in terms of k and fac(k).

As a second example the function $\exp_2$ could be defined by

Definition 5.12. $\exp_2$ is the function from $\mathbb{N}$ to $\mathbb{N}$ defined by

1. $\exp_2(0) = 1$ and
2. $\forall k \in \mathbb{N}$, $\exp_2(k+1) = 2 \cdot \exp_2(k)$.

Or using the usual exponent notation

Definition 5.13. The function "2^n" from $\mathbb{N}$ to $\mathbb{N}$ is defined by

1. $2^0 = 1$ and
2. $\forall k \in \mathbb{N}$, $2^{k+1} = 2 \cdot 2^k$.

As a third example the definition of the function sumsqrs by recursion would be

Definition 5.14. sumsqrs is the function from $\mathbb{N}$ to $\mathbb{N}$ defined by recursion as follows:

1. sumsqrs$(0) = 0$ and
2. $\forall k \in \mathbb{N}$, sumsqrs$(k+1) =$ sumsqrs$(k) + (k+1)^2$.

or using the $\sum$ notation

Definition 5.15. $\sum_{i=0}^{n} i^2$ is the function from $\mathbb{N}$ to $\mathbb{N}$ defined by recursion as follows:

1. $\sum_{i=0}^{0} = 0$ and
2. $\forall k \in \mathbb{N}$, $\sum_{i=0}^{k+1} i^2 = \left(\sum_{i=0}^{k} i^2\right) + (k+1)^2$.

More generally the $\sum$ notation and the $\prod$ notation whose definitions using the three dots are respectively $\sum_{i=0}^{n} g(i) = g(0) + g(1) + \cdots + g(n)$ and $\prod_{i=1}^{n} g(i) = g(0) \cdot g(1) \cdot g(2) \cdots g(n)$ (where g is some function whose domain includes $\mathbb{N}$.) May be defined by recursion as follows:

Definition 5.16. Assume that g is a function whose domain includes $\mathbb{N}$ then

1. $\sum_{i=0}^{n} g(i)$ is defined by recursion using the following two equations
   (a) $\sum_{i=0}^{0} g(i) = g(0)$
   (b) $\forall k \in \mathbb{N}$, $\sum_{i=0}^{k+1} g(i) = \left(\sum_{i=0}^{k} g(i)\right) + g(k+1)$
2. $\prod_{i=0}^{n} g(i)$ is defined by recursion using the following two equations

(a) $\prod_{i=0}^{0} g(i) = g(0)$

(b) $\forall k \in \mathbb{N}, \prod_{i=0}^{k+1} g(i) = \left(\prod_{i=0}^{k} g(i)\right) \cdot g(k+1)$

Definition 5.15 is a special case of 5.16 with $g(i) = i^2$. Here's another example, $\sum_{i=0}^{n} i^3$ is defined by the two equations

1. $\sum_{i=0}^{0} = 0^3 = 0$ and
2. $\sum_{i=0}^{k+1} i^3 = \left(\sum_{i=0}^{k} i^3\right) + (k+1)^3$.

In this example the function g is the function from $\mathbb{N}$ to $\mathbb{N}$ defined by $g(n) = n^3$.

Similarly, $\sum_{i=0}^{n} \frac{i}{i+1}$ is defined by the equations

1. $\sum_{i=0}^{0} \frac{i}{i+1} = \frac{0}{0+1} = 0$ and
2. $\sum_{i=0}^{k+1} \frac{i}{i+1} = \left(\sum_{i=0}^{k} \frac{i}{i+1}\right) + \frac{(i+1)}{1+(i+1)}$.

When proving theorems about functions defined by recursion, it is frequently the case that mathematical induction works well. For example:

Theorem 5.17. $\forall n \in \mathbb{N}, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Proof. We are going to prove $\forall n \in \mathbb{N}, P(n)$ where $P(n)$ is the sentence "$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.". $P(0)$ is the equation whose left hand side is $\sum_{i=0}^{0} i$ which by definition is equal to 0 and whose right hand side is $\frac{0 \cdot 1}{2} = 0$. It follows that $P(0)$ is true.

For the second step in the induction proof, assume that $k \in \mathbb{N}$ and that $P(k)$. This means that $k \in \mathbb{N}$ and

$$\sum_{i=0}^{k} i = \frac{k(k+1)}{2} \tag{5.13}$$

We must prove $P(k+1)$, that is we must prove

$$\sum_{i=0}^{k+1} i = \frac{(k+1)((k+1)+1)}{2}. \tag{5.14}$$

Working with the left hand side of (5.14) using definition 1 we get

$$\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + (k+1) \tag{5.15}$$

Using the assumption (5.13) this is equal to $\frac{(k(k+1)}{2} + (k+1)$. Adding and simplifying we obtain $\frac{(k+1)(k+2)}{2}$ which is equal to the right hand side of (5.14). This completes the proof of $P(k+1)$ and the proof of the theorem. □

Note that if you were using the "three dots" definition of the $\sum$ notation then equation (5.15) in the proof above would be considered to be an obvious consequence of the (three dots) definition.

The precise version of the Recursion Theorem is

Theorem 5.18. *Recursion Theorem Assume we are given the following: A set A, an element $a_0 \in A$ and a function $h : \mathbb{N} \times A \to A$. Then there is one and only one function $f : \mathbb{N} \to A$ with the following properties*

1. $f(0) = a_0$
2. $\forall k \in \mathbb{N},\ f(k+1) = h(k, f(k))$

To justify the definition of the function fac above we would use the formal version of the Recursion Theorem with $A = \mathbb{N}$, $a_0 = 1$ and $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $h(x, y) = (x+1)y$. Note that the formula for the function h is chosen so that it gives $(k+1)f(k)$ when x is replaced by k and y is replaced by $f(k)$.

To say this all more formally: Let $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be defined by $h(x, y) = (x+1)y$. Then, by the Recursion Theorem (formal version), there is a unique function $f : \mathbb{N} \to \mathbb{N}$ for which $f(0) = 1$ and $\forall k \in \mathbb{N},\ f(k+1) = h(k, f(k)) = (k+1)f(k)$. This unique f is the factorial function.

A proof of the formal version of the Recursion Theorem is outlined in the exercises. See exercises 5.31 to 5.36.

5.6 Exercises

5.1. Prove the set form of the Principle of Mathematical Induction (5.2) using the Well Ordering Property of $\mathbb{N}$ (Axiom 1. (Hint: Let S be an inductive set of natural numbers. Prove that $S = \mathbb{N}$ by contradiction: If $S \neq \mathbb{N}$ then, by the Well Ordering Property of $\mathbb{N}$, the set $\{n \in \mathbb{N} : n \notin S\}$ has a least element.)

5.2. Prove the Well Ordering Property of $\mathbb{N}$ using the set form of the Principle of Mathematical Induction. (Hint: Assume that S is a set of natural numbers without a least element. Use the Principle of Mathematical Induction to show that $\{n \in \mathbb{N} : \forall k \in \mathbb{N},\ \text{if } k \leq n \text{ then} k \neq S\} = \mathbb{N}$ and therefore that $S = \emptyset$.)

5.3. Prove by mathematical induction that $\forall n \in \mathbb{N}$, $9n^2 + 3n$ is even.

5.4. Prove by mathematical induction that $\forall n \in \mathbb{N}$, $25n^2 + 5n$ is even.

5.5. Prove the following facts about integers using definition 2.1:

(a) If m and n are even integers then $m + n$ is even.

(b) If m and n are odd integers then $m + n$ is even.

(c) If m is an even integer and n is an odd integer then $m + n$ is odd.

(d) If m and n are odd integers then mn is odd.

(e) If m is an even integer and n is an integer then mn is even.

5.6. Give a (non-induction) proof of $\forall n \in \mathbb{N}$, $9n^2 + 3n$ is even (from exercise 5.3) using proof by cases. (Hint: By Corollary 2.5, if n is an integer then either n is even or n is odd.)

5.7. Give a non-induction proof of $\forall n \in \mathbb{N}$, $25n^2 + 5n$ is even (from exercise 5.4). See the hint given for the problem above.

5.8. Prove by mathematical induction that $\forall n \in \mathbb{N}$, $n^3 + 2n$ is a multiple of 3. (Use the definition $m \in \mathbb{Z}$ is a multiple of 3 if $\exists r \in \mathbb{Z}$ such that $m = 3r$.)

5.9. Prove that by mathematical induction that $\forall n \in \mathbb{N}$, $2n^3 + n$ is a multiple of 3.

5.10. By the Division Algorithm, there are natural numbers q and r such that $0 \leq r < 20$ and $257 = 20q + r$. What are q and r.

5.11. Prove by contradiction that no integer is both even and odd. You may use the fact that $\frac{1}{2}$ is not an integer.

5.12. Prove by mathematical induction that $\forall n \in \mathbb{N}$, $n \leq 2^n$.

5.13. Prove by mathematical induction: $\forall n \in \mathbb{N}$, $16^n - 1$ is a multiple of 15.

5.14. Prove by mathematical induction that $\forall n \in \mathbb{N}$, $16^n + 2$ is a multiple of 3.

5.15. Prove by the principle of mathematical induction that $\forall n \in \mathbb{N}$, $13^n + 5$ is a multiple of 6.

5.16. Prove by mathematical induction that $\forall n \in \mathbb{N}$, $15^n - 1$ is a multiple of 7.

5.17. Prove by mathematical induction: $\forall n \in \mathbb{N}$, $2 \cdot 15^n + 2$ is a multiple of 4.

5.18. Use the well ordering property of $\mathbb{N}$ to prove the Division Algorithm. (Hint: The Division Algorithm is "For all positive natural numbers d, $\forall x \in \mathbb{N}$, there are two natural numbers q_1 and r_1 such that $0 \leq r_1 < d$ and $x = q_1 d + r_1$." Assume x and d are integers and $d \geq 0$. Let $S = \{r : r > 0$ and $\exists q \in \mathbb{Z}$ such that $r = x - qd\}$.)

5.19. Prove by mathematical induction that for every $n \in \mathbb{Z}$, if $n \geq 1$ then $n < 2^n$.

5.20. Prove by mathematical induction that for every $n \in \mathbb{Z}$, if $n \geq 7$ then $6n + 4 < n^2$.

5.21. Prove by mathematical induction that for every $n \in \mathbb{Z}$, if $n \geq 3$ then $3n^2 \leq n^3$.

5.22. Prove by mathematical induction that for every $n \in \mathbb{Z}$, if $n \geq 10$ then $n^3 < 2^n$.

5.23. Prove by mathematical induction that for $n \geq 3$, $3^n + 4^n < 5^n$.

5.24. Prove that for every real number $x \geq 1$, $\forall n \in \mathbb{N}, (1 + x)^n \geq 1 + nx$.

5.25. According to the definition of the $\sum$ notation what is $\sum_{i=0}^{k+1}(i + i^2)$?

5.26. Prove by mathematical induction that for any real number $x \neq 1$ and for every natural number n, $\sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}$.

5.27. Prove that for every natural number n, $\sum_{i=0}^{n}(2i+1) = (n+1)^2$.

5.28. Prove by induction that $\forall n \in \mathbb{Z}$, If $n \geq 4$ then $n! > 2^n$.

5.29. Prove that for all integers $n \geq 1$, $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

5.30. In order to use the Recursion Theorem to justify the definition of the function fac we used $A = \mathbb{N}$, $a_0 = 1$ and $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $h(x, y) = (x + 1)y$. (See the discussion following the formal version of the Recursion Theorem, Theorem 5.18) What set A, what element a_0 of A and what function h should be used to justify the definitions of the following function using the formal version of the Recursion Theorem?

(a) The function $\exp_2 : \mathbb{N} \to \mathbb{N}$ defined at the beginning of Section 5.5.

(b) The function sumsqrs : $\mathbb{N} \to \mathbb{N}$ defined at the beginning of Section 5.5.

A proof of the Recursion Theorem is outlined in exercises 5.31 through 5.36. For these exercises assume that A is a set, $a_0 \in A$ and h is a function from $\mathbb{N} \times A$ into A (the hypotheses of the Recursion Theorem). Also for these exercises we will use the following definitions

Definition 5.19. 1. For each $n \in \mathbb{N}$ let $\mathbb{N}_n$ be the set $\{k \in \mathbb{N} : k \leq n\}$

2. A function g is *good* if for some $n \in \mathbb{N}$, $g : \mathbb{N}_n \to A$, $g(0) = a_0$ and $\forall k \in \mathbb{N}$, if $k < n$ then $g(k + 1) = h(k, g(k))$.

   Note that if g is good and $k \in \mathrm{Dom}(g)$ then for every $i < k$, if $i \in \mathbb{N}$ then $i \in \mathrm{Dom}(k)$.

5.31. Prove that if f_1 and f_2 are functions from $\mathbb{N}$ to $\mathbb{N}$ for which $f_1(0) = a_0$, $f_2(0) = a_0$, $\forall k \in \mathbb{N}$, $f_1(k + 1) = h(k, f_1(k))$ and $\forall k \in \mathbb{N}$, $f_2(k + 1) = h(k, f_2(k))$ then $f_1 = f_2$. This is the "only one" part of the Recursion Theorem. (Hint: Use Theorem 4.6, part 2 and use mathematical induction to show that $\forall k \in \mathbb{N}$, $f_1(k) = f_2(k)$.)

5.32. Prove by mathematical induction that $\forall n \in \mathbb{N}$ the following statement is true:

for all good g_1 and g_2, if $n \in \mathrm{Dom}(g)_1 \cap \mathrm{Dom}(g)_2$ then $g_1(n) = g_2(n)$.

5.33. Define f by $f = \{(n, y) :$ there is a good g such that $n \in \mathrm{Dom}(g)$ and $g(n) = y\}$. Prove that f is a function. (Hint: Assume (n, y_1) and (n, y_2) are in f. It must be shown that $y_1 = y_2$. It follows from the assumption that there are two good functions g_1 and g_2 such that $g_1(n) = y_1$ and $g_2(n) = y_2$.)

5.34. Show $\{(0, a_0)\}$ is good. Note $\{(0, a_0)\}$ is the function f with domain $\{0\}$ such that $f(0) = a_0$.

5.35. Prove by mathematical induction $\forall n \in \mathbb{N}$, there is a good function g such that $\text{Dom}(g) = \mathbb{N}_n$. (Hint: For $n = 0$ use the previous exercise. For the second step in the proof, prove that if g is good and $\text{Dom}(g) = \mathbb{N}_k$ then $g' = g \cup \{(k+1, h(k, g(k)))\}$ is good.)

5.36. Prove that for the function f defined in Exercise 5.33 that the following are true:

(a) $f(0) = a_0$

(b) $f : \mathbb{N} \to A$

(c) $\forall k \in \mathbb{N}$, $f(k+1) = h(k, f(k))$.

Chapter 6

Cardinal Numbers and Cantor's Continuum Hypothesis

6.1 Introduction and Definitions

The German mathematician Georg Cantor who lived from 1845 to 1918 proposed a method of comparing the sizes of infinite sets. His idea was to use the same "definition" of size used for finite sets. The definition of "cardinal number" expresses this idea.

Definition 6.1. Assume that A and B are sets

1. *A and B have the same cardinal number* (In symbols $|A| = |B|$.) if there is a one to one function from A onto B.

2. *The cardinal number of A is less than or equal to the cardinal number of B* (In symbols $|A| \leq |B|$.) if there is a one to one function from A into B.

The notation and terminology that we have introduced in these definitions is standard but it may be a little confusing because we have not defined for each set A something called the cardinal number of A.

It is possible to give such a definition, for example the cardinal number of a finite set A is the natural number n where n is the number of elements in A. But a general definition that works for every set A, although possible, is more difficult. We are going to postpone giving this definition until our chapter on axiomatic set theory. For the time being we will simply think of the expression $|A| \leq |B|$ as an abbreviation for the sentence "There is a one to one function from A into B." Similarly, for our purposes, the sentence "$|A| = |B|$" does not assert that two objects are equal but is simply an abbreviation for "There is a

one to one function from A onto B."[1]

Two examples: First $[2,3] \leq [1,7]$ because the function $f : [2,3] \to [1,7]$ defined by $f(x) = x$ is one to one. Secondly, $[2,3] = [3,4]$ because the function $f : [2,3] \to [3,4]$ defined by $f(x) = x + 1$ is one to one and onto $[3,4]$.

Looking at the definition, if A and B are sets and you want to argue that $|A| \leq |B|$ there are ordinarily two steps.

1. Define a function $f : A \to B$. In many instances it will be obvious that $\text{Dom}(f) = A$ and $\text{Range}(f) \subseteq B$ but one or both of these assertions may require a proof.

2. Prove that f is one to one

Similarly, to prove that $|A| = |B|$ we would usually:

1. Define a function $f : A \to B$.

2. Prove that f is onto B.

3. Prove that f is one to one.

In many cases, for both kinds of proofs, the hardest part will be finding a function f that works and this is likely to be more difficult for showing $|A| = |B|$ than for showing $|A| \leq |B|$. We illustrate by proving that $[2,3] = [1,7]$. We've shown above that $[2,3] \leq [1,7]$ and the one to one function from $[2,3]$ into $[1,7]$ was fairly easy to find. Before we begin the proof of the equality we discuss the reasoning that we follow to find a one to one function f from $[2,3]$ onto $[1,7]$. We are going to try for a linear function f such that $f(2) = 1$ and $f(3) = 7$. This means that the graph will go through the points $(2,1)$ and $(3,7)$. It will therefore have slope $\frac{7-1}{3-2} = 6$. Therefore the formula for $f(x)$ will be $f(x) = 6x + b$. Replacing x by 2 and $f(x)$ by 1 we get $1 = 12 + b$. Therefore $b = -11$. So the function that should work is $f(x) = 6x - 11$. Now the proof.

Define the function f with domain $[2,3]$ by $f(x) = 6x-11$. We first show that f is onto $[1,7]$ by showing that $\text{Range}(f) = [1,7]$. To show that $\text{Range}(f) \subseteq [1,7]$ (see Theorem 4.6 part 1.) we assume that $x \in \text{Dom}(f) = [2,3]$ and show that $f(x) \in [1,7]$. Since $2 \leq x \leq 3$, $12 \leq 6x \leq 18$. Subtracting 11 gives $1 \leq 6x - 11 \leq 7$. Therefore $1 \leq f(x) \leq 7$. So $f(x) \in [1,7]$. For the proof that $[1,7] \subset \text{Range}(f)$ assume that $y \in [1,7]$. Let $x = \frac{y+11}{6}$. Then since $1 \leq y \leq 7$, $12 \leq y + 11 \leq 18$. Dividing by 6 we get $2 \leq \frac{y+11}{6} \leq 3$. So $2 \leq x \leq 3$. Further $f(x) = 6x - 11 = 6\left(\frac{y+11}{6}\right) - 11 = y$. This shows that $y \in \text{Range}(f)$. We have therefore shown that $\text{Range}(f) = [1,7]$. Now we complete the proof that $[2,3] = [1,7]$ by showing that f is one to one. Assume $f(x_1) = f(x_2)$ then $6x_1 - 11 = 6x_2 - 11$ and therefore $x_1 = x_2$.

[1] In order to avoid this confusion some authors use the notation $A \approx B$ (or $A \sim B$) rather than $|A| = |B|$.

6.2 Elementary Properties of Cardinal Numbers

Here are some properties of "less than or equal to" and "equal to" for cardinal numbers whose proofs are easy. Note that items 2 through 4 are not simply properties of equality since the sentence "$|X| = |Y|$" does not assert that two objects are equal but is short hand for the sentence "There is a one to one function from X onto Y."

Theorem 6.2. *Assume that A, B and C are sets then*

1. *If $|A| \leq |B|$ and $|B| \leq |C|$ then $|A| \leq |C|$.*
2. *If $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$.*
3. *If $|A| = |B|$ then $|B| = |A|$.*
4. *$|A| = |A|$.*
5. *If $A \subseteq B$ then $|A| \leq |B|$.*
6. *If $|A| = |B|$ then $|A| \leq |B|$.*

Proof. We prove 1 and leave the proofs of the remaining parts for the exercises. Assume $|A| \leq |B|$ and $|B| \leq |C|$, then there are one to one functions f from A into B and g from B into C. By Theorem 4.15 part 1, $g \circ f$ is a one to one function from A to C. Therefore $|A| \leq |C|$. □

We give some more examples.

Example 6.3.

1. $|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|$ because the function $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ defined by $f(n) = n + 1$ is one to one and onto $\mathbb{N} \setminus \{0\}$.
2. $|\mathbb{N}| = |\mathbb{Z}|$. We will define a one to one function f from $\mathbb{N} \to \mathbb{Z}$ by cases. For $n \in \mathbb{N}$ let $f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{(n+1)}{2} & \text{if } n \text{ is odd} \end{cases}$. Since f is defined by cases the arguments that f has the required properties will be by cases. For example, to show that $\text{Range}(f) \subseteq \mathbb{Z}$ assume that $n \in \text{Dom}(f) = \mathbb{N}$. If n is even then $f(n) = \frac{n}{2}$ is clearly in $\mathbb{Z}$. Similarly, if n is odd then $f(n) = -\frac{(n+1)}{2} \in \mathbb{Z}$. To argue that f is one to one, assume that $f(n) = f(m)$. There are four possible cases.

   Case 1. n is even and m is odd. Then, since $f(n) = f(m)$, $\frac{n}{2} = -\frac{(m+1)}{2}$. But this isn't possible since $\frac{n}{2} \geq 0$ and $-\frac{(m+1)}{2} < 0$.

   Case 2. n is odd and m is even. In this case the argument is almost identical to the argument given in case 1.

   Case 3. n and m are both even. In this case, since $f(n) = f(m)$, $\frac{n}{2} = \frac{m}{2}$ and hence $n = m$.

   Case 4. n and m are both odd. In this case $-\frac{(n+1)}{2} = -\frac{(m+1)}{2}$ from which it follows that $n = m$.

3. $|\mathbb{Z}| \leq |\mathbb{Q}|$
4. $|\mathbb{Q}| \leq |\mathbb{R}|$
5. $|[0,1)| \leq |[0,1]|$.

   The previous three examples use Theorem 6.2 part 5.

6. $|[0,1]| = |[0,1)|$. Here again we define a one to one function f from $[0,1]$ to $[0,1)$ by cases. For $x \in [0,1]$ we let

$$f(x) = \begin{cases} \frac{1}{n+1} & \text{if } x = \frac{1}{n} \text{ where } n \text{ is a positive integer} \\ x & \text{otherwise} \end{cases}$$

   As can be seen from the definition $f(1) = \frac{1}{2}$, $f(\frac{1}{2}) = \frac{1}{3}$, $f(\frac{1}{3}) = \frac{1}{4}$ and in general for every positive integer n, $f(\frac{1}{n}) = \frac{1}{n+1}$. We leave the proof that f is a one to one function from $[0,1]$ onto $[0,1)$ for the exercises (exercises 6.5 and 6.6.)

6.3 The Cantor-Bernstein Theorem

In Example 6.3, part 5 that the cardinal inequality $|[0,1)| \leq |[0,1]|$ is easy to prove. It is also reasonably easy to prove that $|[0,1]| \leq |[0,1)|$ (using the function $f(x) = \frac{1}{2}x$, for example.) On the other hand the proof that $|[0,1]| = |[0,1)|$ which we outlined in part 6 of example 6.3 is more difficult. It would simplify matters if for all sets A and B, $|A| = |B|$ followed from $|A| \leq |B|$ and $|B| \leq |A|$. This is the content of the following theorem.

Theorem 6.4. *(Cantor-Bernstein Theorem) For all sets A and B, if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.*

Proof.

Lemma 6.5. *If C and A are sets for which $|A| \leq |C|$ and $C \subseteq A$ then $|A| = |C|$.*

Note that this is a special case of the Cantor-Bernstein Theorem since $C \subseteq A$ implies $|C| \leq |A|$. *Proof.* Assume the hypotheses and let f be a one to one function from A into C. We begin by defining two sequences of sets by recursion. (See section 5.5.) Let $A_0 = A$ and for every natural number k, $A_{k+1} = f^*(A_k)$. Similarly we define $C_0 = C$ and for every natural number k, $C_{k+1} = f^*(C_k)$. (See Section 4.6 for the definition of f^*.) We first note that since Range$(f) \subseteq C$, $A_k \subseteq C$ for $k \geq 1$.

Secondly, we note that

$$\text{for all } n \in \mathbb{N}, f^*(A_n \setminus C_n) = A_{n+1} \setminus C_{n+1}. \tag{6.1}$$

This is a consequence of facts that $f^*(A_n) = A_{n+1}$, $f^*(C_n) = C_{n+1}$ and f is one to one and uses the result of exercise 6.10 from which it follows that $f^*(A_n \setminus C_n) = f^*(A_n) \setminus f^*(C_n)$.

Define the function g with domain A as follows:

$$g(x) = \begin{cases} f(x) & \text{if } x \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n) \\ x & \text{if } x \in A \setminus \left(\bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)\right) \end{cases}$$

We will prove that g is a one to one function from A onto C.

To argue that $\text{Range}(g) \subseteq C$ assume that $x \in A$. Then x is either in $A \setminus C$ or x is in C. If $x \in A \setminus C$ then $x \in A_0 \setminus C_0 \subseteq \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)$ so $g(x) = f(x) \in C$ since $\text{Range}(f) = C$. If $x \in C$ then $g(x)$ is either $f(x)$ or x and in either case $g(x) \in C$.

For the argument that $C \subseteq \text{Range}(g)$ assume that $y \in C$. If $y \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)$ then, since $A_0 \setminus C_0 = A \setminus C$, y must be in $A_n \setminus C_n$ for some $n \geq 1$. Since $A_n = f^*(A_{n-1})$, it must be the case that $y = f(x)$ for some $x \in A_{n-1}$. Hence $y \in \text{Range}(g)$. On the other hand if $y \notin \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)$ then $g(y) = y$ so in this case also $y \in \text{Range}(g)$.

As a preliminary to showing that g is one to one we note that if for some $n_0 \in \mathbb{N}$, $x \in A_{n_0} \setminus C_{n_0}$ then $g(x) = f(x) \in f^*(A_{n_0} \setminus C_{n_0}) = A_{n_0+1} \setminus C_{n_0+1}$. Where the last equality uses (6.1). This shows that

$$\forall x \in A, \text{ if } x \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n), \text{ then } g(x) \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n). \tag{6.2}$$

Similarly

$$\forall x \in A, \text{ if } x \in A \setminus (\bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)), \text{ then } g(x) = x \in A \setminus (\bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)) \tag{6.3}$$

To show that g is one to one assume x_1 and x_2 are in $\text{Dom}(g) = A$ and that $g(x_1) = g(x_2)$. Then either $x_1 \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)$ or $x \in A \setminus (\bigcup_{n\in\mathbb{N}}(A_n \setminus C_n))$. In the first case, by (6.2), $g(x_1) \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)$. Hence $g(x_2) \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)$. Therefore, using (6.3) and an easy proof by contradiction, $x_2 \in \bigcup_{n\in\mathbb{N}}(A_n \setminus C_n)$. By the definition of g we see that $g(x_1) = f(x_1)$ and $g(x_2) = f(x_2)$ and therefore $f(x_1) = f(x_2)$. Since f is one to one we conclude that $x_1 = x_2$. In the second case (where $x_1 \in A \setminus (\bigcup_{n\in\mathbb{N}}(A_n \setminus C_n))$ we can argue in a similar way that $x_2 \in A \setminus (\bigcup_{n\in\mathbb{N}}(A_n \setminus C_n))$. It follows from the definition of g in this case that $g(x_1) = x_1$ and $g(x_2) = x_2$. And hence $x_1 = x_2$. This completes the proof that g is one to one and therefore completes the proof of the lemma. □

To prove Theorem 6.4 assume that A and B are sets for which $|A| \leq |B|$ and $|B| \leq |A|$. Then there is a one to one function h from B into A. Let $C = \text{Range}(h)$. The function h is a one to one function from B onto C and therefore $|C| = |B|$. It follows from Theorem 6.2 that $|A| \leq |C|$. Since $C \subseteq A$ we may use the lemma to conclude that $|A| = |C|$, hence by Theorem 6.2 part 2, $|A| = |B|$. □

6.4 Using The Cantor-Bernstein Theorem

In example 6.3 we saw several examples of cardinal inequalities that will be useful in conjunction with the Cantor-Berstein theorem. We begin this section with a few more.

Example 6.6. 1. $|\mathbb{R}| = |(0,1)|$. (Note that $(0,1)$ denotes the interval.) We prove this by using the function $f : (0,1) \to \mathbb{R}$ defined by $f(x) = \frac{-1}{x} + \frac{1}{1-x}$. We shall prove that f is onto $\mathbb{R}$ and leave the proof that f is one to one for the exercises (See exercises 6.7 through 6.9.)

To prove that f is onto $\mathbb{R}$ assume $y \in \mathbb{R}$. We need to find an $x \in (0,1)$ such that $f(x) = y$. We do this by considering two cases.

Case 1. $y = 0$. In this case we let $x = \frac{1}{2}$. Then $x \in (0,1)$ and a simple calculation shows that $f(x) = y$.

Case 2. $y \neq 0$. In this case we let $x = \frac{y-2+\sqrt{4+y^2}}{2y}$. (This x was obtained by solving the equation $y = \frac{-1}{x} + \frac{1}{1-x}$ for x and simplifying.) since $4 + y^2 > 0$, x is a real number. It is also straightforward algebra to show that $f(x) = y$. It remains to prove that $0 < x < 1$. We do this by considering two subcases.

Subcase a. $y > 0$. In this case $x = \frac{y-2+\sqrt{4+y^2}}{2y} > \frac{-2+\sqrt{4+y^2}}{2y} > 0$. The last of these inequalities is true because both the numerator and denominator of $\frac{-2+\sqrt{4+y^2}}{2y}$ are positive. We argue that $x < 1$ by contradiction. Suppose that $x \geq 1$. Then $\frac{y-2+\sqrt{4+y^2}}{2y} \geq 1$. Multiplying both sides by $2y$ and solving for the square root gives $\sqrt{4+y^2} \geq y + 2$. Squaring both sides gives the inequality $4 + y^2 \geq y^2 + 2y + 4$ which is false since y is positive.

Subcase b. $y < 0$. We first argue that $y - 2 + \sqrt{4+y^2} < 0$ by contradiction. If $y-2+\sqrt{4+y^2} \geq 0$ then $\sqrt{4+y^2} \geq 2-y$. Squaring both sides (since both sides must be positive) we get $4 + y^2 \geq 4 - 4y + y^2$. This is impossible since $-4y$ is positive. Now dividing both sides of the inequality $y - 2 + \sqrt{4+y^2} < 0$ by the negative quantity $2y$ gives $\frac{y-2+\sqrt{4+y^2}}{2y} > 0$ and hence $x > 0$. The proof that $x < 1$ is also by contradiction. Assume that $x \geq 1$ then $\frac{y-2+\sqrt{4+y^2}}{2y} \geq 1$. Multiplying both sides by the (negative) quantity $2y$ and solving for the square root gives $\sqrt{4+y^2} \leq y + 2$. Squaring both sides we get $4 + y^2 \leq y^2 + 4y + 4$ which is impossible since $4y < 0$.

This completes the proof that f is onto $\mathbb{R}$.

2. For any two real numbers a and b, if $a < b$ then $|(0,1)| = |(a,b)|$. The proof is left as an exercise. (Exercise 6.13)

3. $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. In order to prove this we define a function $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by the formula $f(m,n) = 2^m(2n+1)-1$. To prove that h is one to one assume that $h(m_1, n_1) = h(m_2, n_2)$. Then $2^{m_1}(2n_1 + 1) - 1 = 2^{m_2}(2n_2 + 1) - 1$ and so

$$2^{m_1}(2n_1 + 1) = 2^{m_2}(2n_2 + 1). \tag{6.4}$$

We first argue that $m_1 = m_2$ by showing that neither $m_1 > m_2$ nor $m_1 < m_2$ is possible. If $m_1 > m_2$ then dividing both sides of equation (6.4) by 2^{m_2} gives $2^{m_1-m_2}(2n_1 + 1) = (2n_2 + 1)$. But this is not possible since the left hand side of the equation is even and the right hand side is odd. (See exercise 5.11.) In a similar way we arrive at a contradiction if $m_1 < m_2$.

Since $m_1 = m_2$, dividing both sides of equation (6.4) by 2^{m_1} gives $2n_1+1 = 2n_2+1$ from which it follows that $n_1 = n_2$. Therefore $(m_1, n_1) = (m_2, n_2)$ and we have shown that h is one to one.

To prove that h is onto we will prove by the Principle of Complete Induction, Proof Principle 16, that $\forall n \in \mathbb{N}, \exists r, s \in \mathbb{N}$ such that $n = 2^r(2s+1)-1$.

If $n = 0$ then letting $r = s = 0$ an easy calculation shows that $n = 0 = 2^0(2 \cdot 0 + 1) - 1 = 2^r(2s + 1) - 1$.

Assume that $k \in \mathbb{N}$ and that

$$\forall j \leq k, j \in \mathbb{N}, \exists r, s \in \mathbb{N} \text{ such that } j = 2^r(2s + 1) - 1. \tag{6.5}$$

We need to show that there are natural numbers r_0 and s_0 such that $k + 1 = 2^{r_0}(2s_0 + 1) - 1$. It follows from 6.5 (with j = k) that there are natural numbers r_1 and s_1 such that

$$k = 2^{r_1}(2s_1 + 1) - 1. \tag{6.6}$$

It follows from this equality that $s_1 \leq k$ (Adding one to both sides gives $k + 1 = 2^{r_1}(2s_1 + 1)$. Since $2^{r_1} \geq 1$, we get $k + 1 \geq (2s_1 + 1)$ so $k \geq 2s_1$. Therefore $k \geq s_1$.) Therefore by equation 6.5 (this time with $j = s_1$) we conclude that there are natural numbers r_2 and s_2 such that

$$s_1 = 2^{r_2}(2s_2 + 1) - 1. \tag{6.7}$$

By 6.6 $k + 1 = 2^{r_1}(2s_1 + 1) - 1 + 1$. We now consider two cases.

Case 1: $r_1 > 0$. In this case $k+1 = 2^{r_1}(2s_1 + 1) - 1 + 1 = [2 \cdot 2^{r_1-1}(2s_1 + 1) + 1] - 1 = 2^0[2 \cdot 2^{r_1-1}(2s_1 + 1) + 1) - 1 = 2^{r_0}(2s_0 + 1) - 1$ with $r_0 = 0$ and $s_0 = 2^{r_1-1}(2s_1 + 1)$ both of which are natural numbers since $r_1 > 0$.

Case 2: $r_1 = 0$. In this case $k+1 = (2s_1+1)-1+1 = 2(s_1+1)-1$. Using equation 6.7 we get $k+1 = 2(2^{r_2}(2s_2+1)-1+1)-1 = 2_{r_2+1}(2s_2+1)-1 = 2^{r_0}(2s_0 + 1) - 1$ with $r_0 = r_2 + 1$ and $s_0 = s_2$ both of which are natural numbers.

Since we have shown in either of the two possible cases that there are natural numbers r_0 and s_0 such that $k + 1 = 2^{r_0}(2s_0 + 1) - 1$ the proof is complete.

6.5 $|\mathbb{R}|$, $|\mathbb{N}|$, and Cantor's Continuum Hypothesis

Since $\mathbb{N} \subseteq \mathbb{R}$ we know that $|\mathbb{N}| \leq |\mathbb{R}|$. It would be reasonable to ask whether or not $|\mathbb{N}| = |\mathbb{R}|$. More generally, we could ask whether or not $|A| = |B|$ for any two infinite sets A and B. We begin this section by answering the second question in the negative.

Theorem 6.7. *For any set A, $|A| \neq |\mathcal{P}(A)|$.*

Proof. Assume that A is a set. We have to prove that there is no one to one function from A onto $\mathcal{P}(A)$. Toward a proof by contradiction assume that f is such a function. Then for each element x of A, $f(x)$ will be a subset of A and one of "$x \in f(x)$" and "$x \notin f(x)$" will be true. We let C be the set consisting of those elements x of A for which $x \notin f(x)$. That is, $C = \{x \in A : x \notin f(x)\}$. The set C is an element of $\mathcal{P}(A)$ and therefore since f is onto $\mathcal{P}(A)$ there is some $x_0 \in A$ such that $f(x_0) = C$. Either $x_0 \in C$ or $x_0 \notin C$ and we will arrive at a contradiction in either case.
Case 1. $x_0 \in C$. Then since $C = \{x \in A : x \notin f(x)\}$, $x_0 \notin f(x_0)$. But since $x_0 \in C$ and $C = f(x_0)$ we conclude that $x_0 \in f(x_0)$. Hence we have a contradiction.
Case 2. $x_0 \notin C$. By the definition of C this means that it is not the case that $x_0 \notin f(x_0)$, that is, $x_0 \in f(x_0)$. But since $x_0 \notin C$ and $C = f(x_0)$ we conclude that $x_0 \notin f(x_0)$ and again we have a contradiction. □

The theorem tells us that for any set A, $|A| \neq |\mathcal{P}(A)|$. It is not difficult to prove that for any set A, $|A| \leq |\mathcal{P}(A)|$ (See exercise 6.19). This situation is expressed by saying $|A| < |\mathcal{P}(A)|$. Here is the general definition of $<$ for cardinal numbers.

