Foundations of Mathematics

Dr. Richard A. Mitchell, Dr. Deborah Pace, Casey Mann, Jennifer McLoud-Mann*

October 27, 2017

Preface

Contrary to many students' beliefs, mathematics was not brought down from the mountain written on stone tablets; rather, it is the creation of man as he interacts with his environment. We do not intend in this text to present a historical evolution of mathematics, but the student should realize that any subject to be communicated will have a basic vocabulary of words. In that regard mathematics is no exception. Simplistically speaking, mathematics can be viewed as the application of logic to a system of axioms and definitions. Here, the word axioms (or postulates) refers to those statements which, from experience and observation, appear to be true but cannot be proven from more elementary statements. That is, axioms are those statements which we assume to be true and from which we will evolve the rest of mathematics. Those students who have studied plane geometry may have been exposed to a somewhat careful presentation of an axiomatic system. But few who are taking a course such as this will have seen a careful formulation of all axioms nor will we in this text attempt to structure such a meticulous and complete mathematical system.

The student who is moderately confused at this point should ask his teacher some questions! This issue of asking questions brings us to a very important first step in any intellectual endeavor. First, you must want to learn; that is, you quest for knowledge. The not so tacit implication of that statement is that you must learn to question – yourself, your fellow students, your teacher, and whatever other sources are available to you. Thus, you must make a decision to have the courage to overcome your fear of being wrong (a temporary state) because you recognize that questioning is the right path to knowledge.

The second crucial step in learning is the development of the vocabulary required to understand and do mathematics. Each new definition must be carefully examined and reinforced by examples, each subtlety explored until the thought intended by that definition is real and part of your thinking processes. At times some definitions are constructed by combining other more elementary thoughts, but sometimes we must consider some terms which are themselves definable only by attempting to communicate the thought behind them. Examples of both these types of definitions occur in early chapters. For many of you, this course in Foundations will be your first course in which the basic purpose is to

*C. Mann and J. McLoud-Mann received permission from the original authors of this text, R. Mitchell and D. Pace, to modify this book. The current version of this book is a substantially edited version of the original.

understand proofs and begin to develop the ability to prove things yourselves. Computers can add, subtract, multiply, divide, find derivatives, integrate, solve equations, etc., much more rapidly and accurately than we can. The factors which characterize us and make us superior to these computers is our ability to understand mathematics, to think, to create new mathematics and new approaches to problems.

0 Basic Concepts about Numbers

We will discuss the concept of sets in detail later in Chapter 2, but for now, it will suffice for you to know only that a *set* is collection of objects called *elements*. Certain sets occur so frequently in mathematics that we will give them permanent names and notations. A few such sets that we need right away are the following.

- The Natural Numbers: $\mathbb{N} = \{1, 2, 3, 4, 5, 6, \ldots\}$
- The Integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- The Rational Numbers: $\mathbb{Q} = \{x \,|\, x = m/n \text{ where } m, n \in \mathbb{Z} \text{ and } n \neq 0\}$

One of the primary objectives of this course is for students to learn how to make convincing arguments, or *proofs*, of the truth or falsity of mathematical statements. Mathematical statements having to do with integers and rational numbers are, due to students' familiarity with these kinds of numbers, an excellent place to start our journey in learning to write proofs. To that end, let's start thinking about what is involved in the process of writing proofs with a few examples.

Exercise 0.1

Based only on your current knowledge, prove that the following statements are true.

- For any even integer n, the square of n, n^2, is also even.
- Let n be an integer. Then $n^2 + n$ is even.
- For any integer n, if n^2 is even, then n is also even.
- For any positive integer n, the following equation is true.

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(n+2)}{6}$$

You may find it fun to save your argument so that later you may look back upon it through the lens of hindsight! Here are a few questions to consider as you attempt to make convincing arguments of the preceding statements.

- What does "prove" mean anyway? How might the meaning of proof vary for different people? How to lawyers define proof? How about chemists? Biologists? Psychologists?
- What exactly does it mean to say a number is even? Or that 4 divides a number evenly?

The purpose of Exercise 0.1 was to get you to start thinking about a few foundational things.

- One important thing to consider in mathematical proof are the ground rules; what things do you get to assume are true? These are the axioms referred to in the Preface. Somewhat surprisingly, not all mathematicians agree on all of the common axioms.
- Precise definitions of mathematical terms is also very important. For example, how do you prove something about even numbers if you do not have a precise definition of the term "even?"
- Finally, what are mathematical standards for proof? This last question cannot be answered in simple way; however, this course will introduce you to several proof techniques that are justified on the basis of formal logic (Chapter 1) and are familiar to any professional mathematician. What constitutes a "proof" is somewhat dependent on the audience who will be reading the proof and the subfield of mathematics relating to the statement to be proven. Like most fields of science, you must learn the conventions (spoken and unspoken!) through experience.

0.1 Integer Axioms

We will assume that you are familiar with basic arithmetic operations on integers and accept the truth of the following properties.

Axiom 0.2

For any integers a, b, and c, the following statements are assumed to be true.

1. $a + b$ is an integer.
2. $-a$ is an integer.
3. ab is an integer.
4. $a + b = b + a$.
5. $ab = ba$.
6. $(a + b) + c = a + (b + c)$
7. $0 + a = a + 0 = a$.
8. $a + (-a) = 0$.
9. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Generally speaking, mathematicians try to keep their list of axioms as small as possible. Anything that can be deduced from other axioms is generally not listed as a separate axiom. Indeed, statements that can be deduced from axioms are usually called "Propositions," "Facts," "Lemmas," "Theorems," and other similar terms. For example, one can deduce that $a - b$ is an integer on the basis of the axioms, so we will call that a fact. The operation of subtraction itself can be thought of as a kind of addition:

$$a - b := a + (-b).$$

Note: the notation ":=" is commonly used to indicate that the formula is defining the term on the left side.

Fact 0.3

For any integers a and b, $a - b$ is also an integer.

Proof. Let a and b be integers. By Axiom 0.2 Part 2, $-b$ is an integer, and consequently, by Axiom 0.2 Part 1, $a + (-b)$ is an integer. Therefore, $a - b$ is an integer. □

This is our first example of a proof. We will discuss proof techniques later, but for now, just observe that the proof begins by stating the assumptions being made (here, only that a and b are integers). Then, the proof makes use of assumed facts (axioms) to justify a certain conclusion.

0.2 Basic Number Theoretical Definitions

Definition 0.4

An integer n is ***even*** if there exists an integer r such that $n = 2r$. Similarly, an integer m is ***odd*** if there exists an integer s such that $m = 2s + 1$.

For example, 24 is even since there exists an integer, 12, such that $24 = 2(12)$. Similarly, 37 is odd since there exists an integer, 18, such that $37 = 2(18) + 1$.

Definition 0.5

Let a and b be integers such that $a \neq 0$. We say a ***divides*** b, and denote this relationship by $a|b$, if there exists an integer n such that $b = an$. If $a|b$, we also say that a is a ***factor*** of b or b is a ***multiple*** of a.

For example, $6|24$ since there exists an integer, 4, such that $24 = 6 \cdot 4$. We may also say that 6 is a factor of 24 (as is 4). On the other hand, 7 does not divide 24 (denoted $7 \nmid 24$) since there does not exist an integer n such that $24 = 7n$. Also, notice that the statement "a is even" is equivalent to the statement $2|a$.

Note: Do not confuse the notation $a|b$ (which is shorthand for the statement "a divides b") with the notation a/b, which is not a statement at all (it is a fraction). Indeed, if you write

$$6|24 = 4,$$

you are literally stating "6 divides 24 is equal to 4," which is nonsensical.

We now have enough definitions to prove one of the statements from Exercise 0.1.

Example 0.6

Prove that if n is an even integer, then n^2 is also even.

Proof. Assume that n is an even integer. By the definition of even, there exists an integer r such that $n = 2r$. Now we see (using arithmetic axioms in the usual way) that $n^2 = (2r)^2 = 4r^2 = 2(2r^2)$. Since r is an integer, then $2r^2$ is also an integer (by the axioms of the integers). Thus, we see that n^2 has been expressed as 2 times an integer, and so, by definition of even, n^2 is even. □

The proof exhibited here is an example of a *direct proof.* A direct proof is an argument that starts with the hypotheses of the statement to be proven and establishes a sequence of implications that are justified by accepted definitions, axioms, and previously proven facts. The idea is that each implication within the the proof is justifiable based on what is already known.

Exercise 0.7

Modify the proof above to prove the following: If n is an odd integer, then n^2 is an odd integer.

0.3 Modular Arithmetic

The *Division Algorithm* is a statement that essentially says that the process of long division with integers that you learned as a child is mathematically correct. While you may not be surprised that long division is mathematically correct, the proof of the Division Algorithm is sufficiently involved that we must postpone its proof until we have learned more about sets.

Theorem 0.8: Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < b.$$

The numbers q and r are called, respectively, the ***quotient*** and the ***remainder*** upon division of a by b.

Example 0.9

Let $a = 47$ and $b = 5$. Using long division of a by b

$$\begin{array}{r@{}r} & 9 \\ 5\,\big) & \overline{47} \\ & \underline{45} \\ & 2 \end{array}$$

you find a quotient of $q = 9$ with a remainder of $r = 2$. Notice that we have

$$47 = 5 \cdot 9 + 2 \qquad \text{and} \qquad 0 \leq 2 < 5$$

as specified by the Division Algorithm.

Example 0.10

Let $a = -47$ and $b = 5$. Here, upon division of a by b, bearing in mind that the remainder must be nonnegative, we get a quotient of $q = -10$ and a remainder of $r = 3$. We see that q and r satisfy the Division Algorithm:

$$-47 = 5(-10) + 3 \qquad \text{and} \qquad 0 \leq 3 < 5$$

Definition 0.11

For integers a, b, and $n \geq 2$, we say a is ***congruent*** to b ***modulo*** n, written $a \equiv b \pmod{n}$ or $a \equiv_n b$, if $n | (a - b)$.

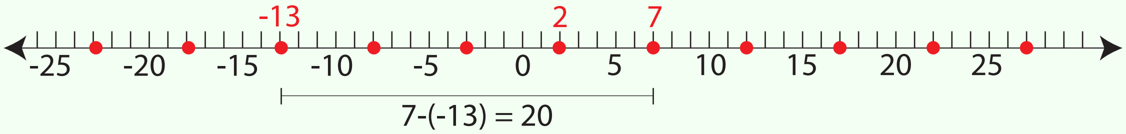
Example 0.12

Consider the following.

- $27 \equiv_7 6$ (since $7|(27-6)$)
- $157 \equiv 1 \pmod{2}$ (since $2|(157-1)$)
- $-2 \equiv_5 3$ (since $5|(-2-3)$)

Example 0.13

(Equlivalent integers modulo 5)



All of the red points on the number line above represent numbers that are congruent to each other modulo 5. This is visually apparent; since each dot is a distance of 2 from a multiple of 5, the difference between any two of the numbers represented by red dots (7 and -13, for example) will be a multiple of 5.

Given an integer n that you are "modding" by (we call n the *modulus*) and an integer a, you can use the Division Algorithm to find another integer r satisfying $0 \leq r < n$ such that $a \equiv_n r$. Specifically, r is the remainder upon division of a by n. By the Division Algorithm, there exist unique integers q and r with $0 \leq r < n$ such that $a = nq + r$. This implies that $a - r = nq$, which in turn means (by the definition of divides) that $n|(a - r)$. Thus, by the definition of congruence modulo n, $a \equiv_n r$.

Nice Fact: If r is the remainder upon division of a by $n \geq 2$, then $a \equiv_n r$.

Definition 0.14

Let $a, n \in \mathbb{Z}$ with $n \geq 2$ and let r be the remainder upon division of a by n. Then we call r the ***common residue*** of a modulo n, and write

$$r = a \bmod n \qquad \text{or} \qquad r = a \;\%\; n.$$

Example 0.15

We compute a mod n by finding a congruent integer r satisfying $0 \leq r < n$.

- 27 mod 5 = 2 (since 2 is the remainder upon division of 27 by 5)
- 156 mod 13 = 0 (since 0 is the remainder upon division of 156 by 13)
- -6 mod 18 = 12 (since 12 is the remainder upon division of -6 by 18)

Definition 0.16

(Addition and Multiplication Modulo n). Let a, b, and n be integers with $n \geq 2$.

- We define addition modulo n, denoted $+_n$, by
$$a +_n b = (a + b) \bmod n.$$
- We define multiplication modulo n, denoted $\cdot_n$, by
$$a \cdot_n b = (a \cdot b) \bmod n.$$

It will be proven later (Chapter 5) that these definitions are not nonsensical.

Example 0.17

(Calculating using modular operations)

- $12 +_7 19 = (12 + 19) \bmod 7 = 31 \bmod 7 = 3$.
- $12 \cdot_7 19 = (12 \cdot 19) \bmod 7 = 228 \bmod 7 = 4$.

So far, we have offered no motivation as to why someone might want to perform modular arithmetic calculations. It turns modular arithmetic is used extensively computer programming, cryptography, and many other areas of science. To give one motivational example, consider a list of length n whose entries are enumerated 0, 1, 2, ..., $n - 1$; perhaps this is an array in a computer program. Modular arithmetic gives you a way to jump from entry to entry of this list. For example, suppose the length of the list is $n = 100$. What position in the list is 75 positions in front of the 50th entry? Of course, you cannot move forward in the list 75 steps from the 50th position (that would be the 125th position, which doesn't exist!), but you can "wrap around" back to the beginning after you hit the end of the list. So, the position that is 75 steps ahead of the 50th position would be

$$50 +_{100} 75 = 25\text{th position.}$$

0.4 We need tools!

Let us consider another of the statements from 0.1 and how we might prove it.

Example 0.18

Prove that for any integer n, if n^2 is even, then n is even.

We will begin a direct proof and see where trouble arises.

Proof. Suppose that n is an integer and that n^2 is even. By the definition of even, there exists an integer k such that $n^2 = 2k$.

pause: How can we deduce anything about n from the fact that $n^2 = 2k$? The only thing I can think of is to solve that equation for n to get $n = \pm\sqrt{2k}$. But is that helpful? I find it impossible to deduce anything about whether n is even from the equation $n = \pm\sqrt{2k}$. What to do . . .?

It turns out that we will need to develop so-called indirect methods of proof to handle this sort of problem. Indirect proof methods are based on facts from logic. Thus, we will take a detour into the field of logic, then return to this problem later in Chapter 1.

Chapter 0 Exercises

1. (a) In terms of the definition of *even* integer (Definition 0.4), explain why 48 is an even integer.

   (b) In terms of the definition of *odd* integer (Definition 0.4), explain why 21 is an odd integer.

   (c) In terms of the definition of *divides* (Definition 0.5), explain why $12|60$.

   (d) In terms of the definition of *congruence modulo n* (Definition 0.11), explain why $17 \equiv_{12} 53$.

2. What is wrong with the following explaination that $3|7$?

   3 *divides* 7 *since* $7 = 3 \cdot \frac{7}{3}$.

3. For the following pairs of integers a and b with $b > 0$, find the quotient q and the remainder r with $0 \leq r < b$ as specified by the Division Algorithm.

   (a) $a = 142$, $b = 15$

   (b) $a = 20$, $b = 7$

   (c) $a = -212$, $b = 8$

4. In terms of the definition of congruence modulo n, explain why $17 \equiv_{12} 53$.

5. Compute the residue a mod n (see Definition 0.14 and Example 0.15).

   (a) 9 mod 10

   (b) 25 mod 2

   (c) 169 mod 13

   (d) -10 mod 3

   (e) 1,234,679,123,007,221 mod 2

6. Compute the following. See Definition 0.16 and 0.17.

   (a) $34 +_8 44$

   (b) $7 \cdot_6 17$

7. Prove that if m is an even integer and n is an odd integer, then $m+n$ is an odd integer.

1 Logic

1.1 Introduction

As noted in the preface, one useful definition of mathematics is the body of knowledge obtained by applying logic (deductive and inductive) to a system of axioms. Our first thought is to deal with things which conform to a bivalent system of logic; that is, things which are either true or false.

Definition 1.1

A ***statement*** (or ***proposition***) is a sentence which is either true or false. We will notationally speak of a statement p or a statement q.

Example 1.2

Each of the following are statements:

1. George Washington was the first President of the United States.
2. $2 + 3 = 5$.
3. There are 12 inches in a foot.
4. Harry S. Truman was the second President of the United States.
5. $4 \times 8 = 12$.
6. There are 30 inches in a yard.

Certainly we each recognize some underlying knowledge is required in interpreting the sentences in Example 1.2. For instance, in the sentence "$2 + 3 = 5$", we assume recognition of the concepts of 2, 3, 5, and addition base 10. Nevertheless, we must make some general knowledge assumptions, and certainly the six sentences of Example 1.2 are statements. (The first three sentences are true while the last three are false.)

Example 1.3

The following are not statements:

1. Three is a nice number.
2. It is going to rain today.
3. Paul Newman is a handsome man.

Clearly, the problem in each of these sentences is that their truth or falsity cannot be uniquely determined. You may dislike numbers and thus, in your mind, no number is nice, while someone else might think three is a very nice number. Depending on the date and location when it is read, the truth of sentence (2) could vary. Some foolish people might not agree that Paul Newman is handsome!

Example 1.4

Consider the following sentence. "This sentence is false." This is not a statement. Why? The sentence in question is an example of what is known in mathematics as a *paradox*. If it is true, then it is false, while on the other hand, if it is false, then it is true. Such paradoxes are not statements.

Now we return to the concept of axioms. What is an axiom? Surely it must be a statement, but also something more. As we study a body of mathematical knowledge, we encounter new statements, some of which can be proven from the existing system (These are called Lemmas, Theorems, Facts, etc.) while others, though statements, cannot be proven. If we can in fact prove that the truth value of the statement is independent of the existing system, we have a potential axiom. We can either assume the statement is true, adding it to our system as an axiom, or we could assume the statement is false, adding its negative (or some form of its negative) to our system as an axiom. Surely, quite different bodies of knowledge would evolve depending on what axiom we added. A excellent example of this idea can be seen in the difference between *Euclidean geometry* (which includes an axiom called the "parallel postulate") and *hyperbolic geometry* (which includes an a different kind of "parallel postulate"); the modification of a single axiom results in a completely different kind of geometry!

Logicians as well as some other mathematicians are deeply concerned with such questions of creating minimal systems of axioms and developing mathematics very systematically from them. Such important but esoteric questions are beyond the scope and intent of this course. However, the remainder of this chapter will attempt to create a firm, logical base which will be used throughout this text and many subsequent courses the student will encounter. For our purposes the student needs a basic feel for the flow of mathematics and a concrete understanding of the concept of bivalent logic (T or F) applied to statements.

1.1 Exercises

1. Determine whether or not the following sentences are statements. If yes, state the truth value of the statement.

   (a) $8 \equiv_4 99$.

   (b) My hair is brown.

   (c) There are more males than females registered in this class.

   (d) $64 \div 2 = 37$.

   (e) The metric system of measurement is difficult to learn.

   (f) The summer months are June, July, and August.

1.2 Compound Statements

In Section 1.1 we defined a statement to be a sentence which is either true or false. Many statements we are interested in studying are actually combinations of several simpler ones. Then the problem of determining the truth value (truth or falsity) of such statements becomes one of discovering the truth value of the statements being combined as well as understanding the methods of combination. We will at this time consider the *negation*, *conjunction*, and *disjunction* of statements.

Definition 1.5

Let p be a statement. The ***negation*** of p, denoted $\sim p$, is a statement forming the denial of p. The statement $\sim p$, read "not p," has the opposite truth value of p.

Example 1.6

Consider the statement: "Austin is the capital of Texas." The negation of that statement would be the statement: "Austin is not the capital of Texas." If the original statement had been "Austin is not the capital of Texas" then the negation would be obtained by deleting the negative to obtain the negation "Austin is the capital of Texas."

Example 1.7

The statement "$2 + 3 = 5$" has as its negation the statement "$2 + 3 \neq 5$."

Since one of our stated concerns in this section is the determination of the truth value of a given statement based upon the truth values of its component statements, we consider the concept of a truth table. Very simply, a ***truth table*** is exactly a table which indicates the relationships between the truth values of the statements forming the table. Table 1 indicates the relationship between the statements p and $\sim p$, giving us the basic table for a negation.

p	$\sim p$
T	F
F	T

Table 1: Truth table for negation

Notice that the table shows that if p is true, then $\sim p$ is false and if p is false, then $\sim p$ is true. Truth tables become very useful when we deal with more complicated statements.

The first type of compound statement we consider is the conjunction. When combining statements in logic, the most important aspect of the definition is the truth value of the resulting statement in terms of the component statements.

Definition 1.8

Let p and q be statements. The ***conjunction*** of p and q, denoted $p \wedge q$, is the compound statement obtained by connecting p and q with the English connective "and". The conjunction is true only when both p and q are true.

Example 1.9

The compound statement "Austin is the capital of Texas, and five is greater than two" is obtained by using "and" to connect the two statements "Austin is the capital of Texas" and "five is greater than two." Since both statements are true the conjunction is true.

The key to understanding the conjunction is the Table 2, which systematically exhibits the four possible combinations of the truth values for p and q.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 2: Truth table for conjunction

Thus, we see that the conjunction of two statements is true only in the case when both statements are true.

Definition 1.10

The ***disjunction*** of two statements p and q, denoted $p \vee q$, is the statement obtained by using the English connective "or". The disjunction is true when at least one of the statements being combined is true.

A brief comment about "or" must be noted. As used in a mathematical/logical sense, "or," is interpreted in the inclusive sense. That is, "or" is interpreted as and/or, meaning one and/or the other is true. Consider carefully Table 3.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 3: Truth table for disjunction

So we see the disjunction is false only when both p and q are false. The exclusive use of "or," referred to as "xor," would yield truth only if exactly one of the two statements were true. We will not make use of "xor" in this text, but its use is common in computer science.

Example 1.11

Consider the four disjunctions:

1. Austin is the capital of Texas or five is greater than two.
2. Austin is the capital of Texas or five is less than two.
3. Austin is not the capital of Texas or two is less than five.
4. Austin is not the capital of Texas or five is less than two.

Here we see the first three compound sentences are disjunctions which are true, while the disjunction in (4) is false.

Another way of logically combining statements is the *conditional statement*, which is the heart of mathematical logic.

Definition 1.12

Let p and q be statements. A ***conditional statement*** is a compound statement of the form "If p, then q" or "p implies q," and is denoted $p \to q$. The conditional is true unless p is true and q is false.

In mathematics/logic the truth table for a conditional statement is given below.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 4: Truth table for a conditional statement

In a conditional statement, "$p \to q$", p is called the ***antecedent*** or ***hypothesis*** and q is called the ***consequence*** or ***conclusion***.

Caution: Table 4 indicates (correctly) that the conditional statement $p \to q$ is true whenever p is false regardless of the truth value of q. A conditional statement $p \to q$ in which p is false is said to be ***vacuously true***. At first this may seem confusing, but with some thought it makes sense. It is helpful to think about whether or not a person stating a conditional statement "p implies q" is telling the truth or lying; a person making such a statement is only lying if the hypothesis is true but the conclusion is false. To this end, consider the following example (Example 1.13).

Example 1.13

In the sentence "If the moon is full on October 12, then I will turn into a werewolf." Under what conditititions would a person making this statement be lying? Only if it is true that the moon is full on October 12 but the person failed to turn into a werewolf! Indeed, the person has made no claims about his or her transmutation possibilities when the moon is not full or if it is not October 12.

In viewing conditional statements are purely logical contructs, there need not be any actual causal relationship between the hypothesis and conclusion. Consider the following example.

Example 1.14

Consider the following four conditional statements:

1. If Austin is the capital of Texas, then five is greater than two.
2. If Austin is the capital of Texas, then five is less than two.
3. If Austin is not the capital of Texas, then five is greater than two.
4. If Austin is not the capital of Texas, then two is greater than five.

In Example 1.14 we see by the truth table defining the truth value of a conditional statement that (1), (3), and (4) are true conditional statements while (2) is a false conditional statement. Even though the hypotheses and conclusions of these statements appear to be totally unrelated in terms of cause and effect, we can in a formal way state the truth or falsity of the conditionals. This is somewhat at odds with the use of conditionals in ordinary language, and as will be discussed a little later, we will reserve a different notation ($p \Rightarrow q$) to indicate causal implication.

We emphasize that the student must understand that conditional statements have truth values precisely as assigned by the definition. That is, to determine truth value, we do not need to be able to "prove" or "disprove" the consequence from the hypothesis. Certainly "proving" things will be the ultimate focus of this course, but at this time we are simply discovering the ways of combining statements logically and the resulting truth values of such combinations.

The last compound statement we will introduce is the *biconditional statement*.

Definition 1.15

Consider two statements p and q. A ***biconditional statement*** is a compound statement of the form "p if and only if q" or "p is equivalent to q," denoted "$p \leftrightarrow q$." Frequently we write "p iff q" as a shorthand notation for "p if and only if q".

The truth table which defines the biconditional is as follows.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Hence, we see that two statements, no matter how complicated, are equivalent when they have precisely the same truth value.