Definition 6.8. If A and B are sets then $|A| < |B|$ means that $|A| \leq |B|$ and $|A| \neq |B|$.

We now give several examples with the goal of outlining an argument that $|\mathbb{N}| < |\mathbb{R}|$. As a result of the theorem above we know that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$ so we could accomplish our goal if we could show that $|\mathcal{P}(\mathbb{N})| = |\mathcal{R}|$.

From example 6.3 part 2 we know that $|\mathbb{Z}| = |\mathbb{N}|$ and from example 6.6 part 3 we know that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$. Combining these two equalities with exercise 6.16 we obtain the following string of equalities.

$$|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}| \tag{6.8}$$

We can argue that $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$ by defining the function $F : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ by

$$F(q) = \begin{cases} (0,0) & \text{if } q = 0 \\ (a,b) & \text{if } q \neq 0 \text{ and } q = \frac{a}{b} \text{ where } b > 0 \text{ and } a \text{ and } b \text{ have no common factors} \end{cases}.$$

We omit the proof that F is one to one. It follows from this and equation 6.8 that

$$|\mathbb{N}| = |\mathbb{Q}| \tag{6.9}$$

a fact that was first proved by Cantor.

Using exercise 6.21 we conclude that $|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{Q})|$. The function $H : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ defined by $H(x) = \{q \in \mathbb{Q} : q \leq r\}$ is one to one (we omit the proof) so it follows that

$$|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|. \tag{6.10}$$

To show that $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$ we define the function $K : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ by $K(A) = \sum_{n \in A} \left(\frac{1}{10}\right)^n$. The function K is one to one but the proof of this fact requires some knowledge of infinite series and we omit it. Combining this with (6.10) gives us the result:

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| \tag{6.11}$$

and therefore

$$|\mathbb{N}| < |\mathbb{R}| \tag{6.12}$$

Cantor conjectured, and spent many years trying to prove, that there are no sets A with cardinal number between that of $\mathbb{N}$ and $\mathbb{R}$. This conjecture is known as Cantor's Continuum Hypothesis. More precisely, Cantor's Continuum Hypothesis is the conjecture that there is no set A for which $|\mathbb{N}| < |A| < |\mathbb{R}|$.

6.6 Exercises

For exercises 6.1 through 6.4, (as we said in the paragraph preceding Theorem 6.2), these are not simply properties of equality since the sentence "$|X| = |Y|$" does not assert that two objects are equal but is short hand for the sentence "There is a one to one function from X onto Y."

6.1. Prove part 2 of Theorem 6.2. (Use Theorem 4.15.)

6.2. Prove part 3 of Theorem 6.2. (Use Theorem 4.13.)

6.3. Prove part 4 of Theorem 6.2.

6.4. Prove part 5 of Theorem 6.2.

6.5. Prove that the range of the function f from part 6 of example 6.3 is equal to $[0, 1)$.

6.6. Prove that the function f from part 6 of example 6.3 is one to one.

6.7. Prove that if $0 < x_1 < 1$ and $0 < x_2 < 1$ then $1 - x_1 - x_2 + x_1 x_2 > 0$

6.8. Using exercise 6.7 prove that if $0 < x_1 < 1$ and $0 < x_2 < 1$ then $1 - x_1 - x_2 + 2x_1 x_2 > 0$.

6.9. Prove that the function f from example 6.6 part 1 is one to one. (Hint: Assume that $0 < x_1 < 1$ and $0 < x_2 < 1$ and that $f(x_1) = f(x_2)$. This will give an equation which can be put in the form $(x_1 - x_2) \cdot E = 0$ where E is an expression involving x_1 and x_2. Show that $E \neq 0$. This will use the results of the previous exercise.)

6.10. Prove that if $f : A \to B$ is one to one and X and Y are subsets of A, then $f^*(X \setminus Y) = f^*(X) \setminus f^*(Y)$.

6.11. Prove that $|[2, 7]| = |[0, 3]|$ by finding a one to one function from $[2, 7]$ onto $[0, 3]$.

6.12. Show that $|[2, 7]| \leq |[0, 3]|$ by using the Cantor-Bernstein Theorem and Example 6.6, part 1.

6.13. Prove part 2 of Example 6.6. (Hint: Find a linear function f such that $f(0) = a$ and $f(1) = b$.)

6.14. Use the results of Example 6.6 parts 1 and 2 to prove that for any two real numbers a and b, if $a < b$ then $|(a, b)| = |\mathbb{R}|$.

6.15. Use the results of the pervious exercise to prove that for any two real numbers a and b, if $a < b$ then $|[a, b]| = |\mathbb{R}|$.

6.16. Prove that for all sets A_1, A_2, B_1 and B_2, if $|A_1| = |A_2|$ and $|B_1| = |B_2|$ then $|A_1 \times B_1| = |A_2 \times B_2|$.

6.17. Prove that $|\mathbb{Z}| = |\{0, 1\} \times \mathbb{N}|$.

6.18. Prove that $|\{0, 1\} \times \mathbb{Z}| = |\mathbb{Z}|$.

6.19. Prove that for any set A, $|A| \leq |\mathcal{P}(A)|$.

6.20. Prove that for all sets A and B, if $|A| \leq |B|$ then $|\mathcal{P}(A)| \leq |\mathcal{P}(B)|$.

6.21. Prove that for all sets A and B, if $|A| = |B|$ then $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.

6.22. Show that if Cantor's Continuum Hypothesis is false, that is, if there is a set A for which $|\mathbb{N}| < |A| < |\mathbb{R}|$ then there must be such an $A \subseteq \mathbb{R}$.

Chapter 7

Relations

7.1 Introduction

A relation, speaking in imprecise terms, is a way of comparing elements of a set. In previous courses you have studied particular relations, for example the relation $<$ on the set of real numbers, but you may not have studied relations in an abstract setting. The situation is different for functions (which were the topic of Chapter 4.) In calculus and other elementary math courses you are likely to encounter a brief study of functions in an abstract setting. That is to say, the word "function" is defined and certain classes of functions are studied. For example, there are general theorems that you probably know about the class polynomial functions or the class of continuous functions or the class of differentiable functions. In elementary math courses, there is seldom a definition of the word "relation" or a study of relations in a general setting.

In this chapter we will see how relations can be treated in a precise way.

7.2 Definitions

Relations are the verbs of mathematics.[1] When you combine a symbol representing a relation with symbols representing objects you obtain a mathematical sentence. For example, $4 < 2x$ combines the relation symbol $<$ with the two symbols 4 and $2x$ both of which represent objects and the result is a sentence. On the other hand when a symbol representing an *operation* is combined with symbols representing objects the result is a sequence of symbols representing another object, for example $4 + 2x$ combines the operation symbol $+$ with two symbols representing objects and the result is a sequence representing an another object. We will study binary operations in a later chapter where they will be defined to be functions whose inputs are ordered pairs.

Here is the way the word "relation" is usually defined.

[1] Here and throughout this chapter the word "relation" will mean "binary relation".

Definition 7.1. 1. A *relation* R is a set of ordered pairs.

2. If R is a relation, the *domain* of R (denoted $\text{Dom}(R)$) is the set of first components of pairs on R. That is, $\text{Dom}(R) = \{a : \exists b \text{ such that } (a, b) \in R\}$.

3. If R is a relation, the *range* of R (denoted $\text{Range}(R)$) is the set of second components of pairs in R. That is $\text{Range}(R) = \{b : \exists a \text{ such that } (a, b) \in R\}$. (Note that the definitions of "domain" and "range" for relations are identical to the definitions of "domain" and "range" for functions given in chapter 4.)

4. If A is a set and R is a relation *R is a relation on A* means that $\text{Dom}(R) \subseteq A$ and $\text{Range}(R) \subseteq A$.

Even though a relation is officially a set of ordered pairs, we will use the standard notation: If R is a relation, then $a\ R\ b$ will be short hand notation for $(a, b) \in R$ and $a \not R\ b$ will be short hand notation for $(a, b) \notin R$.

Here are two examples:

$$R_1 = \{(1, 2), (1, 3), (1, 4), (2, 3)\} \text{ and} \tag{7.1}$$

$$R_2 = \{(a, b) : a \text{ and } b \text{ are in } \mathbb{R} \text{ and } \exists c \in \mathbb{R} \text{ such that } c \geq 0 \text{ and } a + c = b\}. \tag{7.2}$$

All of the following are true mathematical statements: $1\ R_1\ 3$, $3 \not R_1\ 1$, $\sqrt{2}\ R_2\ \frac{107}{7}$, and $0 \not R_2\ -1$. The domain of R_1 is the set $\{1, 2\}$, $\text{Range}(R_1) = \{2, 3, 4\}$ and $\text{Dom}(R_2) = \text{Range}(R_2) = \mathbb{R}$. The relation R_2 is the usual $\leq$ relation on the set of real numbers and in the future we will use $\leq$ rather than R_2 for this relation.

Frequently a relation R is defined by giving a set A and a sentence $P(x, y)$ with two free variables giving the criteria for $x\ R\ y$. For example, "R_3 is the relation on $\mathbb{R}$ defined by $x\ R_3\ y$ if and only if $|x - y| \leq 10$." In terms of ordered pairs, this means that $R_3 = \{(x, y) : x \in \mathbb{R} \text{ and } y \in \mathbb{R} \text{ and } |x - y| \leq 10\}$.

In general the meaning of "R is the relation on A defined by $x\ R\ y$ if and only if $P(x, y)$" means that $R = \{(x, y) : x \text{ and } y \text{ are in } A \text{ and } P(x, y)\}$.

Here is another example: The relation $|$ is defined on $\mathbb{Z}$ by $n \mid m$ if and only if $\exists t \in \mathbb{Z}$ such that $m = nt$. "$n \mid m$" is read "n divides m". For example, $7 \mid 35$ since $35 = 7 \cdot 5$.

If R_1 and R_2 are two relations described as sets of ordered pairs then we can us the principle of extensionality (2) to prove that $R_1 = R_2$. On the other hand

Proof Principle 18. Proving Relations are Equal. If R_1 and R_2 are relations on a set X then in order to prove that $R_1 = R_2$ it suffices to prove that for all x and y in X, $x\ R_1\ y$ if and only if $x\ R_2\ y$. □

7.3 Properties of Relations

There are several important properties which a relation may or may not have. In this section we give the definitions of these properties and look at several examples.

Definition 7.2. Assume that R is a relation

1. R is *symmetric* if $\forall x$ and $\forall y$, If $x\ R\ y$ then $y\ R\ x$.
2. R is *anti-symmetric* if $\forall x$ and $\forall y$, if $x\ R\ y$ and $y\ R\ x$, then $x = y$.
3. R is *transitive* if for all x, y and z, if $x\ R\ y$ and $y\ R\ z$ then $x\ R\ z$.
4. For any set A, R is *reflexive on* A if $\forall x \in A$, $x\ R\ x$.

The relation R_3 described in section 7.2 is symmetric and reflexive or $\mathbb{R}$ but neither anti-symmetric nor transitive. The relation R_2 (which was $\leq$) from section 7.2 is anti-symmetric, transitive and reflexive on $\mathbb{R}$, but not symmetric. The relation R_1 is anti-symmetric and transitive but not symmetric. It is reflexive on the empty set.

In understanding these examples and the examples to follow it is helpful to have in mind the meanings of the negations of these four properties. For example, a relation R fails to be anti-symmetric if (simplifying the negation of the sentence defining "anti-symmetry")

$$\exists x \text{ and } \exists y \text{ such that } x\ R\ y \text{ and } y\ R\ x \text{ and } x \neq y.$$

Remembering that a relation is a set of ordered pairs, this means that there are two different objects x and y such that (x, y) and (y, x) are both in R. This is clearly not the case for the relation R_1 defined in the previous section and that's how we came to the conclusion that R_1 is anti-symmetric.

Writing the negations of the other three properties is left for the exercises but I recommend that you do it now. See exercises 7.3, 7.4 and 7.5.

Note that the reflexive property is not just a property of a relation but a property of a relation and a set. Every relation is reflexive on the empty set and for every relation R there is a largest set on which R is reflexive, namely $\{x : (x, x) \in R\}$. Also note that "anti-symmetric" is not the negation of "symmetric". There is a relation (at least one) which is both symmetric and anti-symmetric and there is a relation which is neither symmetric nor anti-symmetric. This is investigated further in the exercises. (See exercises 7.10 and 7.11.)

Example 7.3.

1. Let R_4 be the relation on $\mathbb{R}$ defined by $x\ R_4\ y$ if $x < y$, where $<$ is ordinary "less than" for real numbers. We will almost always use the symbol $<$ for this relation.
2. R_5 is the relation on $\mathbb{Z}$ defined by $m\ R_5\ n$ if $n - m$ is a multiple of 5. This relation is usually denoted by $\equiv_5$ and this is the symbol we will usually use. So we could write $m \equiv_5 n$ if $\exists t \in \mathbb{Z}$ such that $n - m = 5t$ or we could write $m \equiv_5 n$ if $5 \mid (n - m)$.

3. R_6 is the relation defined on $\mathbb{R}$ by $x\ R_6\ y$ if $|y - x| < 4$.

4. R_7 is the relation defined on $\mathbb{R}$ by $x\ R_7\ y$ if and only if $x + y \neq 1$.

5. R_8 is the relation defined on $\mathbb{R}$ by $x\ R_8\ y$ if $x \geq 3$ and $y \geq 3$.

6. For any set A *the equality relation on* A is the usual relation "is equal to" on A. That is, the equality relation on A is the relation $\{(x, x) : x \in A\}$.

7. For any set A, the empty relation on A is the empty set (of ordered pairs.) If we denote this relation by E then $\forall x$ and $y \in A$, $x \not E\ y$.

8. For any set A, the universal relation on A is the set $A \times A$. If we denote this relation by U then $\forall x$ and $y \in A$, $x\ U\ y$.

We shall investigate the properties of some of these relations and leave the investigation of the properties of others for the exercises. For example, R_5 is symmetric, transitive and reflexive on $\mathbb{Z}$ but fails to be anti-symmetric. Here are the arguments.

Symmetry: m and n are in $\mathbb{Z}$ and that $m \equiv_5 n$. Then $\exists t \in \mathbb{Z}$ such that $n - m = 5t$. It follows that $m - n = -5t$ and hence there is an $s \in \mathbb{Z}$ (namely $s = -t$) for which $m - n = 5s$. By the definition of $\equiv_5$ we conclude that $n \equiv_5 m$.

Transitive: Assume that m, n and p are integers and that $m \equiv_5 n$ and $n \equiv_5 p$. Then there are integers t_1 and t_2 such that $n - m = 5t_1$ and $p - n = 5t_2$. Adding these two equations gives $p - m = 5(t_1 + t_2)$. Since $s = t_1 + t_2$ is an integer, we conclude that $p - m = 5s$ for some integer s and therefore $p \equiv_5 m$.

Reflexive: For every integer m, $m - m = 5 \cdot 0$ and therefore $m \equiv_5 m$.

Not Anti-Symmetric: Since $5 \equiv_5 10$ and $10 \equiv_5 5$ but $5 \neq 10$, we have a counter example to the anti-symmetric property.

The relation R_7 is symmetric, but neither anti-symmetric nor transitive. The largest set on which it is reflexive is $\mathbb{R} \setminus \{\frac{1}{3}\}$. R_7 is clearly symmetric. It is not anti-symmetric since $2\ R_7\ 5$ and $5\ R_7\ 2$ but $5 \neq 2$. It is not transitive because $\frac{1}{4}\ R_7\ 3$ and $3\ R_7\ \frac{3}{4}$ but $\frac{1}{4}\ \not R_7\ \frac{3}{4}$. The largest set on which R_7 is reflexive is $\{x : x \in \mathbb{R} \text{ and } x\ R_7\ x\} = \{x : x \in \mathbb{R} \text{ and } x + x \neq 1\} = \{x : x \in \mathbb{R} \text{ and } 2x \neq 1\} = \{x : x \in \mathbb{R} \text{ and } x \neq \frac{1}{2}\} = \mathbb{R} \setminus \{\frac{1}{2}\}$.

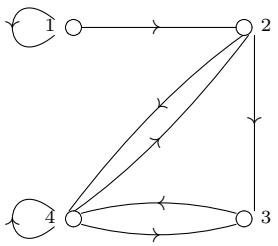
Example 7.4. Find a set A and a relation on A which is reflexive on A but neither transitive nor symmetric.

When trying to find an example of a relation with a certain combination of properties it is sometimes easier to give the relation as a set of ordered pairs. Let's try for a relation on the set $A = \{1, 2, 3\}$. In order for the relation (we'll call it R) to be reflexive on A we must include the pairs $(1, 1), (2, 2)$ and $(3, 3)$. We could insure that the relation was not transitive if we included $(1, 2)$ and $(2, 3)$ but left out $(1, 3)$. If we also made sure we left out the pair $(2, 1)$

(after including $(1,2)$) we would have a non-symmetric relation. Any set of ordered pairs satisfying the conditions described above will work. For example, $R = \{(1,1),(2,2),(3,3),(1,2),(2,3)\}$ or any larger set of pairs which excludes $(1,3)$ and $(2,1)$.

7.4 Diagrams of Relations

If A is a finite set and R is a relation on A it is possible to draw a diagram of R. The elements of A are represented by points (frequently labelled) and if for two elements a and b of A it is the case that $a\ R\ b$ then the diagram includes an arrow from the point representing a to point representing b. For example, suppose that $A = \{1,2,3,4\}$ and $R = \{(1,1),(1,2),(2,3),(2,4),(3,4),(4,2),(4,3),(4,4)\}$ then R is represented by the diagram:



7.5 Equivalence Relations

Definition 7.5. If A is a set, an *equivalence relation on* A is a relation on A which is symmetric, transitive and reflexive on A.

The equality relation of any set A is an equivalence relation on A and the universal relation $U = A \times A$ on a set A is an equivalence relation. A more interesting equivalence relation is the relation $\equiv_5$ defined in example 7.3. Frequently an equivalence relation is denoted by the symbol $\equiv$ with some subscript or simply by $\equiv$ with no subscript if there is only one such relation under consideration. Here are several other examples of equivalence relations.

Example 7.6. 1. Define the relation $\equiv_{\mathbb{Z}}$ on $\mathbb{R}$ by $x \equiv_{\mathbb{Z}} y$ if and only if $x - y \in \mathbb{Z}$. Here's the argument that $\equiv_{\mathbb{Z}}$ is an equivalence relation on $\mathbb{R}$. First we note that for every x and y in $\mathbb{R}$, if $x \equiv_{\mathbb{Z}} y$ then $x - y$ is an integer so $-(x-y) = y - x$ is an integer. Therefore $y \equiv_{\mathbb{Z}} x$. This shows that $\equiv_{\mathbb{Z}}$ is symmetric. To show that $\equiv_{\mathbb{Z}}$ is transitive, assume that $x \equiv_{\mathbb{Z}} y$ and $y \equiv_{\mathbb{Z}} z$, then both $x - y$ and $y - x$ are integers and therefore $(x-y)+(y-z) = x - z$ is an integer. Hence $x \equiv_{\mathbb{Z}} z$. For the argument that $\equiv_{\mathbb{Z}}$ is reflexive on $\mathbb{R}$ we note that for any $x \in \mathbb{R}$, $x - x = 0$ which is an integer so that $x \equiv_{\mathbb{Z}} x$.

2. Define the relation $\equiv$ on $\mathbb{N} \times \mathbb{N}$ by $(a, b) \equiv (c, d)$ if and only if $a+d = c+b$. We leave the verification that $\equiv$ is an equivalence relation for the exercises. (See exercise 7.33.)

3. Let $\mathcal{A} = \{\{1, 2, 3\}, \{4, 5\}, \{6, 7, 8, 9, 10\}\}$. Note that any two (different) sets from $\mathcal{A}$ have empty intersection and that the union of the sets in $\mathcal{A}$ is the set $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. The relation $R_{\mathcal{A}}$ on X is defined by $x \; R_{\mathcal{A}} \; y$ if and only if $\exists A \in \mathcal{A}$ such that $x \in A$ and $y \in A$.

   So, for example $1 \; R_{\mathcal{A}} \; 2$ since 1 and 2 are both in $\{1, 2, 3\}$ which is in $\mathcal{A}$.

Item 3 is a special case of a general method for constructing equivalence relations on a set X. Here is a description of the method.

Definition 7.7. Let X be a set, then a *partition* of X is a collection $\mathcal{A}$ of subsets of X such that

1. $\bigcup_{u \in \mathcal{A}} u = X$ and

2. For all u_1 and u_2 in $\mathcal{A}$, if $u_1 \neq u_2$ then $u_1 \cap u_2 = \emptyset$.

The elements of the partition $\mathcal{A}$ are called the *cells* of $\mathcal{A}$.

We note that it is sometimes useful to use condition 2 from the above definition in the form

(2') For all u_1 and u_2 in $\mathcal{A}$, if $u_1 \cap u_2 \neq \emptyset$ then $u_1 = u_2$.

For example, $\mathcal{A}_1 = \{\{1, 3, 5\}, \{2, 4, 6\}, \{7, 8, 9\}\}$ is a partition of the set $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ but $\mathcal{A}_2 = \{\{1, 3, 5\}, \{2, 3, 4, 5, 6\}, \{7, 8, 9\}\}$ is not a partition of X since $\{1, 3, 5\}$ and $\{2, 3, 4, 5, 6\}$ are in $\mathcal{A}_2$ but $\{1, 3, 5\} \cap \{2, 3, 4, 5, 6\} \neq \emptyset$. Similarly, $\mathcal{A}_3 = \{[k, k + 1) : k \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$ but $\mathcal{A}_4 = \{[k, k + 1] : k \in \mathbb{Z}\}$ is not a partition of $\mathbb{R}$.

Definition 7.8. I $\mathcal{A}$ is a partition of a set X then the relation $\sim_{\mathcal{A}}$ is defined by $x \sim_{\mathcal{A}} y$ if and only if x and y are in the same cell of the partition $\mathcal{A}$, that is, $x \sim_{\mathcal{A}} y$ if and only if $\exists u \in \mathcal{A}$ such that $x \in u$ and $y \in u$.

For example, using the partition $\mathcal{A}_1$ above $7 \sim_{\mathcal{A}_1} 9$ since 7 and 9 are both elements of the cell $\{7, 8, 9\}$. It's also true that $7 \sim_{\mathcal{A}_1} 7$ since $7 \in \{7, 8, 9\}$ (and $7 \in \{7, 8, 9\}$.)

Theorem 7.9. *If X is a set and $\mathcal{A}$ is a partition of X, then $\sim_{\mathcal{A}}$ is an equivalence relation on X.*

The proof of the theorem is an exercise.

Our next task is to prove that every equivalence relation on a set X is $\sim_{\mathcal{A}}$ for some partition $\mathcal{A}$ of X. To make things easier we introduce some notation and terminology.

Definition 7.10. If $\equiv$ is an equivalence relation of a set X and $t \in X$ then

1. $[t]_{\equiv}$ denotes the set $\{s \in X : t \equiv s\}$. The set $[t]_{\equiv}$ is called *the* $\equiv$-*equivalence class of* t or simply *the equivalence class of* t if it's clear which equivalence relation is intended.

2. $EC_{\equiv}$ denotes the set of all $\equiv$ classes, that is $EC_{\equiv} = \{[t]_{\equiv} : t \in X\}$.

Before stating and proving the theorem we give a few examples.

If $\equiv$ is the equality relation on a set X, then for every $t \in X$, $[t]_{=} = \{t\}$ and so $EC_{=} = \{\{t\} : t \in X\}$.

If U is the universal relation on a set X (that is, $U = X \times X$) then for each $t \in X$, $[t]_U = X$ and so $EC_U = \{X\}$.

For each $n \in \mathbb{Z}$, $[n]_{\equiv_5} = \{n + 5k : k \in \mathbb{Z}\}$. So, for example, $[0]_{\equiv_5} = \{5k : k \in \mathbb{Z}\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ and $[1]_{\equiv_5} = \{1 + 5k : k \in \mathbb{Z}\} = \{\ldots - 9, -4, 1, 6, 11, \ldots\}$. In this case $EC_{\equiv_5} = \{[0]_{\equiv_5}, [1]_{\equiv_5}, [2]_{\equiv_5}, [3]_{\equiv_5}, [4]_{\equiv_5}\}$

Theorem 7.11. *If $\equiv$ is an equivalence relation on a set X then $\equiv$ is $\sim_{\mathcal{A}}$ where $\mathcal{A} = EC_{\equiv}$.*

Proof. We first prove that $EC_{\equiv}$ is a partition of X. It is clear from the definition that $EC_{\equiv}$ is a collection of subsets of X and therefore $\bigcup_{u \in EC_{\equiv}} u \subseteq X$. On the other hand if $t \in X$ then $t \equiv t$ so $t \in [t]_{\equiv} \in EC_{\equiv}$. Therefore $t \in \bigcup_{u \in EC_{\equiv}} u$. This shows that $X \subseteq \bigcup_{u \in EC_{\equiv}} u$. So we conclude that $X = \bigcup_{u \in EC_{\equiv}} u$. So $EC_{\equiv}$ meets requirement 1 in definition 7.7. To argue for requirement 2 we assume that u and v are in $EC_{\equiv}$ and that $u \cap v \neq \emptyset$ and prove that $u = v$. (This is "Proving the contrapositive", Proof Principle 9.) Since $u \cap v \neq \emptyset$, there is some element t of X in $u \cap v$. Since u and v are in $EC_{\equiv}$ there are elements x and y of X such that $u = [x]_{\equiv}$ and $v = [y]_{\equiv}$. It follows that $x \equiv t$ and $y \equiv t$. By the symmetric property of equivalence relations $t \equiv y$. By the transitive property $x \equiv y$. And by the symmetric property $y \equiv x$. We argue that $u \subseteq v$. Assume that $s \in u$, then $x \equiv s$. Using the transitive property and the fact that $y \equiv x$ we conclude that $y \equiv s$. Therefore $s \in [y]_{\equiv} = v$. This completes our proof that $u \subseteq v$. The proof that $v \subseteq u$ is similar, hence $u = v$.

We shall use our proof principle for showing relations are equal (Proof Principle 18) to prove that $\equiv = \sim_{\mathcal{A}}$ where $\mathcal{A} = EC_{\equiv}$. Assume that x and y are in X and that $x \equiv y$. Then $y \in [x]_{\equiv}$. Since $x \equiv x$, it's also the case that $x \in [x]_{\equiv}$ and therefore $\exists u \in \mathcal{A}$ such that $x \in u$ and $y \in u$. Therefore $x \sim_{\mathcal{A}} y$.

Next assume that $x \sim_{\mathcal{A}} y$. Then for some $z \in X$, $x \in [z]_{\equiv}$ and $y \in [z]_{\equiv}$. Since $\mathcal{A} = EC_{\equiv}$ is a partition of X and $[x]_{\equiv}$ and $[z]_{\equiv}$ have a common element (namely x), we conclude that $[x]_{\equiv} = [z]_{\equiv}$. It follows that $y \in [x]_{\equiv}$. Therefore $x \equiv y$. □

Example 7.12. Let $\equiv_3$ be the relation defined on $\mathbb{Z}$ by $x \equiv_3 y$ if and only if $3 \mid (x - y)$. The proof that $\equiv_3$ is an equivalence relation is left as an exercise. The equivalence class $[0]_{\equiv_3}$ is the set $\{\ldots, -6, -3, 03, 6, \ldots\}$. Also $[1]_{\equiv_3} = \{\ldots - 5, -2, 1, 4, 7, \ldots\}$ and $[2]_{\equiv_3} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$. Since the equivalence classes form a partition of $\mathbb{Z}$ there are no more equivalence classes. That is, for every integer n, $[n]_{\equiv_3}$ is one of $[0]_{\equiv_3}$, $[1]_{\equiv_3}$, or $[2]_{\equiv_3}$. Therefore $EC_{\equiv_3} = \{[0]_{\equiv_3}, [1]_{\equiv_3}, [2]_{\equiv_3}\}$.

7.6 Order Relations

Definition 7.13. Assume that X is a set.

1. A *partial order on* X is a relation R on X which is reflexive on X, transitive and anti-symmetric.

2. A *linear order on* X is a partial order on X which also satisfies

$$\forall x \in X, \forall y \in X, x \; R \; y \text{ or } y \; R \; x. \tag{7.3}$$

Partial orders (including linear orders) are frequently denoted by the symbol $\leq$ with a superscript or subscript or by the symbol $\leq$ with no superscript or subscript if it's clear which partial order is being discussed. If the symbol $\leq$ with a super or subscript is used to denote a partial order on a set X then the symbol $<$ with the same super or subscript denotes the relation on X defined by $x < y$ if and only if $x \leq y$ and $x \neq y$.[2]

It will sometimes be convenient to use the following terminology.

Definition 7.14. 1. A *partially ordered set* is an ordered pair $(X, \leq)$ where X is a set and $\leq$ is an partial order on X.

2. A *linearly ordered set* is an ordered pair $(X, \leq)$ where X is a set and $\leq$ is a linear order on X.

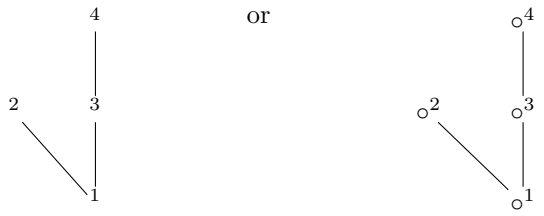
Example 7.15. 1. The usual $\leq$ is a linear order on each of the sets $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ or $\mathbb{N}$. Note that the usual $<$ is not a partial ordering.

2. The subset relation $\subseteq$ is a partial ordering on any set of sets.

3. The relation $\leq_3$ on $\mathbb{R} \times \mathbb{R}$ defined by $(a, b) \leq_3 (c, d)$ if and only if $a \leq c$ or $(a = c$ and $b \leq d)$. Here $\leq$ denotes the usual ordering of the real numbers.

4. The relation $\leq_4 = \{(1,1), (2,2), (3,3), (4,4), (1,2), (1,3), (1,4), (3,4)\}$ is a partial ordering on the set $\{1, 2, 3, 4\}$.

If the set X is finite then a partially ordered set $(X, \leq)$ has a graphical representation called it's *Hasse diagram*. This differs from the diagram of a relation which was discussed in section 7.4. Before describing in detail how to get the Hasse diagram of a partially ordered set we look at an example. Here is a diagram of the partial ordering $\leq_4$ of the set $\{1, 2, 3, 4\}$ given in example 4 above.



[2] The relation $<$ is transitive, anti-symmetric and satisfies $\forall x \in X$, $x \not< x$. A relation with these properties is sometimes called a *strict partial order*.

We can see from the diagram, for example, that $1 \leq_4 4$ since there is an upward path through the diagram from 1 to 4. In general a partially ordered set $(X, \leq)$ can be recovered from its Hasse diagram (as a set of ordered pairs, say) by noting that for all x and y in X, $x \leq y$ if and only if there is a path from x to y that follows line segments in the diagram and always goes upward as you go from x to y. In order to describe the process of drawing the Hasse diagram from some other description of a partially ordered set, some terminology will be helpful.

Definition 7.16. Assume that $(X, \leq)$ is a partially ordered set and x and y are in X.

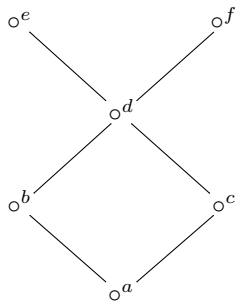
1. x is a *maximum element of X relative to* $\leq$ if $\forall t \in X$, $t \leq x$.
2. x is a *maximal element of X relative to* $\leq$ if $\forall t \in X$, $x \not\leq t$.
3. x is a *minimum element of X relative to* $\leq$ if $\forall t \in X$, $x \leq t$.
4. x is a *minimal element of X relative to* $\leq$ if $\forall t \in X$, $t \not\leq x$.
5. The phrase y *is an immediate successor of x relative to* $\leq$ means that $x < y$ and there is no element $z \in X$ such that $x < z$ and $z < y$. (Recall that $t < s$ means that $t \leq s$ and $t \neq s$.) We sometimes also say under these circumstances that x *is an immediate predecessor of y relative to* $\leq$.

If it is clear which partial ordering is intended then will usually leave off the pharse "relative to $\leq$" in each of the above.

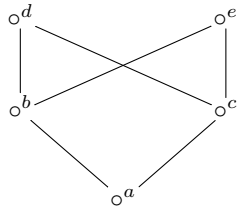
Looking at the diagram of $\leq_4$ above we see that 4 and 2 are maximal elements and that there is no maximum element. The number 1 is both minimum and minimal. The numbers 2 and 3 are both immediate successors of 1 (and therefore 1 is an immediate predecessor of both 2 and 3). It is also the case that 4 is an immediate successor of 2 and 2 is an immediate predecessor of 4.

In the Hasse diagram of a partially ordered set $(X, \leq)$, each element of X must be placed below all of its immediate successors and above all of its immediate predecessors and must be connected to each one of these immediate successors and immediate predecessors with a line segment.

Here are some more examples



(A)



(B)

(C)

For the partially ordered set pictured in (A) there are two maximal elements e and f. There is no maximum element. There is one minimum element, namely a and a is the only minimal element.

Definition 7.17. Assume that $(X, \leq)$ is a partially ordered set and that Y is a subset of X

1. An element x of X is an *upper bound of Y (relative to $\leq$)* if $\forall t \in Y$, $t \leq x$.

2. An element z of X is an *lower bound of Y (relative to $\leq$)* if $\forall t \in Y$, $z \leq t$.

3. An element u of X is a *least upper bound of Y (relative to $\leq$)* if u is an upper bound for Y and for every upper bound x of Y, $u \leq x$.

4. An element v of X is a *greatest lower bound of Y (relative to $\leq$)* if v is a lower bound for Y and for every lower bound z of Y, $z \leq v$.

If $(X, \leq)$ is the partially ordered set pictured in diagram (A) above and $Y = \{a, b, c, d\}$ then Y has three upper bounds: d, e and f. The set Y also has a least upper bound, namely d. There is one lower bound for Y, namely a and a is the greatest lower bound for Y. Now let $(X, \leq)$ be the partially ordered set pictured in (B) and let $Y = \{b, c, d, e\}$. In this example Y has no upper bounds and therefore no least upper bounds. The element a is the only lower bound for Y and a is the only greatest lower bound.

As our examples show, a set may have more that one upper bound or more than one lower bound (or both). This is not the case for least upper bounds or greatest lower bounds as we now prove.

Theorem 7.18. *If $(X, \leq)$ is a partially ordered set and $Y \subseteq X$, the Y has at most one least upper bound and at most one greatest lower bound.*

Proof. Assume the hypotheses. We shall prove that Y has at most one least upper bound. The proof that Y has at most one greatest lower bound is similar. To prove that Y has at most one least upper bound we use Proof Principle 13 (Proving "at most one").

Assume that x_1 and x_2 are least upper bounds for Y. Then by definition 3 x_1 is an upper bound for Y and $x_2 \leq x$ for every upper bound x of Y. Therefore $x_2 \leq x_1$. Similarly, $x_1 \leq x_2$. By the anti-symmetry property of $\leq$ we conclude that $x_1 = x_2$. □

7.7 Exercises

7.1. Let $R = \{(2, 3), (3, 3), (2, 7), (3, 9)\}$. What are Dom($R$) and Range($R$)?

7.2. Let $R = \{(x, y) : x, y \in \mathbb{R} \text{ and } x \leq 2y + 1\}$. What are Dom($R$) and Range($R$)?

7.3. Write the negation of the sentence defining "R is symmetric" in readable symbolic form. As usual this means to write an equivalent sentence with the negation moved inside as far as possible.