Example 1.16

Consider the four biconditional statements:

1. Austin is the capital of Texas iff two is less than five.
2. Austin is the capital of Texas iff two is greater than five.
3. Austin is not the capital of Texas iff two is less than five.
4. Austin is not the capital of Texas iff two is greater than five.

Here we see that (1) and (4) are true biconditional statements while (2) and (3) are false.

It is important to note that other expressions are often used by mathematicians to describe conditional and biconditional statements. A few of the most common such expressions are given below.

• "$p \rightarrow q$"	"If p, then q"
• "$p \rightarrow q$"	"p only if q"
• "$p \rightarrow q$"	"q if p"
• "$p \rightarrow q$"	"p is sufficient for q"
• "$p \rightarrow q$"	"q is necessary for p"
• "$p \leftrightarrow q$"	"p if and only if q" or "p iff q"
• "$p \leftrightarrow q$"	"p is a necessary and sufficient condition for q"
• "$p \leftrightarrow q$"	"p is equivalent to q"

Since it is easy to confuse these expressions, the student must always carefully identify the hypothesis and conclusion before working with any conditional type statement.

We stress that we are not attempting to "prove" anything yet, but rather only define a compound statement and its truth value in terms of the truth values of the statements used to obtain it. In order to determine the truth values of more complicated statements, it is critical that the student thoroughly understand and remember these five basic truth tables.

That is, sufficient time should be spent digesting these tables and examples in order that the student need not constantly refer back to the basic tables when working on more difficult ones.

Before going on to the last definition and fact of this section, we give an example of a more involved statement along with a step-by-step approach to constructing the associated table.

Example 1.17

Construct the truth table for the statement $(q \wedge p) \vee [q \wedge (\sim p)]$.

After listing the component statements and all possible combinations of truth values associated with them in the table, the remaining compound statements should be given in the order that they will be considered. (This is done much like ordering of operations in an arithmetic problem or an algebraic expression.) In this statement the order we have chosen is indicated below.

p	q	$q \wedge p$	$\sim p$	$q \wedge (\sim p)$	$(q \wedge p) \vee [q \wedge (\sim p)]$
T	T	T	F	F	T
T	F	F	F	F	F
F	T	F	T	T	T
F	F	F	T	F	F

There may be some variation here, but the major connective ("$\vee$" in this case) will be dealt with last. Once the ordering is determined, we proceed with each column until we have determined the truth value of every connective.

A final definition is given below which relates conditional statements and negation.

Definition 1.18

Let p and q be statements. The statement $q \to p$ is the ***converse*** of $p \to q$. The statement $(\sim q) \to (\sim p)$ is the ***contrapositive*** of $p \to q$. The statement $(\sim p) \to (\sim q)$ is the ***inverse*** of $p \to q$.

In ordinary parlance, the words "inverse" and "negation" are often used to mean "opposite." But, the student should also note that as mathematical terms, "inverse" and "negation" are not interchangeable. This problem rears its head often in mathematics; mathematicians give highly specific and context sensitive meanings ordinary English words (or words from other languages) which can cause confusion unless the reader is aware of the context.

The student should be aware that there are conventions governing the use or lack of use of parentheses in logical statements which are similar to those used to interpret algebraic expressions. Although we sometimes use grouping symbols for emphasis, such grouping symbols are often unnecessary for clarity of meaning. For example, in the expression

$$\sim p \wedge q \to \sim r \vee \sim s,$$

the meaning of the statement is unambiguous but could have been written

$$[(\sim p) \wedge q] \to [(\sim r) \vee (\sim s)].$$

It is especially important for the student to realize that the negation symbol preceding the statement p applies only to p unless indicated otherwise. The grouping symbols in the expressions $[(\sim p) \wedge q] \rightarrow [(\sim r) \vee (\sim s)]$ and $\sim \{(p \wedge q) \rightarrow [(\sim r) \rightarrow (\sim s)]\}$ produce statements with entirely different meanings.

1.2 Exercises

1. Consider the sentences

   p: "The Dow Jones industrial average drops below 10,000."

   q: "I will sell all of my stocks."

   Discuss the truth value of $p \to q$ for all four possible combinations of truth values of p and q by considering if a person making the statement $p \to q$ is telling the truth.

2. For each English sentence below, translate the sentence to propositional notation by identifying the parts the statement (labeling them as "p," "q," etc.) and giving the form of the proposition (e.g. $(p \vee q) \to r$)

   (a) An integer is odd if and only if its square is odd.

   (b) If I do not study, then I will fail this class.

   (c) Either I will go shopping or I will go to a movie.

   (d) I was well qualified, but I did not get the job.

   (e) If n is an integer, then n is even or n is odd.

   (f) The square of an even integer is an even integer.

3. Negate each of the following statements.

   (a) A positive number is larger than zero.

   (b) If today is Saturday, then I do not have to go to work.

   (c) Dogs can bark and cats can climb trees.

   (d) If $x^2 - 9 = 0$, then either $x = 3$ or $x = -3$.

   (Note: The difficulties of negating compound statements will be vastly simplified by the tautologies studied in the next section!)

4. For the conditional statements given below, give the converse, the inverse, and the contrapositive.

   (a) If I do not get to class on time, then I will not be allowed to take the exam.

   (b) I will return the calls and dictate the letter when I arrive at the office.

   (c) If $(x + 1)(x - 4) = 0$, then $x = -1$ or $x = 4$.

   (d) If my weight drops below 170 pounds, then I will eat 2 cheeseburgers and a chocolate cake.

5. In the following statements, remove those grouping symbols which are unnecessary for clarity of meaning.

(a) $p \vee [(\sim p) \wedge q]$

(b) $[\sim (p \rightarrow q)] \wedge q$

(c) $[p \wedge (\sim q)] \vee (p \wedge q)$

(d) $\{\sim [p \vee (\sim r)] \wedge (q \vee p)\} \rightarrow p$

6. Construct truth tables for the following compound statements.

   (a) $p \vee (\sim p \wedge q)$

   (b) $\sim (p \rightarrow q) \wedge q$

   (c) $(p \wedge \sim q) \vee (p \wedge q)$

   (d) $[\sim (p \vee \sim r) \wedge (q \vee p)] \rightarrow p$

7. For integers x and y, find the inverse, the converse, the contrapositive, and the negation of each of the following statements.

   (a) If $x = 3$, then $x^4 = 81$.

   (b) If $x < 0$, then $x \neq -4$.

   (c) If x is odd and y is even, then xy is even.

   (d) If $x^2 = x$, then either $x = 0$ or $x = 1$.

   (e) If $xy \neq 0$, then $x \neq 0$ and $y \neq 0$.

1.3 Tautologies and Contradictions

By definition, a simple statement is either true or false. In mathematics/logic, compound statements that are always true or always false, regardless of the truth values of their component statements, are of great value. We give the formal definitions below.

Definition 1.19

A compound statement which is always true, regardless of the truth values of its component statments, is called a ***tautology***, while a compound statement which is always false is called a ***contradiction***.

Example 1.20

The statement $p \wedge (\sim p)$ is a contradiction since the truth table below indicates this statement is always false.

p	$\sim p$	$p \wedge (\sim p)$
T	F	F
F	T	F

Table 5: $p \wedge (\sim p)$ is a contradiction

Example 1.21

The statement $[\sim(\sim p)] \leftrightarrow p$ is a tautology since the truth table below indicates that the statement is always true.

p	$\sim p$	$\sim(\sim p)$	$\sim(\sim p) \leftrightarrow p$
T	F	T	T
F	T	F	T

Table 6: $[\sim(\sim p)] \leftrightarrow p$ is a tautology

When $p \leftrightarrow q$ is a tautology, p and q are understood to be logically equivalent statements. So, $\sim(\sim p)$ logically means the same thing as p.

The following theorem enumerates a list of tautologies which will be useful to us. The tautologies are useful because they tell us how to express compound statements in logically equivalent forms. The proofs will be left as exercises.

Theorem 1.22

Let p, q, and r be statements. Then the following are tautologies.

1. Basic Properties

   (a) $p \leftrightarrow p$

   (b) $[\sim(\sim p)] \leftrightarrow p$

   (c) $[(p \to q) \wedge p] \to q$ Modus Ponens

   (d) $[(p \to q) \wedge (\sim q)] \to (\sim p)$ Modus Tollens

   (e) $\sim(p \vee q) \leftrightarrow [(\sim p) \wedge (\sim q)]$ DeMorgan's Law

   (f) $\sim(p \wedge q) \leftrightarrow [(\sim p) \vee (\sim q)]$ DeMorgan's Law

   (g) $\sim(p \to q) \leftrightarrow [p \wedge (\sim q)]$

   (h) $\sim(p \leftrightarrow q) \leftrightarrow \{[p \wedge (\sim q)] \vee [q \wedge (\sim p)]\}$

   (i) $(p \vee q) \leftrightarrow [(\sim p) \to q]$

   (j) $(p \to q) \leftrightarrow [(\sim q) \to (\sim p)]$ Contraposition

   (k) $[(\sim p) \to (\sim q)] \leftrightarrow (q \to p)$

   (l) $[(p \to q) \wedge (q \to p)] \leftrightarrow (p \leftrightarrow q)$

   (m) $\{(\sim p) \to [q \wedge (\sim q)]\} \to p$

   (n) $(p \leftrightarrow q) \to [(r \wedge p) \to (r \wedge q)]$

   (o) $(p \leftrightarrow q) \to [(r \vee p) \leftrightarrow (r \vee q)]$

2. Additional Laws

   (a) $(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$ Symmetric Property

   (b) $(p \wedge q) \leftrightarrow (q \wedge p)$ Commutative Property

   (c) $(p \vee q) \leftrightarrow (q \vee p)$ Commutative Property

   (d) $[(p \to q) \wedge (q \to r)] \to (p \to r)$ Transitive Property

   (e) $[(p \leftrightarrow q) \wedge (q \leftrightarrow r)] \to (p \leftrightarrow r)$ Transitive Property

   (f) $[p \vee (q \wedge r)] \leftrightarrow [(p \vee q) \wedge (p \vee r)]$ Distributive Property

   (g) $[p \wedge (q \vee r)] \leftrightarrow [(p \wedge q) \vee (p \wedge r)]$ Distributive Property

   (h) $[p \vee (q \vee r)] \leftrightarrow [(p \vee q) \vee r]$ Associative Property

   (i) $[p \wedge (q \wedge r)] \leftrightarrow [(p \wedge q) \wedge r]$ Associative Property

The following theorem lists some useful contradictions, and again, its verification requires construction of the appropriate truth tables and is left to the student.

Theorem 1.23

Let p and q be statements. The following statements are contradictions:

1. $(p \to q) \wedge [p \wedge (\sim q)]$
2. $[(p \vee q) \wedge (\sim p)] \wedge (\sim q)$
3. $(p \wedge q) \wedge (\sim p)$

We wish to make the student aware that the list of possible tautologies and contradictions we could have chosen is virtually endless. We have simply chosen those which will be of most benefit to us later.

Before leaving this section we provide the following example of a truth table involving three statements.

Example 1.24

The following table verifies that

$$[(p \to q) \vee r] \leftrightarrow \{[(p \wedge (\sim q)] \to r\}$$

is a tautology.

p	q	r	$p \to q$	$(p \to q) \vee r$	$\sim q$	$p \wedge (\sim q)$	$p \wedge (\sim q) \to r$	$[(p \to q) \vee r] \leftrightarrow \{[(p \wedge (\sim q)] \to r\}$
T	T	T	T	T	F	F	T	T
T	T	F	T	T	F	F	T	T
T	F	T	F	T	T	T	T	T
T	F	F	F	F	T	T	F	T
F	T	T	T	T	F	F	T	T
F	T	F	T	T	F	F	T	T
F	F	T	T	T	T	F	T	T
F	F	F	T	T	T	F	T	T

Since all entries in the last column are true, we have proven that the given statement is a tautology.

1.3.1 Tautologies and Logical Equivalence

Definition 1.25

Two statements p and q are ***logically equivalent*** if the biconditional statement $p \leftrightarrow q$ is a tautology.

Theorem 1.22 provides us with many useful tautologies that can be used to find logically equivalent versions of statements. For example, consider the statement

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

If we take

$$P = \text{"}n^2 \text{ is even."} \qquad \text{and} \qquad Q = \text{"}n \text{ is even."}$$

then our statement, in logical notation, reads

$$P \to Q.$$

By Theorem 1.22 (1j) we know that the statement $P \to Q$ is logically equivalent to the statement $(\sim Q) \to (\sim P)$. Thus, a logically equivalent form of our original statement is the statement

"If n is not an even integer, then n^2 is not an even integer."

Or, removing the negative language, we can write

"If n is odd, then n^2 is odd."

When two statements are logically equivalent, they must have the same truth value (either both are true or both are false). Since the two colored statements above are logically equivalent, either both are true or both are false. Therefore, if you can establish the truth of either statement, the other is also true. We will explore this idea further in the next chapter where we discuss methods of proof. But, for now, we will make the following general observation.

Observation 1.26

If p and q are logically equivalent statements, establishing the truth of p automatically establishes the truth of q, and vice versa.

1.3.2 Logical Implication and Logical Equivalence

The truth and falsity of formal logical statements $p \to q$ and $p \leftrightarrow q$ are dependent on the truth values of p and q separately. For example, the sentence

If Austin is the capitol of Texas, then $5 > 2$

is technically a true statement of the form $p \to q$. However, in ordinary language this sentence is nonsensical because it would normally be interpreted to mean that somehow Austin being the capital of Texas implies that $5 > 2$, yet we know there is no logical connection between the truth of Austin being the capitol of Texas and the fact that $5 > 2$. In mathematics and in ordinary language, a statement of the form "If p, then q" is understood to mean "The truth of p implies the truth of q," or "The truth of q follows as consequence of the truth of p." That is, ordinarily, we do not consider every possible truth value of p and q. To distinguish the purely logical form $p \to q$ from the ordinary use of the conditional, we will use the following notation.

$p \Rightarrow q$ means "If p is true, then q is true."

That is, $p \Rightarrow q$ means that the truth of q follows as a consequence of the assumed truth of p. We will call a statement of the form $p \Rightarrow q$ a ***logical implication***. The idea here is that

$p \Rightarrow q$ indicates a causal relationship from p to q, whereas in the notation $p \to q$, no causal relationship need exist, regardless of the truth of the conditional.

In a similar way, we will use the following notation.

$p \Leftrightarrow q$ means "p is logically equivalent to q."

Here, $p \Leftrightarrow q$ is understood to mean "p is true if and only if q is true," though it certainly also means "p is false if and only if q is false." (we just do not usually care to consider the negative version).

1.3 Exercises

1. Use a truth table to prove part 1c of Theorem 1.22 is a tautology.
2. Use a truth table to prove part 1h of Theorem 1.22 is a tautology.
3. Use a truth table to prove part 2d of Theorem 1.22 is a tautology.
4. Use a truth table to prove part 1 of Theorem 1.23 is a contradiction.
5. Use the appropriate tautologies from Theorem 1.22 to negate the following statements:

   (a) A foot has 12 inches and a yard has three feet.

   (b) Either I will get a job or I will not be able to pay my bills.

   (c) If I study, then I will do well in this course.

   (d) If $x^2 - 5x + 6 = 0$, then $x - 3 = 0$ or $x - 2 = 0$.

   (e) An integer m is odd if and only if m^2 is odd.

6. Verify that the following logical expressions are tautologies.

   (a) $[(\sim p) \wedge (p \vee q)] \to q$

   (b) $[(p \to q) \wedge (\sim q)] \to (\sim p)$

   (c) $[(\sim p) \to (q \wedge (\sim q)] \to p$

1.4 Propositional Functions and Quantifiers

In mathematics we frequently wish to consider sentences (propositions) which involve variables. Since for different values of the variables (called propositional variables) we get different propositions with possibly different truth values, we call such sentences ***propositional functions*** or ***open sentences***.

Example 1.27

For each real number x consider the sentence $x^2 + x = 2$. We see that $x^2 + x = 2$ is a propositional function which has different truth values, depending on the value of the propositional variable, x. The proposition is true for $x = -2$ and $x = 1$ and false for all other values of the propositional variable.

We can limit propositional functions by prefixing various expressions we call quantifiers, the most important of which are ***existential quantifiers*** and ***universal quantifiers***. Phrases such as

- "there exists a value x",
- "there are x, y, and z",
- "for some values of x", and
- "at least one value of x"

make use of existential quantifiers. On the other hand, phrases such as

- "for each value of x",
- "for every value of x",
- "for all values of x", and
- "no value of x"

employ what are called universal quantifiers.

Example 1.28

For each real number consider the propositional function $p(x)$ which states "$x^2+x = 2$." We can alter that propositional function using the two types of quantifiers, changing it into a statement.

1. <u>There exists</u> an x such that $p(x)$ is true.
2. <u>For all</u> x we have $p(x)$ is true.

Clearly by inspection, (1) is true and (2) is false.

Notationally, we will let $p(x)$ be a propositional function which states p is true for each x. Using the existential quantifier, we change $p(x)$ into a proposition, namely "There exists

x such that $p(x)$." As a mathematical shorthand, we replace "there exists" by the symbol $\exists$ and we replace the statement above by

$$\exists x, p(x),$$

which is read "There exists x such that $p(x)$ is true." Similarly, we use the symbol $\forall$ for the universal quantifier and we have the proposition

$$\forall x, p(x),$$

which is read "For all x, $p(x)$ is true."

Example 1.29

Consider all states in the USA and the propositional function $p(x)$, which states that x is a state which borders on the Pacific Ocean. The proposition $\forall x, p(x)$ is false, while the proposition $\exists x, p(x)$ is true.

The following fact is extremely important in dealing with quantifiers and negations.

Fact 1.30

Let $p(x)$ be a propositional function with propositional variable x.

1. $\sim[\forall x, p(x)] \Leftrightarrow \exists x, (\sim p(x))$.
2. $\sim[\exists x, p(x)] \Leftrightarrow \forall x, (\sim p(x))$.

Proof. Let $\sim[\forall x, p(x)]$ be true. Then $\forall x, p(x)$ must be false, so the values of x for which $p(x)$ is true is not the universe. This clearly means that for some x, possibly more than one, we have $p(x)$ is false; that is, for some x we have $(\sim p(x))$ is true, which is written $\exists x, (\sim p(x))$.

Conversely, let $\exists x, (\sim p(x))$ be true. Then for some x, $\sim(p(x))$ is true, which means for some x, we have $p(x)$ is false. Then $p(x)$ is not true for every x in the universe, meaning the statement $\forall x, p(x)$ is false and hence, $\sim[\forall x, p(x)]$ is true.

Since if either proposition in (1) is true, the other must be true, they must have the same truth value, and so are logically equivalent. The proof of part (2) is similar and left for the student. □

The student should study this fact and its proof until it is thoroughly understood since the concepts involved will be critical to the structure of a great many proofs!

1.4 Exercises

1. Use Fact 1.30 and tautologies from Threorem 1.22 to write useful negations of the following quantified statements.

   (a) All cows eat grass.

   (b) There exists at least one real number x such that $x^2 = 9$.

   (c) There is a car that is blue and weighs less than 4000 pounds.

   (d) There is no real number x such that $x^2 = -1$.

   (e) Some students attend night school.

   (f) No children are allowed in this building.

   (g) There is some number that is both odd and even.

   (h) Every math book is either white or hard to read.

   (i) All college students are math or engineering majors.

   (j) For all real numbers x, if x is positive, then $-x$ is negative.

   (k) Some cars are red, and all students take math.

   (l) There is no real number x that makes the sentence "$x^2 = -1$" true.

   (m) There are some people who go to school in the morning and work in the afternoons.

   (n) Not all numbers are rational and positive.

2. Prove part (2) of Fact 1.30

3. The following sentences are quantified in an implicit way (i.e. the wording "for all" or "there exists" is not explicitly stated). Find the implicit quantifiers in each of the following statements by rewording the statement in such a way to make the quantification explicit.

   (a) A sheep can be black.

   (b) The sum of two integers is even if and only if they are both even or both odd.

4. Consider the proposition

   "For every real number x, there is a real number y such that $2^y = x$."

   In symbols, this statement can be denoted by $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(2^y = x)$. This statement would be negated, using Fact 1.30, as follows:

$$\sim (\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(2^y = x) \Leftrightarrow (\exists x \in \mathbb{R})[\sim (\exists y \in \mathbb{R})(2^y = x)] \Leftrightarrow (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})[\sim (2^y = x)]$$

$$\Leftrightarrow (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(2^y \neq x)$$

   This, then, can be converted to English as

   "There exists a real number x such that for every real number y, $2^y \neq x$."

   This example illustrates what you are to do in the following two problems.

(a) (A real example from abstract algebra) A group G is **cyclic** provided that there is a member a of G such that for each member g of G, there is an integer n such that $a^n = g$.

   i. Express the definition of cyclic group using the condensed quantifier notation as above.

   ii. Explain in a useful way, using an English sentence, what it means to say that a group G is not cyclic.

(b) (A real example from analysis) A sequence $\{x_n\}$ is a **Cauchy** sequence provided that for each $\epsilon > 0$, there is a natural number N such that if $m, n > N$, then $|x_n - x_m| < \epsilon$.

   i. Express the definition of Cauchy Sequence using the symbolic notation as above. (Hint: There are three quantifiers here; one is implicit.)

   ii. Without using any negative words, state an English sentence for what it means to say that $\{x_n\}$ is not a Cauchy sequence.

1.5 Proofs

As we stated both in the preface as well as earlier in this chapter, our working definition of mathematics is that it is the application of inductive and deductive logic to a system of axioms. It is not our purpose in this text to formalize the logical procedure required to provide formalistic proofs. Rather, we wish to arm the student with the basic logic and methods of attack used to form convincing arguments of the validity of the statements encountered in a reasonably careful study of the foundations of mathematics.

Since we will need a working definition of the word "proof," we agree that a proof is a logical sequence of steps which validate the truth of the proposition in question. In this vein the reader should review those statements which we have "proven" and note that usually we merely showed that certain definitions were satisfied. For example, when we proposed certain statements were equivalent, we established that they had the same truth value. Surely, as we proceed further, we will be forced to provide proofs which require longer and at times more subtle sequences of logical statements. Our endeavor, as well as yours, will be to convince the reader of the truth of the propositions in question.

There are, however, some general approaches to proofs which are based on the various tautologies and contradictions presented in Section 1.3. Most theorems are merely conditional statements of the form, "If p, then q." Certainly, p and q might themselves be complicated compound statements, but that should not be allowed to cloud the issue at this time.

Direct Proofs

To prove that a particular statement of the form $p \to q$ is true, recall from the truth table of a conditional sentence that when p is false, q can have any truth value and the conditional $p \to q$ will still be true. Thus, we need only consider the case when p is true and argue that q must also be true. That is, we prove $p \Rightarrow q$ is true. Hence, in a direct proof of the statement $p \to q$, we assume p is true and by applying various known tautologies and apparent implications, we argue q is also true.

Example 1.31

Let m and n be integers. Prove that if m is even and n is even, then $m + n$ is even.

Before beginning any proof, one must have precise mathematical definitions of all terms in the statement to be proven. In this case, the term "even" needs a precise definition, which we recall from a previous chapter (Definition 0.4).

Proof. Assume the hypothesis, "m is even and n is even", is true. By definition of conjunction, it follows that the component statements "m is even" and "n is even" are true. By definition of even integer, there must exist integers r and s such that $m = 2r$ and $n = 2s$. Then substitution yields $m + n = 2r + 2s = 2(r + s)$. Since we have written $m + n$ as 2 times an integer, we have shown $m + n$ is even. That is, the conclusion "$m + n$ is even" is true whenever the hypothesis "m is even and n is even" is true. □

Proof by Contradiction

A *proof by contradiction* is based on Tautology 1m from Theorem 1.22, which we reprint here:

$$[(\sim A) \to (B \wedge (\sim B))] \to A. \tag{1}$$

The idea is that to prove a statement A is true, assume the opposite of A, $(\sim A)$, is true, then logically deduce that an obvious contradiction of the form $B \wedge (\sim B)$ results. Reaching a contradiction in this way implies that your original hypothesis (that $(\sim A)$ is true) is false; therefore, A is true.

To prove statements of the form $p \to q$ using the method of contradiction, we must substitute $p \to q$ into Tautology 1 above in place of the variable A. This requires that we make use of Tautology 1g of Theorem 1.22, which states

$$\sim (p \to q) \Leftrightarrow [p \wedge (\sim q)] \, .$$

Thus, to prove a statement of the form $p \to q$ is true using the method of contradiction, you start by assuming that $p \wedge (\sim q)$ is true; that is, assume that both p and $\sim q$ are true. Then, through a sequence of logical deductions, you attempt to arrive at a contradiction of a known or assumed truth (e.g. something like $1 = 2$). Once such a contradiction is reached, the truth of $p \to q$ is established.

Example 1.32

Let x and y be positive real numbers. Prove that if $x \neq y$, then $x^2 \neq y^2$.