7.4. Write the negation of the sentence defining "R is transitive" in readable symbolic form.

7.5. Write the negation of the sentence defining "R is reflexive on A" in readable symbolic form

7.6. Which of the properties symmetric, anti-symmetric, and transitive are true of the relation defined in exercise 7.1.

7.7. What is the largest set on which the relation from exercise 7.1 is reflexive?

7.8. Which of the properties symmetric, anti-symmetric, and transitive are true of the relation defined in exercise 7.2.

7.9. What is the largest set on which the relation from exercise 7.2 is reflexive?

7.10. Prove that if a relation R is both symmetric and anti-symmetric the $\forall x, \forall y$ if $x \; R \; y$ then $x = y$.

7.11. Give an example of a relation R which is neither symmetric nor anti-symmetric. (It might be easiest to give R as a set of ordered pairs.)

7.12. Which of the properties symmetric, anti-symmetric, and transitive does R_4 from example 7.3 have? What is the largest set on which R_4 is reflexive?

7.13. Which of the properties symmetric, anti-symmetric, and transitive does R_6 from example 7.3 have? What is the largest set on which R_6 is reflexive?

7.14. Which of the properties symmetric, anti-symmetric, and transitive does the equality relation on a set have (see example 7.3)?

7.15. Which of the properties symmetric, anti-symmetric, and transitive does the empty relation from example 7.3 have?

7.16. Let A be a set and let U be the universal relation on A (See example 7.3.) Which of the properties symmetric, anti-symmetric, and transitive does U have. What is the largest set on which U is reflexive?

For each relation R described in exercises 7.17 through 7.24 decide whether R is symmetric, anti-symmetric or transitive and find the largest set A on which R is reflexive. Give arguments for your answers.

7.17. The relation $\geq$ on $\mathbb{R}$.

7.18. The relation $>$ on $\mathbb{R}$.

7.19. The relation $\mid$ on $\mathbb{Z}$ defined by $m \mid n$ if $\exists t \in \mathbb{Z}$ such that $n = mt$. ("$m \mid n$ is read "m divides n.")

7.20. Let A be a non-empty set, R is the relation $\subseteq$ on $\mathcal{P}(A)$.

7.21. The relation R on $\mathbb{R}$ defined by $a\ R\ b$ if $|b-a| \geq 4$.

7.22. The relation R defined on $\mathbb{R}$ by $x\ R\ y$ if $xy > 0$.

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

7.24. The relation $R = \{(1,2),(2,1),(1,1)\}$

7.25. Find a set A and a relation R which is transitive but neither symmetric nor reflexive on A.

7.26. Find a set A and a relation R which is reflexive on A but neither transitive nor symmetric.

7.27. Find a set A and a relation R which is transitive and reflexive on A but not symmetric.

7.28. Find a set A and a relation R which is symmetric and reflexive on A but not transitive.

7.29. Find a set A and a relation which is symmetric and transitive but not reflexive on A.

7.30. Prove that if $\equiv$ is an equivalence relation on a set A and B is a subset of A, then the relation $R = \{(x,y) : x \equiv y \text{ and } (x,y) \in B \times B\}$ is an equivalence relation on B.

7.31. Let $\mathcal{A}$ be any collection of sets (not necessarily pairwise disjoint) and let $R_{\mathcal{A}}$ be the relation defined by $a\ R_{\mathcal{A}}\ b$ if and only if $\exists A \in \mathcal{A}$ such that $a \in A$ and $b \in A$. Prove that $R_{\mathcal{A}}$ is symmetric and reflexive on the set $\bigcup_{A\in\mathcal{A}} A = \{a : \exists A \in \mathcal{A} \text{ such that } a \in A\}$. Give an example to show that $R_{\mathcal{A}}$ need not be transitive.

7.32. Referring to exercise 7.31, assume that R is a relation which is symmetric and reflexive on $\text{Dom}(R) \cup \text{Range}(R)$. Is there a collection of sets $\mathcal{A}$ such that $R = R_{\mathcal{A}}$?

7.33. Prove that the relation $\equiv$ defined in example 7.6 part 2 is an equivalence relation.

7.34. For the equivalence relation of the previous exercise describe $[(4,9)]_{\equiv}$.

7.35. Let $\mathcal{A}$ be the partition $\{[k,k+1) : k \in \mathbb{Z}\}$ of $\mathbb{R}$. Are the following true or false?

1. $1 \sim_{\mathcal{A}} 2$
2. $\frac{3}{2} \sim_{\mathcal{A}} \frac{5}{4}$
3. $\frac{5}{4} \sim_{\mathcal{A}} \frac{3}{2}$

4. $-1 \sim_{\mathcal{A}} 1$

5. $0 \sim_{\mathcal{A}} 0$

7.36. Prove Theorem 7.9

7.37. Prove that the relation $\equiv_3$ defined on $\mathbb{Z}$ by $m \equiv_3 n$ if and only if $3 \mid (n-m)$ is an equivalence relation.

7.38. Let k be a fixed integer. Prove that the relation $\equiv_k$ defined on $\mathbb{Z}$ by $m \equiv_k n$ if and only if $k \mid (n-m)$ is an equivalence relation.

7.39. For the equivalence relation $\equiv_6$ what are $[0]_{\equiv_6}$ and $[3]_{\equiv_6}$?

7.40. How many equivalence classes are there for the equivalence relation $\equiv_6$?

7.41. What is $EC_{\equiv_7}$?

7.42. Define a relation R on $\mathbb{R}$ by $x \; R \; y$ if and only if $xy > 0$. Prove that R is not an equivalence relation on $\mathbb{R}$. (Compare this with Exercise 7.43.)

7.43. Let $\mathbb{R}^*$ be the set of non-zero real numbers. Define a relation R on $\mathbb{R}^*$ by $x \; R \; y$ if and only if $xy > 0$. Prove that R is an equivalence relation on $\mathbb{R}^*$.

7.44. What are the equivalence classes for the relation R defined in Exercise 7.43?

7.45. Assume that X is a set and f is a function with domain X. Define the relation R_f on X by $x \; R_f \; y$ if and only if $f(x) = f(y)$. Prove that R_f is an equivalence relation on X.

7.46. Assume that X is a set and that $\mathcal{Y}$ is a set of subsets of X (that is, for every $z \in \mathcal{Y}$, $z \subseteq X$). Let $R_{X,\mathcal{Y}}$ be the relation on X defined by

$\forall s, t \in X, s \; R_{X,\mathcal{Y}}$ if and only if for all $z \in \mathcal{Y}$, either ($s \in z$ and $t \in z$) or ($s \notin z$ and $t \notin z$).

Prove that $R_{X,\mathcal{Y}}$ is an equivalence relation on X.

7.47. Let $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and let $Y = \{\{1, 2, 3, 4, 5\}, \{3, 4, 5, 6, 7, 8\}, \{4, 5, 8, 9, 10\}\}$. By Exercise 7.46 the relation $R_{X,\mathcal{Y}}$ is an equivalence relation on X. Are the following true or false?

(a) $1 \; R_{X,\mathcal{Y}} \; 2$

(b) $1 \; R_{X,\mathcal{Y}} \; 9$

(c) $3 \; R_{X,\mathcal{Y}} \; 4$

(d) $4 \; R_{X,\mathcal{Y}} \; 5$

(e) $7 \; R_{X,\mathcal{Y}} \; 8$

7.48. Using X and Y from Exercise 7.47 give $EC_{R_{X,\mathcal{Y}}}$ (the set of all $R_{X,\mathcal{Y}}$ equivalence classes) by the listing method.

7.49. Which of the following relations are partial orders on $\mathbb{Z}$?

1. $m \, R \, n$ if and only if $m = 0$.
2. $m \, R \, n$ if and only if $m \equiv_5 n$.
3. $m \, R \, n$ if and only if $m \geq n$. ($\geq$ is the usual "greater than or equal to" on $\mathbb{Z}$.)
4. $m \, R \, n$ if and only if $m^2 \leq n^2$.
5. $m \, R \, n$ if and only if m does not divide n.
6. $m \, R \, n$ if and only if $m \leq n^2$.

7.50. Prove that the "divides" relation | is a partial order on $\mathbb{N} \setminus \{0\}$.

7.51. Prove that the "divides" relation | is not a partial order on $\mathbb{Z}$.

7.52. Is the "divides" relation a partial order on $\mathbb{N}$.

7.53. Give an example of a relation on $\mathbb{Z}$ which is transitive and anti-symmetric but not reflexive on $\mathbb{Z}$.

7.54. Give an example of a relation on $\mathbb{Z}$ which is reflexive on $\mathbb{Z}$, anti-symmetric but not transitive.

7.55. Prove: If $<$ is a strict partial order on a set X then the relation $\leq$ on X defined by $x \leq y$ if and only if $x < y$ or $x = y$. ("$<$ is a strict partial order on X" means that $<$ is a relation on X which is transitive, anti-symmetric and satisfies $\forall x \in X$, $x \not< x$.)

7.56. Draw the Hasse diagram of the relation | restricted to the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

7.57. Draw the Hasse diagram of the relation | restricted to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

7.58. What are the immediate successors of 1 in the relation in problem 7.56?

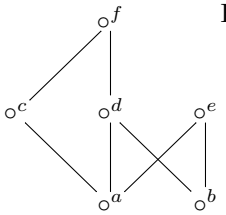
7.59. For the ordering of exercise 7.56 identify all maximal elements, all maximum elements, all minimal elements and all minimum elements.

7.60. For the ordering of exercise 7.57 identify all maximal elements, all maximum elements, all minimal elements and all minimum elements.

7.61. For the ordering of exercise 7.56 list all upper bounds of the set $\{2, 3\}$. List all lower bounds of this set. Give the least upper bound if there is one and the greatest lower bound if there is one.

7.62. For the ordering of exercise 7.56 list all upper bounds of the set $\{6, 9\}$. List all lower bounds of this set. Give the least upper bound if there is one and the greatest lower bound if there is one.

Following is the Hasse diagram of a partial ordering on the set $\{a, b, c, d, e, f\}$ Exercises 7.63 to 7.69 refer to this partial ordering.



7.63. What are the immediate successors of a.

7.64. What are the immediate predecessors of f.

7.65. What are the maximal elements?

7.66. What are the minimal elements?

7.67. Is there a maximum or minimum element?

7.68. Find a subset which has an upper bound but no least upper bound.

7.69. What are the upper bounds of $\emptyset$?

7.70. Give a partially ordered set $(X, \leq)$ and a subset Y of X such that Y has no upper bounds and no lower bounds.

7.71. Give a partially ordered set $(X, \leq)$ and a subset Y of X such that Y has an upper bound and no least upper bound.

7.72. Give a partially ordered set $(X, \leq)$ and a subset Y of X such that Y has a least upper bound which is an element of Y.

7.73. Give a partially ordered set $(X, \leq)$ and a subset Y of X such that Y has a least upper bound which is not an element of Y.

7.74. Assume that $(X, \leq)$ is a linearly ordered set. Prove that every minimal element is a minimum element.

7.75. Prove or disprove: If $(X, \leq)$ is partially ordered set in which every minimal element is a minimum element and every maximal element is a maximum element then $(X, \leq)$ is a linearly ordered set.

7.76. Prove or disprove: If $(X, \leq)$ is a partially ordered set in which every non-empty subset of X has a least upper bound and a greatest lower bound then $(X, \leq)$ is a linearly ordered set.

7.77. Prove or disprove: If $(X, \leq)$ is a partially ordered set in which every non-empty subset has a least element then $(X, \leq)$ is a linearly ordered set. (t is a least element of Y if $t \in Y$ and $\forall x \in Y$, $t \leq x$.)

7.78. Prove or disprove: If $(X, \leq)$ is a partially ordered set in which every non-empty subset of X has a least upper bound then every non-empty subset of X has a greatest lower bound.

7.79. Prove or disprove: If $(X, \leq)$ is a partially ordered set in which every non-empty subset of X with an upper bound has a least upper bound then every non-empty subset of X with a lower bound has a greatest lower bound.

Chapter 8

Basics of Number Theory

8.1 Induction and Well Ordering

For the Record we will need the following definitions:

Definition 8.1. Assume that A is a set of real numbers and that a is a real number then

1. The number a is a *lower bound* for A if (and only if) $\forall x \in A, a \leq x$.
2. The number a is an *upper bound* for A if $\forall x \in A, x \leq a$.

   Note that lower an upper bounds for a set may or may not be in the set.
3. The number a is a *least element* of A if
   (a) $a \in A$ and
   (b) $\forall x \in A, a \leq x$.
4. The number a is a *greatest element* of A if
   (a) $a \in A$ and
   (b) $\forall x \in A, x \leq a$.

Two important tools for working with natural numbers and integers are the *Well Ordering Property* and *Mathematical Induction*.

The generalized well ordering property: Any non-empty set of integers with a lower bound has a least element. In more symbolic form

$$\begin{aligned} &\text{If } A \text{ is a non-empty subset of } \mathbb{Z} \\ &\qquad \text{and } \exists m \in \mathbb{Z} \text{ such that } \forall n \in A, m \leq n \\ &\qquad\qquad \text{then } \exists m_0 \in A \text{ such that } \forall n \in A, m_0 \leq n \end{aligned} \tag{8.1}$$

The Principle of Mathematical Induction: If $P(n)$ is a sentence in which the variable n occurs and n_0 is an integer then in order to prove $P(n)$ is true for every integer greater than or equal to n_0 it suffices to prove two things:

(a) $P(n_0)$ is true.

(b) For all integers $k \geq n_0$, if $P(k)$ then $P(k+1)$.

Another closely related and useful principle is

The Greatest Element Property: If A is a non-empty set of integers which has an upper bound the A has a greatest element.

See exercise 8.3 for a proof.

The principles discussed in this section are the tools we will use in in studying the integers and the various relationships among them. In particular the *divides* relation which we look at in the next section.

8.2 The *Divides* Relationship and Greatest Common Divisors

Definition 8.2. Assume that a and b are integers. "a *divides* b" (or "a is a divisor of b" or "b is a multiple of a") means that there exists an integer k such that $b = ak$. The short hand notation for "a divides b" is $a \mid b$

For example $6 \mid 54$ since $54 = 6 \cdot 9$ and -6 divides 42 since $42 = (-6) \cdot 7$.

Theorem 8.3. *The following are true of the* divides *relation.*

$\forall n \in \mathbb{Z}, n \mid n$.

$\forall n, m$ *and* k *in* $\mathbb{Z}$, *if* $n \mid m$ *and* $m \mid k$ *then* $n \mid k$.

$\forall m$ *and* n *in* $\mathbb{Z}$, *if* $m \mid n$ *then* $-m \mid n$ *and* $m \mid -n$.

$\forall m$ *and* n *in* $\mathbb{Z}$, *if* $m \mid n$ *and* $1 \leq n$ *then* $m \leq n$. *(It follows that if* $n \neq 0$ *and* $m \mid n$ *then* $m \leq |n|$.*)*

The proof is an exercise (8.7).

The meaning of the phrase "the *greatest common divisor* of two integers" is relatively clear but here is a precise description.

Definition 8.4. Assume that at least one of a and b is not zero. The *greatest common divisor of* a *and* b is the largest integer d for which $d \mid a$ and $d \mid b$. In other words the greatest common divisor of a and b is the integer d for which

1. $d \mid a$ and $d \mid b$
2. $\forall n \in \mathbb{Z}$, if $n \mid a$ and $n \mid b$ then $n \leq d$.

The short hand notation for the greatest common divisor of a and b is $\gcd(a, b)$

Note that we have defined the greatest common divisor of two integers as *the* integer with certain properties. This means we are assuming that there is an integer with the required properties and that there is only one such integer. So to be mathematically correct, before giving definition 8.4 above, we should prove that for every pair of integers a and b (at least one of which is not zero) there is an integer d satisfying (1) and (2) and that there is only one such integer d. Here's an outline of the argument: Assume that a and b are integers and at least one of a and b is not zero.

To show that there is an integer d satisfying (1) and (2) we use the Greatest Integer Property. Let A be the set of integers which are divisors of both a and b. Now show A has an upper bound (This is why we require that at least one of a and b be non-zero.) and that $A \neq \emptyset$. The greatest element of A will fulfil conditions (1) and (2) in the definition of gcd. To show that there is *only* one such integer assume d_1 and d_2 are two integers satisfying (1) and (2) and show that $d_1 = d_2$.

In exercises 8.8 and 8.9 you are asked to give proofs using the outline above.

Why do we require that at least one of a and b be non-zero? The answer is that every integer is a divisor of 0. (To see this let b be any integer. To argue that $b \mid 0$ we would have to find an integer k such that $0 = b \cdot k$ and $k = 0$ works.) Therefore every integer is a common divisor of 0 and 0

One way of finding the gcd of two integers is to list the positive divisors of both and choose the largest number common to both lists.

Example 8.5. Find the greatest common divisor of 24 and 30. **Solution:** The positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12$ and 24. The positive divisors of 30 are $1, 2, 3, 5, 6, 10, 15$ and 30. The common divisors are $1, 2, 3$ and 6. The largest of the common divisors if 6 so $\gcd(24, 30) = 6$.

An indispensable tool for finding and working with greatest common divisors is a theorem known as the *division algorithm.*

8.3 The Division Algorithm

We know from elementary school mathematics that if a and d are two integers and $d \neq 0$ then it is possible to divide a by d and get a quotient q and a remainder r. For example, if $a = 87$ and $d = 7$ then the quotient $q = 12$ and the remainder is $r = 3$. The result of this division could be written in equation form as $87 = 12 \cdot 7 + 3$. The theorem known as the *division algorithm* says that this division is always possible.

Theorem 8.6. ***The Division Algorithm.*** *For all integers a and all positive integers d, there unique integers q and r such that $a = qd + r$ and $0 \leq r < d$.*

Given a and d as in the theorem, one way to find q and r is to rewrite the equation $a = qd + r$ in the form $r = a - qd$. Then plug in values of q until the corresponding r satisfies the inequality $0 \leq r < d$. For example if $a = 38$ and $d = 11$ we know that we want $r = 38 - 11q$. Trying $q = 0, 1, 2, 3$, etc. we get

the following values of r: $38, 27, 16, 5, -6$, The value of r for which $0 \leq r < 11$ is $r = 5$ and this occurs when $q = 3$. So the values of r and q which satisfy the conclusion of the theorem are 5 and 3 respectively.

One reason for finding q and r by the method described above is that it reflects what we will do in the proof of the division algorithm.

There are really two parts to the proof of Theorem 8.6., the existence of q and r and the uniqueness of q and r. These are exercises 8.11 and 8.12

Example 8.7. Show that the greatest common divisor of 30 and 17 can be written in the form $30s + 17t$ where s and t are integers. This can be done by listing the multiples of 17 until you find one that differs from a multiple of 30 by the gcd.

Example 8.5 gives what turns out to be an inefficient method for fining the greatest common divisor of two integers. It's also true that writing $\gcd(a, b)$ as $sa + tb$ by the method described in Example 8.7 is not usually easiest. The division algorithm provides a more efficient way of doing both of these calculations.

8.4 Uses of the Division Algorithm

8.4.1 Find the Greatest Common Divisor

8.4.2 Writing the $\gcd(a, b)$ as $sa + tb$

Theorem 8.8. *For any two integers a and b with at least one of a and b not equal to zero, there exists integers s and t such that* $\gcd(a, b) = sa + tb$.

The proof of this theorem is Exercise 8.14.

One way of looking at the remainder r from the division algorithm is to use the idea of *congurence*. That's what we study in the next section.

8.5 Congurence and Modular Arithmetic

Definition 8.9. If a and d are integers and $d \geq 1$, then the phrase "q is the quotient and r is the remainder when a is divided by d" means that q and r are the unique integers for which $a = qd + r$ and $0 \leq r < d$. (In Theorem 8.6 we showed that such a q and d exist and that they are unique.) We shall use the shorthand notation $a \pmod d$ for the remainder when a is divided by d.

Definition 8.10. Assume that a, b and m are integers and that $m \geq 2$. Then we say *a is congruent to b modulo m* and write $a \equiv_m b$ if and only if $m \mid (b - a)$. The congruence $a \equiv_m b$ may also be writen $a \equiv b \pmod m$ or $a \equiv b \mod m$. There is less chance for confusing notation if we use $a \equiv_m b$.

Using the Definition 8.10 there are several equivalent formulations of the sentence $a \equiv_m b$):

$$a \equiv_m b \text{ iff } \begin{cases} b - a = km \text{ for some } k \in \mathbb{Z} \\ b = a + km \text{ for some } k \in \mathbb{Z} \\ a \text{ and } b \text{ give the same remainder when divided by } m \\ a \,(\text{mod } m) = b \,(\text{mod } m) \end{cases} \tag{8.2}$$

Also note that any integer a is congruent modulo m to the remainder when a is divided by m and that any multiple of m is congruent to 0 modulo m. Writing these facts in symbolic form gives us (assuming m is an integer greater than 1.)

$$\forall a \in \mathbb{Z},\ a \equiv_m [a \,(\text{mod } m)] \tag{8.3}$$

and

$$\forall k \in \mathbb{Z},\ km \equiv_m 0. \tag{8.4}$$

Since the only possible remainders when an integer is divided by m are $\{0, 1, 2, \ldots, m-1\}$, every integer is congruent to one of these modulo m.

Example. Prove that for all integers a, b, c, d and m, if $a \equiv_m b$ and $c \equiv_m d$ then $a + c \equiv_m b + d$ and $ac \equiv_m bd$. (Use Definition 8.10 or any of the equivalent statements in equation (8.2).)

Example. Prove that for all integers a, b and c, the following are true :

1. If $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$. (Use any of the characterizations of $a \equiv_m b$ from displayed formula (8.2)).

2. $a \equiv_m a$.

3. If $a \equiv_m b$ then $b \equiv_m a$.

Sometimes it's easier to work with the remainders. We let $\mathbb{Z}_m$ be the set of possible remainders when an integer is divided by m. In other words $\mathbb{Z}_m = \{0, 1, 2, \ldots m-1\}$. We then define and addition $+_m$ and a multiplication $\cdot_m$ on $\mathbb{Z}$ as follows:

Definition 8.11. Assume m is an integer, that $m \geq 2$ and that a and b are in $\mathbb{Z}$.

1. $a +_m b$ is the integer $s \in \mathbb{Z}_m$ for which $a + b \equiv_m s$. That is, $a +_m b$ is the remainder when $a + b$ is divided by m or in abbreviated form $a +_m b = (a + b) \,(\text{mod } m)$.

2. $a \cdot_m b$ is the integer $p \in \mathbb{Z}_m$ for which $ab \equiv_m p$. That is, $a \cdot_m b$ is the remainder when ab is divided by m which could be written $a \cdot_m b = (ab) \,(\text{mod } m)$.

We will frequently use the equation formulation of these definitions: $a +_m b = (a + b) \pmod m$ and $a \cdot_m b = (ab) \pmod m$.

Although $a +_m b$ and $a \cdot_m b$ are defined for all integers a and b, the result is always in $\mathbb{Z}_m$ so $\mathbb{Z}_m$ is closed under the two operations $+_m$ and $\cdot_m$. That is, $\forall a$ and b in $\mathbb{Z}_m$, $a +_m b$ and $a \cdot_m b$ are in $\mathbb{Z}_m$. Sometimes this fact is expressed by saying that $+_m$ and $\cdot_m$ are operations on $\mathbb{Z}_m$.

One connection between congruence modulo m and the system $(\mathbb{Z}_m, +_m, \cdot_m)$ is given by the following theorem.

Theorem 8.12. *Assume $m \geq 2$ is an integer and that x and y are in $\mathbb{Z}$. Then*

1. $x + y \equiv_m x +_m y$
2. $xy \equiv_m x \cdot_m y$
3. *if $x = y$ then $x \equiv_m y$.*
4. *if x and y are in $\mathbb{Z}_m$ and $x \equiv_m y$ then $x = y$.*

Example. Prove Theorem 8.12. (For part 1 note that by definition 8.11, $x +_m y = (x + y) \pmod m$ and by Equation (8.3) letting $a = x + y$, $x + y \equiv_m [(x + y) \pmod m]$.)

The system $(\mathbb{Z}_m, +_m, \cdot_m)$ has many of the properties of the integers with ordinary addition and multiplication. For example $\forall x \in \mathbb{Z}_m, 0 +_m x = x$ and $1 \cdot_m x = x$. It is also easy to verify properties like $\forall x, y$ and $z \in \mathbb{Z}_m, x +_m (y +_m z) = (x +_m y) +_m z$.

In general any identity involving only the operations $+$ and $\cdot$ which holds in the system $(\mathbb{Z}, +, \cdot)$ also holds in the system $(\mathbb{Z}_m, +_m, \cdot_m)$ if every occurrence of $+$ is replaced by $+_m$ and every occurrence of $\cdot$ is replaced by $\cdot_m$. We will assume this from now on.

See the exercises for a more careful statement of this principle and for a proof.

Another property of the integers is that $\forall x \in \mathbb{Z}$, there is a $y \in \mathbb{Z}$ (namely $y = -x$) such that $x + y = 0$. The corresponding statement is also true in $(\mathbb{Z}_m, +_m, \cdot_m)$.

Example. Prove $\forall x \in \mathbb{Z}_m, \exists y \in \mathbb{Z}_m$ such that $x +_m y = 0$. (Note that $y = -x$ will not work since for $x \in \mathbb{Z}_m$, $-x \in \mathbb{Z}_m$ only if $x = 0$. Show that $y = -x \pmod m$ works.)

Turning to another property, the only two integers x for which there is some integer y such that $x \cdot y = 1$ are $x = 1$ and $x = -1$. In the system $(\mathbb{Z}_m, +_m, \cdot_m)$ more is true.

Theorem 8.13. *For all integers $m \geq 2$ and x, the following are equivalent*

1. $\gcd(m, x) = 1$
2. *$\exists y \in \mathbb{Z}$ such that $xy \equiv 1 \mod m$.*

Proof. We will prove that 1 implies 2. Assume the hypotheses of the theorem and assume that $\gcd(m, x) = 1$. We need to construct a $y \in \mathbb{Z}$ such that $xy \equiv 1 \mod m$. Using the result of problem 8 from Handout 1 we know that there are integers s and t such that $sm + tx = 1$. Therefore $sm + tx \equiv 1 \mod m$. But $sm \pmod m = 0$ so $sm \equiv 0 \mod m$. So, replacing sm by 0 in the previous congruence we obtain $tx \equiv 1 \mod m$. Therefore $y = t$ fulfills the required conditions. □

Example. From Theorem 8.13, prove that part 2 implies part 1.

Congruence and Fermat's Little Theorem

We have seen that if p is a prime integer then

$$\forall x \in \mathbb{Z}, \text{ if } p \nmid x \text{ then } \exists y \in \mathbb{Z} \text{ such that } xy \equiv_p 1 \tag{8.5}$$

(This is because $p \nmid x$ implies that $\gcd(p, x) = 1$.) Translated into a fact about the system $(\mathbb{Z}_p, +_p, \cdot_p)$ this becomes is

$$\forall x \in \mathbb{Z}_p \text{ if } x \neq 0 \text{ then } \exists y \in \mathbb{Z}_p \text{ such that } x \cdot_p y = 1 \tag{8.6}$$

The theorem known as *Fermat's Little Theorem* is another fact which can be stated either as a fact about congruence $\mod p$ or as a fact about the system $(\mathbb{Z}_p, +_p, \cdot_p)$ (where p is a prime). Here is the theorem in its two forms.

Theorem 8.14. *Assume that $p \in \mathbb{Z}$ is prime then*

1. *(First Form) For all integers x, if $p \nmid x$ then $x^{p-1} \equiv_p 1$.*
2. *(Second Form) For all $x \in \mathbb{Z}_p$, if $x \neq 0$ then $\underbrace{x \cdot_p x \cdot_p \cdots \cdot_p x}_{p-1 \text{ factors}} = 1$.*

Note that the the First Form the assumption $p \nmid x$ is equivalent to $x \not\equiv 0 \mod p$ and the conclusion could be written as $x^p \equiv 1 \mod p$. Also note in the Second Form that $\underbrace{x \cdot_p x \cdot_p \cdots \cdot_p x}_{p-1 \text{ factors}}$ could be written in the shorter form $x^{p-1} \pmod p$.

In order to prove the theorem we will need the following facts:

1. If A is any finite set then a one to one function from A into A is onto A.[1] (Recall that a function f with domain D is *one to one* if $\forall x$ and y in D, if $f(x) = f(y)$ then $x = y$ and f is *onto* B if $\forall z \in B, \exists x \in D$ such that $f(x) = z$.)
2. If $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set of integers and f is a one to one function from A onto A then $a_1 \cdot a_2 \cdot \cdots \cdot a_n = f(a_1) \cdot f(a_2) \cdot \cdots \cdot f(a_n)$. (This is because the sequence $(f(a_1), f(a_2), \ldots, f(a_n))$ is just a rearrangement of the sequence $(a_1, a_2, \ldots, a_n)$.

[1] Although this fact is fairly obvious, it is possible to prove it by mathematical induction on the number of elements in A.

3. Also recall that $x +_m y \equiv x + y \mod m$ and that $x \cdot_m y \equiv xy \mod m$.

Proof. (of the theorem, First Form) Assume $p \in \mathbb{Z}$ is prime and that x is an integer for which $p \nmid x$. By our assumptions the remainder when x is divided by p, that is $x \pmod p$, is not zero and therefore is in $A = \{1, 2, \ldots, p-1\}$. Let a be this remainder. Using our notation for the remainder $a = x \pmod p$. In order to complete the proof of the theorem we have to prove that $x^{p-1} \equiv 1 \mod p$. Since $x \equiv a \mod p$ it will be enough to prove

$$1 \equiv a^{p-1} \mod p \tag{8.7}$$

We now consider the multiples $a, a \cdot_p 2, a \cdot_p 3, \ldots, a \cdot_p (p-1)$ of a in $\mathbb{Z}_p$.

Lemma 8.15. *For all $k \in A = \{1, 2, \ldots, p-1\}$, $a \cdot_p k$ is not zero, that is $ak \pmod p \neq 0$ and therefore $a \cdot_p k = ak \pmod p \in A$.*

Example. Prove Lemma 8.15. (Hint: Use a proof by contradiction and Equation (8.6.)

Lemma 8.16. *For all k_1 and k_2 in A, if $a \cdot_p k_1 = a \cdot_p k_2$ then $k_1 = k_2$.*

Example. Prove Lemma 8.16.

The next step in the proof is to define the function f with domain A by the formula $f(k) = a \cdot_p k$. Lemma 8.15 tells us that f is a function into A and by Lemma 8.16, f is one to one. Therefore by Fact 1 f is onto A and so by Fact 2 we have

$$1 \cdot 2 \cdot \cdot 3 \ldots \cdot (p-1) = f(1) \cdot f(2) \cdot f(3) \cdot \ldots \cdot f(p-1) \text{ therefore} \tag{8.8}$$

$$1 \cdot 2 \cdot \cdot 3 \ldots \cdot (p-1) \equiv f(1) \cdot f(2) \cdot f(3) \cdot \ldots \cdot f(p-1) \mod p \tag{8.9}$$

So using the definition of f gives

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv a(a \cdot_p 2)(a \cdot_p 3 \cdot \cdots \cdot (a \cdot_p (p-1)) \mod p \tag{8.10}$$

Since for all z and w, $z \cdot_p w \equiv zw \mod p$ equation (8.10) is equivalent to

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv a(a \cdot 2)(a \cdot 3) \cdots (a \cdot (p-1)) \mod p \text{ or} \tag{8.11}$$

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv a^{p-1}(1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)) \mod p \tag{8.12}$$

If we let $b = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ then the congruence (8.12) can be written

$$b \equiv a^{p-1} b \mod p \tag{8.13}$$

Since $\gcd(b, p) = 1$ we may use Equation (8.5) to conclude that there is an integer c such that $bc \equiv 1 \mod p$. Multiplying both sides of the congruence (8.13) by c gives

$$1 \equiv a^{p-1} \mod p \tag{8.14}$$

But this is Equation (8.7) so the proof is complete. □

Example. Prove the converse of Theorem 8.14. That is, assume $m \geq 2$ is an integer for which $\forall x \in \mathbb{Z}$, if $m \nmid x$ then $x^{m-1} \equiv 1 \mod m$ and prove that m is prime. (Hint: It is enough to show that $\forall x \in \mathbb{Z}$ such that $2 \leq x \leq m-1$ that x is not a divisor of m. Toward a proof by contradiction assume that $2 \leq x \leq m-1$ and that $x \mid m$. Then $m = zx$ where z is an integer between 2 and $m-1$. It follows from this that $zx \equiv 0 \mod m$.)

An easy consequence of Fermat's Little Theorem is the following corollary.

Corollary 8.17. *If p is prime then for all integers x, $x^p \equiv x \mod p$.*

Note that the requirement that $p \nmid x$ is missing from the corollary. This is because in the case that $p \mid x$ both sides of the congruence are congruent to 0.

From this corollary it is easy to prove

Corollary 8.18. *If p is prime then for all integers x and y, $(x+y)^p \equiv x^p + y^p \mod p$.*

This follows since by Corollary 8.17 both sides of the congruence in Corollary 8.18 are congruent to $x + y$.

We know by Problem 8.5 that Fermat's Theorem holds only for primes. We now investigate whether or not either of the two corollaries can hold for integers that are not prime.

To summarize what we have done and to describe what we want to do we will use $\mathcal{R}(m)$, $\mathcal{S}(m)$ and $\mathcal{T}(m)$ for the following sentences:
$\mathcal{R}(m)$ is the sentence $\forall x \in \mathbb{Z}, if\, m \nmid x$ then $x^{m-1} \equiv 1 \mod m$.
$\mathcal{S}(m)$ is the sentence $\forall x \in \mathbb{Z}, x^m \equiv x \mod m$ and
$\mathcal{T}(m)$ is the sentence $\forall x$ and y in $\mathbb{Z}$, $(x+y)^m \equiv x^m + y^m \mod m$.

Using these abbreviations, Fermat's Little Theorem is "If p is prime then $\mathcal{R}(p)$", Problem 8.5 is "If $\mathcal{R}(m)$ then m is prime", Corollary 8.17 is "If p is prime then $\mathcal{S}(p)$" and Corollary 8.18 is "If p is prime then $\mathcal{T}(p)$."

Example. Prove that for all integers $m \geq 2$, if $\mathcal{S}(m)$ then $\mathcal{T}(m)$. (See the paragraph following Corollary 8.18.)

Example. Prove that for all integers $m \geq 2$, if $\mathcal{T}(m)$ then $\forall w \in \mathbb{Z}$, if $w \geq 0$ then $w^m \equiv w \mod m$. (Note that the conclusion of this "if ... then" is almost $\mathcal{S}(m)$, just restricted to non-negative values of w.) This new version of Problem 8.5. can be proved by mathematical induction on w. That is, assume $T(m)$ and then prove by mathematical induction that $\forall w \in Z$ if $w \geq 0$ then $w^m \equiv w \mod m$.

8.6 Exercises

8.1. Prove that if A is a set of real numbers then A has at most one least element and at most one greatest element. (Hint: To show A has at most one least element assume that a_1 and a_2 are least elements of A and show that $a_1 = a_2$.)

8.2. Prove the generalized well ordering property from the well ordering property using the following outline.

OUTLINE: Assume that $A \subseteq Z$, $A \neq \emptyset$ and $\exists m \in \mathbb{Z}$ such that $\forall n \in A$, $m \leq n$. (We have to find an $m_0 \in A$ such that $\forall n \in A$, $m_0 \leq n$.)

Assuming that m is an integer for which $\forall n \in A$, $m \leq n$ we shift A to the right by $-m$ units to get a new set of integers A'. That is, let $A' = \{n - m : n \in A\}$. Now we argue that A' is non-empty and that $A' \subseteq \mathbb{N}$. Assuming that this has been done, by the well ordering property of $\mathbb{N}$, A' has a least element, call it k_0. Let $m_0 = k_0 + m$.

To complete the argument we have to show that this choice of m_0 works.

8.3. Prove the greatest element property. (Hint: Let U be the set of integer upper bounds of A, i.e. $U = \{b \in \mathbb{Z} : \forall x \in A, x \leq b\}$. Show that U is non-empty and has a lower bound. By the *generalized well ordering property* U has a least element.)

8.4. What are the divisors of zero? Why? For what integers k is it true that $0 \mid k$? Why?

8.5. If k is a non-zero integer what is the greatest divisor of k?

8.6. What is the greatest common divisor of -60 and -26? If a and b are any integers at least one of which is non-zero why is it true that $\gcd(a, b) > 0$?

8.7. Prove the following properties of the *divides* relation.

1. $\forall n \in \mathbb{Z}, n \mid n$.
2. $\forall n, m$ and k in $\mathbb{Z}$, if $n \mid m$ and $m \mid k$ then $n \mid k$.
3. $\forall m$ and n in $\mathbb{Z}$, if $m \mid n$ then $-m \mid n$ and $m \mid -n$.
4. $\forall m$ and n in $\mathbb{Z}$, if $m \mid n$ and $1 \leq n$ then $m \leq n$. (It follows that if $n \neq 0$ and $m \mid n$ then $m \leq |n|$.)

8.8. Show that there is an integer d satisfying conditions 1 and 2 of Definition 8.4 using the outline given in the paragraph following the definiton.

8.9. Show that there is *only* one integer satisfying conditions 1 and 2 of Definition 8.4. Use the outline given after the definition.

8.10. Find the q and the r which satisfy the conclusion of the theorem for $a = 76$ and $d = 15$ using the method described in the paragraph above. Repeat with $a = -76$ and $d = 15$.

8.11. Prove that for all integers a and all positive integers d that there exist integers q and r such that $a = qd + r$ and $0 \leq r < d$. (Hint: Let $A = \{r' \in \mathbb{Z} : r' \geq 0 \text{ and for some } q' \in \mathbb{Z}, r' = a - q'd\} = \{a - q'd : a - q'd \geq 0 \text{ and } q' \in \mathbb{Z}\}$. Show that $A \neq \emptyset$ and use the Well Ordering Property.)

8.12. Prove the uniqueness of q and r in Theorem 8.6. by assuming that a and d are integers with $d > 0$. Assume further that q_1, r_1, q_2 and r_2 are integers satisfying $a = q_1 d + r_1$, $a = q_2 d + r_2$, $0 \leq r_1 < d$ and $0 \leq r_2 < d$. Prove that $r_1 = r_2$ and $q_1 = q_2$.

8.13. For the following pairs of integers a and b find $\gcd(a, b)$ and write it in the form $sa + tb$ where s and t are integers.

1. $a = 84$, $b = 525$.
2. $a = 75$, $b = 1024$.
3. $a = 6825$, $b = 168$.
4. $a = -24$, $b = 16$.
5. $a = -82$, $b = -110$

8.14. Prove Theorem 8.8. I.e., prove that for any two integers a and b with at least one of a and b not equal to zero, there exists integers s and t such that $\gcd(a, b) = sa + tb$. (Hint: Let A be the set of positive integers which can be written in the form $\sigma a + \tau b$ where σ and τ are integers. Show that $A \neq \emptyset$ and then use the Well Ordering Property.)

8.15. By Theorem 8.8 if a and b are integers at least one of which is not zero then there are integers s and t such that $gcd(a, b) = sa + tb$. But the following statement is not true: For all integers a and b at least one of which is non-zero and for all integers w, if $w = sa + tb$ for some integers s and t then w is $\gcd(a, b)$. Show that this statement is not true by finding four counter examples: With $a = 18$ and $b = 64$, with $a = 25$ and $b = 45$, with $a = 100$ and $b = 30$ and with $a = 7$ and $b = 13$.

8.16. Assume that a and b are integers at least one of which is non-zero. Formulate a conjecture about those integers w which can be written in the form $w = sa + tb$ for some $s, t \in \mathbb{Z}$.

8.17. Prove the conjecture you formulated in problem 8.16.

8.18. Recall that for integers a and b, not both zero, $\gcd(a, b)$ was defined to be the the largest integer d for which $d \mid a$ and $d \mid b$. In other words the greatest common divisor of a and b is the integer d for which

(a) $d \mid a$ and $d \mid b$

(b) $\forall n \in \mathbb{Z}$, if $n \mid a$ and $n \mid b$ then $n \leq d$.

Also recall that

$$\text{for positive integers } n \text{ and } r, \text{ if } n \mid r \text{ then } n \leq r. \tag{8.15}$$

Prove the following fact about $\gcd(a, b)$: $\forall n \in \mathbb{Z}$, if $n \mid a$ and $n \mid b$ then $n \mid \gcd(a, b)$. (Note that if $n \mid a$ and $n \mid b$ then by condition (b) in the definition of gcd we can say that $n \leq d$. In this problem we're showing that the conclusion $n \leq d$ can be replaced by the stronger conclusion $n \mid d$. Hint: Use Theorem 8.8.)

Chapter 9

The Topology of the Real Line

9.1 Introduction

In this chapter we shall investigate the real numbers $\mathbb{R}$, subsets of the real numbers and certain properties that a subset of the real numbers may or may not have. We will begin with subsets of the real numbers with which you are familiar, namely intervals. This will lead naturally to the study of *open* and *closed* subsets of the real numbers and to the concepts of the *boundary* and *interior* of a set of real numbers. This study of open and closed subsets of $\mathbb{R}$ is sometimes referred to as the study of the topology of $\mathbb{R}$. (In fact the collection of all open subsets of $\mathbb{R}$ is called *the* topology of $\mathbb{R}$.)

We shall use the topology of $\mathbb{R}$ to illustrate the rôle of variables and quantifiers in mathematical statements and in mathematical proofs. In the process we shall introduce several new proof principles.

9.2 Open and Closed Sets of Real Numbers

In this section we will rely heavily on the interval notation introduced in Chapter **??**, Definition 1.2. Recall that if a and b are in $\mathbb{R}$, then $(a, b) = \{x \in \mathbb{R} : a < x < b\}$. That is (a, b) is the set of all real numbers between a and b not including a and not including b. (a, b) is called the *open interval* from a to b. $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$. $[a, b]$ is the *closed interval* from a to b. Note also that the notation (a, b) is also used for the ordered pair whose first component is a and whose second component is b. This is unfortunate but standard. It should always be clear from the context which meaning, ordered pair or interval, is intended.

We will also be using the *denseness property* of the ordering on the real numbers which we state as a theorem.

Theorem 9.1. *(**Denseness Property of** $\mathbb{R}$) For all real numbers a and b, if $a < b$ then there is a real number c such that $a < c < b$.*

Proof. (The argument will use the Archimedian Property from Exercise 4.45 in Chapter 4.) Assume that a and b are real numbers and that $a < b$. Then $0 < b - a$. By the Archimedian Property there exist $n \in \mathbb{N}$ such that $0 < \frac{1}{n} < b - a$. Adding a to all three parts of this inequality gives $a < a + \frac{1}{n} < b$. Hence $c = a + \frac{1}{n}$ fulfils the required conditions. □

Before giving the next definition, we make two remarks. The first is that if a, b, c and d are real numbers with $a < b$ and $c < d$, then saying $(a, b) \subseteq (c, d)$ is equivalent to saying $c \leq a < b \leq d$. Secondly, if a is a real number and ϵ is a positive real number, then $(a - \epsilon, a + \epsilon)$ is an open interval of length 2ϵ (or sometimes we say "of radius ϵ") centered at a.

We now give definitions of "open" and "closed" for arbitrary sets of real numbers (which may or may not be intervals.)

Definition 9.2. A set A of real numbers is *open* if for every $x \in A$, there is a positive number ϵ such that $(x - \epsilon, x + \epsilon) \subseteq A$.

Example 9.3. If $a < b$ (where a and b are real numbers) then the open interval (a, b) us open sets of real numbers in the sense of the definition just given. *Proof.* Assume $x \in (a, b)$.

Before continuing the proof we pause to note that by the definition of *open* we need to construct a positive number ϵ for which the interval of radius ϵ centered at x (that is, $(x - \epsilon, x + \epsilon)$) is a subset of (a, b). By the remarks before the definition of "open" this means that for the ϵ we construct $a \leq x - \epsilon < x + \epsilon \leq b$. The inequality $x - \epsilon < x + \epsilon$ will be true for any positive ϵ therefore we will have to make sure that $a \leq x - \epsilon$ and $x + \epsilon < b$. Solving these inequalities for ϵ gives $\epsilon \leq x - a$ and $\epsilon \leq b - x$. Letting ϵ be the smaller of $x - a$ and $b - x$ would make both of these inequalities true. This paragraph is the scratch work for the construction of ϵ. We now continue the proof.

Let ϵ be the smaller of $x - a$ and $b - x$. Since $a < x < b$, both $x - a$ and $b - x$ are positive and therefore $\epsilon > 0$. Further $\epsilon \leq x - a$ and $\epsilon \leq b - x$. It follows from these two inequalities that $a \leq x - \epsilon$ and $x + \epsilon \leq b$. Combining these inequalities with $x - \epsilon < x + \epsilon$ we obtain $a \leq x - \epsilon < x + \epsilon \leq b$. Therefore $(x - \epsilon, x + \epsilon) \subseteq (a, b)$. □

Other examples of open sets are $(-1, 4) \cup (6, 11), \mathbb{R}^+ = (0, \infty), \mathbb{R}$ and $\emptyset$ (the empty set).

Definition 9.4. A set A of real numbers is *closed* if its complement $\mathbb{R} - A = \{x \in \mathbb{R} : x \notin A\}$ is open.

Closed intervals are closed sets of real numbers using the meaning of "closed" just given. For example $[0, 2]$ is the complement of $(-\infty, 0) \cup (2, \infty)$ which is open. $(-\infty, 0]$ is closed since it is the complement of $(0, \infty)$ which is open. Sets

consisting of a single real number are closed. For example, $\left\{\frac{1}{2}\right\}$ (the set whose only element is $\frac{1}{2}$) is closed. Finite sets of real numbers like $\{-1, 0, 2, \frac{5}{2}\}$ are closed. How does one prove that all these sets are closed? We'll look at some examples in class and others will be in the exercises.

Definition 9.5. If $A \subseteq \mathbb{R}$ and $b \in \mathbb{R}$ then b is a emphcluster point of A (or a emphlimit point of A or an emphaccumulation point of A) if for every positive number ϵ, the open interval $(b-\epsilon, b+\epsilon)$ contains at least one point of A different from b.

For example 0 is a cluster point of the set

$$A = \left\{ \frac{1}{n} : n \in \mathbb{N} \text{ and } n \neq 0 \right\}$$

1/2 is a cluster point of the interval $(0, 1)$ and 0 is a cluster point of the interval $(0, 1)$. In fact, every real number in [0,1] is a cluster point of (0,1).

Definition 9.6. Assume $A \subseteq \mathbb{R}$ then the emphboundary of A is the set of all points which are both cluster points of A and cluster points of $\mathbb{R} \setminus A$. That is, x is in the boundary of A if x is a real number such that for every positive number ϵ, the open interval $(x - \epsilon, x + \epsilon)$ contains and element of A different from

9.3 Exercises

9.1. Assume that $a \in \mathbb{R}$. Give the definitions of (a, ∞), $[a, \infty)$, $(-\infty, a)$ and $(-\infty, a]$.

9.2. Prove that the open interval $(-1, 3)$ is an open set.

9.3. Prove that the set $(-1, 3) \cup (5, 9)$ is open.

9.4. Prove that $\emptyset$ is an open set.

9.5. Prove that if A and B are open subsets of $\mathbb{R}$ then $A \cup B$ is open.

9.6. Prove that if A and B are open subsets of $\mathbb{R}$ the $A \cap B$ is open.

Chapter 10

The Axiomatic Method

10.1 Introduction

The first know use of axioms occurred in the geometry of the Greeks sometime before 300 B. C. They probably arose partly as an answer to the question "what does it mean to prove a geometric proposition" and partly because of a realization that not every geometric fact can be proved. There must be some starting point: Some geometric facts must be assumed and used without proving them.

The basic idea behind the Greek's axiomatic approach to geometry (say the geometry of a plane) was fairly simple: Begin by assuming some obvious facts (like "Given any two distinct points there is exactly one line containing both of the points") These obvious facts are called the axioms or postulates. All other facts must be proved from the axioms.

10.2 The Two Ways The Axiomatic Method is Used

In modern mathematics there are two ways in which axioms are used. The first is similar to that employed by the Greeks. Using axioms in this first way we have some particular mathematical structure that we wish to study. We give a list of axioms (or set of axioms or system of axioms) - obvious properties of the structure - which serve as our starting point. These we assume without proof and all other properties of the structure are proved from the axioms. This approach has been used to study the geometry of a plane, to study the structure consisting of the set $\mathbb{N}$ of natural numbers together with the operations of addition and multiplication and the relation $<$, to study the structure consisting of the set of real numbers $\mathbb{R}$ together with addition, multiplication and $<$, the structure consisting of the universe of sets and the relation $\in$ and many other mathematical systems. One goal in using axioms in this way is to choose the

axioms so that every true statement about the structure being studied can be proved from the chosen axioms. This would mean, among other things, that given any statement P about the structure, either P or it's negation $\neg P$ would be provable from the axioms.

We use axioms in the second way when we have several similar mathematical structures that we want to study which, although not identical in any sense, have some common properties. The first step is to list the particular properties that interest us. These are the axioms. We then give a name to systems that have these common properties.

This was the procedure that we followed in our definition of *partially ordered set* (Definition 7.14 part 1 from Chapter 7). There are many structures, for example the structures $(\mathbb{R}, \leq)$, $(\mathbb{N}, \leq)$, $(\mathbb{N}, |)$ (where $|$ is the "divides" relation), and $(\mathcal{P}(A), \subseteq)$ where A is any set, consisting of a set and a relation on that set with the properties that the relation is anti-symmetric, transitive and reflexive on the set. Any structure of this type and satisfying these properties we call a partially ordered set.

Here's the definition again in expanded form.

Definition 10.1. The structure (X, R) is called a *partially ordered set* if

(P1) $\forall x$ and $\forall y$, if $x \; R \; y$ and $y \; R \; x$, then $x = y$. (Anti-symmetric property)

(P2) For all x, y and z, if $x \; R \; y$ and $y \; R \; z$ then $x \; R \; z$. (Transitive property)

(P3) $\forall x \in X$, $x \; R \; x$. (Reflexive property)

The properties (P1), (P2) and (P3) are the axioms. They constitute the definition of what it means for a set and a relation on that set to be a partially order set and are referred to as the *partial order axioms*.

This second way of using axioms can be a great time saving device since any mathematical structure in which the axioms are true will also satisfy any property proved from the axioms. So, for example, if we prove a theorem from the partial orders axioms, then we have something that is true of every structure in which (P1), (P2) and (P3) are true. The important point is that when the axioms are formulated we are not attempting to characterize a single mathematical structure. Rather we are listing some properties common to several mathematical structures.

Either use of the axiomatic method provides a way of organizing mathematical knowledge. If we use axioms in the second way we have classified mathematical structures according to their properties: All structures satisfying (P1), (P2) and (P3) are partial orders. If we use axioms in the first way and succeed in finding a small number of relatively simple formulas from which all known theorems about a particular structure can be derived, then, in a sense, our knowledge about the structure has been distilled into this set of formulas.

10.3 A Geometric Example

We now give an axiom system for a kind of geometry. Specifically, we intend to describe a structure (P, L, On) where P and L are sets (referred to as *the set of points* and *the set of lines* respectively) and On is a binary relation on $P \cup L$. For x and y in $P \bigcup L$, $x\ On\ y$ will be read "x is on y" or "y contains x." We have chosen the name *simple plane* for the kind of structure we are describing. Here are the "simple plane" axioms given as a definition.

Definition 10.2. A *simple plane* is a triple (P, L, On) where P and L are sets and On is a relation on $P \cup L$ for which the following are true:

(SP1) There are at least two elements in P.

(SP2) $\forall x, z \in P \cup L$, if $x\ On\ z$ then $x \in P$ and $z \in L$.

(SP3) $\forall x$ and $y \in P$, if $x \neq y$ then there is exactly one $z \in L$ such that $x\ On\ z$ and $y\ On\ z$.

(SP4) $\forall z \in L$, $\exists x \in P$ such that $\neg x\ On\ z$.

(SP5) $\forall z \in L$, $\forall x \in P$, if $\neg x\ On\ z$ then there is exactly one $z' \in L$ such that $x\ On\ z'$ and $\forall y \in P$ it's not the case that $y\ On\ z$ and $y\ On\ z'$.

We now introduce the following definition.

Definition 10.3. For z and z' in $P \cup L$, *"z is parallel to z'"* or *"z and z' are parallel"* means z and z' are in L and $\forall x \in P$, either $\neg x\ On\ z$ or $\neg x\ On\ z'$.

Using this definition and the terminology introduced in the paragraph preceding definition 10.2 (SP1) through (SP5) could be written as follows:

(SP1) There are at least two points.

(SP2) If x is on z then x is a point and z is a line.

(SP3) If x and y are distinct points then there is exactly one line containing x and y.

(SP4) If z is a line there is a point not on z.

(SP5) If z is a line and x is a point not on z then there is exactly one line containing x and parallel to z.

Note that if P and L are the points and lines respectively of a coordinate plane and $x\ On\ z$ means that x is on z in the usual sense, then (P, L, On) is a simple plane, in other words the simple plane axioms (SP1) through (SP5) are true of (P, L, On). This is sometimes expressed by saying that (P, L, On) is a *model* of the simple plane axioms.

We will sometimes draw pictures as a guide for our proofs. For example

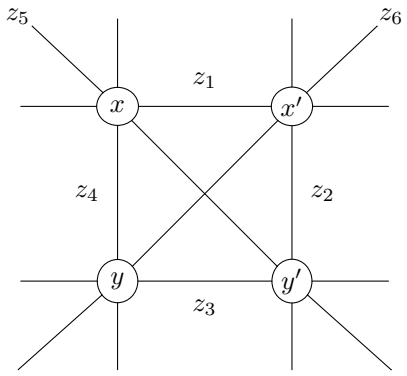


Figure 10.1: A model of the simple plane axioms

The four labeled circles represent four points x, x', y and y' and the six line segments labeled z_1 through z_6 represents lines. In general a diagram like this will represent only part of a simple plane and there may be other points and lines which are not pictured. However this particular diagram is a model of the simple plane axioms (if we let P be the set consisting of the four circles labeled x, x', y and y', if we let L consist of the six line segments and if $t\ s$ means that $t \in P$ and $s \in L$ and t is on s). It is easy although slightly time consuming to check that all of (SP1) through (SP5) are true under this interpretation.

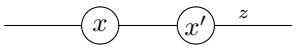
The Here are a couple of sample theorems about simple planes.

Theorem 10.4. *In a simple plane every point is on at least two distinct lines.*

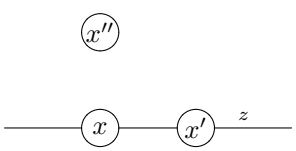
Proof. Assume that (P, L, On) is a simple plane and that x is a point. We need to show that there are two lines z and z' such that $z \neq z'$, x is on z and x is in z'. (If we were drawing a picture as an aid to doing this proof we might start with what we are given, namely a point x: (x))

By (SP1) there must be at least one point x' different from x. Which gives us the picture

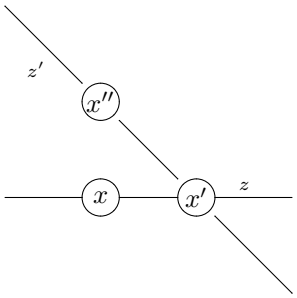
By (SP3) there is a line z containing x and x'.



Using (SP4) there is a point x'' not on z.



By (SP5) there is a line z' containing x and x'' so both z and z' contain the point x.



Further $z \neq z'$ since x'' is on z' but not on z. □

Theorem 10.5. *In a simple plane every line contains at least one point.*

The proof is left as an exercise.

Theorem 10.6. *In a simple plane every line contains at least two points.*

Proof. Assume that (P, L, On) is a simple plane and let z be a line. By Theorem 10.5 z contains at least one point which we'll call x. By (SP4) there is a point x' not on z. The points x and x' are not equal since x is on z and x' is not hence there is a line z' containing x and x'. Note that z and z' are not equal since x' is on z' but x' is not on x. By (SP4) there is a point x'' not on z'. Applying (SP5) there is a line z'' containing x'' where z'' is parallel to z'. The point x is not on z'' since x is on z and z is parallel to z''. We now know the following things about x

1. x is not on z''
2. z' contains x and is parallel to z''
3. z contains x and is not equal to z'

Since there can be only one line through x parallel to z'' it follows that z is not parallel to z'' and therefore there is a point y which is on both z and z'. The point y is not equal to x since y is on z'' and x is not. Therefore we have found two distinct points x and y on z. □

10.4 Properties of Axiom Systems

In this section we discuss several properties which any given axiom system may or may not have. Let Σ be a set of axioms. For example, Σ might be the set consisting of the axioms (SP1) through (SP5) from the previous section or possibly the set $\{(\text{P1}), (\text{P2}), (\text{P3})\}$ consisting of the partial order axioms.

Definition 10.7. Σ is *consistent* if it is not possible to prove a contradictory sentence from the axioms in Σ.

A natural question to ask is how would one go about proving that an axiom system is consistent. A proof using the definition of consistency directly would be difficult. In order to argue that no proof of a certain kind exists would require a careful analysis of the meaning of the word "proof". However there is another method of showing that an axiom system is consistent and this is the method which is usually used. The method is to show that there is an object which is a model of the axiom system. The idea is that if there is some mathematical object of which all the axioms in the system are true then every thing proved from the axioms will also be true of the object. Since no contradictory sentence can be true of an object no contradictory sentence will be provable from the axioms.

For example the system of simple plane axioms is consistent since there is a model. In fact we've seen that these axioms have at least two models.

Another property we will consider is given by the following definition.

Definition 10.8. Assume that Σ is a set of sentences (in particular Σ may be an axiom system) and that P is a sentence.

1. P is *independent of* Σ if neither P nor $\neg P$ is provable from the sentences in Σ.

2. Σ is *independent* if for every P in Σ, P is independent of $\Sigma \setminus \{P\}$.

The usual way of showing that a sentence P is independent of a set of sentences Σ is to find two models, one of the set of sentences $\Sigma \cup \{P\}$ and one of $\Sigma \cup \{\neg P\}$. The first model would show that $\neg P$ is not provable from Σ and the second would show that P is not provable from Σ.

We might ask, for example, whether the simple plane axioms are independent. To argue that they are would require showing that each of (SP1) through (SP5) is independent of the other axioms. For example, we would have to show that (SP1) is independent of the set $\Sigma' = \Sigma \setminus \{(\text{SP1})\} = \{(\text{SP2}), (\text{SP3}), (\text{SP4}), (\text{SP5})\}$ and if we use the normal method for showing this independence we would have to find two models, one for $\Sigma' \cup \{(\text{SP1})\} = \Sigma$ and one for $\Sigma \cup \{\neg(\text{SP1})\}$. Since we already have seen that there are models of Σ all we really have to do is find a model of $\Sigma' \cup \{\neg(\text{SP1})\} = \{\neg(\text{SP1}), (\text{SP2}), (\text{SP3}), (\text{SP4}), (\text{SP5})\}$. The fact that the negation of (SP1) must hold narrows the search for a model considerably. Here's one possibility.

Example 10.9. Let the set of points P consist of just one point, say $P = \{x\}$ and let the set of lines L and the relation On be empty. Then it's clear that (SP1) is true in the system (P, L, On). It's also easy to see that (SP2) through (SP5) are true in this system since (looking at the simplified versions of (SP2) through (SP5)) the hypotheses of these four axioms are never true.

A similar comment applies to showing the independence of each of (SP2) through (SP5) from the other axioms: Let σ be one of (SP2) through (SP5). In

order to show that σ is independent of $\Sigma \setminus \{\sigma\}$ it is enough to find a model of $(\Sigma \setminus \{\sigma\}) \cup \{\neg\sigma\}$. (Since we already have a model of Σ.)

Example 10.10. Here is a model for the system $\{(\text{SP1}), \neg(\text{SP2}), (\text{SP3}), (\text{SP4}), (\text{SP5})\}$ which is what is required to show the independence of (SP2) from the other simple plane axioms. The model will be obtained from the model pictured in Figure 10.3 by altering the relation On slightly. Let $P = \{x, x', y, y'\}$, $L = \{z_1, z_2, z_3, z_4, z_5, z_6\}$ and let On be the relation pictured in Figure 10.3 with the additional stipulation that z_1 On x. To be more precise we could describe On as a set of order pairs:

$$On = \{(x, z_1),(x, z_4), (x, z_5), (x', z_1), (x', z_2), (x', z_6), (y, z_3), (y, z_4), (y, z_6), (y', z_2), (y', z_3), (y', z_5), (z_1, x)\}$$

Example 10.11. To show that (SP3) is independent of the other simple plane axioms we would need a model of the set $\Gamma = \{(\text{SP1}), (\text{SP2}), \neg(\text{SP3}), (\text{SP4}), (\text{SP5})\}$. The negation of (SP3) is "There exist two distinct points x and y such that either there is no line containing both x and y or there is more than one line containing x and y." If we let the set of points be the circles in the following diagram and the set of lines be the line segments in the diagram with a point being on a line if the circle is on the line segment then (SP3) is false since there is no line which contains both of the points u and w. Nor is there a line containing both v and w.

Verification of the other axiom ((SP1), (SP2), (SP4) and (SP5)) is fairly easy.

Example 10.12. We now give a model for the simple plane axioms in which the set of points and lines aren't disjoint. You may have been assuming that a point could never be a line. If so you have encountered a pitfall associated with the axiomatic approach: Assuming something that is not a consequence of the axioms just because its true under the interpretations you have considered. Here is a model for (SP1) through (SP5) in which there are objects which are both points and lines. In this model the points are the numbers in the set $\{1, 2, 3, 4\}$ and the lines are numbers in the set $\{1, 2, 3, 4, 5, 6\}$. The relation On is described as a set of pairs:

$$On = \{(1,1), (2,1), (3,2), (4,2), (1,3), (3,3), (2,4), (4,4), (3,5), (2,5)(1,6), (4,6)\}$$

10.5 Exercises

10.1. Prove that in every simple plane there are at least three lines.

10.2. Prove Theorem 10.5 by contradiction and using Theorem 10.4.

10.3. Prove that in every simple plane there are at least four lines.

10.4. Prove that in every simple plane there are at least four points.

10.5. Let $P = L = On = \emptyset$. Is the system (P, L, On) a model for the axioms (SP1) through (SP5)?

10.6. Find a model for $\Gamma = \{(\text{SP1}), (\text{SP2}), \neg(\text{SP3}), (\text{SP4}), (\text{SP5})\}$ in which there are two distinct points x and y with more than on line containing x and y. (See Example 10.11.)

10.7. Show that (SP4) is independent of the other simple plane axioms.

10.8. Show that (SP5) is independent of the other simple plane axioms.

10.9. Show that the set $\{(\text{P1}), (\text{P2}), (\text{P3})\}$ of partial order axioms is an independent set. (See definitions 10.8 and 10.1.)

Chapter 11

numbers

Chapter 12

Construction of the Number Systems

12.1 Introduction

In this chapter we begin with the system $\mathbb{N}$ of natural numbers and construct in order the integers, the rational numbers, the real numbers and the complex numbers. There are two possible ways of approaching the natural numbers. The first is to define them to be certain specific sets and then to prove their properties using principles of set theory.[1] The second approach to the natural numbers is to give axioms for them and prove their properties from the axioms. This is the approach we shall take.

12.2 The Axioms for $\mathbb{N}$

12.3 Exercises

12.1.

[1]The standard way of defining the natural numbers as sets is to first define an operation S on sets called the *successor operation*: For any set x, $S(x) = x \cup \{x\}$. Then the natural number 0 is defined to be the empty set. The natural number 1 is the successor of 0. So $1 = S(0) = 0 \cup \{0\} = \emptyset \cup \{\emptyset\} = \{\emptyset\} = \{0\}$. Two is the successor of 1, so $2 = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$. In general the natural number $n + 1$ is the successor $S(n)$ of n.

Appendix A

Summary of Proof Principles

A. **Proving a Universally Quantified Statement:** To prove "$\forall x \in A, P(x)$ " assume $x \in A$ and using only that fact about x, prove $P(x)$.

B. **Proving Implications:** To prove an implication "If Q then R" assume Q and using this assumption prove R.

C. The two proof principles above are frequently used together - To prove a universally quantified implication "$\forall x \in A$ if $Q(x)$ then $R(x)$" assume $x \in A$ and $Q(x)$ and using these assumptions prove $R(x)$.

D. It is not a valid method of proof to begin with the statement you want to prove and prove something known to be true. In particular when you are proving an equality do Not start with the equality you want to prove and derive something true.

E. **Proof by Cases:** If P and Q are two statements for which you know "P or Q" is true and you want to prove the statement R, it suffices to do two things: First assume P and prove R; second (eliminate P as an assumption and)assume Q and prove R.

F. **Proving "P or Q".** In order to prove a statement of the form "P or Q" it suffices to assume that one of the two sentences P or Q is false and, using this assumption, prove the other is true. Therefore there are two possibilities

   1. Add $\neg P$ to the active hypotheses and prove Q.
   2. Add $\neg Q$ to the active hypotheses and prove P.

   Note that you only have to do one of these.

G. **Proving two sets are equal:** If A and B are sets then in order to prove $A = B$, it suffices to do two things

1. Prove $\forall x \in A$, $x \in B$ and
2. Prove $\forall x \in B$, $x \in A$.

H. **Using Universally Quantified Statements:** If $\forall x \in A, P(x)$ an active hypothesis and τ is an expression representing an object for which $\tau \in A$ is an active hypothesis, then you may conclude (that is, add to your active hypotheses) $P(\tau)$

I. Two Special cases are

If "$\forall x \in A$, if $Q(x)$ then $R(x)$" an active hypothesis and τ is an expression representing an object for which $\tau \in A$ and $Q(\tau)$ are active hypotheses, then you may conclude (that is, add to your active hypotheses) $R(\tau)$.

If "$\forall x \in A$, $Q(x)$ if and only if $R(x)$" an active hypothesis and τ is an expression representing an object for which $\tau \in A$ and $Q(\tau)$ are active hypotheses, then you may conclude (that is, add to your active hypotheses) $R(\tau)$.

J. **Changing Bound Variables:** If $P(x)$ is a sentence with free variable x and t is a variable not occurring in $P(x)$ then the two statements "$\exists x$ such that $P(x)$" and "$\exists t$ such that $P(t)$" are equivalent and may be used interchangeably. Similarly for the two statements "$\forall x, P(x)$" and "$\forall t, P(t)$".

K. **Using Existentially Quantified Statements:** If "$\exists x \in A$ such that $P(x)$" is an active hypothesis then you can introduce a new object symbol (say x_0) and add "$x_0 \in A$" and "$P(x_0)$" to the active hypotheses.

L. **Proving Two Functions are Equal:** In order to show that two functions f_1 and f_2 are equal it suffices to show that $\mathrm{Dom}(f_1) = \mathrm{Dom}(f_2)$ and that for all x in the common domain, $f_1(x) = f_2(x)$.

M. **Proofs of Existence Statements:** In order to prove a statement of the form $(\exists x \in S)(P(x))$ there are ordinarily two steps the first of which will usually not appear in the finished proof

1. Using the assumptions, you must identify, define or construct the object you want to use for x. This will ordinarily require some scratch work which will not appear in the finished proof.
2. The first line of the proof (of $\exists x \in S$ such that $P(x)$) will be a statement of the form "Let x_0 be ..." or "define x_0 by ..." or "let $x_0 = \ldots$" or some similar statement where x_0 is a new object symbol and ... is a description of x_0 in terms of the active object symbols and which may use the active hypotheses. The statement "$x_0 = \ldots$" is added to the active hypotheses. The word "Let" or "Define" is used to indicate that a new object symbol is being introduced. The last line of the proof will be "$x_0 \in S$ and $P(x_0)$". The object symbol x_0 and the assumption $x_0 = \ldots$ are only active for the proof of "$x_0 \in S$ and $P(x_0)$".

N. **Proving "and" Statements:** To prove "P and Q" where P and Q are statements, prove P and prove Q.

O. **Proof by Contradiction.** To prove a statement P by contradiction, assume that P is false, that is, add the negation of P to the active hypotheses and then prove any contradictory statement.

P. And a special case of *Proof by Contradiction*

Proving the Contrapositive: In order to prove "If R then S" it suffices to prove "If not S then not R".

Q. **Proofs of "There exists a unique ..."** Assume that $P(x)$ is a sentence with free variable x. In order to prove "There exists a unique x such that $P(x)$" prove "$\exists x$ such that $P(x)$" and "There is at most one x such that (x)".

Appendix B

Solutions to Selected Exercises

B.1 Chapter 1

1.1.

(a) The variable x is bound and the variable y is free.

(b) Both x and y are bound.

(c) n is free and k is bound.

(d) x is free.

(e) x is free.

(f) x is bound by an implicit universal quantifier.

1.2.

(a) The variable x is bound.

(b) x is bound and y and z are free.

(c) x is free.

(d) x is bound and w is free.

1.3.

(a) $x = 1$ (or any positive number)

(b) $x = -1$ (or any $x \leq 0$)

1.4.

(a) $y = 2$

(b) $y = \frac{1}{2}$

1.5.

(a) Let $A(x)$ be the sentence $x^2 \geq 0$.

(b) Let $P(x)$ be the sentence $x > 0$.

1.6. The following statements are implications. Identify the hypothesis and conclusion of each. Assume these are theorems to be proved. Give your answer in the form: Assume *hypothesis* we have to show *conclusion*.

(a) The hypothesis is "A, B and C are sets" and the conclusion is "$A \times (B \cup C) = (A \times B) \cup (A \times C)$."

(b) The hypothesis is "A, B and C are sets" and the conclusion is "$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$."

(c) The hypothesis is " $\{x\}_{n=1}^{\infty}$ is a bounded sequence" and the conclusion is "$\{x\}_{n=1}^{\infty}$ has a convergent subsequence."

(d) The hypothesis is "both A and B are closed sets" and the conclusion is "$A \cup B$ is a closed set."

(e) The hypothesis is "$\{I_n : n \in \mathbb{N}\}$ is a nested sequence of closed intervals" and the conclusion is "$\bigcap_{n\in\mathbb{N}} I_n$ is non-empty."

(f) The hypothesis is "A given set is open" and the conclusion is "that set is either empty of contains its cluster points." (It might be better to rephrase f as "an open set A is either empty or contains one of its cluster points" and then identify the hypothesis as "A is an open set" and the conclusion as "A is either empty of contains on of its cluster points."

(g) The hypothesis is "A is a set of real numbers with more than one element" the conclusion is "the least upper bound of A is greater than the greatest lower bound of A."

1.7.

(a) False, $(x = -1)$

(b) True

(c) True

(d) False

(e) False

(f) True

(g) True

(h) False

(i) True

(j) False

(k) True

(l) False

(m) True

(n) True

(o) False

(p) True

(q) True

1.8.

(a) False

(b) True

(c) False

(d) True

(e) False

(f) True

(g) False

1.9. Assume that m and n are variables whose range is the set $\mathbb{Z}$ of integers. Rewrite the following by making all the implicit quantifiers explicit.

(a) $\forall n \in \mathbb{Z}$, If n is an odd integer then n^2 is odd.

(b) $\forall n \in \mathbb{Z}$, $(n+1)^2 = n^2 + 2n + 1$.

(c) $\forall n \in \mathbb{Z}$, if n is an even integer, then there is an integer m such that $m^2 + n + 1 = 0$.

1.10.

(a) $\exists \epsilon > 0$ such that $\forall \delta > 0, \exists x \exists y \in R$ such that $|x-y| < \delta$ and $|x^2 - y^2| \geq \epsilon$.

(b) $\exists x \exists y \in R$ such that $x < y$ and $x^2 \geq y^2$.

(c) $\forall x \in R$,$\exists y \in R$ such that$y \geq x$ and $\frac{1}{y} > 1$.

(d) $\exists x \in R$ such that $\forall y \in R, y \leq x^2$.

(e) $\forall x \in R, x^2 + x + 1 \neq 0$.

1.11.

(a) $a = 6$, $b = 3$, $c = 4$; $6|12$ but 6 is not divisible by 4 or 3.

(b) $a = \frac{1}{4}$, $b\frac{1}{3}$, $c = \frac{1}{2}$; $\frac{1}{4} < \frac{1}{3}$, $\frac{1}{4} < \frac{1}{2}$, but $\frac{1}{4} \not< \frac{1}{6}$.

(c) $x = 4$.

1.12. Hence $\exists k \in \mathbb{Z}$ such that $w^2 - 2 = 2k$. Therefore, $w^2 - w$ is even.

1.13.

(a) False

(b) False

(c) False

(d) False

B.2 Chapter 2

2.1.