Proof (by contradiction). For positive real numbers x and y, assume $x \neq y$ and $x^2 = y^2$. Then $x^2 - y^2 = 0$, so that $(x-y)(x+y) = 0$. Hence, either $x - y = 0$ or $x + y = 0$. We assumed $x \neq y$, so $x - y \neq 0$, and so we see that $x + y = 0$. But this implies $x = -y$, which contradicts the assumption that x and y are both positive. Hence, if $x \neq y$, then $x^2 \neq y^2$. □

Proof by Contraposition

To prove a statement of the form $p \to q$, a *proof by contraposition* takes advantage of Tautology 1j of Theorem 1.22, restated here:

$$(p \to q) \Leftrightarrow [(\sim q) \to (\sim p)]$$

By this tautology, if the statement $(\sim q) \to (\sim p)$ is proven to be true, then $p \to q$ is true as well. This method is illustrated by the following example.

Example 1.33

Let x and y be positive real numbers. Prove that if $x \neq y$, then $x^2 \neq y^2$.

Proof (by contraposition). For positive real numbers x and y, assume $x^2 = y^2$. Then $x^2 - y^2 = 0$, so that $(x-y)(x+y) = 0$. Hence, either $x - y = 0$ or $x + y = 0$. Since x and y are positive numbers, then so is $x + y$; hence, $x + y \neq 0$. Therefore, the alternative possibility, that $x - y = 0$, must be true, and this implies that $x = y$. □

Proofs of Biconditional Statements

There are a few ways to prove biconditional statements. The first way is to take make repeated use of the transitive property of biconditional statements,

$$[(p \leftrightarrow q) \wedge (q \leftrightarrow r)] \Leftrightarrow (p \leftrightarrow r).$$

A typical proof of a statement of the form $p \leftrightarrow q$ using this method would look something like this:

Proof. Suppose p is true. Then

$$\begin{aligned}
&p \Leftrightarrow r_1, \text{ and}\\
&r_1 \Leftrightarrow r_2, \text{ and}\\
&\vdots\\
&r_{n-1} \Leftrightarrow r_n, \text{ and}\\
&r_n \Leftrightarrow q
\end{aligned}$$

Therefore, p is true if and only if q is true. □

This first method is very efficient if it can be applied. However, much of the time, it is difficult or impossible to connect p and q with a sequence of "iff's." For this reason, a second method based on the logical equivalence

$$(p \leftrightarrow q) \Leftrightarrow [(p \to q) \land (q \to p)]$$

is often the preferred method of proving biconditional statements. This tautology tells us that if we wish to prove at statement of the form "p iff q," it suffices to prove $p \Rightarrow q$, and separately, $q \Rightarrow p$. The following example illustrates this method.

Example 1.34

Let n be an integer. Prove that n is even if and only if n^2 is even.

Proof.
($\Longrightarrow$): Suppose that n is even. Then there exists an integer k such that $n = 2k$. Thus, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Therefore, n^2, being expressed as 2 times an integer, is even.

($\Longleftarrow$): (By contraposition). Suppose that n is not even; that is, suppose n is odd. Then there exists an integer k such that $n = 2k + 1$. Thus, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Let $r = 2k^2 + 2k$ and note that r is an integer. Now $n^2 = 2r + 1$, and we see that n^2 satisfies the definition of odd integer. That is, n^2 is not even. Therefore, if n^2 is even, then n must be even as well. □

Proof by Cases

Content to be updated at a later time...

Proving and Disproving Universally Quantified Statements

A universally quatified statement of the form "$\forall x, p(x)$" can be shown to be false (i.e. *disproven*) by producing a single value of x for which the statement is false. Such an example is called a ***counterexample***. Consider the following statement.

Example 1.35

For all real numbers x and y, $\sqrt{x^2+y^2} = x+y$.

This non-identity that algebra-phobic calculus students attempt to use on a regular basis can be easily disproven by demonstrating a counterexample. Indeed, if we take $x = 2$ and $y = 3$, the statement above yields the falsehood "$\sqrt{13} = 5$." The observant student will notice that this method of disproof is based on the tautology

$$\sim (\forall x, p(x)) \longleftrightarrow (\exists x, \sim (p(x))).$$

Unnecessary of Proof by Contradiction

When students first learn about proofs by contradiction and realize how powerful this method is, they often want to apply the method to all proofs! However, sometimes in our enthusiasm for this method, we apply it unnecessarily, producing a proof that is technically correct but not as clear as possible. Consider the following proof.

Example 1.36

Prove that if n is an even integer, then n^2 is an even integer.

Proof. (by contradiction). Suppose to the contrary that n is an even integer an n^2 is odd. Since n is even, then $n = 2k$ for some integer k. Thus, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, showing that n^2 is even. But this stands in contradiction to our hypothesis that n^2 is odd. Therefore, if n is even, then n^2 is even. □

Notice in this proof that we never really used the hypothesis that n^2 is odd; the proof really just directly showed that n being even implies n^2 is even. This proof employed rather useless logical equivalence

$$(p \to q) \Leftrightarrow [(p \wedge (\sim q)) \to q] .$$

There are a few lessons to be learned by this example:

1. Unless you have a compelling reason to use an indirect method (e.g. the original statement involves negative statements, such as "$\neq$,"), it is probably best to try a direct proof first.

2. If in a proof by contradiction you do not use both hypotheses (p and $(\sim q)$), you probably did not need to use a proof by contradiction; a direct proof or proof by contraposition (if you used $(\sim q)$ but not p) probably would have been clearer.

Parting words on proofs

The student's ability to master the subtleties involved in various methods of proof and to follow logically presented sequences of implications is a large step in mathematics. A major focus in this text is to aid the student in making this leap successfully. An even greater achievement for each student will be the ability to initiate and prove things for him/herself. The cultivation of these abilities is a never-ending project in your growth as a mathematician, and we caution you to proceed slowly and carefully and not be too harsh in your self-criticism. Persistence and patience pay great dividends here!

Because the skills associated with reading and writing sound proofs are developed over time it is not assumed that students will master them in one set of exercises! Thus, there are a few statements given in the exercise set below to allow the students to practice the illustrated methods. However, the real practice will be done as the various techniques are applied throughout this course, beginning in the next chapter.

1.5 Exercises

1. Let m and n represent integers. Prove the following by the direct method.
   (a) If n is even, then $-n$ is even.
   (b) If n is odd, then $-n$ is odd.
   (c) If m is even and n is odd, then $m+n$ is odd.
   (d) If m is odd, then m^2+1 is even.

2. Let n be an integer. Prove by contraposition that if $5n-7$ is even, then n is odd.

3. Let n be an integer. Prove that if n^2 is even, then n^2 is divisible by 4. *Hint: You may use the fact we proved in class that states "Let $n \in \mathbb{Z}$. If n^2 is even, then n is even."*

4. Let A, B, and C be integers. Prove by contradiction that if $A^2+B^2=C^2$, then A is even or B is even. *Hint: See the previous hint.*

5. Prove or disprove: For every integer n, if $4|(n^2-1)$, then $4|(n-1)$.

6. Let $m, n \in \mathbb{Z}$. Prove that if $3 \nmid m$ and $3 \nmid n$, then $3|(m^2-n^2)$.

   Hint: It will help to consider cases based on what the remainders are.

7. Let $n \in \mathbb{Z}$. Prove that $3|(2n^2+1)$ if and only if $3 \nmid n$.

8. State the assumptions and what one would show for the following statements and proof methods:
   (a) Proving 'if S is closed and bounded, then S is compact' using a direct proof.
   (b) Proving 'if f is one-to-one and g is one-to-one, then $g \circ f$ is one-to-one' using a proof by contradiction.
   (c) Proving 'if g is not onto, then $g \circ f$ is not onto' using a proof by contraposition.

9. Prove the following statement by the method indicated.

   If $m+n$ is even and m is odd, then n is odd.

   (a) Direct method.
   (b) Contraposition.
   (c) Contradiction.

10. Let n be an integer. Prove that n is odd if and only if n^2 is odd.

11. Let n be an integer. Prove that $n^2 + n$ is even.

12. Prove or disprove the following: For all real numbers $x \neq 0$ or 2,

$$\frac{1}{x-2} = \frac{1}{x} - \frac{1}{2}.$$

2 Sets

2.1 Basic Definitions

In the preface we emphasized that one of the keys to understanding and being able to do mathematics is knowing and thoroughly understanding the definitions. The student is highly encouraged to take that to heart as we begin to apply our basic knowledge of logic to new mathematical concepts. Another thought conveyed in the preface is that while some definitions are based on a combination of known terms, others are so fundamental that one can really only use synonyms to attempt to communicate the concept. The first definition we give in this chapter is of that genre.

Definition 2.1

A ***set*** is a collection of distinct objects which are called the ***elements*** of the set. We will use capital letters to denote sets; for example A, B, S, T, etc. If x is an element of a set S, we use the notation $x \in S$. As is frequently done in mathematics, if y is *not* an element of a set S, we denote this by $y \notin S$.

In the definition of set, be sure to notice the word "distinct." We will say more about this, but we need some notational devices first. There are a few standard devices used to define particular sets; all use braces, but in the first method we just *enumerate* (list) the elements in the set.

Example 2.2

Consider the set $\{1, 3, 5, 2\}$ whose elements are precisely the numbers 1, 2, 3, and 5. Then we have, for example,

$$3 \in \{1, 3, 5, 2\} \text{ and } 6 \notin \{1, 3, 5, 2\}\,.$$

When simply listing all of the elements of a set is impractical (because the set has many elements) or impossible (because the set is infinite), a second notational device is used in describing the set; that of a *defining statement*. Again we use braces and inside is a vertical bar "|", which is read "such that" or "with the property that".

Example 2.3

Consider the set

$$\{x \,|\, x \text{ is an integer with } |x| \leq 2\}\,,$$

which we read as "the set of all x's such that, or with the property that, x is an integer with absolute value less than or equal to 2."

Here we are assuming the student understands the concepts of integer, absolute value, and inequality. Surely it occurs to you that the set in Example 2.3 has as elements precisely -2, -1, 0, 1, and 2, so one thinks (correctly so) that it is *equal* to the set $\{-2, -1, 0, 1, 2\}$. But before making that declaration, we must be very clear about what is meant by "equal" sets.

A third notational device in mathematics frequently used when speaking of sets is the ellipsis (a sequence of dots) to indicate that the established pattern is to continue.

Example 2.4

The set of positive even integers is the set

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

and the set of all odd integers is the set

$$\{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$$

Definition 2.5

Two sets, A and B, are said to be ***equal***, denoted $A = B$, if and only if they have precisely the same elements.

Now indeed we can state that

$$\{x \,|\, x \text{ is an integer with } |x| \leq 2\} = \{-2, -1, 0, 1, 2\}\,,$$

since these two sets have precisely the same elements. Frequently we use the notion of set equality in naming a set. For example, when we write $T = \{2, 5, -9\}$, we are defining T to be equal to the set $\{2, 5, -9\}$.

Certain sets occur so frequently in mathematics (and, in particular, in this course) that we will give them permanent names and notations that we will reserve and use for them throughout this text. For these reasons, these sets are included in the following definition.

Definition 2.6

The ***natural numbers*** ($\mathbb{N}$), the ***integers*** ($\mathbb{Z}$), the ***rational numbers*** ($\mathbb{Q}$), and the ***real numbers*** ($\mathbb{R}$) are defined as follows.

$$\mathbb{N} = \{x \,|\, x \text{ is a natural number}\} = \{1, 2, 3, 4, 5, 6, \ldots\}$$

$$\mathbb{Z} = \{x \,|\, x \text{ is an integer}\} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

$$\mathbb{Q} = \{x \,|\, x \text{ is a rational number}\} = \{x \,|\, x = m/n \text{ where } m, n \in \mathbb{Z} \text{ and } n \neq 0\}$$

$$\mathbb{R} = \{x \,|\, x \text{ is a real number}\}$$

The next example shows how sets can be described in multiple (but equivalent) ways. The student is encouraged to check that the multiple descriptions of the sets are in fact equal.

Example 2.7

- Observe that stating $T = \{2, 4, 6, 8, \ldots\}$ is just a lazy way of defining the set
$$T = \{2n \,|\, n \in \mathbb{N}\} = \{n \in \mathbb{N} \,|\, n/2 \in \mathbb{Z}\}\,.$$
- $S = \{\ldots, -3, -1, 1, 3, \ldots\} = \{n \in \mathbb{Z} \,|\, n \text{ is odd}\} = \{2n+1 \,|\, n \in \mathbb{Z}\}$.
- $W = \{1, 2, \ldots, 10\} = \{n \in \mathbb{Z} \,|\, 1 \leq n \leq 10\} = \{n \in \mathbb{N} \,|\, n < 11\}$

Example 2.8

Consider the following set equalities.