(a) $q = 30$, $r = 2$

(b) $q = 37$, $r = 10$

(c) $q = -47$, $r = 4$

(d) $q = 0$, $r = 47$

(e) $q = -1$, $r = 1$

(f) $q = 20$, $r = 0$

2.2. *Proof.* Assume $n \in \mathbb{Z}$ and n is odd. That is, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore, $n^2+3n+4 = (2k+1)^2+3(2k+1)+4 = (4k^2+4k+1)+(6k+3)+4 = 4k^2 + 10k + 8 = 2(2k^2 + 5k + 4)$. Let $i = 2k^2 + 5k + 4$ where $i \in \mathbb{Z}$. Then $n^2 + 3n + 4 = 2i$. Therefore, $n^2 + 3n + 4$ is even. □

2.3. *Proof.* Assume $n \in \mathbb{Z}$ and n is odd. That is, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore, $6n^2 + 5n + 4 = 6(2k + 1)^2 + 5(2k + 1) + 4 = 6(2k + 1)^2 + 10k + 9 = 2[3(2k + 1)^2 + 5k + 4] + 1$. Let $i = 3(2k + 1)^2 + 5k + 4$ where $i \in \mathbb{Z}$. Then $6n^2 + 5n + 4 = 2i + 1$. Therefore, $6n^2 + 5n + 4$ is odd. □

2.4. *Proof.* Assume $n \in \mathbb{Z}$ and n is even. That is, $n = 2k$ for some $k \in \mathbb{Z}$. Therefore, $25n^2 + 20n + 3 = 25(2k)^2 + 20(2k) + 3 = 100k^2 + 40k + 3 = 2(50k^2 + 20k + 1) + 1$. Let $i = 50k^2 + 20k + 1$ where $i \in \mathbb{Z}$. Then $25n^2 + 20n + 3 = 2i + 1$. Therefore, $25n^2 + 20n + 3$ is odd. □

2.5. *Proof.* Assume $n \in \mathbb{Z}$. Then either n is even or n is odd. We consider two cases

Case 1. n is even. That is, $n = 2k$ for some $k \in \mathbb{Z}$. Then $9n^2 + 9n + 2 = 9(2k)^2 + 9(2k) + 2 = 2(18k^2 + 9k + 1)$. Let $i = 18k^2 + 9k + 1$ where $i \in \mathbb{Z}$. Then $9n^2 + 9n + 2 = 2i$. Therefore, $9n^2 + 9n + 2$ is even.

Case 2. n is odd. That is, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $9n^2 + 9n + 2 = 9(2k+1)^2 + 9(2k+1) + 2 = (36k^2 + 36k + 9) + (18k + 9) + 2 = 36k^2 + 54k + 20 = 2(18k^2 + 27 + 10)$. Let $i = 36k^2 + 54k + 10$ where $i \in \mathbb{Z}$. Then $9n^2 + 9n + 2 = 2i$. Therefore, $9n^2 + 9n + 2$ is even.

Therefore, $\forall n \in \mathbb{Z}$, $9n^2 + 9n + 2$ is even. □

2.6. *Proof.* For the first half, assume that $x \in \mathbb{R}^+$ and $1 < x$. We will prove that $x < x^2$ using the third fact in the list above. Assume that $a = 1$, $b = x$ (so $a < b$), and $c = x$ since $x > 1 > 0$. Then $ac < bc = 1 * x < x * x = x < x^2$.

For the second half, assume that $x \in \mathbb{R}^+$ and $x < 1$. We will prove that $x^2 < x$ using the third fact in the list above. Assume that $a = x$, $b = 1$ (so $a < b$), and $c = x$ since x is a positive real number. Then $ac < bc = x * x < 1 * x = x^2 < x$. □

2.7. *Proof.* For the first half, assume that $\forall x, y \in \mathbb{R}^+$ and $x < y$. We will prove that $x^2 < y^2$ by using the fifth fact in the list above. Assume that $a = x, b = y, c = x$, and $d = y$. Then $0 < a < b$ becomes $0 < x < y$, $0 < c < d$ becomes $0 < x < y$, and $ac < bd$ becomes $x * x < y * y = x^2 < y^2$.

For the second half, assume that $\forall x, y \in \mathbb{R}^+$ and $x \leq y$. We will prove that $x^2 \leq y^2$ using the fifth fact in the list above and the fact that we can replace $<$ with $\leq$. Assume that $a = x, b = y, c = x$, and $d = y$. Then $0 \leq a \leq b$ becomes $0 \leq x \leq y$, $0 \leq c \leq d$ becomes $0 \leq x \leq y$, and $ac \leq bd$ becomes $x * x \leq y * y = x^2 \leq y^2$. □

2.8. *Proof.* Assume that $\forall x, y \in \mathbb{R}^+$ and $x < y$. To prove that $\sqrt{x} < \sqrt{y}$ we will

prove that $\sqrt{x} \geq \sqrt{y}$ is impossible. Since $\sqrt{x} \geq \sqrt{y}$ is the same as $\sqrt{y} \leq \sqrt{x}$, we can then use exercise 3.6. According to 3.6, $(\sqrt{y})^2 \leq (\sqrt{x})^2 = y \leq x$. However, we were looking for this to be true when $x < y$ not $y \leq x$, so $\sqrt{x} \geq \sqrt{y}$ is impossible for $x < y$. □

2.9. *Proof.* If we rearrange the inequality, $\sqrt{\frac{9}{2}} - 2 > 0 = \sqrt{\frac{9}{2}} > 2 = \sqrt{4} < \sqrt{\frac{9}{2}}$, we can use the fact from exercise 3.7 to prove $\sqrt{\frac{9}{2}} - 2 > 0$. Using 3.7, assume that $y = \frac{9}{2}$ and $x = 4$. Since $x < y$, it follows that $\sqrt{x} < \sqrt{y}$. Since $\sqrt{4} = 2$, we get $2 < \sqrt{\frac{9}{2}}$, then subtracting 2 from both sides, we get $0 < \sqrt{\frac{9}{2}} - 2$, which is equivalent to $\sqrt{\frac{9}{2}} - 2 > 0$. □

2.10. *Proof.* To prove this, we'll start with the known inequality $64 > 63$ and work backwards.
First, we'll take the square root of each side:
$\sqrt{64} > \sqrt{63}$, which gives us $8 > \sqrt{63}$.
Then we'll break down $\sqrt{63}$:
$\sqrt{63} \to \sqrt{4 * \frac{63}{4}} \to 2\sqrt{\frac{63}{4}} \to 2\sqrt{\frac{9}{2} * \frac{7}{2}} \to 2\sqrt{\frac{9}{2}}\sqrt{\frac{7}{2}}$.
Now, our inequality reads $8 > 2\sqrt{\frac{9}{2}}\sqrt{\frac{7}{2}}$. Next, we'll add 8 to each side:
$16 > 8 + 2\sqrt{\frac{9}{2}}\sqrt{\frac{7}{2}}$.
Then, we'll take the square root of each side again:
$\sqrt{16} > \sqrt{8 + 2\sqrt{\frac{9}{2}}\sqrt{\frac{7}{2}}} \to 4 > \sqrt{8 + 2\sqrt{\frac{9}{2}}} \to 4 > \sqrt{\frac{9}{2}} + \sqrt{\frac{7}{2}}$.
Therefore, since we could work from the true inequality $64 > 63$, we prove that $4 > \sqrt{\frac{9}{2}} + \sqrt{\frac{7}{2}}$ is also true. □

2.11. *Proof.* Let $\forall \epsilon \in \mathbb{R}^+$ with $\epsilon < 4$. Since $\epsilon > 0$, by subtracting ϵ from both sides, we get $-\epsilon < 0$. This then implies that $-\epsilon < 0 < \epsilon$, so by the transitive law of inequality we have $-\epsilon < \epsilon$. Adding 4 to both sides gives us $4 - \epsilon < 4 + \epsilon$.

Since $\epsilon < 4$, we see that $4 - \epsilon > 0$. This means we can take the square root of both sides. By one of our problems, we know that $0 < x < y$ implies that $0 < \sqrt{x} < \sqrt{y}$. Applying this here gives us $\sqrt{4 - \epsilon} < \sqrt{4 + \epsilon}$. Adding 2 to both sides gives us $\sqrt{4 - \epsilon} + 2 < \sqrt{4 + \epsilon} + 2$.

Now, the product $(\sqrt{4 - \epsilon} + 2) * (\sqrt{4 + \epsilon} + 2)$ is positive, so we can divide both sides by this product without changing the sign. This gives us $\frac{1}{\sqrt{4+\epsilon}+2} < \frac{1}{\sqrt{4-\epsilon}+2}$. Since $\epsilon > 0$, we may multiply both sides by ϵ without changing the sign to get $\frac{\epsilon}{\sqrt{4+\epsilon}+2} < \frac{\epsilon}{\sqrt{4-\epsilon}+2}$.

We have a principle that says for $c \neq 0$, $\frac{a}{b} = \frac{ac}{bc}$. Applying this on the left hand side with $c = \sqrt{4 + \epsilon} - 2$, we find the left hand side equals $\sqrt{4 + \epsilon} - 2$. Applying this on the right hand side with $c = -\sqrt{4 - \epsilon}+2$, we find the right hand side equals $2 - \sqrt{4 - \epsilon}$. Substituting each in, we get the conclusion $\sqrt{4 + \epsilon} - 2 < 2 - \sqrt{4 - \epsilon}$. □

2.12. *Proof.* We can assume that $\epsilon < 4$ and that $\epsilon < 4$ and $|x-2| < \sqrt{4+\epsilon}-2$. Since we can assume that these inequalities are true, we can use the second inequality and work backwards to prove that $|x^2 - 4| < \epsilon$.
Starting with $|x-2| < \sqrt{4+\epsilon} - 2$, add 2 to both sides:
$|x| < \sqrt{4+\epsilon}$.
We can then square each side:
$|x^2| < 4 + \epsilon$.
Then, subtract 4 from each side, reaching the conclusion:
$|x^2 - 4| < \epsilon$. □

2.13. *Proof.* Assume that A, B and C are sets. To prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$ it suffices to show that $\forall (x, y) \in A \times (B \cup C)$ where (x, y) is an ordered pair, $(x, y) \in (A \times B) \cup (A \times C)$ and $\forall (x, y) \in (A \times B) \cup (A \times C), (x, y) \in A \times (B \cup C)$.
First assume that $(x, y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in B \cup C$. Therefore $x \in A$ and $y \in B$ or $y \in C$. We cosider two cases

Case 1. $y \in B$. If $x \in A$ and $y \in B$, then $(x, y) \in A \times B$. Therefore, $(x, y) \in (A \times B) \cup (A \times C)$.

Case 2. $y \in C$. If $x \in A$ and $y \in C$, then $(x, y) \in A \times C$. Therefore, $(x, y) \in (A \times B) \cup (A \times C)$.
In either case, $\forall (x, y) \in A \times (B \cup C), (x, y) \in (A \times B) \cup (A \times C)$.
Next assume that $(x, y) \in (A \times B) \cup (A \times C)$. Then $(x, y) \in A \times B$ or $(x, y) \in A \times C$. We consider two cases

Case 1. $(x, y) \in A \times B$. Then $x \in A$ and $y \in B$. Since $y \in B, y \in B \cup C$. Therefore $(x, y) \in A \times (B \cup C)$.

Case 2. $(x, y) \in A \times C$. Then $x \in A$ and $y \in C$. Since $y \in C, y \in B \cup C$. Therefore $(x, y) \in A \times (B \cup C)$.
In either case, $\forall (x, y) \in (A \times B) \cup (A \times C), (x, y) \in A \times (B \cup C)$. □

2.14. *Proof.* Assume that A, B and C are sets. To prove that $A \times (B \cap C) = (A \times B) \cap (A \times C)$, it suffices to show that $\forall (x, y) \in A \times (B \cap C)$ where (x, y) is an ordered pair, $(x, y) \in (A \times B) \cap (A \times C)$ and $\forall (x, y) \in (A \times B) \cap (A \times C), (x, y) \in A \times (B \cap C)$.

First assume that $(x, y) \in A \times (B \cap C)$. Then $x \in A$ and $y \in B \cap C$. Therefore $y \in B$ and $y \in C$. Hence $(x, y) \in A \times B$ and $(x, y) \in A \times C$. So $(x, y) \in (A \times B) \cap (A \times C)$.

Next assume that $(x, y) \in (A \times B) \cap (A \times C)$. Then $(x, y) \in A \times B$ and $(x, y) \in A \times C$. Therefore $x \in A$, $y \in B$, and $y \in C$. So $y \in B \cap C$. Hence $(x, y) \in A \times (B \cap C)$. □

2.15. *Proof.* Assume that A, B and C are sets. To prove that $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$, it suffices to prove that $\forall (x, y) \in A \times (B \setminus C)$ where (x, y) is an ordered pair, $(x, y) \in (A \times B) \setminus (A \times C)$ and $\forall (x, y) \in (A \times B) \setminus (A \times C), (x, y) \in A \times (B \setminus C)$.

First assume that $(x, y) \in A \times (B \setminus C)$. Then $x \in A$ and $y \in B \setminus C$. Therefore $y \in B$ and $y \notin C$. So $(x, y) \in A \times B$ and $(x, y) \notin A \times C$. Hence, $(x, y) \in (A \times B) \setminus (A \times C)$.

Next assume that $(x, y) \in (A \times B) \setminus (A \times C)$. Then $(x, y) \in A \times B$ and $(x, y) \notin A \times C$. According to the statement $(x, y) \in A \times B$, $x \in A$ and $y \in B$. From this and the second statement $(x, y) \notin A \times C$ it follows that $x \in A$ yet $y \notin C$. Therefore $y \in B \setminus C$. Hence $(x, y) \in A \times (B \setminus C)$. □

2.16. *Proof.* Assume that A, B and C are sets and that $A \cap B = \emptyset$. To prove that $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$ we need to prove that $\forall X \in \mathcal{P}(A) \setminus \mathcal{P}(B), X \in \mathcal{P}(A \setminus B)$. So assume that $X \in \mathcal{P}(A) \setminus \mathcal{P}(B)$. Then we know that $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. This means that $X \subseteq A$ and $X \nsubseteq B$. Therefore, $X \subseteq A \setminus B$. Hence, $X \in \mathcal{P}(A \setminus B)$. So $\forall X \in \mathcal{P}(A) \setminus \mathcal{P}(B), X \in \mathcal{P}(A \setminus B)$. □

2.17. *Proof.* Assume $n \in \mathbb{N}$ and that $n > 2$. Then, since n is a natural number, $n \geq 3$. It follows that $n + 1 \geq 4$ and therefore that $(n + 1)^2 \geq 16$. Multiplying both sides by $\frac{1}{16(n+1)^2}$ gives $\frac{1}{16} \geq \frac{1}{(n+1)^2}$. That is $\frac{1}{(n+1)^2} \leq \frac{1}{16}$. Since $\frac{1}{16} < \frac{1}{10}$ we conclude that $\frac{1}{(n+1)^2} \leq \frac{1}{10}$ □

2.18. *Proof.* Since we're given the inequality $n > 99$ and can assume that it is true, we will use that to prove that $\frac{1}{\sqrt{n+1}} < \frac{1}{10}$.
First, add 1 to each side:
$99 < n \to 100 < n + 1$.
Then, since $n + 1 > 0$, we can take the square root of each side:
$\sqrt{100} < \sqrt{n + 1} \to 10 < \sqrt{n + 1}$.
We can then divide each side by the common denominator $10\sqrt{n + 1}$ to get the conclusion:
$\frac{1}{\sqrt{n+1}} < \frac{1}{10}$. □

2.19. *Proof.* Since we're given the inequality $n > \frac{1}{\sqrt{\epsilon}} - 1$, we can assume that it is true and use it along with the inequality $\epsilon < 1$ to prove that $\frac{1}{(n+1)^2} < \epsilon$.
First, add 1 to each side:
$n > \frac{1}{\sqrt{\epsilon}} - 1 \to n + 1 > \frac{1}{\sqrt{\epsilon}}$
Then, since we know that $0 < \epsilon < 1$, we can square both sides to get:
$(n + 1)^2 < (\frac{1}{\sqrt{\epsilon}})^2 \to (n + 1)^2 < \frac{1}{\epsilon}$
We can then multiply both sides by $\frac{\epsilon}{(n+1)^2}$ to get the conclusion:
$\epsilon > \frac{1}{(n+1)^2} \to \frac{1}{(n+1)^2} < \epsilon$. □

2.20.

(a) This is not a proof because, according to Proof Principle 12, we cannot prove that $A = B$ by starting with the equation $A = B$ and deriving an equation known to be true.

(b) $\sin^2 x \cot^2 x + \sin^2 x = \sin^2 x(\cot^2 x + 1)$

$= \sin^2 x(\csc^2 x)$ because $\cot^2 x + 1 = \csc^2 x$
$= \frac{sin^2 x}{sin^2 x}$ because $\csc^2 x = \frac{1}{sin^2} x$
$= 1$

2.21. This is not a proof because of Proof Principle 12. We cannot start with the statement we're trying to prove and derive a statement that we know to be true. This would be assuming that the statement in question is true without having proved it first.

2.22. *Proof.* $\tan^3\theta = \tan\theta \tan^2\theta$
$= \frac{sin\theta}{cos\theta}(\frac{sin^2\theta}{cos^2\theta})$ because $\tan\theta = \frac{sin\theta}{cos\theta}$ and $\tan^2\theta = \frac{sin^2\theta}{cos^2\theta}$
$= \frac{\frac{1}{cos\theta}}{\frac{1}{sin\theta}}(\frac{sin^2\theta}{cos^2\theta})$ inverting the first fraction
$= \frac{sec\theta}{csc\theta}(\frac{sin^2\theta}{cos^2\theta})$ because $\frac{1}{cos\theta} = \sec\theta$ and $\frac{1}{sin\theta} = \csc\theta$
$= \frac{sec\theta}{csc\theta}(\frac{1-cos^2\theta}{1-sin^2\theta})$ because $\sin^2\theta = 1 - \cos^2\theta$ and $\cos^2\theta = 1 - \sin^2\theta$. □

2.23. *Proof.* $\frac{1}{csc\theta} - \frac{1}{csc^3\theta} = \frac{1}{csc\theta}(1 - \frac{1}{csc^2\theta})$
$= \frac{1}{csc\theta}(1 - sin^2\theta)$ because $\frac{1}{csc^2\theta} = \frac{1}{\frac{1}{sin^2\theta}} = sin^2\theta$
$= \frac{1}{csc\theta}(\cos^2\theta)$ because $1 - \sin^2\theta = \cos^2\theta$
$= \sin\theta \cos^2\theta$ because $\frac{1}{csc\theta} = \sin^2$
$= \cos^2\theta \sin\theta$ because of the commutative property of multiplication. □

2.24. *Proof.* $(\frac{t(t+1)}{2})^2 + (t+1)^3 = (\frac{t^2+t}{2})^2 + (t+1)^3$ by the distributive property
$= \frac{(t^2+t)(t^2+t)}{2*2} + (t+1)^3$ expanding the first fraction
$= \frac{t^4+2t^3+t^2}{4} + (t+1)^3$ by the distributive property
$= \frac{t^4+2t^3+t^2}{4} + (t+1)(t+1)(t+1)$ expanding $(t+1)^3$
$= \frac{t^4+2t^3+t^2}{4} + (t^3 + 3t^2 + 3t + 1)$ by the distributive property
$= \frac{t^4+2t^3+t^2}{4} + \frac{4(t^3+3t^2+3t+1)}{4}$
$= \frac{t^4+2t^3+t^2}{4} + \frac{4t^3+12t^2+12t+4}{4}$ by the distributive property
$= \frac{t^4+6t^3+13t^2+12t+4}{4}$
$= \frac{(t^2+3t+2)^2}{2^2}$
$= (\frac{t^2+3t+2}{2})^2$
$= (\frac{(t+1)(t+2)}{2})^2$
$= (\frac{(t+1)(t+1+1)}{2})^2$
$= (\frac{(t+1)[(t+1)+1]}{2})^2$ by the associative property of addition. □

2.25. *Proof.* $\frac{1}{2}(x+1)(3(x+1)-1) = \frac{1}{2}(x+1)(3x+2)$ by the distributive property
$= \frac{1}{2}(3x^2 + 5x + 2)$
$= \frac{1}{2}(3x^2 - x + 6x + 2)$
$= \frac{1}{2}(3x^2 - x) + \frac{1}{2}(6x + 2)$ by the associative property

$= \frac{1}{2}(3x^2 - x) + (3x + 1)$ by the distributive property
$= \frac{1}{2}x(3x - 1) + (3x + 1)$
$= \frac{1}{2}x(3x - 1) + (3x + 3 - 2)$
$= \frac{1}{2}x(3x - 1) + ((3x + 3) - 2)$ by the associative property
$= \frac{1}{2}x(3x - 1) + (3(x + 1) - 2)$ by the distributive property. □

2.26. *Proof.* $4(y + 1)^2 - (y + 1) = 4(y^2 + 2y + 1) - (y + 1)$ by the distributive property
$= (4y^2 + 8y + 4) - (y + 1)$
$= 4y^2 + 8y + 4 - y - 1$
$= 4y^2 - y + 8y + 4 - 1$ by the commutative property
$= 4y^2 - y + 8y + 3$ by the distributive property
$= (4y^2 - y) + (8y + 3)$ by the associative property
$= (4y^2 - y) + (8y + 8 - 5)$ by the distributive property
$= (4y^2 - y) + ((8y + 8) - 5)$ by the associative property
$= (4y^2 - y) + (8(y + 1) - 5)$ by the distributive property. □

2.27. *Proof.* $2^{n+2} - 2 = 2^{n+1+1} - 2$ by the distributive property
$= 2^{(n+1)+1} - 2$ by the associative property
$= 2^{n+1} * 2^1 - 2$
$= 2(2^{n+1}) - 2$ by the commutative property
$= 2^{n+1} + 2^{n+1} - 2$ by the distributive property
$= 2^{n+1} - 2 + 2^{n+1}$ by the commutative property. □

2.28. *Proof.* The right hand side of the equation can be simplified as follows: $\left(\frac{(2n)!}{n!2^n}\right)(2(n + 1) - 1) = \frac{(2n)!(2n+1)}{n!2^n} = \frac{(2n+1)!}{n!2^n}$.

Simplifying the right hand side gives $\frac{(2(n+1))!}{(n+1)!2^{n+1}} = \frac{(2n+2)!}{(n+1)!2^{n+1}} = \frac{(2n+2)(2n+1)!}{(n+1)n!2\cdot 2^n} = \frac{2(n+1)(2n+1)!}{(n+1)n!2\cdot 2^n} = \frac{(2n+1)!}{n!2^n}$ □

2.29. *Proof.* $\frac{a(r^{n+1}-1)}{r-1} = \frac{ar^{n+1}-a}{r-1}$ by the distributive property
$= \frac{ar^{n+1}-a+ar^n-ar^n}{r-1}$
$= \frac{(ar^n-a)+(ar^{n+1}-ar^n)}{r-1}$ by the commutative and associative properties
$= \frac{ar^n-a}{r-1} + \frac{ar^{n+1}-ar^n}{r-1}$
$= \frac{ar^n-a}{r-1} + \frac{ar^n r-ar^n}{r-1}$
$= \frac{a(r^n-1)}{r-1} + \frac{ar^n(r-1)}{r-1}$ by the distributive property
$= \frac{a(r^n-1)}{r-1} + ar^n$ by the cancellation property. □

2.30. *Proof.* By definition, a divides b is equivalent to saying that $\exists n \in \mathbb{N}$ such that $b = a \cdot n$. Similarly, $\exists m \in \mathbb{N}$ such that $c = a \cdot m$. Then

$$b + c = a \cdot n + a \cdot m = a(n + m)$$

Thus there exists an integer $n+m \in \mathbb{N}$ such that $b+c = a(n+m)$, so $b+c$ is divisible by a. But this is what we mean when we say that a divides $b+c$. □

2.31. *Proof.* By definition, a divides b is equivalent to saying that $\exists n \in \mathbb{N}$ such that $b = a \cdot n$. Similarly, $\exists m \in \mathbb{N}$ such that $c = a \cdot m$. Then

$$bc = (a \cdot n)(a \cdot m) = a^2 \cdot nm$$

Thus there exists an integer $nm \in \mathbb{N}$ such that $bc = a^2 \cdot nm$, so bc is divisible by a^2. But this is what we mean when we say that a^2 divides bc. □

2.32. *Proof.* To prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ it suffices to show that $\forall x \in A \cap (B \cup C), x \in (A \cap B) \cup (A \cap C)$, and $\forall x \in (A \cap B) \cup (A \cap C), x \in A \cap (B \cup C)$.

First, assume that $x \in A \cap (B \cup C)$. This means that $x \in A$ and $x \in B \cup C$. Therefore $x \in A$ and $x \in B$ or $x \in C$. We consider two cases.

Case 1. $x \in B$. This means that $x \in A \cap B$. Therefore, $x \in (A \cap B) \cup (A \cap C)$.

Case 2. $x \in C$. This means that $x \in A \cap C$. Therefore, $x \in (A \cap B) \cup (A \cap C)$.

In either case, $\forall x \in A \cap (B \cup C), x \in (A \cap B) \cup (A \cap C)$.

Next, assume that $x \in (A \cap B) \cup (A \cap C)$. This means that $x \in A \cap B$ or $x \in A \cap C$. We consider two cases.

Case 1. $x \in A \cap B$. This means that $x \in A$ and $x \in B$. If $x \in B$, then $x \in B \cup C$. Therefore, $x \in A \cap (B \cup C)$.

Case 2. $x \in A \cap C$. This means that $x \in A$ and $x \in C$. If $x \in C$, then $x \in B \cup C$. Therefore, $x \in A \cap (B \cup C)$.

In either case, $\forall x \in (A \cap B) \cup (A \cap C), x \in A \cap (B \cup C)$. □

2.33. *Proof.* To prove that $(A \setminus B) \cap (A \setminus C) = (A \setminus (B \cup C))$ it suffices to show that $\forall x \in (A \setminus B) \cap (A \setminus C), x \in (A \setminus (B \cup C))$, and $\forall x \in (A \setminus (B \cup C)), x \in (A \setminus B) \cap (A \setminus C)$.

First, assume that $x \in (A \setminus B) \cap (A \setminus C)$. This means that $x \in A \setminus B$ and $x \in A \setminus C$. If $x \in A \setminus B$, then $x \in A$ and $x \notin B$, and if $x \in A \setminus C$, then $x \in A$ and $x \notin C$. Therefore, $x \in A$ and $x \notin B, C$. Hence, $x \in (A \setminus (B \cup C))$.

Next, assume that $x \in (A \setminus (B \cup C))$. This means that $x \in A$ and $x \notin B \cup C$. If $x \notin B \cup C$, x cannot be in either B or C, so $x \notin B$ and $x \notin C$. Therefore, $x \in A \setminus B$ and $x \in A \setminus C$. Hence, $x \in (A \setminus B) \cap (A \setminus C)$. □

2.34. *Proof.* To prove that $(A \setminus B) \cup (A \setminus C) = (A \setminus (B \cap C))$ it suffices to prove that $\forall x \in (A \setminus B) \cup (A \setminus C), x \in (A \setminus (B \cap C))$, and $\forall x \in (A \setminus (B \cap C)), x \in (A \setminus B) \cup (A \setminus C)$.

First, assume that $x \in (A \setminus B) \cup (A \setminus C)$. This means that $x \in A \setminus B$ or $x \in A \setminus C$. We consider two cases.

Case 1. $x \in A \setminus B$. This means that $x \in A$ and $x \notin B$. If $x \notin B$, then $x \notin B \cap C$. Therefore, $x \in (A \setminus (B \cap C))$.

Case 2. $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. If $x \notin C$, then $x \notin B \cap C$. Therefore, $x \in (A \setminus (B \cap C))$.

In either case, $\forall x \in (A \setminus B) \cup (A \setminus C), x \in (A \setminus (B \cap C))$.

Next, assume that $x \in (A \setminus (B \cap C))$. This means that $x \in A$ and $x \notin B \cap C$. Therefore $x \in A$, $x \notin B$, and $x \notin C$. So, $x \in A \setminus B$ and $x \in A \setminus C$. Hence, $x \in (A \setminus B) \cup (A \setminus C)$. □

2.35. *Proof.* Toward a proof by contradiction assume $\exists y \in \mathbb{R}$ such that $\frac{3y-2}{4y-6} = \frac{3}{4}$. Multiplying both sides of this equation by $4(4y-6)$ gives $12y-8 = 12y-18$. Subtracting $12y$ from both sides gives $-8 = -18$ a contradiction. □

2.36. *Proof.* We will prove this by contradiction, so assume that $\forall y \in \mathbb{R}$, $\frac{4y-2}{y-6} = 4$. Multiply both sides by $(y-6)$ to get $4y-2 = 4(y-6)$. Using the distributive property to multiply through on the right hand side, we get $4y - 2 = 4y - 24$. Subtracting $4y$ from each side, we get $-2 = -24$. This is a contradiction. Therefore, $\forall y \in \mathbb{R}$, $\frac{4y-2}{y-6} \neq 4$. □

B.3 Chapter 3

3.1.

(a) $\{1, 2, 3, 4\}$

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

(c) $\{-1, 0, 1, 2, 3, 4\}$

(d) $\{\{\}, \{1\}, \{2\}, \{1, 2\}\}$ or $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$

(e) $\{\{\}\}$ or $\{\emptyset\}$ (But **not** $\{\}$ or $\emptyset$)

(f) $\{0, 3, 6, 9, 12, \ldots, 750\}$

(g) $\{0, 5, 10, 15, \ldots\}$

3.2.

(a) $\{x \mid 2 \leq x < 4\}$

(b) $\{x \mid x \subseteq \{1, 2, 3, 4\}\}$

(c) $\{x \mid x \subseteq \mathbb{R}\}$

(d) $\{x \mid x \in \mathbb{N} \text{ and } 1 \leq x \leq 7\}$

(e) $\{x \mid a \leq x \leq b\}$

(f) $\{x \mid a < x < b\}$

3.3.

(a) $\{k \mid \exists n \in \mathbb{Z} \text{ such that } k = 3n\}$

(b) $\{y \mid \exists x \in \mathbb{R} \text{ such that } y = x^2 - 1\}$

(c) $\{r \mid \exists p \in \mathbb{Z} \text{ and } \exists q \in \mathbb{Z} \text{ such that } q \neq 0 \text{ and } r = \frac{p}{q}\}$

(d) $\{x \mid x \in \mathbb{Z} \text{ and } x^2 = 1\}$

(e) $\{n \mid n \in \mathbb{N} \text{ and } n \text{ is even}\}$

3.4. The two sets are equal because every element of the first set is an element of the second and every element of the second is an element of the first. This, according to the axiom of extensionality, is a sufficient condition for two sets to be equal.

3.5.

(a) $A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$.

(b) $A \cap B = \{2, 4\}$.

(c) $A \setminus B = \{1, 3, 5\}$.

(d) $(A \cap B) \cup C = \{2, 4, 5, 8\}$

(e) $C \times A = \{(4,1), (4,2), (4,3), (4,4), (4,5), (5,1), (5,2), (5,3), (5,4), (5,5), (8,1), (8,2), (8,3), (8,4), (8,5)\}$

(f) $C \times C = \{(4,4), (4,5), (4,8), (5,4), (5,5), (5,8)(8,4), (8,5), (8,8)\}$

3.6.

(a) $A = \{1, 2\}$, $B = \{1, 2, 3\}$ and $C = \{2, 3\}$.

(b) $A = \{1, 2\}, B = \{3, 4\}$ and $C = \{4, 5\}$.

(c) $A = \{1, 2\}, B = \{3, 4\}$ and $C = \{4, 5\}$.

(d) $A = \{1, 2\}, B = \{3, 4\}$ and $C = \{1, 2, 3, 4, 5\}$.

(e) $A = \{1, 2\}$ and $B = \{3, 4\}$.

(f) Any two sets A and B will work since $\emptyset \in \mathcal{P}(A \setminus B)$ but $\emptyset \notin \mathcal{P}(A) \setminus \mathcal{P}(B)$ for any sets.

(g) $A = \{1, 2\}$ and $B = \{3, 4\}$.

(h) $A = \{1, 2\}$ and $B = \{3, 4\}$.

3.7.

(a) $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$ and $C = \{1, 2, 3\}$.

(b) Not Possible since $\emptyset \in \mathcal{P}(A \setminus B)$ but $\emptyset \notin \mathcal{P}(A) \setminus \mathcal{P}(B)$ for any sets A and B.

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

(d) Not Possible since $(\emptyset, \emptyset) \in \mathcal{P}(A) \times \mathcal{P}(B)$ but $(\emptyset, \emptyset) \notin \mathcal{P}(A \times B)$ for any two sets A and B.[1]

3.9. *Proof.* Assuming that A, B and C are sets we'll show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ by the principle of extensionality.

For the first part of the proof assume that $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. This means that $x \in A$ and in either B or C. We consider two cases

Case 1. $x \in B$. In this case since $x \in A$ we have $x \in A \cap B$ so $x \in (A \cap B) \cup (A \cap C)$.

Case 2. $x \in C$. In this case since $x \in C$ we have $x \in A \cap C$ so that $x \in (A \cap B) \cup (A \cap C)$.

In either case $x \in (A \cap B) \cup (A \cap C)$.

For the second part of the proof assume $x \in (A \cap B) \cup (A \cap C)$ then $x \in (A \cap B)$ or $x \in (A \cap C)$. Case 1. $x \in (A \cap B)$. In this case $x \in A$ and $x \in B$. Therefore $x \in A$ and $x \in B \cup C$ so that we may conclude that $x \in A \cap (B \cup C)$.

Case 2. $x \in (A \cap C)$. Here $x \in A$ and $x \in C$ so that $x \in A$ and $x \in B \cup C$. It follows that $x \in A \cap (B \cup C)$.

Therefore in either possible case $x \in A \cap (B \cup C)$. □

3.10. *Proof.* Assume that A and B are sets and that $B \subseteq A$. We will show that $B = A \cap B$ by the principle of extensionality.

First assume that $x \in B$, then since $B \subseteq A$, it is also true that $x \in A$. Since $x \in A$ and $x \in B$, $x \in A \cap B$.

Secondly assume that $x \in A \cap B$. Then (by definition of $\cap$) $x \in B$. □

3.11. *Proof.* Assume that X, A and B are sets that that $X \subseteq A \setminus B$. We first show that $X \subseteq A$: Assume $t \in X$, then by our assumptions $t \in A \setminus B$. It follow from this that $t \in A$.

Next we show that $X \cap B = \emptyset$ by showing that $\forall t$, $t \in X \cap B$ is impossible. Assume t is an object for which $t \in X \cap B$. Then $t \in X$ from which it follows that $t \in A \setminus B$ and hence $t \notin B$. It also follows from $t \in X \cap B$ that $t \in B$. It is not possible for both $t \notin B$ and $t \in B$ to be true so $t \in X \cap B$ is impossible. □

3.12.

(a) False

(b) True

(c) False

(d) True

[1] However, without knowing exactly what an order pair is it's not possible to prove that for all sets A and B, $(\emptyset, \emptyset) \notin \mathcal{P}(A \times B)$.

(e) False

(f) True

(g) True

(h) True

(i) False

(j) True

3.13. *Proof.* Assume A and B are sets we will prove that $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$ and that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

For the first part assume that $x \in \mathcal{P}(A \cap B)$. Then $x \subseteq A \cap B$. It follows that $x \subseteq A$ and $x \subseteq B$. Hence $x \in \mathcal{P}(A)$ and $x \in \mathcal{P}(B)$ and therefore $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

Secondly, assume $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Then $x \in \mathcal{P}(A)$ and $x \in \mathcal{P}(B)$. By the definition of the power set operation, $x \subseteq A$ and $x \subseteq B$. We may therefore conclude that $x \subseteq A \cap B$. Hence $x \in \mathcal{P}(A \cap B)$. □

3.14. *Proof.* To prove this, we'll rename y as y_1 and y_2 and then prove that $y_1 = y_2$. Renamed, the sets would be as follows:

$1 \in x$ and $\forall y_1 \in x, y_1 = 1$

and $1 \in x$ and $\forall y_2 \in x, y_2 = 1$.

Even though these statements have different free variables, y_1 and y_2, both of the variables equal 1, so $y_1 = y_2$. □

3.15. *Proof.* Assume that A, B, and C are sets. We'll prove that $(A \cap B) \cup C = A \cap (B \cup C)$ using the principle of extensionality.

First assume that $x \in (A \cap B) \cup C$. Then $x \in A \cap B$ or $x \in C$. We consider two cases

Case 1. $x \in A \cap B$. This means that $x \in A$ and $x \in B$. With $x \in B$ it follows that $x \in B \cup C$. Therefore $x \in A \cap (B \cup C)$.

Case 2. $x \in C$. If $x \in C$ and $C \subseteq A$ then it follows that $x \in A$. Therefore $x \in A$ and $x \in B \cup C$, so $x \in A \cap (B \cup C)$.

In either case, $x \in A \cap (B \cup C)$.

Next, assume that $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. We consider two cases

Case 1. $x \in B$. Since $x \in A$, then $x \in A \cap B$, and $x \in (A \cap B) \cup C$.