(a) $\{1, 3, 5\} = \{5, 3, 1\}$

(b) $\{1, 1, 4\} = \{1, 4\}$

In part (a) of Example 2.8 the student is encouraged to recognize that the definition of set does not include any concept of the order of its elements. In part (b) another important point arises. A set is a collection of distinct objects, so the student should note the two sets in question have precisely the same distinct elements 1 and 4. Certainly $\{1, 4\}$ is the preferred notation (just as $\frac{1}{2}$ is usually the preferred representation of $\frac{3}{6}$), but $\{1, 1, 4\}$ is not incorrect.

The final point of this section is much deeper and we must ask the student to accept the ramifications of what is being said. This point has to do with putting appropriate restraints on sets to ensure that their definitions make sense. It is easy to define a set in such a way that the set is nonsensical. For example, defining a set U to be the set containing all sets cannot make sense. Indeed, this thought is known as *Russell's Paradox*. The student is encouraged to Google that. To avoid any potential inaccuracy or confusion, one should have in mind a set called a ***universal set*** when defining a set. A universal set will contain all elements that are important to the context in which the set is defined, but will not be so large so as to contain unrelated or unimportant elements. A universal set will limit scope of consideration to sets that are *well defined*, that is, sets which make sense. The choice of universal set is context sensitive. For example, the universal set in a standard calculus course is $\mathbb{R}$. But in a course on complex variables, the universal set might be $\mathbb{C}$, the complex numbers. When speaking in generalities, we will refer to a universal set using the symbol U.

Example 2.9

(a) $W = \{x \in \mathbb{Z} \,|\, x/2 \in \mathbb{Z}\}$ is a well defined set with $\mathbb{Z}$ being the universal set.

(b) $S = \{x \in \mathbb{R} \,|\, x^3 = 1\}$ is a well defined set with $\mathbb{R}$ being the universal set. Students who have learned about complex numbers may be aware that $T = \{x \in \mathbb{C} \,|\, x^3 = 1\}$ is not equal to S. Indeed,

$$S = \{1\}\,, \text{ but } T = \left\{1, -1/2 + \frac{\sqrt{3}}{2}i, -1/2 - \frac{\sqrt{3}}{2}i\right\},$$

thus illustrating that the choice of universal set matters.

(c) $P = \{\text{teachers at UWB} \,|\, \text{they are good}\}$ is not well defined. The universal set is the set of all teachers at UWB, but the defining condition is based on a subjective quality, so does not uniquely define a specific set.

2.1 Exercises

Label the following statements as True or False, and explain your answer.

1. $3 \in \left\{n \in \mathbb{Z} \,|\, \frac{n}{2} \in \mathbb{Z}\right\}$
2. $3 \in \{n \in \mathbb{Z} \,|\, n \text{ is and odd integer}\}$
3. $5 \in \{x + 1 \,|\, x \text{ is an even integer}\}$
4. $5 \in \{m^2 \,|\, m \in \mathbb{R}\}$
5. $5 \in \{m^2 \,|\, m \in \mathbb{Z}\}$
6. $\frac{1}{2} \in \left\{\frac{2}{6}, \frac{2}{4}, \frac{3}{12}\right\}$
7. $\frac{1}{2} \in \left\{\frac{1}{3}, \frac{1}{5}, \frac{2}{7}\right\}$
8. $\{n \in \mathbb{Z} \,|\, n \leq 5\} = \{1, 2, 3, 4, 5\}$
9. $\{n \in \mathbb{N} \,|\, n \leq 5\} = \{1, 2, 3, 4, 5\}$
10. $\{x \in \mathbb{R} \,|\, x^2 - 3x - 40 = 0\} = \{8, -5\}$
11. $\{2, 1, 7\} = \{7, 1, 2\} = \{7, 2, 1\} = \{2, 7, 1\} = \{1, 2, 7\} = \{1, 7.2\}$
12. $\{-3, -2, \ldots, 10\} = \{n \in \mathbb{Z} \,|\, -4 < n < 11\} = \{n \in \mathbb{Z} \,|\, -3 \leq n \leq 10\}$
13. $\{1, 2, 3, \ldots\} = \{n \in \mathbb{Z} \,|\, n > 0\}$
14. {mountains in Washington | they are pretty} is a set.
15. $\{x \,|\, x^4 = 1\}$ is a set.
16. $\{a, b, c\} = \{a, b, a, c\}$

2.2 Combinations of Sets

Once the student is comfortable with the concept of sets, a number of ideas occur that build on that definition. For the purposes of all these definitions, we will let U be some universal set.

Definition 2.10

A set S which is comprised of some (or all) of the elements of U is called a ***subset*** of U and is denoted $S \subseteq U$. If $A \subseteq U$ and $B \subseteq U$, we further state A is a ***subset*** of B, denoted $A \subseteq B$, if each element of A is also an element of B. Moreover, if $A \subseteq B$ but $A \neq B$, we write $A \subset B$ and A is called a ***proper subset*** of B.

Example 2.11

Let $U = \{a, b, c, \ldots, z\}$, $S = \{a, b, s, u\}$, $T = \{u, a\}$, and $W = \{b, d\}$. Then

- $S \subseteq U$, $T \subseteq U$, $W \subseteq U$, and $T \subseteq S$
- $W \nsubseteq S$, $W \nsubseteq T$, $T \nsubseteq W$, and $S \nsubseteq W$
- $S \subset U$, $T \subset U$, $W \subset U$, and $T \subset S$

Here, “$\nsubseteq$” is read “is not a subset of.” The student is encouraged to write out the negation of the statement “$A \subseteq B$” to obtain a precise statement for what “$A \nsubseteq B$” means.

The student, in referring to the definition of subset, should note that to prove $A \subseteq B$ we would naturally consider an arbitrary element x of A and prove $x \in B$. Succinctly stated, we show the conditional statement “If $x \in A$, then $x \in B$” is true.

Example 2.12

Let $A = \{x \in \mathbb{R} \,|\, x^2 = 1\}$ and $B = \{x \in \mathbb{R} \,|\, x^4 - 10x^2 = -9\}$. Prove that $A \subseteq B$.

Proof. For such a simple example, we could enumerate $A = \{-1, 1\}$ and $B = \{-3, -1, 1, 3\}$ and observe that $A \subseteq B$. But to indicate a general method of proof, let us try to argue $A \subset B$ by direct proof. If $y \in A$, then by definition of A we know y is real and $y^2 = 1$. That is, $y^2 - 1 = 0$. But B contains all reals satisfying the equation $x^4 - 10x^2 = -9$. Rewriting this equation, we have $x^4 - 10x^2 - 9 = (x^2 - 1)(x^2 - 9) = 0$. Then since $y^2 - 1 = 0$, we see $(y^2 - 1)(y^2 - 9) = 0$ so that $y^4 - 10y^2 = -9$ and hence, $y \in B$. We have shown “If $y \in A$, then $y \in B$” is true, so $A \subseteq B$. □

If the reader considers the appropriate definitions, the following fact is apparent and furnishes a useful method of attack for proving equality of sets.

Fact 2.13

Let A and B be sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. (We sometimes designate proofs using this fact as "proofs by double inclusion.")

Without entering into a philosophical argument, we define $\emptyset$ to be the set with no elements, called the ***empty set***, ***void set***, or ***null set***. This set is extremely useful and should be understood carefully.

Fact 2.14

Let U be any universal set and $A \subset U$. Then $\emptyset \subseteq A$; indeed, $\emptyset \subseteq U$.

Proof. By definition of subset, we must show each element in $\emptyset$ is also an element of A (or U, if we are proving $\emptyset \subseteq U$); however, since there are no elements in $\emptyset$ to check, the definition is satisfied. □

Before continuing, let us consider the proof above logically. Recall $A \subseteq B$ is a conditional statement (If $x \in A$, then $x \in B$). So we need to examine "If $x \in \emptyset$, then $x \in A$." But $\emptyset$ has no elements, so $x \in \emptyset$ is false, meaning the conditional is true. In other words, we say the conclusion is *vacuously true*.

The next definition introduces several basic ways of combining sets which are used throughout mathematics.

Definition 2.15

Let U be the universal set with A and B subsets of U. Then

1. $A \cup B = \{x \in U \,|\, x \in A \text{ or } x \in B\}$ and is called A ***union*** B.
2. $A \cap B = \{x \in U \,|\, x \in A \text{ and } x \in B\}$ and is called A ***intersect*** B.
3. $\overline{A} = \{x \in U \,|\, x \notin A\}$ is called the ***complement*** of A.
4. $A \setminus B = \{x \in U \,|\, x \in A \text{ and } x \notin B\}$ is read A ***minus*** B. $A \setminus B$ is sometimes denoted $A - B$ is also called the ***complement of*** A ***relative to*** B***.***
5. A and B are said to be ***disjoint*** if $A \cap B = \emptyset$.

A number of facts follow directly from this definition and are noted in Fact 2.16 below. While the proofs of most of these properties are left for the reader, we will provide several as examples.

Fact 2.16

Let A, B, and D be subsets of a universal set U.

1. $A \subseteq A \cup B$.
2. $A \cap B \subseteq A$.
3. $A \setminus B \subseteq A$.
4. $A \setminus B$ and $B \setminus A$ are disjoint.
5. A and $\overline{A}$ are disjoint.
6. If $A \subseteq B$ and $B \subseteq D$, then $A \subseteq D$.
7. $A \cup B = B \cup A$. Commutative Property
8. $A \cap B = B \cap A$. Commutative Property
9. $A \cap (B \cap D) = (A \cap B) \cap D$. Associative Property
10. $A \cup (B \cup D) = (A \cup B) \cup D$. Associative Property
11. $A \cap (B \cup D) = (A \cap B) \cup (A \cap D)$. Distributive Property
12. $A \cup (B \cap D) = (A \cup B) \cap (A \cup D)$. Distributive Property
13. $A \subseteq B$ if and only if $\overline{B} \subseteq \overline{A}$.
14. $A \setminus B = A \cap \overline{B}$.
15. $\overline{A \cup B} = \overline{A} \cap \overline{B}$. DeMorgan's Law
16. $\overline{A \cap B} = \overline{A} \cup \overline{B}$. DeMorgan's Law
17. $\overline{\overline{A}} = A$.
18. $A \cup \emptyset = \emptyset \cup A = A$.
19. $A \cap \emptyset = \emptyset \cap A = \emptyset$.
20. $U \cup A = A \cup U = U$.
21. $U \cap A = A \cap U = A$.

2.2.1 Element Chasing

Proving the set containment $A \subset B$ by establishing the truth of the conditional statement "If $x \in A$, then $x \in B$" is often called *element chasing*. The following two examples illustrate this technique.

Example 2.17

Prove $A \setminus B \subseteq A$.

Proof. Let $x \in A \setminus B$. Then, by definition of $A \setminus B$, $x \in A$ but $x \notin B$. In particular, $x \in A$, and by definition of subset, we have $A \setminus B \subseteq A$. □

Example 2.18

Prove that $A \subseteq B$ if and only if $\overline{B} \subseteq \overline{A}$.

Proof.
(⇒): Suppose $A \subseteq B$. To prove that $\overline{B} \subseteq \overline{A}$, let $x \in \overline{B}$. By defintion of $\overline{B}$, $x \notin B$. Since $A \subseteq B$ and $x \notin B$, then x is certainly not in A; that is, $x \in \overline{A}$. This shows $\overline{B} \subseteq \overline{A}$.

(⇐): Suppose $\overline{B} \subseteq \overline{A}$. To prove that $A \subseteq B$, let $x \in A$. Then by definition of $\overline{A}$, $x \notin \overline{A}$. Since $x \notin \overline{A}$ and $\overline{B} \subseteq \overline{A}$, it is clear that $x \notin \overline{B}$, and thus, by defiition of $\overline{B}$, $x \in B$. This shows that $A \subseteq B$. □

2.2.2 Double Inclusion

Our next proof makes use of Fact 2.13 to prove that two sets are equal. Such proofs are called *proofs by double inclusion.*

Example 2.19

Prove that $A \cup B = B \cup A$

Proof. (by double inclusion)
($\subseteq$): Let $x \in A \cup B$. Then by definition of $A \cup B$, $x \in A$ or $x \in B$. The commutative property of disjunction then provides that $x \in B$ or $x \in A$. Now, by definiton of $B \cup A$, it is seen that $x \in B \cup A$. This shows that $A \cup B \subseteq B \cup A$.
($\supseteq$): Let $x \in B \cup A$. Then by definition of $B \cup A$, $x \in B$ or $x \in A$. Using the communtivity of disjunction gives $x \in A$ or $x \in B$. Therefore, by the defintion of $A \cup B$, $x \in A \cup B$. This shows that $B \cup A \subseteq A \cup B$.
Since it has been shown that $A \cup B \subseteq B \cup A$ and $B \cup A \subseteq A \cup B$, then by Fact 2.13, $A \cup B = B \cup A$. □

It is important that the student not confuse proofs by double inclusion (which are used only to prove set equality) and proofs of biconditional statements. Both types of proofs have two "directions," but the directions of a double inclusion proof are set containments ($\subseteq$ and $\supseteq$), while the directions of a proof of a biconditional statement are proofs of conditional statements ($\Rightarrow$ and $\Leftarrow$).