Case 2. $x \in C$. If $x \in C$, then $x \in (A \cap B) \cup C$.

In either case, $x \in (A \cap B) \cup C$. □

3.16. *Proof.* Assume that A, B, and C are sets and that $(A \cap B) \cup C = A \cap (B \cup C)$. We will prove that $C \subseteq A$.

Assume that $x \in C$. This means that $x \in (A \cap B) \cup C$, and it follows that $x \in A \cap (B \cup C)$. Since $x \in C$, $x \in B \cup C$, and since $x \in A \cap (B \cup C)$, $x \in A$.

Since $x \in C$ and $x \in A$ and since x could represent any object in C and that object would also be in A, then C is a subset of $A, C \subseteq A$. □

3.17. *Proof.* Assume that A, B and C are sets. To prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$ it suffices to show that $\forall (x, y) \in A \times (B \cup C)$ where (x, y) is an ordered pair, $(x, y) \in (A \times B) \cup (A \times C)$ and $\forall (x, y) \in (A \times B) \cup (A \times C), (x, y) \in A \times (B \cup C)$.
First assume that $(x, y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in B \cup C$. Therefore $x \in A$ and $y \in B$ or $y \in C$. We cosider two cases

Case 1. $y \in B$. If $x \in A$ and $y \in B$, then $(x, y) \in A \times B$. Therefore, $(x, y) \in (A \times B) \cup (A \times C)$.

Case 2. $y \in C$. If $x \in A$ and $y \in C$, then $(x, y) \in A \times C$. Therefore, $(x, y) \in (A \times B) \cup (A \times C)$.
In either case, $\forall (x, y) \in A \times (B \cup C), (x, y) \in (A \times B) \cup (A \times C)$.
Next assume that $(x, y) \in (A \times B) \cup (A \times C)$. Then $(x, y) \in A \times B$ or $(x, y) \in A \times C$. We consider two cases

Case 1. $(x, y) \in A \times B$. Then $x \in A$ and $y \in B$. Since $y \in B, y \in B \cup C$. Therefore $(x, y) \in A \times (B \cup C)$.

Case 2. $(x, y) \in A \times C$. Then $x \in A$ and $y \in C$. Since $y \in C, y \in B \cup C$. Therefore $(x, y) \in A \times (B \cup C)$.
In either case, $\forall (x, y) \in (A \times B) \cup (A \times C), (x, y) \in A \times (B \cup C)$. □

3.18. *Proof.* Assume that A, B and C are sets. To prove that $A \times (B \cap C) = (A \times B) \cap (A \times C)$, it suffices to show that $\forall (x, y) \in A \times (B \cap C)$ where (x, y) is an ordered pair, $(x, y) \in (A \times B) \cap (A \times C)$ and $\forall (x, y) \in (A \times B) \cap (A \times C), (x, y) \in A \times (B \cap C)$.

First assume that $(x, y) \in A \times (B \cap C)$. Then $x \in A$ and $y \in B \cap C$. Therefore $y \in B$ and $y \in C$. Hence $(x, y) \in A \times B$ and $(x, y) \in A \times C$. So $(x, y) \in (A \times B) \cap (A \times C)$.

Next assume that $(x, y) \in (A \times B) \cap (A \times C)$. Then $(x, y) \in A \times B$ and $(x, y) \in A \times C$. Therefore $x \in A$, $y \in B$, and $y \in C$. So $y \in B \cap C$. Hence $(x, y) \in A \times (B \cap C)$. □

3.19. *Proof.* Assume that A, B and C are sets. To prove that $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$, it suffices to prove that $\forall (x, y) \in A \times (B \setminus C)$ where (x, y) is an ordered pair, $(x, y) \in (A \times B) \setminus (A \times C)$ and $\forall (x, y) \in (A \times B) \setminus (A \times C), (x, y) \in A \times (B \setminus C)$.

First assume that $(x, y) \in A \times (B \setminus C)$. Then $x \in A$ and $y \in B \setminus C$. Therefore $y \in B$ and $y \notin C$. So $(x, y) \in A \times B$ and $(x, y) \notin A \times C$. Hence, $(x, y) \in (A \times B) \setminus (A \times C)$.

Next assume that $(x, y) \in (A \times B) \setminus (A \times C)$. Then $(x, y) \in A \times B$ and $(x, y) \notin A \times C$. According to the statement $(x, y) \in A \times B$, $x \in A$ and $y \in B$. From this and the second statement $(x, y) \notin A \times C$ it follows that $x \in A$ yet $y \notin C$. Therefore $y \in B \setminus C$. Hence $(x, y) \in A \times (B \setminus C)$. □

3.20. *Proof.* Assume that A, B and C are sets and that $A \cap B = \emptyset$. To prove

that $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$ we need to prove that $\forall X \in \mathcal{P}(A) \setminus \mathcal{P}(B), X \in \mathcal{P}(A \setminus B)$. So assume that $X \in \mathcal{P}(A) \setminus \mathcal{P}(B)$. Then we know that $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. This means that $X \subseteq A$ and $X \nsubseteq B$. Therefore, $X \subseteq A \setminus B$. Hence, $X \in \mathcal{P}(A \setminus B)$. So $\forall X \in \mathcal{P}(A) \setminus \mathcal{P}(B), X \in \mathcal{P}(A \setminus B)$. □

3.21. *Proof.* To prove that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ it suffices to show that $\forall x \in A \cap (B \cup C), x \in (A \cap B) \cup (A \cap C)$, and $\forall x \in (A \cap B) \cup (A \cap C), x \in A \cap (B \cup C)$.

First, assume that $x \in A \cap (B \cup C)$. This means that $x \in A$ and $x \in B \cup C$. Therefore $x \in A$ and $x \in B$ or $x \in C$. We consider two cases.

Case 1. $x \in B$. This means that $x \in A \cap B$. Therefore, $x \in (A \cap B) \cup (A \cap C)$.

Case 2. $x \in C$. This means that $x \in A \cap C$. Therefore, $x \in (A \cap B) \cup (A \cap C)$.
In either case, $\forall x \in A \cap (B \cup C), x \in (A \cap B) \cup (A \cap C)$.

Next, assume that $x \in (A \cap B) \cup (A \cap C)$. This means that $x \in A \cap B$ or $x \in A \cap C$. We consider two cases.

Case 1. $x \in A \cap B$. This means that $x \in A$ and $x \in B$. If $x \in B$, then $x \in B \cup C$. Therefore, $x \in A \cap (B \cup C)$.

Case 2. $x \in A \cap C$. This means that $x \in A$ and $x \in C$. If $x \in C$, then $x \in B \cup C$. Therefore, $x \in A \cap (B \cup C)$.
In either case, $\forall x \in (A \cap B) \cup (A \cap C), x \in A \cap (B \cup C)$. □

3.22. *Proof.* To prove that $(A \setminus B) \cap (A \setminus C) = (A \setminus (B \cup C))$ it suffices to show that $\forall x \in (A \setminus B) \cap (A \setminus C), x \in (A \setminus (B \cup C))$, and $\forall x \in (A \setminus (B \cup C)), x \in (A \setminus B) \cap (A \setminus C)$.

First, assume that $x \in (A \setminus B) \cap (A \setminus C)$. This means that $x \in A \setminus B$ and $x \in A \setminus C$. If $x \in A \setminus B$, then $x \in A$ and $x \notin B$, and if $x \in A \setminus C$, then $x \in A$ and $x \notin C$. Therefore, $x \in A$ and $x \notin B, C$. Hence, $x \in (A \setminus (B \cup C))$.

Next, assume that $x \in (A \setminus (B \cup C))$. This means that $x \in A$ and $x \notin B \cup C$. If $x \notin B \cup C$, x cannot be in either B or C, so $x \notin B$ and $x \notin C$. Therefore, $x \in A \setminus B$ and $x \in A \setminus C$. Hence, $x \in (A \setminus B) \cap (A \setminus C)$. □

3.23. *Proof.* To prove that $(A \setminus B) \cup (A \setminus C) = (A \setminus (B \cap C))$ it suffices to prove that $\forall x \in (A \setminus B) \cup (A \setminus C), x \in (A \setminus (B \cap C))$, and $\forall x \in (A \setminus (B \cap C)), x \in (A \setminus B) \cup (A \setminus C)$.

First, assume that $x \in (A \setminus B) \cup (A \setminus C)$. This means that $x \in A \setminus B$ or $x \in A \setminus C$. We consider two cases.

Case 1. $x \in A \setminus B$. This means that $x \in A$ and $x \notin B$. If $x \notin B$, then $x \notin B \cap C$. Therefore, $x \in (A \setminus (B \cap C))$.

Case 2. $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. If $x \notin C$, then $x \notin B \cap C$. Therefore, $x \in (A \setminus (B \cap C))$.
In either case, $\forall x \in (A \setminus B) \cup (A \setminus C), x \in (A \setminus (B \cap C))$.

Next, assume that $x \in (A \setminus (B \cap C))$. This means that $x \in A$ and $x \notin B \cap C$. Therefore $x \in A$, $x \notin B$, and $x \notin C$. So, $x \in A \setminus B$ and $x \in A \setminus C$. Hence, $x \in (A \setminus B) \cup (A \setminus C)$. □

B.4 Chapter 4

4.1.

$$\begin{array}{c} f \\ 2 \to 3 \\ 3 \to 4 \\ 4 \to 4 \\ 5 \to 4 \end{array}$$

4.2. $f(2) = 3, f(3) = 4$, and $f(4) = 4$.

4.3.

$$\begin{array}{c} f \\ 1 \to 2 \\ 2 \to 3 \\ 3 \to 2 \\ 4 \to 5 \end{array}$$

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

4.4. $g = \{(x, \frac{x-1}{x^2+1}) : x \in \mathbb{R}\}$

4.5. Sets (a), (b), and (d) are functions.

4.6. *Proof.* Assume that a, b_1 and b_2 are objects for which (a, b_1) and (a, b_2) are in f. (We need to argue that $b_1 = b_2$.) By the definition of f, $(a, b_1) = (3x_1 + 9, x_1)$ for some $x_1 \in \mathbb{R}$ and $(a, b_2) = (3x_2 + 9, x_2)$ for some $x_2 \in \mathbb{R}$. It follows that

$$a = 3x_1 + 9 \text{ and that } a = 3x_2 + 9 \qquad (*)$$

(by the fundamental property of ordered pairs). Similarly, $b_1 = x_1$ and $b_2 = x_2$. By (*) $3x_1 + 9 = 3x_2 + 9$ so $x_1 = x_2$. Therefore $b_1 = b_2$. □

4.7. *Proof.* Assume (a_1, b_1) and (a_2, b_2) are in the set and that $a_1 = a_2$. To show that this set is a function, we need to prove that $b_1 = b_2$. From the first part of the assumption it follows that there are elements x_1 and x_2 of $\mathbb{R}$ such that $(a_1, b_1) = (3x_1 + 9, 2x_1 - 7)$ and $(a_2, b_2) = (3x_2 + 9, 2x_2 - 7)$. Using the fundamental property of ordered pairs we conclude that $a_1 = 3x_1 + 9, a_2 = 3x_2 + 9$, and

$$b_1 = 2x_1 - 7, \text{ and } b_2 = 2x_2 - 7. \quad (1)$$

Since $a_1 = a_2$, we get $3x_1 + 9 = 3x_2 + 9$. Subtracting 9 from each side and then dividing each side by 3, we find that $x_1 = x_2$. Combining this with (1) we conclude that $b_1 = b_2$. □

4.8. Both functions have domain and range equal to $\mathbb{R}$.

4.9. *Proof.* Assume (a_1, b_1) and (a_2, b_2) are in the set and that $a_1 = a_2$. To show that this set is a function, we need to prove that $b_1 = b_2$. Using the first assumption, we know that $a_1 = \frac{3b_1+2}{b_1+7}$ and $a_2 = \frac{3b_2+2}{b_2+7}$. We also know that $a_1 = a_2$, so $\frac{3b_1+2}{b_1+7} = \frac{3b_2+2}{b_2+7}$. Multiplying both sides by $(b_1 + 7)(b_2 + 7)$, we get $(b_2 + 7)(3b_1 + 2) = (b_1 + 7)(3b_2 + 2)$. Using the distributive property, we get $3b_1b_2 + 21b_1 + 2b_2 + 14 = 3b_2b_1 + 21b_2 + 2b_1 + 14$. It follows that $b_1 = b_2$. Therefore, this set is a function. □

4.10. $\text{Dom}(f) = \mathbb{R} \setminus \{-7\}$. $\text{Range}(f) = \mathbb{R}$.

4.12.

(a) A number b is in the range of k if and only if for some $a \in \mathbb{R}\setminus\{-4\}, k(a) = b$. That is, if and only if $\frac{3a-2}{2a+8} = b$. If we attempt to solve this equation for a starting by multiplying both sides by $(2a+8)$ we get $3a-2 = 2ab+8b$. Collecting the terms involving a on one side, we get $3a - 2ab = 8b + 2$. Using the distributive property to factor an a out of the left hand side, we get $a(3 - 2b) = 8b + 2$. Then, we can divide both sides by $(3 - 2b)$ to get $a = \frac{8b+2}{3-2b}$. It looks like this should be possible for every $b \neq \frac{3}{2}$, so $\text{Range}(k) = \mathbb{R} \setminus \{\frac{3}{2}\} = \{z \in \mathbb{R} : z \neq \frac{3}{2}\}$.

(b) *Proof.* Since both $\text{Range}(k)$ and $\{z \in \mathbb{R} : z \neq \frac{3}{2}\}$ are sets, to prove that $\text{Range}(k) = \{z \in \mathbb{R} : z \neq \frac{3}{2}\}$ we need to show that $\text{Range}(k) \subseteq \{z \in \mathbb{R} : z \neq \frac{3}{2}\}$ and $\{z \in \mathbb{R} : z \neq \frac{3}{2}\} \subseteq \text{Range}(k)$.

We'll begin with the proof that $\{z \in \mathbb{R} : z \neq \frac{3}{2}\} \subseteq \text{Range}(k)$. Assume $y \in \{z \in \mathbb{R} : z \neq \frac{3}{2}\}$. Then $y \in \mathbb{R}$ and $y \neq \frac{3}{2}$. Let $x_0 = \frac{8y+2}{3-2y}$. Since $y \neq \frac{3}{2}$, it is clear that $x_0 \in \mathbb{R}$. We prove $x_0 \neq -4$ by contradiction. Assume that $x_0 = -4$, then $\frac{8y+2}{3-2y} = -4$. Multiplying both sides by $(3 - 2y)$ gives us $8y + 2 = -12 + 8y$. Subtracting $8y$ from each side gives us $2 = -12$ which is a contradiction. We also have that $k(x_0) = \frac{3x_0-2}{2x_0+8} = \frac{3(\frac{8y+2}{3-2y})-2}{2(\frac{8y+2}{3-2y})+8} = \frac{3(8y+2)-2(3-2y)}{2(8y+2)+8(3-2y)} = \frac{24y+6-6+4y}{16y+4+24-16y} = \frac{28y}{28} = y$. Hence $x_0 \in \mathbb{R} \setminus \{-4\}$ and $y = k(x_0)$. So $\exists x \in \mathbb{R}\setminus\{-4\}$ such that $y = k(x)$. Therefore $y \in \text{Range}(k)$.

Now we'll prove that $\text{Range}(k) \subseteq \{z \in \mathbb{R} : z \neq \frac{3}{2}\}$. Assume $t \in \text{Range}(k)$, then $\exists t \in \mathbb{R} \setminus \{-4\}$ such that $k(x) = t$. Assume $x_0 \in \mathbb{R} \setminus \{-4\}$ and $k(x_0) = t$. Using the formula for k, this means that $t = \frac{3x_0-2}{2x_0+8}$. Since $x_0 \neq -4$ it is clear that t is a real number. In addition, $t \neq \frac{3}{2}$ can be proved by contradiction, for suppose $t = \frac{3}{2}$, then $\frac{3x_0-2}{2x_0+8} = \frac{3}{2}$. Multiplying both sides by $(2x_0 + 8)$ and collecting like terms gives $-2 = 12$ which is a contradiction. We have shown that $t \in \mathbb{R}$ and that $t \neq \frac{3}{2}$ hence $t \in \{z \in \mathbb{R} : z \neq \frac{3}{2}\}$. □

4.13. *Proof.* To prove that f is not onto $\mathbb{R}$, we'll prove it by contradiction. Assume f is onto $\mathbb{R}$. If f were onto $\mathbb{R}$, all real numbers would be in the range of

f. A number b is in the range of f if and only if for some $a \in \mathbb{R} \setminus \{2, -2\}$, $f(a) = \frac{1}{a^2-4}$. That is, if and only if $b = \frac{1}{a^2-4}$. If we attempt to solve this equation for a starting by multiplying both sides by $(a^2 - 4)$ we get $b(a^2 - 4) = 1$. Dividing both sides by b and then adding 4 to each side gives us $a^2 = \frac{1}{b} + 4$. Taking the square root of both sides, we find that $a = \sqrt{\frac{1}{b} + 4}$. Since a and b are real numbers, this should be possible for every $0 \not\leq b \not< -\frac{1}{4}$ since we can't divide by 0 and any fraction between 0 and $-\frac{1}{4}$ would produce a negative number under the square root which would not give us a real number. Since b cannot equal 0 or a negative fraction such as $-\frac{1}{5}$, which are real numbers, not all real numbers are in the range of f. This is a contradiction. Therefore, f is not onto $\mathbb{R}$. □

4.14. *Proof.* We will prove that f is not onto $\mathbb{R}$ (by contradiction) by showing that $1 \notin \text{Range}(f)$. Assume that $1 \in \text{Range}(f)$ then for some $x \in \text{Dom}(f)$, $1 = f(x) = \frac{x^2}{x^2-9}$. Multiplying both sides of this equation by $(x^2 - 9)$ and subtracting x^2 from both sides gives $0 = -9$ a contradiction. □

4.15. *Proof.* Toward a proof by contradiction assume that A and B are sets for which $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$ and $A \cap B \neq \emptyset$ and $A \not\subseteq B$. By the last two assumptions $\exists x \in A \cap B$ and $\exists y \in A$ such that $y \notin B$. We therefore have

1. $x \in A$
2. $x \in B$
3. $y \in A$ and
4. $y \notin B$.

Let $C = \{x, y\}$. We shall complete the proof by showing that $C \in \mathcal{P}(A) \setminus \mathcal{P}(B)$ and $C \notin \mathcal{P}(A \setminus B)$ contradicting the assumption that $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$.

We first note that by (a) and (c), $C \subseteq A$ and by (d) $C \not\subseteq B$. This means that $C \in \mathcal{P}(A)$ and $C \notin \mathcal{P}(B)$. So $C \in \mathcal{P}(A) \setminus \mathcal{P}(B)$. Secondly, by (b) $C \not\subseteq A \setminus B$ and therefore $C \notin \mathcal{P}(A \setminus B)$. □

4.16.

(a) A number b is in the range of k if and only if for some $a \in \mathbb{R}, k(a) = b$. That is, if and only if $a^2 - 3a + 7 = b$. If we attempt to solve this problem for a, we'll start by subtracting b from each side to get $a^2 - 3a + 7 - b = 0$ and then using the quadratic formula. Using the quadratic formula we get:

$$a = \frac{3 \pm \sqrt{9 - 4(7-b)}}{2} = \frac{3 \pm \sqrt{9 - 28 + 4b}}{2} = \frac{3 \pm \sqrt{4b - 19}}{2}$$

Since the portion under the square root has to be greater than or equal to 0 to be a real number, $b \geq \frac{19}{4}$. This means that $\text{Range}(k) = \{z \in \mathbb{R} : z \not< \frac{19}{4}\}$.

(b) *Proof.* Since both Range(k) and $\{z \in \mathbb{R} : z \not< \frac{19}{4}\}$ are sets, to prove that Range(k) $= \{z \in \mathbb{R} : z \not< \frac{19}{4}\}$ we need to show that Range(k) $\subseteq \{z \in \mathbb{R} : z \not< \frac{19}{4}\}$ and $\{z \in \mathbb{R} : z \not< \frac{19}{4}\} \subseteq$ Range(k).

We'll begin with the proof that $\{z \in \mathbb{R} : z \not< \frac{19}{4}\} \subseteq$ Range(k). Assume that $y \in \{z \in \mathbb{R} : z \not< \frac{19}{4}\}$. Then $y \in \mathbb{R}$ and $y \not< \frac{19}{4}$. Let $x_0 = \frac{3 \pm \sqrt{4y-19}}{2}$. Since $y \not< \frac{19}{4}$ it is clear that $x_0 \in \mathbb{R}$. We also have that $k(x_0) = x_0^2 - 3x_0 + 7 = (\frac{3 \pm \sqrt{4y-19}}{2})^2 - 3(\frac{3 \pm \sqrt{4y-19}}{2}) + 7 = (\frac{9}{4} \pm \frac{3\sqrt{4y-19}}{2} + \frac{4y-19}{4}) - (\frac{9}{2} \pm \frac{3\sqrt{4y-19}}{2}) + 7 = \frac{9}{4} + \frac{4y-19}{4} - \frac{9}{2} + 7 = \frac{4y-10}{4} - \frac{9}{2} + 7 = \frac{2y-5}{2} - \frac{9}{2} + \frac{14}{2} = \frac{2y-5}{2} + \frac{5}{2} = \frac{2y}{2} = y$. Hence $x_0 \in \mathbb{R}$ and $y = k(x_0)$. So $\exists x \in \mathbb{R}$ such that $y = k(x)$. Therefore $y \in$ Range(k).

Now we'll prove that Range(k) $\subseteq \{z \in \mathbb{R} : z \not< \frac{19}{4}\}$. Assume $t \in$ Range(k), then $\exists t \in \mathbb{R}$ such that $k(x) = t$. Assume $x_0 \in \mathbb{R}$ and $k(x_0) = t$. Using the formula for k, this means that $t = x_0^2 - 3x_0 + 7$. Since t is a polynomial and $x_0 \in \mathbb{R}$, it is clear that t is a real number. In addition, $t \not< \frac{19}{4}$ can be proved by contradiction, for suppose $t < \frac{19}{4}$, then $x_0^2 - 3x_0 + 7 < \frac{19}{4}$. By completing the square, we see that $x_0^2 - 3x_0 + \frac{9}{4} - \frac{9}{4} + 7 = (x_0 - \frac{3}{2})^2 + \frac{19}{4} < \frac{19}{4}$, or $(x_0 - \frac{3}{2})^2 < 0$. Since $(x_0 - \frac{3}{2}) \in \mathbb{Z}$, this is a contradition since the square of any real must be greater than or equal to zero. We have shown that $t \in \mathbb{R}$ and that $t \not< \frac{19}{4}$, hence $t \in \{z \in \mathbb{R} : z \not< \frac{19}{4}\}$. □

4.17. *Proof.* To prove that Range(f) $= \{y \in \mathbb{R} : y \neq 5\}$ if suffices to show that Range(f) $\subseteq \{y \in \mathbb{R} : y \neq 5\}$ and $\{y \in \mathbb{R} : y \neq 5\} \subseteq$ Range(f).

First, we'll prove that $\{y \in \mathbb{R} : y \neq 5\} \subseteq$ Range(f). Assume $y \in \{y \in \mathbb{R} : y \neq 5\}$. Then $y \in \mathbb{R}$ and $y \neq 5$. Let $x_0 = \frac{7y-1}{y-5}$. Since $y \neq 5$ it is clear that $x_0 \in \mathbb{R}$. We prove that $x_0 \neq 7$ by contradiction. Assume that $x_0 = 7$, then $\frac{7y-1}{y-5} = 7$. Multiplying both sides by $(y-5)$ gives us $7y - 1 = 7(y-5)$ which equals $7y - 1 = 7y - 35$ after using the distributive property. Subtracting $7y$ from both sides gives us $-1 = -35$. This is a contradiction. We also have that $f(x_0) = \frac{5x_0-1}{x_0-7} = \frac{5(\frac{7y-1}{y-5})-1}{(\frac{7y-1}{y-5})-7} = \frac{5(7y-1)-1(y-5)}{(7y-1)-7(y-5)} = \frac{35y-5-y+5}{7y-1-7y+35} = \frac{34y}{34} = y$. Hence $x_0 \in \mathbb{R} \setminus \{7\}$ and $y = f(x_0)$. So $\exists x \in \mathbb{R} \setminus \{7\}$ such that $y = f(x)$. Therefore $y \in$ Range(f).

Next, we'll prove that Range(f) $\subseteq \{y \in \mathbb{R} : y \neq 5\}$. Assume $t \in$ Range(f), then $\exists t \in \mathbb{R} \setminus \{7\}$ such that $t = f(x)$. Assume $x_0 \in \mathbb{R}$ and $f(x_0) = t$. Using the formula for f, this means that $t = \frac{5x_0-1}{x_0-7}$. Since $x_0 \neq 7$ it is clear that t is a real number. In addition, $t \neq 5$ can be proved by contradiction. Assume that $t = 5$, then $\frac{5x_0-1}{x_0-7} = 5$. Multiplying both sides by $(x_0 - 7)$ gives us $5x_0 - 1 = 5(x_0 - 7)$. Using the distributive property on the right hand side gives us $5x_0 - 1 = 5x_0 - 35$, and subtracting $5x_0$ from each side gives us $-1 = -35$. This is a contradiction. We have shown that $t \in \mathbb{R}$ and $t \neq 5$, hence $t \in \{z \in \mathbb{R} : z \neq 5\}$. □

4.18. *Proof.* To prove that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ it suffices to show that $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$ and $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$.

First, to prove that $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$, assume that $x \in (A \cup B) \cap C$. This means that $x \in A \cup B$ and $x \in C$. So $x \in C$ and $x \in A$ or $x \in B$. We consider two cases:

Case 1. $x \in A$. Since $x \in A$ and $x \in C$, $x \in A \cap C$. Therefore, $x \in (A \cap C) \cup (B \cap C)$.

Case 2. $x \in B$. Since $x \in B$ and $x \in C$, $x \in B \cap C$. Therefore, $x \in (A \cap C) \cup (B \cap C)$.

In either case, $\forall x \in (A \cup B) \cap C, x \in (A \cap C) \cup (B \cap C)$.

To prove that $(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$, assume that $x \in (A \cap C) \cup (B \cap C)$. This means that $x \in A \cap C$ or $x \in B \cap C$. We consider two cases:

Case 1. $x \in A \cap C$. This means that $x \in A$ and $x \in C$. If $x \in A$, then $x \in A \cup B$. Therefore, $x \in (A \cup B) \cap C$.

Case 2. $x \in B \cap C$. This means that $x \in B$ and $x \in C$. If $x \in B$, then $x \in A \cup B$. Therefore, $x \in (A \cup B) \cap C$.

In either case, $forallx \in (A \cap C) \cup (B \cap C), x \in (A \cup B) \cap C$. □

4.19. *Proof.* To prove that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ it suffices to show that $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$ and $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$.

First, to prove that $A \setminus (B \cup C) \subseteq (A \setminus B) \cap (A \setminus C)$, assume that $x \in A \setminus (B \cup C)$. This means that $x \in A$ and $x \notin B \cup C$. So $x \in A$, $x \notin B$, and $x \notin C$. Hence, $x \in A \setminus B$ and $x \in A \setminus C$. Therefore, $x \in (A \setminus B) \cap (A \setminus C)$.

Next, to prove that $(A \setminus B) \cap (A \setminus C) \subseteq A \setminus (B \cup C)$, assume that $x \in (A \setminus B) \cap (A \setminus C)$. This means that $x \in A \setminus B$ and $x \in A \setminus C$. So, $x \in A$, $x \notin B$, and $x \notin C$. Hence, $x \notin B \cup C$. Therefore, $x \in A \setminus (B \cup C)$. □

4.20. *Proof.* To prove that $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ it suffices to show that $A \setminus (B \cap C) \subseteq (A \setminus B) \cup (A \setminus C)$ and $(A \setminus B) \cup (A \setminus C) \subseteq A \setminus (B \cap C)$.

First, to prove that $A \setminus (B \cap C) \subseteq (A \setminus B) \cup (A \setminus C)$, assume that $x \in A \setminus (B \cap C)$. This means that $x \in A$ and $x \notin B \cap C$. If $x \notin B \cap C$, then either $x \in B$ and $x \notin C$ or $x \in C$ and $x \notin B$. We consider two cases:

Case 1. $x \in B$ and $x \notin C$. If $x \in A$ and $x \notin C$, then $x \in A \setminus C$. Therefore, $x \in (A \setminus B) \cup (A \setminus C)$.

Case 2. $x \in C$ and $x \notin B$. If $x \in A$ and $x \notin B$, then $x \in A \setminus B$. Therefore, $x \in (A \setminus B) \cup (A \setminus C)$.

In either case, $\forall x \in A \setminus (B \cap C), x \in (A \setminus B) \cup (A \setminus C)$.

Next, to prove that $(A \setminus B) \cup (A \setminus C) \subseteq A \setminus (B \cap C)$, assume that $x \in (A \setminus B) \cup (A \setminus C)$. This means that $x \in A \setminus B$ or $x \in AsetminusC$. We consider two cases:

Case 1. $x \in A \setminus B$. This means that $x \in A$ and $x \notin B$. If $x \notin B$, then $x \notin B \cap C$. Therefore, $x \in A \setminus (B \cap C)$.

Case 2. $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. If $x \notin C$, then $x \notin B \cap C$. Therefore, $x \in A \setminus (B \cap C)$.

In either case, $\forall x \in (A \setminus B) \cup (A \setminus C), x \in A \setminus (B \cap C)$. □

4.21. *Proof.* Assume that A and B are sets. We will prove that $\mathcal{P}(A \cap B) =$

$\mathcal{P}(A) \cap \mathcal{P}(B)$ using the principle of extensionality.

First assume that $X \in \mathcal{P}(A \cap B)$. Then, by definition, $X \subseteq (A \cap B)$. This means that $X \subseteq A$ and $X \subseteq B$. Therefore $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$, so $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

Next assume that $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. This means that $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. Therefore $X \subseteq A$ and $X \subseteq B$, which means that $X \subseteq (A \cap B)$. So, by definition, $X \in \mathcal{P}(A \cap B)$. □

4.22. *Proof.* Assume a_1 and a_2 are in $\text{Dom}(f)$ and that $f(a_1) = f(a_2)$. By the definition of f, $4a_1 + 9 = 4a_2 + 9$. Subtracting 9 from each side and then dividing each side by 4 gives us $a_1 = a_2$. This shows that f is one to one. □

4.23. *Proof.* To prove that f is one to one, assume that a_1 and a_2 are in $\text{Dom}(f)$ and that $f(a_1) = f(a_2)$. By the definition of f, $3a_1 + 7 = 3a_2 + 7$. Subracting 7 from each side and then dividing each side by 3 gives us $a_1 = a_2$. This shows that f is one to one.

To prove that f is onto $[7, 10]$, we need to show that $\text{Range}(f) \subseteq [7, 10]$ and $[7, 10] \subseteq \text{Range}(f)$. Assume that $y \in \text{Range}(f)$. Then for some $x \in [0, 1], f(x) = y$. That is $y = 3x + 7$. Since $0 \leq x \leq 1$, $0 \leq 3x \leq 3$. Adding 7 gives us $7 \leq 3x + 7 \leq 10$, so $7 \leq y \leq 10$. Hence $y \in [7, 10]$. Next, assume that $y \in [7, 10]$. Let $x = \frac{y-7}{3}$. Since $7 \leq y \leq 10$, $0 \leq y - 7 \leq 3$. Dividing by 3 gives us $0 \leq \frac{y-7}{3} \leq 1$, so $0 \leq x \leq 1$. Hence $x \in [0, 1]$. Further, $f(x) = 3x + 7 = 3(\frac{y-7}{3}) + 7 = (y - 7) + 7 = y$. Therefore, $y \in \text{Range}(f)$. □

4.24. *Proof.* Assume that a_1 and a_2 are in $\text{Dom}(f)$ and that $f(a_1) = f(a_2)$. By the definition of f, $\frac{2a_1}{a_1-3} = \frac{2a_2}{a_2-3}$. Multiplying both sides of this equation by $(a_1 - 3)(a_2 - 3)$ gives us $(a_2 - 3)(2a_1) = (a_1 - 3)(2a_2)$. Using the distributive property to multiply through on both sides, we get $2a_1a_2 - 6a_1 = 2a_1a_2 - 6a_2$. Subtracting $2a_1a_2$ from each side and then dividing each side by 6, we get $a_1 = a_2$. This shows that f is one to one. □

4.25. We're given that the domain of f is $[3, 8]$, and by finding the straight line joining (3, 1) and (8, 7) we know that a formula for $f(x)$ is $f(x) = \frac{6}{5}x - \frac{13}{5}$. We will now prove that this function is one to one. Assume a_1 and a_2 are in $\text{Dom}(f)$ and that $f(a_1) = f(a_2)$. Using the formula we found for f, $\frac{6}{5}a_1 - \frac{13}{5} = \frac{6}{5}a_2 - \frac{13}{5}$. By adding $\frac{13}{5}$ to each side of the equation and then multiplying both sides by $\frac{5}{6}$ we get that $a_1 = a_2$. This proves that $f(x)$ is one to one. Therefore, we can define $f : [3, 8] \to [1, 7]$ by $f(x) = \frac{6}{5}x - \frac{13}{5}$.

4.26. Since f is a function, $f^{-1} = \{(3, 2), (4, 3), (5, 4), (7, 5)\}$.

4.27. To find a formula for $f^{-1}(y)$, assume that $f^{-1}(y) = x$. We want to find a formula for x in terms of y. Using the formula for f, $4x + 9 = y$. Solving for x, we'll subtract 9 from each side and then divide both sides by 4 to get $x = \frac{y-9}{4}$. Hence, $f^{-1}(y) = \frac{y-9}{4}$.

4.28. To find a formula for $f^{-1}(y)$, assume that $f^{-1}(y) = x$. We want to find a formula for x in terms of y. Using the for f, $\frac{3x-2}{x-3} = y$. We will now solve for x. Multiply both sides by $x-3$ to get $y(x-3) = 3x-2$, and then use the distributive property on the left hand side to get $xy-3y = 3x-2$. Then add $3y$ to each side and subtract $3x$ from each side to get all parts containing x on the left hand side, giving us $xy-3x = 3y-2$. Next, use the distributive property on the left hand side to factor out the x, giving us $x(y-3) = 3y-2$. Lastly, divide both sides by $y-3$ to get $x = \frac{3y-2}{y-3}$. Hence, $f^{-1}(y) = \frac{3y-2}{y-3}$.

4.29. *Proof.*

(a) To prove this, we need some definitions. According to Definition 4.7, a function is one to one if for all (a_1, b_1) and (a_2, b_2) in f, if $b_1 = b_2$ then $a_1 = a_2$. Therefore, a one to one function will not have any second components repeating unless they have the same first components, too. According to Definition 4.10, if f is a function then $f^{-1} = \{(b, a) : (a, b) \in f\}$. Therefore, the inverse function will reverse the first and second components of the original function. According to Definition 4.1, a function is a set whose elements are ordered pairs such that for all pairs (a_1, b_1) and (a_2, b_2), if $a_1 = a_2$ then $b_1 = b_2$. In the one to one function f, the second components couldn't repeat. Since the inverse switches the first and second components, the inverse function's first components won't repeat, and this is the definition of a function (Def. 4.1). Therefore, f^{-1} is a function.

(b) The range of f is the set of all second components of pairs in f. Definition 4.10 (stated above) shows that the inverse function of f switches the first and second components of f. Since the domain is the set of all first components, and the second components of f are the first components of f^{-1}, then $\text{Dom}(f^{-1}) = \text{Range}(f)$.

(c) The domain of f is the set of all first components of pairs in f. Definition 4.10 (stated above) shows that the inverse function of f switches the first and second components of f. Since the range is the set of all second components, and the first components of f are the second components of f^{-1}, then $\text{Range}(f^{-1}) = \text{Dom}(f)$.

(d) A function g is one to one if and only if the inverse relation g^{-1} is a function. If we apply this using $g = f^{-1}$ we get the statement 'a function f^{-1} is one to one if and only if the inverse relation $(f^{-1})^{-1}$ is a function. Since $(f^{-1})^{-1} = f$ and we already know that f is a function, we know that f^{-1} is one to one.

□

4.30. $g \circ f = \{(2, 1), (3, 2), (4, 2), (5, 12)\}$

4.31. $(h \circ k)(t) = h(k(t)) = h(3t^3 + 4t^2 + 8) = 8(3t^3 + 4t^2 + 8) - 17 = 24t^3 + 32t^2 + 64 - 17 = 24t^3 + 32t^2 + 47$
$(k \circ h)(t) = k(h(t)) = k(8t - 17) = 3(8t - 17)^3 + 4(8t - 17)^2 + 8$

4.32. *Proof.* Assume that $f : A \to B$ and $g : B \to C$. Prove that if f and g are one to one then $g \circ f$ is one to one.