Another important point: When a set has been defined in a logically complicated way, it is sometimes useful to use rules from logic to express the defining conditions in alternative (but equivalent) ways. An example of this is as follows.

Example 2.20

Consider the statement $x \in \overline{A \cap B} = \{x \in U \,|\, x \notin A \cap B\}$. So we know that $x \notin A \cap B = \{x \in U \,|\, x \in A \text{ and } x \in B\}$. Thus, it is not true that ($x \in A$ and $x \in B$.). The parenthesis were added to emphasis the logical structure of the preceeding sentence. This logical structure is $\sim (p \wedge q)$, which we know by DeMorgan's Law of logic is equivalent to $(\sim p) \vee (\sim q)$. Thus, we can say it is true that $x \notin A$ or $x \notin B$. Equivalently, we can write $x \in \overline{A}$ or $x \in \overline{B}$. Finally, this last statement is equivalent to saying $x \in \overline{A} \cup \overline{B}$. Exactly this logical manipulation is central to the proof of the next fact.

Example 2.21

Prove: $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Proof. (by double inclusion)
($\subseteq$): Let $x \in \overline{A \cap B}$. Then $x \notin A \cap B$, and so it is not true that $x \in A$ *and* $x \in B$. Using DeMorgan's Law for negating a disjunction, we then know that it is not true that $x \in A$ *or* it is not true that $x \in B$. That is, $x \notin A$ or $x \notin B$. By definition of $\overline{A} \cup \overline{B}$, it is now clear that $x \in \overline{A} \cup \overline{B}$.
($\supseteq$): Let $x \in \overline{A} \cup \overline{B}$. Then, by definition of union of sets, $x \in \overline{A}$ or $x \in \overline{B}$. Thus, $x \notin A$ or $x \notin B$, so we may say that it is not true that x is in A or it is not true that x is in B. Applying DeMorgan's Law for negating a disjunction once again, we see that is is not true that $x \in A$ and $x \in B$; that is, $x \notin A \cap B$. Therefore, by definition of set complement, $x \in \overline{A \cap B}$ □

2.2.3 Step Format

The following two proofs illustate a *step format* of writing proofs. The step format, which uses less prose and more symbols (e.g. $\Rightarrow, \exists, \forall$, etc.) and formatting, is often easier to read. This is especially true for proofs involving a incremental sequence of steps, algebraic manipulations, logical equivalences, etc.

Example 2.22

This example is a restatement of the proof of Theorem 2.16, Part 3 given earlier.

Proof. Let $x \in A \setminus B$.

$\Rightarrow x \in U$, $x \in A$, and $x \notin B$	(definition of $A \setminus B$)
$\Rightarrow x \in A$	(logic: $p \wedge q \to p$)
$\Rightarrow A \setminus B \subseteq A$	(definition of $\subseteq$) □

In keeping with our discussion on "logical implication" in Chapter 1, the symbol "$\Rightarrow$ denotes causal implication and literally reads as "implies" or "it follows that," and the justification for the implication (where not fully obvious) are stated in parentheses.

Example 2.23

The example is a restatement of the proof of Theorem 2.16, Part 16 given earlier.

Proof.

($\subseteq$): Let $x \in \overline{A \cap B}$

$\Rightarrow x \notin A \cap B$ (Definition of complement)

$\Rightarrow x \notin A$ or $x \notin B$ (Definition of $\cap$, DeMorgan's Laws for logic)

$\Rightarrow x \in \overline{A}$ or $x \in \overline{B}$ (Definition of complement)

$\Rightarrow x \in \overline{A} \cup \overline{B}$ (Defintion of union)

$\therefore \overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ (Definition of $\subseteq$)

($\supseteq$): Let $y \in \overline{A} \cup \overline{B}$

$\Rightarrow y \in \overline{A}$ or $y \in \overline{B}$ (Definition of $\cup$)

$\Rightarrow y \notin A$ or $y \notin B$ (Definition of complement)

$\Rightarrow y \notin A \cap B$ (Definition of $\cap$, DeMorgan's Laws for logic)

$\Rightarrow y \in \overline{A \cap B}$ (Definition of complement)

$\therefore \overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$ (Definition of $\subseteq$)

Now by Fact 2.13, since we have shown that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ and $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$, we can conclude equality. (Recall that $\therefore$ means "therefore.") □

2.2.4 Proofs of Set Equality via Membership Equivalence

We now offer another method of proving set equality. This method involves showing that the conditions that define set membership of the two sets are logically equivalent.

Example 2.24

The example is another proof of Theorem 2.16, Part 16.

Proof.

$\overline{A \cap B} = \{x \in U \mid x \notin A \cap B\}$ (definition of complement)

$= \{x \in U \mid x \notin A \text{ or } x \notin B\}$ (definition of $\cap$, Demorgan's Laws of logic)

$= \big\{x \in U \mid x \in \overline{A} \text{ or } x \in \overline{B}\big\}$ (definition of complement)

$= \overline{A} \cup \overline{B}$ (definition of union)

□

2.2 Exercises

1. Let $U = \{1, 2, \ldots, 10\}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 3, 5\}$, $D = \{1, 3, 5, 7, 9\}$, and $E = \{2, 4, 6, 8, 10\}$. Label each of the following statements as True of False and explain.

   (a) D and E are disjoint.
   (b) $A \subseteq E$.
   (c) $B \subseteq A$.
   (d) $A \subset U$.
   (e) $(A \cap D) \subset A$.
   (f) $(A \cup E) \subset U$.
   (g) $(D \cup E) \subset U$.
   (h) $(D \cup E) = U$.
   (i) $6 \in D$.
   (j) $\{8\} \in E$.
   (k) $\emptyset \subseteq B$.
   (l) $\{2, 3\} \subseteq B$.
   (m) $5 \subseteq B$.
   (n) $\emptyset \subseteq \emptyset$.
   (o) $\overline{D} = E$.
   (p) $\overline{B \cup D} \subseteq E$.

2. Using the sets given in #1 above, find:

   (a) $\overline{B}$
   (b) $D \setminus A$
   (c) $\overline{D} \cap \overline{A}$
   (d) $\overline{D \cup A}$
   (e) $E \cap (B \cup D)$
   (f) $\overline{A} \cup (B \setminus D)$
   (g) $\overline{D \cap E}$
   (h) $\overline{D \setminus E}$

3. Label the following statements as True or False, and explain your answer.

   (a) $1 \in \{\{1\}\}$
   (b) $\{1\} \in \{\{1\}\}$
   (c) $1 \subseteq \{\{1\}\}$
   (d) $\{1\} \subseteq \{\{1\}\}$
   (e) $\emptyset \in \{\{1\}\}$
   (f) $\{\emptyset\} \in \{\{1\}\}$
   (g) $\emptyset \subseteq \{\{1\}\}$
   (h) $\{\emptyset\} \subseteq \{\{1\}\}$

4. Prove Part (1) of Fact 2.16.

5. Prove Part (2) of Fact 2.16.

6. Prove Part (4) of Fact 2.16.

7. Prove Part (5) of Fact 2.16.

8. Prove Part (6) of Fact 2.16.

9. Prove Part (8) of Fact 2.16.

10. Prove Part (9) of Fact 2.16.

11. Prove Part (10) of Fact 2.16.

12. Prove Part (11) of Fact 2.16.

13. Prove Part (12) of Fact 2.16.

14. Prove Part (14) of Fact 2.16.

15. Prove Part (15) of Fact 2.16.

16. Prove Part (17) of Fact 2.16.

17. Prove Part (18) of Fact 2.16.

18. Prove Part (19) of Fact 2.16.

19. Prove Part (20) of Fact 2.16.

20. Prove Part (21) of Fact 2.16.

21. For each of the following problems, assume A, B, C, and D are subsets of some universal set U. Prove each of the following.

    (a) If $C \subseteq A$ or $C \subseteq B$, then $C \subseteq A \cup B$.

    (b) If $A \subseteq C$ and $B \subseteq C$, then $A \cap B \subseteq C$.

    (c) $A \setminus A = \emptyset$.

    (d) $A \setminus (A \setminus B) \subseteq B$.

    (e) If A and B are disjoint, then $B \subseteq \overline{A}$.

    (f) If $A \subseteq C$ and $B \subseteq D$, then $A \setminus D \subseteq C \setminus B$.

    (g) $A \setminus (B \setminus C) = A \cap (\overline{B} \cup C)$

    (h) $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

    (i) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

    (j) $A \subseteq B$ if and only if $A \cap B = A$.

    (k) $A \subseteq B$ if and only if $A \cup B = B$.

    (l) $B \subseteq A$ if and only if $A \cup \overline{B} = U$.

    (m) If $A \subseteq B$ and $C \subseteq D$, then

        i. $A \cup C \subseteq B \cup D$, and

        ii. $A \cap C \subseteq B \cap D$.

22. Prove or disprove:

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

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

23. Define the *symmetric difference* between two sets A and B to be the set

$$A \triangle B = (A \setminus B) \cup (B \setminus A).$$

Prove or disprove the following:

(a) $A \triangle B = B \triangle A$.

(b) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$

(c) $A \triangle \emptyset = A$.

(d) $A \triangle A = \emptyset$.

(e) $A \triangle B = (A \cup B) \setminus (A \cap B)$.

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

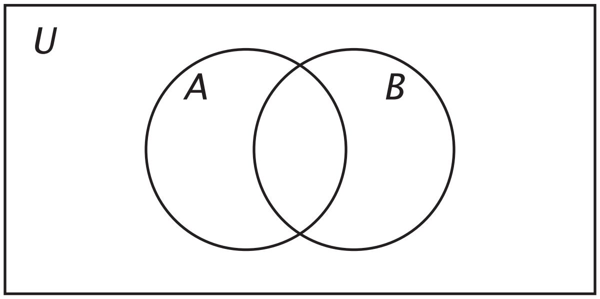
(g) $A \cup (B \triangle C) = (A \cup B) \triangle (A \cup C)$.

(h) $A \cap B = \emptyset$ if and only if $A \triangle B = A \cup B$.

2.3 Venn Diagrams and Cartesian Products

2.3.1 Venn Diagrams

A very useful skill in understanding many mathematical concepts is the ability to draw pictures to aid that understanding. In set theory this visualization process is referred to as drawing a *Venn diagram*. The student is encouraged to use Venn diagrams as an aid but is cautioned that pictures do not themselves prove anything. In drawing a Venn diagram one associates the elements of a set with the points enclosed by a geometric figure. Consider the following Venn diagram.



The box represents the universal set U, and the circles enclose the sets A and B. Using such Venn diagrams, we can visualize set theoretic concepts, including unions, intersections, complements, and set differences.

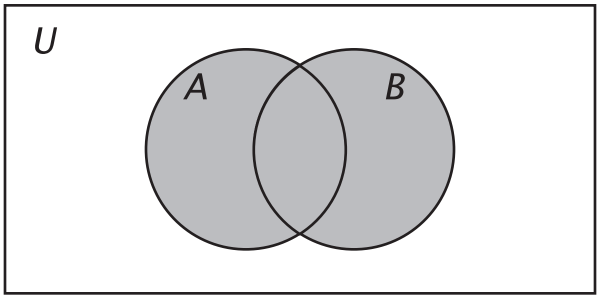


Figure 1: The shaded region represents $A \cup B$

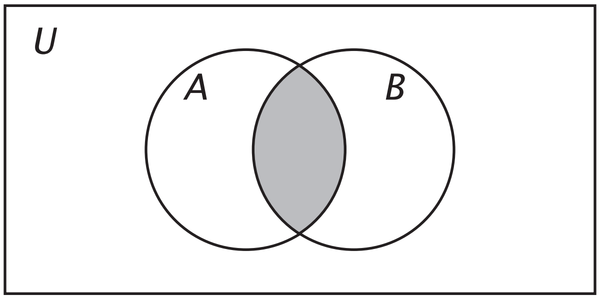


Figure 2: The shaded region represents $A \cap B$

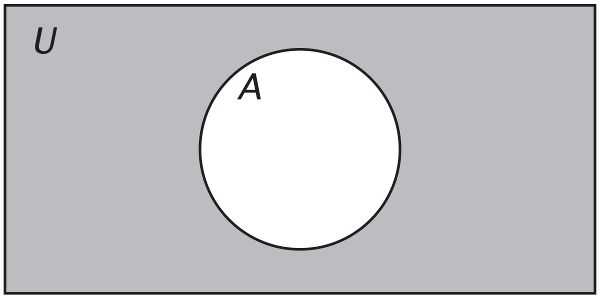


Figure 3: The shaded region represents $\overline{A}$

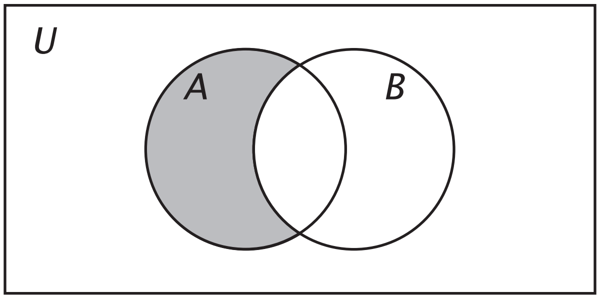


Figure 4: The shaded region represents $A \setminus B$

The student should draw Venn diagrams to aid his understanding of each of the 21 parts of Fact 2.16.