If f is one to one, then for all a_1 and a_2 in $\text{Dom}(f) = A$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$. Similarly, if g is one to one, then for all a_1 and a_2 in $\text{Dom}(g) = B$, if $g(a_1) = g(a_2)$ then $a_1 = a_2$.

For $g \circ f$ to be one to one, then for all a_1 and a_2 in $\text{Dom}(g \circ f) = A$, if $(g \circ f)(a_1) = (g \circ f)(a_2)$ then $a_1 = a_2$. We know that $(g \circ f)(a_1) = g(f(a_1))$ and $(g \circ f)(a_2) = g(f(a_2))$. Since we know that f is one to one, we know that $f(a_1) = f(a_2)$. Therefore $g(f(a_1)) = g(f(a_2))$. Since $(g \circ f)(a_1) = (g \circ f)(a_2)$, we know that $a_1 = a_2$, and this makes $g \circ f$ one to one. □

4.33. *Proof.* Assume that $f : A \to B$ and $g : B \to C$. Prove that if f is onto B and g is onto C then $g \circ f$ is onto C.

Let $z \in C$. Since g is onto $C, \exists y \in B$ such that $g(y) = z$. Since f is onto $B, \exists x \in A$ such that $f(x) = y$. Thus we have $g(f(x)) = g(y) = z$, and we see that $g \circ f$ is onto C. □

4.34. *Proof.* Assume that $f : A \to B, g : B \to C$, and $h : C \to D$. Prove that $h \circ (g \circ f) = (h \circ g) \circ f$.

We can assume that $f = f(x), g = g(x)$, and $h = h(x)$. We know that $g \circ f = g(f(x))$, so the second function $f(x)$ is used as the x in $g(x)$. Using this same principle, we can deduce that $h \circ (g \circ f) = h(g \circ f) = h(g(f(x)))$. This is the left hand side of the equation. For the right hand side, we use the same idea. We know that $h \circ g = h(g(x))$, so for $(h \circ g) \circ f$ we would replace the x in $h \circ g$ with $f(x)$, giving us $h(g(f(x)))$. Hence,since $h(g(f(x))) = h(g(f(x))), h \circ (g \circ f) = (h \circ g) \circ f$. □

4.35.

(a) This is possible. If $f(x) = e^x$ and $g(x) = x^2$ then f is one to one, g is not one to one, and $g \circ f = g(f(x)) = (e^x)^2 = e^{2x}$ which is one to one. The key here is that the range of f is contained in that part of the domain of g on which it *is* one to one.

(b) This is possible. (What would happen if f were constant, for example?)

(c) Not possible. Since f is not one to one, there exist two different values a and b for which $f(a) = f(b) (= c$, say). Then $g(f(a)) = g(c) = g(f(b))$, which is precisely the statement that g is not one to one.

(d) This is possible. (What if $B = mathbbR$ but C equals the set of real numbers greater than or equal to 0?)

(e) Not possible.

4.36. Note: f^* is defined for every subset of $\text{Dom}(f) = \{2, 3, 4, 5, 6, 7\}$.

(a) $f^*(\emptyset) = \{\emptyset\}$??

(b) $f^*(\{2, 4, 5, 7\}) = \{f(2), f(4), f(5), f(7)\} = \{3, 3, 5, 1\} = \{3, 5, 1\}$

(c) $f^*(\{3\}) = \{f(3)\} = \{6\}$

(d) $f^*(\{4, 5, 6\}) = \{f(4), f(5), f(6)\} = \{3, 5, 6\}$

4.37.

(a) $g^*(\{1, 2, 3\}) = \{g(1), g(2), g(3)\} = \{\frac{14}{3}, \frac{16}{3}, 6\}$

(b) $g^*([-1, 1]) = \{g(x) : x \in [-1, 1]\} = \{\frac{2}{3}x + 4 : -1 \leq x \leq 1\}$. Using y for $\frac{2}{3}x + 4$ and $x = \frac{3}{2}y - 6$ we can write this set as $\{y : -1 \leq \frac{3}{2}y - 6 \leq 1\} = \{y : 5 \leq \frac{3}{2}y \leq 7\} = \{y : \frac{10}{3} \leq y \leq \frac{14}{3}\}$. So $g^*([-1, 1]) = [\frac{10}{3}, \frac{14}{3}]$.

(c) $g^*([3, \infty)) = \{g(x) : x \in [3, \infty)\} = \{\frac{2}{3}x + 4 : 3 \leq x < \infty\}$. Using y for $\frac{2}{3}x + 4$ and $x = \frac{3}{2}y - 6$ we can write this set as $\{y : 3 \leq \frac{3}{2}y - 6 < \infty\} = \{y : 9 \leq \frac{3}{2}y < \infty\} = \{y : 6 \leq y < \infty\}$. So $g^*([3, \infty)) = [6, \infty)$.

(d) $g^*(\mathbb{R}) = \{g(x) : x \in \mathbb{R}\} = \{\frac{2}{3}x + 4 : -\infty < x < \infty\}$. Using y for $\frac{2}{3}x + 4$ and $x = \frac{3}{2}y - 6$ we can write this set as $\{y : -\infty < \frac{3}{2}y - 6 < \infty\} = \{y : -\infty < y < \infty\}$. So $g^*(\mathbb{R}) = (-\infty, \infty)$.

4.38.

(a) $h^*(\{-2, -1, 0, 1, 3, 5\}) = \{h(-2), h(-1), h(0), h(1), h(3), h(5)\} = \{4, 1, 0, 1, 9, 25\}$

(b) $h^*([2, 3)) = \{h(x) : x \in [2, 3)\} = \{x^2 : 2 \leq x < 3\}$. Using y for x^2 and $x = \pm\sqrt{y}$ we can write this set as $\{y : 2 \leq \pm\sqrt{y} < 3\}$. Since $\pm\sqrt{y}$ has to be a postive real number (between 2 and 3), we can safely drop the $\pm$ and keep it positive, so we set can be written as $\{y : 2 \leq \sqrt{y} < 3\} = \{y : 4 \leq y < 9\}$. So $h^*([2, 3)) = [4, 9)$.

(c) $h^*([-3, 5]) = \{h(x) : x \in [-3, 5]\} = \{x^2 : -3 \leq x \leq 5\}$. Using y for x^2 and $x = \pm\sqrt{y}$ we can write this set as $\{y : -3 \leq \pm\sqrt{y} \leq 5\} = \{y : -3 \leq -\sqrt{y} \leq 5$ and $-3 \leq \sqrt{y} \leq 5\}$. Since $-\sqrt{y}$ has to be a negative number, we can replace the 5 with a 0. Similarly, $\sqrt{y}$ has to be positive, so we can replace the -3 with a 0. This gives us the set $\{y : -3 \leq -\sqrt{y} \leq 0$ and $0 \leq \sqrt{y} \leq 5\} = \{y : 0 \leq \sqrt{y} \leq 3$ and $0 \leq \sqrt{y} \leq 5\}$. Since $3 < 5$ we really only need to use the first inequality, which gives us the set $\{y : 0 \leq \sqrt{y} \leq 3\} = \{y : 0 \leq y \leq 9\}$. So $h^*([-3, 5]) = [0, 9]$.

4.39. *Proof.* Since both sides of the equation are sets, it suffices to show that $f^*(X \cup Y) \subseteq f^*(X) \cup f^*(Y)$ and $f^*(X) \cup f^*(Y) \subseteq f^*(X \cup Y)$.

First we'll prove that $f^*(X \cup Y) \subseteq f^*(X) \cup f^*(Y)$. Assume that $f(x) \in f^*(X \cup Y)$. According to Definition 4.14, $f^*(X) = \{f(x) : x \in X\}$, so $f^*(X \cup$

$Y) = \{f(x) : x \in X \cup Y\}$. So $x \in X \cup Y$, which means that $x \in X$ or $x \in Y$. We consider two cases:

Case 1. $x \in X$. Then $f(x) \in f^*(X)$, so $f(x) \in f^*(X) \cup f^*(Y)$.

Case 2. $x \in Y$. Then $f(x) \in f^*(Y)$, so $f(x) \in f^*(X) \cup f^*(Y)$.

In either case, if $f(x) \in f^*(X \cup Y)$ then $f(x) \in f^*(X) \cup f^*(Y)$, so $f^*(X \cup Y) \subseteq f^*(X) \cup f^*(Y)$.

Next we'll prove that $f^*(X) \cup f^*(Y) \subseteq f^*(X \cup Y)$. Assume that $f(x) \in f^*(X) \cup f^*(Y)$. This means that $f(x) \in f^*(X)$ or $f(x) \in f^*(Y)$. We consider two cases:

Case 1. $f(x) \in f^*(X)$. This means that $x \in X$. So $x \in X \cup Y$. Therefore, $f(x) \in f^*(X \cup Y)$.

Case 2. $f(x) \in f^*(Y)$. This means that $x \in Y$. So $x \in X \cup Y$. Therefore, $f(x) \in f^*(X \cup Y)$.

In either case, if $f(x) \in f^*(X) \cup f^*(Y)$ then $f(x) \in f^*(X \cup Y)$, so $f^*(X) \cup f^*(Y) \subseteq f^*(X \cup Y)$. □

4.40. *Proof.* Assume that $f(x) \in f^*(X \cap Y)$. Then $x \in X \cap Y$, so $x \in X$ and $x \in Y$. Hence, $f(x) \in f^*(X)$ and $f(x) \in f^*(Y)$. So if $f(x) \in f^*(X \cap Y)$ then $f(x) \in f^*(X) \cap f^*(Y)$. Therefore, $f^*(X \cap Y) \subseteq f^*(X) \cap f^*(Y)$. □

4.41. $A, B = \mathbb{R}, f(x) = x^2, X = \{-2, -1, 0\}, Y = \{0, 1, 2\}$
$X \cap Y = \{0\}, f^*(X \cap Y) = \{0\}$
$f^*(X) = \{4, 1, 0\}, f^*(Y) = \{0, 1, 4\}, f^*(X) \cap f^*(Y) = \{0, 1, 4\}$

4.42. *Proof.* Since both sides of the equation are sets, it suffices to show that $f^*(X \cap Y) \subseteq f^*(X) \cap f^*(Y)$ and $f^*(X) \cap f^*(Y) \subseteq f^*(X \cap Y)$.

First we'll prove that $f^*(X \cap Y) \subseteq f^*(X) \cap f^*(Y)$. This is proved previously in 4.40.

Next we'll prove that $f^*(X) \cap f^*(Y) \subseteq f^*(X \cap Y)$. Assume that $f(x) \in f^*(X) \cap f^*(Y)$. This means that $f(x) \in f^*(X)$ and $f(x) \in f^*(Y)$. Then $x \in X$ and $x \in Y$. Hence, $x \in X \cap Y$. Therefore, $f(x) \in f^*(X \cap Y)$. Thus, $f^*(X) \cap f^*(Y) \subseteq f^*(X \cap Y)$, and our proof is complete. □

4.43. *Proof.* Assume that $f(x) \in f^*(X \setminus Y)$. This means that $f(x) \in f^*(X)$ and $f(x) \notin f^*(Y)$. Therefore, $f(x) \in f^*(X) \setminus f^*(Y)$ and $f^*(X \setminus Y) \subseteq f^*(X) \setminus f^*(Y)$. □

4.44. *Proof.* Assume that $f(x) \in f^*(X) \setminus f^*(Y)$. Then $f(x) \in f^*(X)$ and $f(x) \notin f^*(Y)$. So $x \in X$ and $x \notin Y$, which means that $x \in X \setminus Y$. Hence, $f(x) \in f^*(X \setminus Y)$ and $f^*(X) \setminus f^*(Y) \subseteq f^*(X \setminus Y)$. □

4.45. *Proof.* To prove that these statements are equivalent, we must treat this as an "if and only if" statement.

We will first assume part(b) is true to prove part (a). Assume that for every positive real number y there is a natural number n such that $\frac{1}{n} < y$. Assume

$x > 0$ and let $y = \frac{1}{x}$. Then by hypothesis, $\frac{1}{n} < \frac{1}{x}$. Cross multiplying, we find that $x < n$, and part (a) is true.

Next, assume that part (a) is true. Assume that for every positive real number x there exists a natural number n such that $x < n$. Assume $y > 0$ and let $x = \frac{1}{y}$. Then $\frac{1}{y} < n$. Cross multiplying, we find that $\frac{1}{n} < y$, and part (b) is true. Thus, these statements are equivalent. □

4.46. *Proof.* Since both sides of this equation are sets, it suffices to show that $\bigcup_{i\in\mathbb{N}}[0, i+1) \subseteq [0,\infty)$ and $[0,\infty) \subseteq \bigcup_{i\in\mathbb{N}}[0, i+1)$.

First we'll prove that $\bigcup_{i\in\mathbb{N}}[0, i+1) \subseteq [0,\infty)$. Assume $x \in \bigcup_{i\in\mathbb{N}}[0, i+1)$. By Definition 4.16, $x \in \{x|\exists i \in \mathbb{N} \text{ such that } x \in [0, i+1)\}$. Since $x \in [0, i+1)$, then $0 \leq x < i+1$. Hence $x \in \{x|x \geq 0\} = [0,\infty)$.

Next we'll prove that $[0,\infty) \subseteq \bigcup_{i\in\mathbb{N}}[0, i+1)$. Assume $x \in [0,\infty)$. Let i be a natural number such that $i > x$, which is possible by exercise 4.45. Then $0 \leq x < i < i+1 \forall i \in \mathbb{N}$. So $x \in [0, i+1)$. Therefore, $x \in \bigcup_{i\in\mathbb{N}}[0, i+1)$. □

4.47. $\bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}] = [0, 1)$

Proof. Since both sides of this equation are sets, it suffices to show that $\bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}] \subseteq [0, 1)$ and $[0, 1) \subseteq \bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}]$.

First we'll prove that $\bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}] \subseteq [0, 1)$. Assume $x \in \bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}]$. By Definition 4.16, $x \in \{x|\exists i \in \mathbb{N} \text{ such that } x \in [0, \frac{i}{i+1}]\}$. Since $x \in [0, \frac{i}{i+1}]$, then $0 \leq x \leq \frac{i}{i+1} < 1$. Hence $x \in [0, 1)$.

Next we'll prove that $[0, 1) \subseteq \bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}]$. Assume $x \in [0, 1)$. Then $0 \leq x < 1$. By the Archimedian property, there exists a natural number i such that $\frac{x}{1-x} < i$ (since $0 \leq x < 1, 1 - x > 0$). Then, $\frac{x}{1-x} < i \to x < i(1-x) \to x < i - xi \to x + xi < i \to x(1+i) < i \to x < \frac{i}{1+i}$. So $0 \leq x < \frac{i}{i+1}$, and $x \in [0, \frac{i}{i+1})$ Hence, $[0, 1) \subseteq \bigcup_{i\in\mathbb{N}}[0, \frac{i}{i+1}]$. □

4.48. $\bigcap_{i\in\mathbb{N}}[1 - \frac{1}{i+1}, 1 + \frac{1}{i+1}] = \{1\}$

4.49. $\bigcap_{i\in\mathbb{N}}[0, \frac{i}{i+1}] = [0, \frac{1}{2}]$

4.50. $\bigcup \mathcal{A} = \{1, 2, 3, 4, 5, 7, 9, 11\}$
$\bigcap \mathcal{A} = \{3, 9\}$

B.5 Chapter 5

5.3. *Proof.* Let $P(n)$ be the sentence "$9n^2+3n$ is even", then $P(0)$ is "$9\cdot0^2+3\cdot0$ is even", that is "0 is even" which is true since $0 = 2 \cdot 0$.

For the induction step we assume that $k \in \mathbb{N}$ and $P(k)$. That is we are assuming that

$$9k^2 + 3k \text{ is even.} \tag{1}$$

(We need to argue that $P(k+1)$ is true, that is that $9(k+1)^2 + 3(k+1)$ is even.)

By our assumption, $9k^2+3k = 2j$ for some $j \in \mathbb{Z}$. Then $9(k+1)^2+3(k+1) = 9k^2+18k+9+3k+1 = (9k^2+3k)+18k+10 = 2j+18k+10 = 2(j+9k+5)$. Where the second to last equality follows from (1). Letting $i = j + 9k + 5$ we see that i is an integer (since j and k are integers) and further $9(k+1)^2 + 3(k+1) = 2i$. Hence $9(k+1)^2 + 3(k+1) = 2i$ is even. □

5.4. *Proof.* Let $P(n)$ be the sentence "$25n^2 + 5n$ is even", then $P(0)$ is "$25 \cdot 0^2 + 5 \cdot 0$ is even", that is "0 is even" which is true since $0 = 2 \cdot 0$.

For the induction step we assume that $k \in \mathbb{N}$ and $P(k)$. That is we are assuming that

$$25k^2 + 5k \text{ is even.} \tag{1}$$

(We need to show that $P(k+1)$ is true, that is that $9(k+1)^2+3(k+1)$ is even.) By our assumption, $25k^2+5k = 2j$ for some $j \in \mathbb{Z}$. Then $25(k+1)^2+5(k+1) = 25k^2+50k+25+5k+5 = (25k^2+5k)+50k+30 = 2j+50k+30 = 2(j+25k+15)$. The second to last equality follows from (1). Letting $i = j+25k+15$ we see that i is an integer (since j and k are integers) and further $25(k+1)^2+5(k+1) = 2i$. Hence $25(k+1)^2 + 5(k+1) = 2i$ is even. □

5.5.

(a) *Proof.* Assume $m, n \in \mathbb{Z}$ and m and n are even. By definition 1.19, $m = 2i$ and $n = 2j$ for some $i, j \in \mathbb{Z}$. Then $m + n = 2i + 2j = 2(i + j)$. Letting $k = i + j$ we see that k is an integer and further $m + n = 2k$. Hence, $m + n$ is even. □

(b) *Proof.* Assume $m, n \in \mathbb{Z}$ and m and n are odd. By definition 1.19, $m = 2i + 1$ and $n = 2j + 1$ for some $i, j \in \mathbb{Z}$. Then $m + n = (2i + 1) + (2j + 1) = 2i + 2j + 2 = 2(i + j + 1)$. Letting $k = i + j + 1$ we see that k is an integer and further $m + n = 2k$. Hence, $m + n$ is even. □

(c) *Proof.* Assume $m, n \in \mathbb{Z}$ and m is even and n is odd. By definition 1.19, $m = 2i$ and $n = 2j + 1$ for some $i, j \in \mathbb{Z}$. Then $m + n = 2i + 2j + 1 = 2(i + j) + 1$. Letting $k = i + j$ we see that k is an integer and further $m + n = 2k + 1$. Hence, $m + n$ is odd. □

(d) *Proof.* Assume $m, n \in \mathbb{Z}$ and m and n are odd. By definition 1.19, $m = 2i+1$ and $n = 2j+1$ for some $i, j \in \mathbb{Z}$. Then $mn = (2i+1)(2j+1) = 4ij + 2i + 2j + 1 = 2(2ij + i + j) + 1$. Letting $k = 2ij + i + j$ we see that k is an integer and further $mn = 2k + 1$. Hence, mn is odd. □

(e) *Proof.* Assume $m, n \in \mathbb{Z}$ and m is even. By definition 1.19, $m = 2i$ for some $i \in \mathbb{Z}$. By Corollary 5.7, n must be either even or odd. We consider two cases

Case 1. n is even. That is, $n = 2j$ for some $j \in \mathbb{Z}$. Then $mn = (2i)(2j) = 4ij = 2(2ij)$. Letting $k = 2ij$ we see that k is an integer and further $mn = 2k$. Hence, mn is even.

Case 2. n is odd. That is, $n = 2j + 1$ for some $j \in \mathbb{Z}$. Then $mn = (2i)(2j + 1) = 4ij + 2i = 2(2ij + i)$. Letting $k = 2ij + i$ we see that k is an integer and further $mn = 2k$. Hence, mn is even.

In either case, if m is even, then mn is even. □

5.6. *Proof.* Assume that $n \in \mathbb{N}$. By Corollary 5.7, n must be either even or odd. We consider two cases

Case 1. n is even. That is, $n = 2i$ for some $i \in \mathbb{Z}$. Then $9n^2 + 3n = 9(2i)^2 + 3(2i) = 36i^2 + 6i = 2(18i^2 + 3i)$. Letting $k = 18i^2 + 3i$ we see that k is an integer and further $9n^2 + 3n = 2k$. Hence, $9n^2 + 3n$ is even.

Case 2. n is odd. That is, $n = 2i + 1$ for some $i \in \mathbb{Z}$. Then $9n^2 + 3n = 9(2i+1)^2+3(2i+1) = 36i^2+36i+9+6i+3 = 36i^2+42i+12 = 2(18i^2+21i+6)$. Letting $k = 18i^2+21i+6$ we see that k is an integer and further $9n^2+3n = 2k$. Hence, $9n^2 + 3n$ is even.

Therefore, in either case, $9n^2 + 3n$ is even. □

5.7. *Proof.* Assume that $n \in \mathbb{N}$. By Corollary 5.7, n must be either even or odd. We consider two cases

Case 1. n is even. That is, $n = 2i$ for some $i \in \mathbb{Z}$. Then $25n^2 + 5n = 25(2i)^2 + 5(2i) = 100i^2 + 10i = 2(50i^2 + 5i)$. Letting $k = 50i^2 + 5i$ we see that k is an integer and further $25n^2 + 5n = 2k$. Hence, $25n^2 + 5n$ is even.

Case 2. n is odd. That is, $n = 2i + 1$ for some $i \in \mathbb{Z}$. Then $25n^2 + 5n = 25(2i + 1)^2 + 5(2i + 1) = 100i^2 + 100i + 25 + 10i + 5 = 100i^2 + 110i + 30 = 2(50i^2 + 55i + 15)$. Letting $k = 50i^2 + 55i + 15$ we see that k is an integer and further $25n^2 + 5n = 2k$. Hence, $25n^2 + 5n$ is even.

Therefore, in either case, $25n^2 + 5n$ is even. □

5.8. *Proof.* Let $P(n)$ by the sentence "$n^3 + 2n$ is a multiple of 3". Then $P(0)$ is "$0^3 + 2 \cdot 0$ is a multiple of 3" which is true since $0 = 3 \cdot 0$.

For the induction step assume that $k \in \mathbb{N}$ and $P(k)$, that is, $k \in \mathbb{N}$ and $k^3 + 2k$ is a multiple of 3. Then

$$k^3 + 2k = 3j \text{ for some integer } j \tag{1}$$

(We have to show that $(n + 1)^3 + 2(n + 1)$ is a multiple of 3.) We note that $(n + 1)^3 + 2(n + 1) = n^3 + 3n^2 + 3n + 1 + 2n + 2 = (n^3 + 2n) + 3n^2 + 3n + 3 = 3j + 3n^2 + 3n + 3 = 3(j + n^2 + n + 1)$. □

5.9. *Proof.* Let $P(n)$ be the sentence "$2n^3 + n$ is a multiple of 3". Then $P(0)$ is "$2 \cdot 0^3 + 0$ is a multiple of 3" which is true since $0 = 3 \cdot 0$.

For the induction step assume that $k \in \mathbb{N}$ and $P(k)$, that is, $k \in \mathbb{N}$ and $2k^3 + k$ is a multiple of 3. Then

$$2k^3 + k = 3j \text{ for some integer } j \tag{1}$$

(We have to show that $2(k+1)^3 + (k+1)$ is a multiple of 3.) We note that $2(k+1)^3 + (k+1) = 2k^3 + 6k^2 + 6k + 2 + k + 1 = (2k^3 + k) + 6k^2 + 6k + 3 = 3j + 6k^2 + 6k + 3 = 3(j + 2k^2 + 2k + 1)$ □

5.10. $q = 12, r = 17$

5.11. *Proof.* Assume $n \in \mathbb{Z}$. We will prove by contradiction that n cannot be both even and odd.

Suppose n is both even and odd. Then $n = 2i$ and $n = 2j + 1$ for some $i, j \in \mathbb{Z}$. Then $2i = 2j + 1$, which implies that $i = j + \frac{1}{2}$. This contradicts the fact that $i \in \mathbb{Z}$. Therefore, n cannot be both even and odd. □

5.12. *Proof.* Let $P(n)$ be the sentence "$n \leq 2^n$". Then $P(0)$ is "$0 \leq 2^0$" which is true since $0 \leq 2^0 = 1$.

For the induction step assume that $k \in \mathbb{N}$ and that $P(k)$ is true. Then

$$k \leq 2^k. \tag{1}$$

(We want to show that $P(k+1)$ is true, that is that $k + 1 \leq 2^{k+1}$.) Beginning with the left hand side of this inequality, we see that

$$\begin{aligned} k + 1 \leq & 2^k + 1 \text{ by (1)} \\ \leq & 2^k + 2^0 \\ \leq & 2^k + 2^1 \\ \leq & 2^{k+1} \end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.19. *Proof.* Assume $n \geq 1$. Let $P(n)$ be the sentence "$n < 2^n$". Then $P(1)$ is "$1 < 2^1$" which is true since $1 < 2^1 = 2$.

For the induction step assume that $k \in \mathbb{N}$, $k \geq 1$, and that $P(k)$ is true. Then,

$$k < 2^k. \tag{1}$$

We need to show that $P(k+1)$ is true, that is that $k + 1 < 2^{k+1}$. Beginning with the left hand side of this inequality, we see that

$$\begin{aligned} k + 1 < & 2^k + 1 \text{ by (1)} \\ = & 2^k + 2^0 \\ < & 2^k + 2^k \\ = & 2 \cdot 2^k \\ = & 2^{k+1} \end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.20. *Proof.* Assume $n \geq 7$. Let $P(n)$ be the sentence "$6n + 4 < n^2$". Then

$P(7)$ is "$6 \cdot 7 + 4 < 7^2$" which is true since $6 \cdot 7 + 4 = 46 < 7^2 = 49$.

For the induction step assume that $k \in \mathbb{N}$, $k \geq 7$, and that $P(k)$ is true. Then

$$6k + 4 < k^2 \tag{1}$$

We have to argue that $P(k+1)$ is true, that is that $6(k+1) + 4 < (k+1)^2$. Beginning with the left hand side of this inequality, we see that

$$\begin{aligned} 6(k+1) + 4 =& 6k + 10 \\ =& (6k + 4) + 6 \\ <& k^2 + 6 \text{ by (1)} \\ <& k^2 + 2k + 1 \\ =& (k+1)^2 \end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.21. *Proof.* Assume $n \geq 3$. Let $P(n)$ be the sentence "$3n^2 \leq n^3$". Then $P(3)$ is "$3 \cdot 3^2 \leq 3^3$" which is true since $3 \cdot 3^2 = 27 \leq 3^3 = 27$.

For the induction step assume that $k \in \mathbb{N}$, $k \geq 3$, and that $P(k)$ is true. Then

$$3k^2 \leq k^3 \tag{1}$$

We have to argue that $P(k+1)$ is true, that is that $3(k+1)^2 \leq (k+1)^3$. Beginning with the left hand side of this inequality, we see that

$$\begin{aligned} 3(k+1)^2 =& 3k^2 + 6k + 3 \\ \leq& k^3 + 6k + 3 \text{ by (1)} \\ \leq& k^3 + 3k^2 + 3k + 1 \\ & \text{since, at the least, if } k = 4, 4^3 + 6 \cdot 4 + 3 = 91 < 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 1 = 125 \\ =& (k+1)^3 \end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.22. *Proof.* Assume $n \geq 10$. Let $P(n)$ be the sentence "$n^3 < 2^n$". Then $P(10)$ is "$10^3 < 2^{10}$" which is true since $10^3 = 1000 < 2^{10} = 1024$.

For the induction step assume that $k \in \mathbb{N}$, $k \geq 10$, and that $P(k)$ is true. Then,

$$k^3 < 2^k. \tag{1}$$

We need to show that $P(k+1)$ is true, that is that $(k+1)^3 < 2^{k+1}$. Beginning

with the left hand side of this inequality, we see that

$$\begin{aligned}(k+1)^3 =& k^3 + 3k^2 + 3k + 1\\ <& 2^k + 3k^2 + 3k + 1 \text{ by (1)}\\ <& 2^k + 2k\\ & \text{since, at the least, if } k = 11, 3\cdot 11^2 + 3\cdot 11 + 1 = 397 < 2^{11} = 2048\\ =& 2\cdot 2^k\\ =& 2^{k+1}\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.23. *Proof.* Assume $n \geq 3$. Let $P(n)$ be the sentence "$3^n + 4^n < 5^n$". Then $P(3)$ is "$3^3 + 4^3 < 5^3$" which is true since $3^3 + 4^3 = 91 < 5^3 = 125$.

For the induction step assume that $k \in \mathbb{N}$, $k \geq 3$, and that $P(k)$ is true. Then

$$3^k + 4^k < 5^k \tag{1}$$

We have to argue that $P(k+1)$ is true, that is that $3^{k+1} + 4^{k+1} < 5^{k+1}$. Beginning with the left hand side of this inequality, we see that

$$\begin{aligned}3^{k+1} + 4k + 1 =& 3\cdot 3^k + 4\cdot 4^k\\ <& 5\cdot 3^k + 5\cdot 4^k\\ =& 5(3^k + 4^k)\\ <& 5\cdot 5^k \text{ by (1)}\\ =& 5^{k+1}\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.24. *Proof.* Assume $n \in \mathbb{N}$ and let $x \geq 1$. Let $P(n)$ be the sentence "$(1+x)^n \geq 1 + nx$". Then $P(0)$ is "$(1+x)^0 \geq 1 + 0\cdot x$" which is true since $(1+x)^0 = 1 \geq 1 + 0\cdot x = 1$.

For the induction step, assume $k \in \mathbb{N}$, $x \geq 1$, and $P(k)$ is true. Then

$$(1+x)^k \geq 1 + kx \tag{1}$$

We have to argue that $P(k+1)$ is true, that is that $(1+x)^{k+1} \geq 1 + (k+1)x$. Beginning with the left hand side of this inequality, we see that

$$\begin{aligned}(1+x)^{k+1} =& (1+x)(1+x)^k\\ \geq& (1+x)(1+kx) \text{ by (1)}\\ =& 1x + kx + kx^2\\ \geq& 1 + x + kx \text{ since } x \geq 1\\ =& 1 + (k+1)x\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.25. $\sum_{i=0}^{k+1}(i+i^2) = ((k+1)+(k+1)^2) + \sum_{i=0}^{k}(i+i^2)$

5.26. *Proof.* Letting $P(n)$ be the sentence $\sum_{i=0}^{n}(x^i) = \frac{1-x^{n+1}}{1-x}$ we begin the mathematical induction proof $\forall n \in \mathbb{N}$ by noting that $P(0)$ is the statement "$x^0 = \frac{1-x}{1-x} = 1$" which is true.

For the induction step assume that $k \in \mathbb{N}$ and that $P(k)$ is true. Then

$$\sum_{i=0}^{k}(x^i) = \frac{1-x^{k+1}}{1-x}. \qquad (*)$$

We have to argue that $P(k+1)$ is true, that is that $\sum_{i=0}^{k+1}(x^i) = \frac{1-x^{k+2}}{1-x}$. Beginning with the left hand side of this equality, we see that

$$\begin{aligned}
\sum_{i=0}^{k+1}(2i+1) &= \left(\sum_{i=0}^{k}(x^i)\right) + (x^{k+1}) \\
&\qquad \text{by the definition of the } \textstyle\sum \text{ notation} \\
&= \frac{1-x^{k+1}}{1-x} + (x^{k+1}) \qquad \text{by } (*) \\
&= \frac{1-x^{k+1}}{1-x} + \frac{(1-x)x^{k+1}}{1-x} \\
&= \frac{1-x^{k+1}+x^{k+1}-x\cdot x^{k+1}}{1-x} \\
&= \frac{1-x^{k+2}}{1-x}
\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.27. *Proof.* Letting $P(n)$ be the sentence $\sum_{i=0}^{n}(2i+1) = (n+1)^2$ we begin the mathematical induction proof by noting that $P(0)$ is the statement "$2\cdot 0+1 = (0+1)^2$" which is true.

For the induction step assume that $k \in \mathbb{N}$ and that $P(k)$ is true. Then

$$\sum_{i=0}^{k}(2i+1) = (k+1)^2. \qquad (*)$$

We have to argue that $P(k+1)$ is true, that is that $\sum_{i=0}^{k+1}(2i+1) = ((k+1)+1)^2$.

Beginning with the left hand side of this equality, we see that

$$\begin{aligned}\sum_{i=0}^{k+1}(2i+1) &= \left(\sum_{i=0}^{k}(2i+1)\right) + (2(k+1)+1) \\ &\qquad \text{by the definition of the } \textstyle\sum \text{ notation} \\ &= (k+1)^2 + (2(k+1)+1) \qquad \text{by } (*) \\ &= k^2 + 2k + 1 + 2k + 3 = k^2 + 4k + 4 \\ &= (k+2)^2 = ((k+1)+1)^2\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.28. *Proof.* Assume $n \in \mathbb{N}$ for $n \geq 4$. Let $P(n)$ be the sentence "$n! \geq 2^n$". Then $P(4)$ is "$4! \geq 2^4$" which is true since $4! = 24 \geq 2^4 = 16$.

For the induction step, assume $k \in \mathbb{N}$, $k \geq 4$, and $P(k)$ is true. Then

$$k! \geq 2^k \tag{1}$$

We have to argue that $P(k+1)$ is true, that is that $(k+1)! \geq 2^{k+1}$. Beginning with the left hand side of this inequality, we see that

$$\begin{aligned}(k+1)! &= (k!)(k+1) \\ &\geq 2^k(k+1) \text{ by (1)} \\ &\geq 2 \cdot 2^k \text{ since, at the least, } k+1 = 4+1 = 5 > 2 \\ &= 2^{k+1}\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.29. *Proof.* Letting $P(n)$ be the sentence $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ we begin the mathematical induction proof by noting that $P(1)$ is the statement "$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{1}{1+1}$" which is true.

For the induction step assume that $k \in \mathbb{N}$ and that $P(k)$ is true. Then

$$\sum_{i=1}^{k} \frac{1}{i(i+1)} = \frac{k}{k+1}. \tag{*}$$

We have to argue that $P(k+1)$ is true, that is that $\sum_{i=1}^{k+1} \frac{1}{i(i+1)} = \frac{k+1}{k+2}$. Begin-

ning with the left hand side of this equality, we see that

$$\begin{aligned}\sum_{i=1}^{k+1}\frac{1}{i(i+1)} &= \left(\sum_{i=1}^{k}\frac{1}{i(i+1)}\right)+\frac{1}{(k+1)(k+2)}\\ &\qquad\text{by the definition of the } \textstyle\sum \text{ notation}\\ &=\frac{k}{k+1}+\frac{1}{(k+1)(k+2)} \qquad \text{by (*)}\\ &=\frac{k(k+2)}{(k+1)(k+2)}+\frac{1}{(k+1)(k+2)}\\ &=\frac{k^2+2k+1}{(k+1)(k+2)}\\ &=\frac{(k+1)(k+1)}{(k+1)(k+2)}\\ &=\frac{k+1}{k+2}\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.30.

(a) $A=\mathbb{N}, a_0=1, h(x,y)=2y$

(b) $A=\mathbb{N}, a_0=0, h(x,y)=y+(x+1)^2$

5.31. *Proof.* Assume that f_1 and f_2 are functions from $\mathbb{N}$ to $\mathbb{N}$ for which $f_1(0)=a_0, f_2(0)=a_0, \forall k\in\mathbb{N}, f_1(k+1)=h(k,f_1(k))$ and $\forall k\in\mathbb{N}, f_2(k+1)=h(k,f_2(k))$. Note that the domain of both functions is $\mathbb{N}$, thus $\text{Dom}(f_1)=\text{Dom}(f_2)$.

Next we must show that $\forall k\in\mathbb{N}, f_1(k)=f_2(k)$. We will prove this by induction. Let $P(n)$ be the sentence "$f_1(n)=f_2(n)$". Then $P(0)$ is "$f_1(0)=f_2(0)$" which is true since $f_1(0)=a_0=f_2(0)$.

For the induction step, assume that $k\in\mathbb{N}$ and $P(k)$ is true, that is, $k\in\mathbb{N}$ and

$$f_1(k)=f_2(k). \qquad (*)$$

We need to show that $f_1(k+1)=f_2(k+1)$. Beginning with the left hand side of this equation and using the hypothesis, we see that

$$\begin{aligned}f_1(k+1) &= h(k,f_1(k))\\ &= h(k,f_2(k)) \text{ by (*)}\\ &= f_2(k+1) \text{ by hypothesis}\end{aligned}$$

This shows that $P(k+1)$ is true and therefore completes the proof. □

5.32. *Proof.* Assume that g_1 and g_2 are good and that $n\in\text{Dom}(g_1)\cap\text{Dom}(g_2)$.

That is, for some $n \in \mathbb{N}, g_1, g_2 : \mathbb{N}_n \to A, g_1(0), g_2(0) = a_0$, and $\forall k \in \text{Dom}(g_1) \cap \text{Dom}(g_2)$ such that $k < n, g_1(k+1) = h(k, g_1(k))$ and $g_2(k+1) = h(k, g_2(k))$. Let $P(n)$ be the sentence "$g_1(n) = g_2(n)$". Then $P(0)$ is "$g_1(0) = g_2(0)$" which is true since $g_1(0) = a_0 = g_2(0)$.

For the induction step, assume $k \in \text{Dom}(g_1) \cap \text{Dom}(g_2)$ and $P(k)$. That is,

$$g_1(k) = g_2(k). \tag{*}$$

We need to show that $g_1(k+1) = g_2(k+1)$. Beginning with the left hand side of this equation, we see that

$$\begin{aligned} g_1(k+1) &= h(k, g_1(k)) \\ &= h(k, g_2(k)) \text{ by } (*) \\ &= g_2(k+1) \end{aligned}$$

This proves that $P(k+1)$ is true and therefore completes the proof. □

5.33. *Proof.* Let $f = \{(n, y) : \text{there is a good } g \text{ such that } n \in \text{Dom}(g) \text{ and } g(n) = y\}$. Assume $(n, y_1), (n, y_2) \in f$. That is, there are good functions, g_1 and g_2, such that $n \in \text{Dom}(g_1) \cap \text{Dom}(g_2)$, $g_1(n) = y_1$, and $g_2(n) = y_2$. By 5.32, since n is in the intersection of the domains, $g_1(n) = g_2(n)$. Hence, $y_1 = y_2$ and f is a function. □

5.34. *Proof.* For the funtion $f = \{(0, a_0)\}$, $\text{Dom}(f) = \{0\}$. Then for $0 \in \text{Dom}(f)$, $f : \{0\} \to A$, and $f(0) = a_0$. The latter half of the definition of good states that $\forall k \in \{0\}$, if $k < n$ then $g(k+1) = h(k, g(k))$. However, there are no k for which this statement holds. Therefore, the statement is vacuously true, and f is good. □

5.35. *Proof.* Assume $n \in \mathbb{N}$ and let $P(n)$ be the statement "there is a good function g such that $\text{Dom}(g) = \mathbb{N}_n$." Then $P(0)$ means that "there is a good function g such that $\text{Dom}(g) = \mathbb{N}_0$." This is the good function from 5.34.

For the induction step, we will prove that if g is good and if $\text{Dom}(g) = \mathbb{N}_k$ then $g' = g \cup \{(k+1, h(k+1, g(k+1)))\}$ is good. Assume g is good and $\text{Dom}(g) = \mathbb{N}_k$. The function $g'(n)$ can be expressed as follows:

$$g'(n) = \begin{cases} g(n) & \text{if } n \leq k \\ h(k, g(k)) & \text{if } n = k+1 \end{cases}$$

We must show that g' is good and $\text{Dom}(g') = \mathbb{N}_{k+1}$. By the definition of $g'(n)$, $\text{Dom}(g') = \text{Dom}(g) \cup k+1$. Hence, $\text{Dom}(g') = \mathbb{N}_{k+1}$. We will show that $\forall j \in \text{Dom}(g')$ if $j < k+1$ then $g'(j+1) = h(j, g'(j))$. Assume $j \in \text{Dom}(g')$ and $j < k+1$. We consider two cases.

Case 1. $j < k$. Let $n = j+1$. Then $n \leq k$. By the definition of g', $g'(n) = g(n) = h(n-1, g(n-1)) = h(n-1, g'(n-1)) = h(j, g'(j))$.

Case 2. $j = k$. Let $n = j + 1 = k + 1$. By the definition of g', $g'(n) = h(n-1, g(n-1)) = h(n-1, g'(n-1)) = h(j, g'(j))$.

In either case, $g'(j+1) = h(j, g'(j))$, and our proof is complete. □

5.36.

(a) This is proven by Exercise 5.34.

(b) We must first prove that $\forall n \in \mathbb{N}, n \in \text{Dom}(f)$. This is proven in Exercise 5.35. Next, we must prove that $\text{Range}(f) \subseteq A$. We will prove by induction that $\forall n \in \mathbb{N}, f(n) \in A$. First, let $n = 0$. Then $f(0) = a_0 \in A$ by 5.34. Next, assume $k \in \mathbb{N}$ and $\forall k \in \mathbb{N}, f(k) \in A$. If $f(k) \in A$, then $g(k) \in A$ for some good function g by the definition of f. We must show that $f(k+1) \in A$. By definition of f, $f(k+1)$ means that there is some good function g such that $g(k+1) = h(k, g(k))$. Then $h(k, g(k)) = h(k, f(k)) \in A$ since $f(k) \in A$. So $h(k, f(k)) = f(k+1) \in A$.

(c) Assume $k \in \mathbb{N}$. Then $f(k) = g(k)$ for some good g. So $f(k+1) = g(k+1)$. Since g is good, $g(k+1) = h(k, g(k)) = h(k, f(k)) = f(k+1)$.

B.6 Chapter 6

6.1. *Proof.* Part 2 of Theorem 6.2 states that "if $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$." Assume $|A| = |B|$ and $|B| = |C|$. That is, there exists some one to one function $f : A \to B$ onto B and some one to one function $g : B \to C$ onto C. By Theorem 4.13 part 1, since f and g are one to one, then $g \circ f$ is one to also. by Theorem 4.13 part 2, since f is onto B and g is onto C, then $g \circ f$ is onto C. Hence, there exists a one to one function $g \circ f : A \to C$ from A onto C. So $|A| = |C|$. □

6.2. *Proof.* Part 3 of Theorem 6.2 states that "if $|A| = |B|$ then $|B| = |A|$." Assume $|A| = |B|$. That is, there exists a one to one function $f : A \to B$ from A onto B. So $\text{Dom}(f) = A$ and $\text{Range}(f) = B$. Then by Theorem 4.11, f^{-1} is a function, $\text{Dom}(f^{-1}) = \text{Range}(f) = B$, $\text{Range}(f^{-1}) = \text{Dom}(f) = A$, and f^{-1} is one to one. Hence, there exists a one to one function $f^{-1} : B \to A$ from B onto A. So $|B| = |A|$. □

6.3. *Proof.* Part 4 of Theorem 6.2 states that "$|A| = |A|$." Define a function $f : A \to A$ by $f(x) = x$. Assume $a_1, a_2 \in \text{Dom}(f)$ and $f(a_1) = f(a_2)$. Then $a_1 = a_2$. Thus, f is one to one. Also, for each output $x \in A$, there exists an input $x \in A$ such that $f(x) = x$. Hence, f is onto A. Therefore, there exists a one to one funtion f from A onto A, so $|A| = |A|$. □

6.4. *Proof.* Part 5 of Theorem 6.2 states that "if $A \subseteq B$ then $|A| \leq |B|$." Assume $A \subseteq B$. Define a function $f : A \to B$ by $f(x) = x$. As proved in 6.3,

this is a one to one fuction from A onto A. Since $A \subseteq B$, f is function from A into B. Thus, $|A| \leq |B|$. □

6.5. *Proof.* In Example 6.3, we defined a function f from $[0,1]$ to $[0,1)$ by

$$f(x) = \begin{cases} \frac{1}{n+1} & \text{if } x = \frac{1}{n} \text{ where } n \text{ is a positive integer} \\ x & \text{otherwise.} \end{cases}$$

To show that $\text{Range}(f) \subseteq [0,1)$, we assume that $x \in \text{Dom}(f) = [0,1]$ and show that $f(x) \in [0,1)$. Then $0 \leq x \leq 1$. We consider two cases.

Case 1. $x = \frac{1}{n}$. Then $0 \leq \frac{1}{n} \leq 1$. Since n is a positive integer, $0 \leq \frac{1}{n+1} < \frac{1}{n} \leq 1$. Hence, $0 \leq f(x) < 1$, and $f(x) \in [0,1)$.

Case 2. $x \neq \frac{1}{n}$. Then $0 \leq f(x) le 1$, and $f(x) \in [0,1]$.

Thus, $f(x) \in [0,1] \cap [0,1) = [0,1)$.

For the proof that $[0,1) \subset \text{Range}(f)$, assume that $y \in [0,1)$. That is $0 \leq y < 1$. We consider two cases.

Case 1. $y = \frac{1}{n}$ where $n \in \mathbb{N}$. Then $n \neq 1$ since $y \neq 1$. So $n = k+1$ for some $k \in \mathbb{N}$. Then $f(\frac{1}{k}) = \frac{1}{k+1} = \frac{1}{n}$. So $y \in \text{Range}(f)$.

Case 2. $y \neq \frac{1}{n}$. Then $f(y) = y$ and $y \in \text{Range}(f)$.

Thus, $\text{Range}(f) = [0,1)$. □

6.6. *Proof.* We aim to prove that the following function from $[0,1]$ to $[0,1)$ is one to one:

$$f(x) = \begin{cases} \frac{1}{n+1} & \text{if } x = \frac{1}{n} \text{ where } n \text{ is a positive integer} \\ x & \text{otherwise.} \end{cases}$$

Assume $a_1, a_2 \in [0,1]$ and $f(a_1) = f(a_2)$. That is, $0 \leq a_1 \leq 1$ and $0 \leq a_2 \leq 1$. We consider four cases.

Case 1. $a_1 = \frac{1}{n_1}$ and $a_1 = \frac{1}{n_2}$ where $n_1, n_2 \in \mathbb{N}$. Then $f(a_1) = \frac{1}{n_1+1}$ and $f(a_2) = \frac{1}{n_2+1}$. Then by hypothesis, $\frac{1}{n_1+1} = \frac{1}{n_2+1}$. Cross-multiplying and subtracting 1 from each side, we find that $n_1 = n_2$. Thus, $a_1 = \frac{1}{n_1} = \frac{1}{n_2} = a_2$.

Case 2. $a_1 = \frac{1}{n_1}$ and $a_2 \neq \frac{1}{n_2}$ where $n_1, n_2 \in \mathbb{N}$. Since $f(a_1) = f(a_2)$, $\frac{1}{n_1+1} = a_2$. It follows that $n_1 = \frac{1}{a_2} - 1$, which contradicts the fact that $n_1 \in \mathbb{N}$.

Case 3. $a_1 \neq \frac{1}{n_1}$ and $a_2 = \frac{1}{n_2}$ where $n_1, n_2 \in \mathbb{N}$. This argument is almost identical to Case 2.

Case 4. $a_1 \neq \frac{1}{n_1}$ and $a_2 neq \frac{1}{n_2}$ where $n_1, n_2 \in \mathbb{N}$. Since $f(a_1) = f(a_2)$, $a_1 = a_2$. □

6.7. *Proof.* Assume $0 < x_1 < 1$ and $0 < x_2 < 1$. Using the right hand side of each inequality subtracting x_1 and x_2 respectively, we find that $0 < 1 - x_1$ and $0 < 1 - x_2$. Multiplying, we see that $0 < (1-x_1)(1-x_2) = 1 - x_1 - x_2 + x_1 x_2$, and this completes our proof. □

6.8. *Proof.* Assume $0 < x_1 < 1$ and $0 < x_2 < 1$. By 6.7, we know that

$0 < 1 - x_1 - x_2 + x_1x_2$. Since both x_1 and x_2 are positive, $x_1x_2 > 0$. Therefore, $0 < 1 - x_1 - x_2 + x1x_2 < 1 - x_1 - x_2 + x1x_2 + x_1x_2 = 1 - x_1 - x_2 + 2x1x_2$. □

6.9. *Proof.* Assume that $0 < x_1 < 1$, $0 < x_2 < 1$, and $f(x_1) = f(x_2)$. We must prove that $x_1 = x_2$. By the defintion of f, $f(x_1) = \frac{-1}{x_1} + \frac{1}{1-x_1}$ and $f(x_2) = \frac{-1}{x_2} + \frac{1}{1-x_2}$. Hence, $\frac{-1}{x_1} + \frac{1}{1-x_1} = \frac{-1}{x_2} + \frac{1}{1-x_2}$. Adding, we find that $\frac{2x_1-1}{x_1(1-x_1)} = \frac{2x_2-1}{x_2(1-x_2)}$. So $x_2(1-x_2)(2_1-1) = x_1(1-x_1)(2x_2-1)$. Expanding and combining, we see that $0 = 2x_1^2x_2 - 2x_1x_2^2 - x_1^2 + x_2^2 + x_1 - x_2 = (x_1 - x_2)(1 - x_1 - x_2 + 2x_1x_2)$. By Exercise 6.8, we know that $1 - x_1 - x_2 + 2x_1x_2 > 0$, therefore $x_1 - x_2$ must equal 0. Hence, $x_1 = x_2$, and f is one to one. □

6.10. *Proof.* First, assume that $f(x) \in f^*(X \setminus Y)$. This means that $f(x) \in f^*(X)$ and $f(x) \notin f^*(Y)$. Therefore, $f(x) \in f^*(X) \setminus f^*(Y)$ and $f^*(X \setminus Y) \subseteq f^*(X) \setminus f^*(Y)$.

Next, assume that $f(x) \in f^*(X) \setminus f^*(Y)$. This means that $f(x) \in f^*(X)$ and $f(x) \notin f^*(Y)$. Since f is one to one, we know that $x \in X$ and $x \notin Y \forall x \in \text{Dom}(f)$. Hence, $x \in X \setminus Y \forall x \in \text{Dom}(f)$. Thus, $f(x) \in f^*(X \setminus Y)$. So $f^*(X) \setminus f^*(Y) \subseteq f^*(X \setminus Y)$. Therefore, $f^*(X \setminus Y) = f^*(X) \setminus f^*(Y)$. □

6.11. *Proof.* Define $f : [2, 7] \to [0, 3]$ by $f(x) = \frac{3x-6}{5}$. We must show that f is one to one and onto $[0, 3]$. First, assume $a_1, a_2 \in \text{Dom}(f)$ and $f(a_1) = f(a_2)$. That is, $\frac{3a_1-6}{5} = \frac{3a_2-6}{5}$. Multiplying by 5 on each side, adding 6, then dividing by 3, we find that $a_1 = a_2$. Therefore, f is one to one.

We must now show that $\text{Range}(f) = [0, 3]$. Assume $x \in \text{Dom}(f) = [2, 7]$. Since $2 \leq x \leq 7, 0 \leq x - 2 \leq 5$. Then, multiplying by $\frac{3}{5}, 0 \leq \frac{3x-6}{5} \leq 3$. So $0 \leq f(x) \leq 3$, and $f(x) \in [0, 3]$. Thus, $\text{Range}(f) \subseteq [0, 3]$. To prove that $[0, 3] \subset \text{Range}(f)$, assume $y \in [0, 3]$. Let $x = \frac{5y+6}{3}$. Then since $0 \leq y \leq 3, 0 \leq 5y \leq 15$. Adding 6, we find that $6 \leq 5y+6 \leq 21$, and dividing by 3, we get $2 \leq \frac{5y+6}{3} \leq 7$. Hence, $2 \leq x \leq 7$. Further, $f(x) = \frac{3x-6}{5} = \frac{3(\frac{5y+6}{3})-6}{5} = \frac{(5y+6)-6}{5} = \frac{5y}{5} = y$. So $y \in \text{Range}(f)$, and $[0, 3] \subset \text{Range}(f)$. Therefore, f is onto $[0, 3]$. Since f is one to one and onto $[0, 3], |[2, 7]| = |[0, 3]|$. □

6.12. *Proof.* By the Cantor-Bernstein Theorem, since $|[2, 7]| = |[0, 3]|$ by Exercise 6.11, we know that $|[2, 7]| \leq |[0, 3]|$ and $|[0, 3]| \leq |[2, 7]|$. □

6.13. *Proof.* Assume $a, b \in \mathbb{R}$ and $a < b$. Define $f : (0, 1) \to (a, b)$ by $f(x) = a + (b - a)x$. We must show that f is one to one and onto (a, b). First, assume $a_1, a_2 \in \text{Dom}(f)$ and $f(a_1) = f(a_2)$. That is, $a + (b - a)a_1 = a + (b - a)a_2$. Subtracting a on each side and then dividing by $b - a$, we find that $a_1 = a_2$. Therefore, f is one to one.

We must now show that $\text{Range}(f) = (a, b)$. Assume $x \in \text{Dom}(f) = (0, 1)$. Since $0 < x < 1, 0 < (b - a)x < b - a$. Then, adding $a, a < a + (b - a)x < b$. So $a < f(x) < b$, and $f(x) \in (a, b)$. Thus, $\text{Range}(f) \subseteq (a, b)$. To prove that $(a, b) \subset \text{Range}(f)$, assume $y \in (a, b)$. Let $x = \frac{y-a}{b-a}$. Then since $a < y < b, 0 <$

$y - a < b - a$. Dividing by $b - a$, we find that $0 < \frac{y-a}{b-a} < 1$. Hence, $0 < x < 1$. Further, $f(x) = a + (b - a)x = a + (b - a)(\frac{y-a}{b-a}) = a + (y - a) = y$. So $y \in$ Range(f), and $(a, b) \subset$ Range(f). Therefore, f is onto (a, b). Since f is one to one and onto (a, b), $|(0, 1)| = |(a, b)|$. □

6.14. *Proof.* By Example 6.6 part 1, $|\mathbb{R}| = |(0, 1)|$, and by Example 6.6 part 2, $|(0, 1)| = |(a, b)|$ if $a, b \in \mathbb{R}$ and $a < b$. Thus, by Theorem 6.2 part 2, if $a, b \in \mathbb{R}$ and $a < b$, then $|\mathbb{R}| = |(0, 1)|$ by transitivity. □

6.15. *Proof.* By Exercise 6.14, we know that $|\mathbb{R}| = |(a, b)|$, so by the Cantor-Bernstein theorem, $|\mathbb{R}| \leq |(a, b)| \leq |\mathbb{R}|$. By Theorem 6.2 part 5, since $(a, b) \subset [a, b]$, $|(a, b)| \leq |[a, b]|$. So $|\mathbb{R}| \leq |(a, b)| \leq |[a, b]|$. Also, since the identity function $f : [a, b] \to \mathbb{R}$ defined by $f(x) = x$ is one to one and into $\mathbb{R}$, $|[a, b]|le|\mathbb{R}|$. Therefore, $|\mathbb{R}| \leq |[a, b]| \leq |\mathbb{R}|$, and $|\mathbb{R}| = |[a, b]|$ by the Cantor-Bernstein theorem. □

6.16. *Proof.* Assume $|A_1| = |A_2|$ and $|B_1| = |B_2|$. Then there exist one to one functions $f_A : A_1 \to A_2$ and $f_B : B_1 \to B_2$ such that f_A is onto A_2 and f_B is onto B_2. Define $F : A_1 \times B_1 \to A_2 \times B_2$ by $F(a, b) = (f_A(a), f_B(b))$ for all $(a, b) \in A_1 \times B_1$.

To prove that F is one to one, assume $a, a' \in A_1, b, b' \in B_1$, and $F(a, b) = F(a', b')$. Then $(f_A(a), f_B(b)) = (f_A(a'), f_B(b'))$. So $f_A(a) = f_A(a')$ and $f_B(b) = f_B(b')$. Since f_A and f_B are one to one functions, $a = a'$ and $b = b'$.

To prove that F is onto $A_2 \times B_2$, assume $(a', b') \in A_2 \times B_2$ Then $a' \in A_2$ and $b' \in B_2$. Since f_A and f_B are onto, $\exists a \in A_1$ such that $f_A(a) = a'$ and $\exists b \in B_1$ such that $f_B(b) = b'$. So $\exists (a, b) \in A_1 \times B_1$ such that $(f_A(a), f_B(b)) = (a', b')$. So F is onto $A_2 \times B_2$, and $|A_1 \times B_1| = |A_2 \times B_2|$. □

6.17. *Proof.* Define a function $f : \mathbb{Z} \to \{0, 1\} \times \mathbb{N}$ by

$$f(x) = \begin{cases} (0, x) & \text{if } x \geq 0 \\ (1, -1 - x) & \text{if } x < 0. \end{cases}$$

We must show that f is one to one and onto $\{0, 1\} \times \mathbb{N}$. First, assume $a_1, a_2 \in$ Dom(f) and $f(a_1) = f(a_2)$. We consider four cases.

Case 1. $a_1, a_2 \geq 0$. Then $f(a_1) = (0, a_1) = (0, a_2) = f(a_2)$. By the definition of a function, there must be only one output for each input, so a_1 must equal a_2.

Case 2. $a_1, a_2 < 0$. Then $f(a_1) = (1, -1 - a_1) = (1, -1 - a_2) = f(a_2)$. By the definition of a function, there must be only one output for each input, so a_1 must equal a_2.

Case 3. $a_1 \geq 0, a_2 < 0$. Then $f(a_1) = (0, a_1)$ and $f(a_2) = (1, -1 - a_2)$. By hypothesis, $(0, a_1) = (1, -1 - a_2)$, but this is a contradiction since the first components aren't equal.

Case 4. $a_1 < 0, a_2 \geq 0$. This argument is similar to the one in Case 3.

Therefore, f is one to one.
To show that f is onto $\{0,1\}\times\mathbb{N}$, we will first show that Range$(f) \subseteq \{0,1\}\times\mathbb{N}$. Assume that $x \in \text{Dom}(f)$. We must show that $f(x) \in \{0,1\} \times \mathbb{N}$. We consider two cases.

Case 1. $x \geq 0$. Then $f(x) = (0, x)$ where $0 \in \{0,1\}$ and $x \in \mathbb{N}$. Therefore, $f(x) \in \{0,1\} \times \mathbb{N}$.

Case 2. $x < 0$. Then $f(x) = (1, -1 - x)$ where $1 \in \{0,1\}$ and since $x < 0$ and $x \in \mathbb{Z}$, $x \leq -1 \to 0 \leq -1 - x$, so $-1 - x \in \mathbb{N}$.

In either case, Range$(f) \subseteq \{0,1\} \times \mathbb{N}$.
Next, we must show that $\{0,1\}\times\mathbb{N} \subset$ Range(f). Assume that $(a, b) \in \{0,1\}\times\mathbb{N}$. That is, $a \in \{0,1\}$ and $b \in \mathbb{N}$. We consider two cases.

Case 1. $a = 0$. Let $x = b$. Then $f(x) = (0, x) = (0, b) = (a, b)$.

Case 2. $a = 1$. Let $x = -1-b$. Then $f(x) = (1, -1-x) = (1, -1-(-1-b)) = (1, b) = (a, b)$.
In either case, $\exists x \in \mathbb{Z}$ such that $f(x) = (a, b)$, and f is onto $\{0,1\} \times \mathbb{N}$. □

6.18. *Proof.* By Example 6.3 part 2, we know that $|\mathbb{N}| = |\mathbb{Z}|$, and $|\{0,1\}| = |\{0,1\}|$. Therefore, by Exercise 6.16, $|\{0,1\}\times\mathbb{Z}| = |\{0,1\}\times\mathbb{N}| = |\mathbb{Z}|$ by Exercise 6.17. Therefore, $|\{0,1\} \times \mathbb{Z}| = |\mathbb{Z}|$. □

6.19. *Proof.* Define $f : A \to \mathcal{P}(A)$ by $f(x) = \{x\}$ for all $x \in A$. Since for all $x \in A$, $\{x\} \subseteq A$, so $\{x\} \in \mathcal{P}(A)$ and f is into $\mathcal{P}(A)$. We must show that f is one to one. Assume $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$. That is, $\{a_1\} = \{a_2\}$. Therefore, $a_1 = a_2$ and f is one to one. □

6.20. *Proof.* Assume $|A| \leq |B|$. That is, there exists a function $f : A \to B$ that is one to one and into B. We must show that there exists a one to one function from $\mathcal{P}(A)$ into $\mathcal{P}(B)$. Define $F : \mathcal{P}(A) \to \mathcal{P}(B)$ by $F(X) = \{f(x)|x \in X\}$.

To show that F is one to one, assume $A_1, A_2 \in \mathcal{P}(A)$ and $F(A_1) = F(A_2)$. We must show that $A_1 \subseteq A_2$ and $A_2 \subseteq A_1$. Assume $a \in A_1$. Then $f(a) \in F(A_1) = F(A_2)$. So $f(a) = f(a')$ for some $a' \in A_2$ Since f is one to one, $a = a'$. So $a \in A_2$ and $A_1 \subseteq A_2$. A similar proof shows that $\forall a \in A_2, a \in A_1$, so $A_2 \subseteq A_1$. Hence, $A_1 = A_2$ and F is one to one.

To show that F is into $\mathcal{P}(B)$, we must show that $\forall A_1 \in \mathcal{P}(A), F(A_1) \in \mathcal{P}(B)$. Assume $A_1 \in \mathcal{P}(A)$. So $A_1 \subseteq A$. Assume $y \in F(A_1) = \{f(a)|a \in A_1\}$. Then $y = f(a)$ for some $a \in A_1$. Since f is onto, $f(a) \in B$. So $y \in B$. So $F(A_1) \subseteq B$. Hence, $F(A_1) \in \mathcal{P}(B)$, and F is into $\mathcal{P}(B)$. □

6.21. *Proof.* By Exercise 6.20, we know that if $|A| \leq |B|$ then $|\mathcal{P}(A)| \leq |\mathcal{P}(B)|$ and, similarly, if $|B| = |A|$ then $|\mathcal{P}(B)| \leq |\mathcal{P}(A)|$. Assume $|A| = |B|$. That is, $|A| \leq |B|$ and $|B| \leq |A|$. Thus, $|\mathcal{P}(A)| \leq |\mathcal{P}(B)|$ and $|\mathcal{P}(B)| \leq |\mathcal{P}(A)|$. Hence, by the Cantor-Bernstein theorem, $|\mathcal{P}(A)| = |\mathcal{P}(B)|$. □

6.22. *Proof.* Assume there is a set A for which $|\mathbb{N}| < |A| < |\mathbb{R}|$. That is, there exist one to one functions $f_1 : \mathbb{N} \to A$ and $f_2 : A \to \mathbb{R}$ such that f_1 is onto A

and f_2 is onto $\mathbb{R}$. Let $A' = \{f_2(a)|a \in A\}$. Then $A' \subseteq \mathbb{R}$ and $|A'| = |A|$. So $|\mathbb{N}| < |A'| < |\mathbb{R}|$. □

B.7 Chapter 7

7.1. $\text{Dom}(R) = \{2, 3\}$ and $\text{Range}(R) = \{3, 7, 9\}$

7.2. $\text{Dom}(R) = \text{Range}(R) = \mathbb{R}$.

7.3. $\exists x, \exists y$ such that $x \; R \; y$ and $y \not R \; x$.

7.4. $\exists x, y$, and z such that $x \; R \; y, y \; R \; z$, and $x \not R \; z$.

7.5. $\exists x \in A$ such that $x \not R \; x$.

7.6. The relation is anti-symmetric (but not symmetric since $(2, 3) \in R$ but $(3, 2) \notin R$ and not transitive since $(2, 3)$ and $(3, 9)$ are in R but $(2, 9)$ is not in R).

7.7. The largest set on which the relation is reflexive is the set $\{3\}$.

7.8. The relation R is not symmetric since $1 \; R \; 17$ but $17 \not R \; 1$. R is not anti-symmetric since $1 \; R \; 2$ and $2 \; R \; 1$ but $2 \neq 1$. R is not transitive since $3 \; R \; 1$ and $1 \; R \; \frac{1}{2}$ but $3 \not R \; \frac{1}{2}$.

7.9. Applying the definition (of "R is reflexive on A") directly, the largest set on which R is reflexive is $\{x \in \mathbb{R} : x \leq 2x + 1\}$ but solving the inequality $x \leq 2x + 1$ for x gives a better answer: The largest set on which R is reflexive is $\{x \in \mathbb{R} : -1 \leq x\}$, that is, the interval $[-1, \infty)$.

7.10. *Proof.* Assume that R is a relation which is both symmetric and anti-symmetric and assume that x and y are objects for which $x \; R \; y$. By the symmetry of R, $y \; R \; x$. Therefore, since R is anti-symmetric $x = y$. □

7.11. Let R be a relation on the set $A = \{1, 2, 3\}$. Then $R = \{(1, 2), (2, 1)(1, 3)\}$ is neither symmetric nor anti-symmetric.

7.12. The relation R_4 is anti-symmetric and transitive. The largest set on which R_4 is reflexive is $\emptyset$.

7.13. The relation R_6 is symmetric. The largest set on which R_6 is reflexive is $\mathbb{R}$.

7.14. The equality relation on a set is symmetric, anti-symmetric, and transitive.

7.15. The empty relation is symmetric, anti-symmetric, and transitive, each because they are vaccuously true.

7.16. The universal relation is symmetric and transitive but not anti-symmetric. The largest set for which U is reflexive is A.

7.17.

(a) Symmetry: The relation $\geq$ is not symmetric on $\mathbb{R}$. For example, $3 \geq 2$ but $2 \not\geq 3$.

(b) Anti-symmetry: The relation $\geq$ is anti-symmetric on $\mathbb{R}$. Assume $x, y \in \mathbb{R}$ and $x \geq y$ and $y \geq x$. Stringing these inequalities together, we see that $y \geq x \geq y$. Since $y = y$, $y = x = y$, so $x = y$.

(c) Transitive: The relation $\geq$ is transitive on $\mathbb{R}$. Assume $x, y, z \in \mathbb{R}$ and $x \geq y$ and $y \geq z$. We can string these inequalities so that $x \geq y \geq q$. Thus, $x \geq z$.

(d) The largest set on which this relation is reflexive is $\mathbb{R}$ since each real number is equal to (and thus greater than or equal to) itself.

7.18.

(a) Symmetry: The relation $>$ is not symmetric. For example, $3 > 2$ but $2 \not> 3$.

(b) Anti-symmetry: For this relation, the statement of anti-symmetry is vacuously true since there is no case in $\mathbb{R}$ for which $x > y$ and $y > x$ for $x, y \in \mathbb{R}$.

(c) Transitive: The relation is transitive. Let $x, y, z \in \mathbb{R}$ and $x > y$ and $y > z$. We can string these inequalities to find that $x > y > z$ and thus $x > z$.

(d) The largest set for which the relation $>$ is reflexive is the empty set since no real number can be greater than intself.

7.19.

(a) Symmetry: The relation $|$ is not symmetric. For example $3 \mid 12$ but $12 \nmid 3$.

(b) Anti-symmetry: It is not anti-symmetric, for example $-6 \mid 6$ and $6 \mid -6$ but $-6 \neq 6$.

(c) : Transitive: It is transitive. Assume a, b and c are integers and that $a \mid b$ and $b \mid c$ then $b = ta$ and $c = sb$ where t and s are integers. substituting the first equation into the second gives $c = s(ta) = (st)a = ka$ where $k = st$ is an integer. Therefore $a \mid c$.

(d) The relation $|$ is reflexive on $\mathbb{Z}$ since $a \mid a$ for every integer a.

7.20.

(a) Symmetry: This relation is not symmetric. Let $A = \{0, 1, 2\}$. Then $\{0, 2\}, \{0, 1, 2\} \in \mathcal{P}(A)$ and $\{0, 2\} \subseteq \{0, 1, 2\}$ but $\{0, 1, 2\} \nsubseteq \{0, 2\}$.

(b) Anti-symmetry: This relation is anti-symmetric. Let $X, Y \in \mathcal{P}(A)$ and $X \subseteq Y$ and $Y \subseteq X$. By defintion of subsets, this means that $X = Y$.

(c) Transitive: This relation is transitive. Let $X, Y, Z \in \mathcal{P}(A)$ and $X \subseteq Y$ and $Y \subseteq Z$. Then $X \subseteq Y \subseteq Z$ and hence $X \subseteq Z$.

(d) The largest set for which this relation is reflexive is $\mathcal{P}(A)$ because each element of $\mathcal{P}(A)$ is a subset of itself.

7.21.

(a) Symmetry: This relation is symmetric. Let $x, y \in \mathbb{R}$ and let $x \; R \; y$. Then $|y - x| \geq 4$. That is, $y - x \geq 4$ or $y - x \leq -4$. From these inequalities we can deduce that $-4 \geq x - y$ or $4 \leq x - y$. That is, $|x - y| \geq 4$. So $y \; R \; x$.

(b) Anti-symmetry: This relation is not anti-symmetric. For example, $6 \; R \; 1$ since $|1 - 6| = 5 \geq 4$ and $1 \; R \; 6$ since $|6 - 1| = 5 \geq 4$ but $1 \neq 6$.

(c) Transitive: This relation is not transitive. For example, $6 \; R \; 1$ since $|1 - 6| = 5 \geq 4$ and $1 \; R \; 5$ since $|5 - 1| = 4 \geq 4$, but $6 \not R \; 5$ since $|5 - 6| = 1 \ngeq 4$.

(d) The largest set for which this relation is reflexive is the empty set. For each real number x, $|x - x| = 0 \ngeq 4$.

7.22.

(a) Symmetry: This relation is symmetric. Let $x, y \in \mathbb{R}$ and let $x \; R \; y$. That is, $xy > 0$. Since multiplication of the reals is commutative, $xy = yx$. Thus, $yx > 0$ and $y \; R \; x$.

(b) Anti-symmetry: This relation is not anti-symmetric. For example, $2 \; R \; 4$ since $2 \cdot 4 = 8 > 0$ and $4 \; R \; 2$ since $4 \cdot 2 = 8 > 0$ but $2 \neq 4$.

(c) Transitive: This relation is transitive. Let $x, y, z \in \mathbb{R}$ and let $x \; R \; y$ and $y \; R \; z$. That is, $xy > 0$ and $yz > 0$. Each x, y, and z is either positive or negative. We consider two cases.

Case 1. x is positive. Then y must also be positive so that $xy > 0$. If y is positive, then z must be positive so that $yz > 0$. Thus, $xz > 0$ and $x \; R \; z$.

Case 2. x is negative. Then y must also be negative so that $xy > 0$. If y is negative, then z must be negative so that $yz > 0$. Thus, $xz > 0$ and $x \; R \; z$.
In either case, $x \; R \; z$ and this relation is transitive.

(d) The largest set for which this relation is reflexive is $\mathbb{R} \setminus \{0\}$ since for all real numbers other than $0, x \cdot x = x^2 > 0$.

7.23.

(a) Symmetry: This relation is not symmetric. For example, $1\ R\ 4$ but $4 \not R\ 1$.

(b) Anti-symmetry: For this relation, the statement of anti-symmetry is vacuously true since there are no $(x, y) \in R$ for which $x\ R\ y$ and $y\ R\ x$.

(c) Transitive: This relation is transitive. Since this is a relatively small, finite set, we can list all transitivities:

$1\ R\ 2$, $2\ R\ 3$, and $1\ R\ 3$

$1\ R\ 2$, $2\ R\ 4$, and $1\ R\ 4$

$1\ R\ 3$, $3\ R\ 4$, and $1\ R\ 4$

$2\ R\ 3$, $3\ R\ 4$, and $2\ R\ 4$

(d) The largest set for which this relation is reflexive is the empty set since no element is related to itself, i.e. there are no ordered pairs of (x, x).

7.24.

(a) Symmetry: This relation is symmetric since $1\ R\ 2$ and $2\ R\ 1$ and $1\ R\ 1$.

(b) Anti-symmetry: This relation is not anti-symmetric. For example, $1\ R\ 2$ and $2\ R\ 1$ but $1 \neq 2$.

(c) Transitive: This relation is not transitive. For example, $2\ R\ 1$ and $1\ R\ 2$ but $2 \not R\ 2$.

(d) The largest set for which this relation is reflexive is $\{1\}$.

7.25. $A = \mathbb{R}, R$ is the "less than" function $<$

7.26. $A = \{1, 2, 3\}, R = \{(1, 1), (1, 3), (2, 2), (3, 2), (3, 3)\}$

7.27. $A = \{1, 2, 3\}, R = \{(1, 1), (2, 2), (3, 3), (1, 2)\}$

7.28. $A = \{1, 2, 3\}, R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3), (2, 1), (3, 2)\}$

7.29. $A = \{1, 2, 3\}, R = \{(1, 2), (2, 1), (1, 1), (2, 2)\}$

Index