2.3.2 Power Sets

Often it is of interest to consider all subsets of a given set A and so we give the following definition.

Definition 2.25

If A is a set, then the set $\mathcal{P}(A) = \{B \,|\, B \subseteq A\}$ consisting of all subsets of A is called the ***power set*** of A.

Example 2.26

- If $A = \{1, 2\}$, then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
- If $A = \{\alpha, \beta, \gamma\}$, then $\mathcal{P}(A) = \{\emptyset, \{\alpha\}, \{\beta\}, \{\gamma\}, \{\alpha, \beta\}, \{\alpha, \gamma\}, \{\beta, \gamma\}, \{\alpha, \beta, \gamma\}\}$.

The student should check a few examples and attempt to conjecture what is the relationship between the relative sizes of A and $\mathcal{P}(A)$. In a later chapter, once we introduce the concept of proofs using mathematical induction, we will state and prove such a relationship.

2.3.3 Cartesian Products

Another important concept relating sets is that of the ***cross product*** or ***Cartesian product*** of sets. The student is superficially aware of the concept of ordered pairs (possibly not under that name) through his understanding of points in the plane (Cartesian plane). Intuitively, an ***ordered pair*** is a pair of objects with an order, usually denoted (a, b). Here the objects are "a" and "b", with "a" being called the ***first component*** of the ordered pair and "b" being called the ***second component*** of the ordered pair. The order is intentionally important and the student is aware that graphing in the plane the point (ordered pair) $(2, 3)$ yields a different point than $(3, 2)$. We should put this concept on a firm foundation, but the student should recognize and understand that this concept is a well known friend and not be confused by this rigorous definition based only on the set theoretic concepts of this chapter.

Definition 2.27

Let $a, b \in U$. Then the ***ordered pair***, denoted (a, b), is defined to be the set $\{\{a\}, \{a, b\}\}$. The element "a" is called the ***first component*** and "b" is called the ***second component*** of (a, b).

This definition has used set theoretic concepts to define ordered pair, but the student needs to carefully understand how we have accomplished expressing the concept of order by use of sets which did not themselves involve ordering. The next example will hopefully be instructive in that understanding.

Example 2.28

Consider

(a) $(5, 7) = \{\{5\}, \{5, 7\}\}$.

(b) $(7, 5) = \{\{7\}, \{7, 5\}\}$.

(c) $(5, 5) = \{\{5\}, \{5\}\} = \{\{5\}\}$.

In part (a) we see the element of $\{\{5\}, \{5, 7\}\}$ with one element is $\{5\}$, so 5 is the first component of $(5, 7)$. The element of $\{\{5\}, \{5, 7\}\}$ with two elements is $\{7, 5\}$. (Since 5 has already been determined to be the first element, 7 must be the second component of $(5, 7)$.)

In part (b) we use the same reasoning and note 7 is the first component and 5 is the second component; this ordering was achieved through use of the definition.

In part (c) we note 5 is the first component as in part (a). However, when we search for the two element subset, we can only find $\{5\}$, which tells us the second component is the same as the first. In this case, order becomes immaterial.

Whether one uses his intuitive understanding or refers to the careful definition of ordered pairs, it is necessary that we understand what is meant by ***equality of ordered pairs***.

Fact 2.29

Two ordered pairs (a, b) and (c, d) are ***equal*** if and only if their first components are the same and their second components are the same. That is $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Proof.
$(\Rightarrow)$: We will prove that if $(a, b) = (c, d)$, then $a = c$ and $b = d$, leaving the other half of the theorem's proof for the reader. So suppose that $(a, b) = (c, d)$. Then, by definition, $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. It is convenient to consider two cases separately: $a = b$ or $a \neq b$.

Case (1): Suppose $a = b$. Then $\{\{c\}, \{c, d\}\} = \{\{a\}, \{a, b\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$. Thus, $\{\{c\}, \{c, d\}\}$ is equal to a one element set and so must have a single element itself. Thus $\{c\} = \{c, d\}$, which forces $c = d$. We now have $\{\{a\}\} = \{\{c\}\}$, so that $\{a\} = \{c\}$, forcing $a = c$. Now we have $a = b = c = d$.

Case (2): Suppose $a \neq b$. $\{\{a\}, \{a, b\}\}$ is a two element set, so $\{\{c\}, \{c, d\}\}$ must be a two element set; hence, $c \neq d$. Furthermore, since $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, then $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$. The second statement is not possible since $\{a\}$ has a single element and $\{c, d\}$ has two distinct elements. Thus, $\{a\} = \{c\}$, which forces $a = c$. This leaves $\{a, b\} = \{c, d\}$, which in turn forces $b = d$. □

We can now define the product of two sets.

Definition 2.30

Let A and B be sets. Then $A \times B = \{(a, b) \,|\, a \in A \text{ and } b \in B\}$ is called the ***cross product*** or ***Cartesian product*** of A and B.

Example 2.31

Let $A = \{2, \alpha\}$ and $B = \{1, 2, \beta\}$. Then

$$A \times B = \{(2, 1), (2, 2), (2, \beta), (\alpha, 1), (\alpha, 2), (\alpha, \beta)\}.$$

After considering several examples, the student is encouraged to conjecture how the number of elements in $A \times B$ is related to the number of elements in A and B. This relationship will be stated and proven after we have introduced mathematical induction in a later chapter.

Fact 2.32

Let A, B, D, and E be nonempty subsets of a universal set. Then $A \times B = D \times E$ if and only if $A = D$ and $B = E$.

Proof.
($\Rightarrow$): Suppose $A \times B = D \times E$ and note that we must prove that $A = D$ and $B = E$. We will prove these set equalities using double inclusion.

($\subseteq$): Let $a \in A$ and $b \in B$.
$\Rightarrow (a, b) \in A \times B$ (definition of “$\times$”)
$\Rightarrow (a, b) \in D \times E$ ($A \times B = D \times E$)
$\Rightarrow a \in D$ and $b \in E$ (definition of “$\times$”)
$\therefore A \subseteq D$ and $B \subseteq E$

($\supseteq$): Let $d \in D$ and $e \in E$.
$\Rightarrow (d, e) \in D \times E$ (definition of “$\times$”)
$\Rightarrow (d, e) \in A \times B$ ($A \times B = D \times E$)
$\Rightarrow d \in A$ and $e \in B$ (definition of “$\times$”)
$\therefore D \subseteq A$ and $E \subseteq B$.

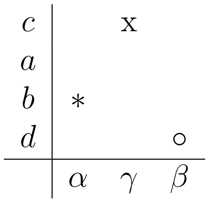
Fact 2.13 then assures that $A = D$ and $E = B$.

($\Leftarrow$): This half of the proof is left to the reader. □

Since the Cartesian plane is a geometric representative of $\mathbb{R} \times \mathbb{R}$, we are encouraged to represent other Cartesian products in the same manner.

Example 2.33

Let $A = \{\alpha, \beta, \gamma\}$ and $B = \{a, b, c, d\}$. Then we could visualize elements of $A \times B$ by placing the elements of A (in some order) along a horizontal line and the elements of B (in some order) along a vertical line. In the following graph, x represents (γ, c), $*$ represents (α, b), and $\circ$ represents (β, d).



Caution in the Cartesian plane: the set $\mathbb{R}$ has a natural order ($<$) and that order is used to obtain the graphical representation. Sets in general do not have orders and unless some ordering is specified, we could get many different representations of $A \times B$.

2.3 Exercises

1. Draw a Venn diagram illustrating the various parts of Fact 2.16. For some of these, the use of multiple colors and/or the use of a shading legend may be helpful.

2. Draw a Venn diagram for $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Do you see why $A \triangle B$ is called the *symmetric difference* of A and B?

3. For sets $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 5, 7, 9\}$, and $C = \{a, b\}$, find:

   (a) $\mathcal{P}(C)$

   (b) $A \times C$

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

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

4. Label as true or false and explain your answers.

   (a) $5 \in A \times B$

   (b) $\{2\} \in \mathcal{P}(B)$

   (c) $\emptyset \in \mathcal{P}(B)$

   (d) $(b, 5) \in C \times B$

   (e) $\{2\} \subseteq \mathcal{P}(A)$

5. If $A, B \in \mathcal{P}(S)$, prove that $A \cup B \in \mathcal{P}(S)$.

6. If $A, B \in \mathcal{P}(S)$, prove that $A \cap B \in \mathcal{P}(S)$.

7. (a) Examine the number of elements in $\mathcal{P}(S)$ where $S = \emptyset$.

   (b) Examine the number of elements in $\mathcal{P}(S)$ where $S = \{1\}$.

   (c) Examine the number of elements in $\mathcal{P}(S)$ where $S = \{1, 2\}$.

   After considering (a), (b), and (c) as well as Example 2.26, the student should be lead to conjecture that if S has n elements, then $\mathcal{P}(S)$ has 2^n elements.

8. Prove that $A \times \emptyset = \emptyset \times A = \emptyset$.

9. How many elements does $A \times B$ have where

   (a) $A = \{1, 2\}$, and $A = \{1, 2, 3\}$?

   (b) $A = \{1\}$, and $A = \{1, 2, 3\}$?

   (c) $A = \{1, 2, 3\}$, and $A = \{1, 2, 3, 4\}$?

   After considering these examples, are you lead to conjecture $A \times B$ has $m \cdot n$ elements when A has m elements and B has n elements?

10. Let $A = \{x \in \mathbb{N} \,|\, 3 < 2x + 1 < 15\}$ and $B = \{2, 4, 5, 8, 9\}$. After working #6 and #8, find the number of elements in the following sets.

    (a) A

    (b) $B \times \mathcal{P}(A)$

11. Find the natural extension of Definition 2.30 by defining $A \times B \times D$ and compare your definition with the definitions of $(A \times B) \times D$ and $A \times (B \times D)$.

12. Prove $A \times (B \cup D) = (A \times B) \cup (A \times D)$.

13. Prove $A \times (B \cap D) = (A \times B) \cap (A \times D)$.

14. Finish the proof of Fact 2.29.

15. Finish the proof of Fact 2.32.

16. Prove or disprove: $(A \times B) \cup (D \times E) = (A \cup D) \times (B \cup E)$.

17. Prove or disprove: $(A \times B) \cap (D \times E) = (A \cap D) \times (B \cap E)$.

2.4 Indexed Families of Sets

If we are asked to deal with four sets or seven sets, we can easily reference these sets with names such as A and B, or A, B, D, E, F, G, and H respectively. However, suppose we are asked to deal with 400 sets. Choosing distinctive names is a bit more difficult unless one uses the concept of *indices* and an *index set*.

Example 2.34

To deal with 400 sets we might choose an index set $I = \{1, 2, ..., 400\} = \{n \in \mathbb{N} \,|\, 1 \leq 400\}$. Using the elements of the index set I as subscripts (indices), we can then label the 400 sets as $A_1, A_2, \ldots A_{400}$.

Frequently, for descriptive purposes, index sets are chosen to be sets that are not subsets of $\mathbb{N}$. Consider the next two examples.

Example 2.35

Let us consider the twenty-six sets each comprised of the names of the presidents of the United States of America whose last names begin with a specific letter of the alphabet. Surely here the most natural index set would be the alphabet itself, where

$$\begin{aligned} P_A &= \{\text{presidents with last names beginning with A}\} \\ P_B &= \{\text{presidents with last names beginning with B}\} \\ &\vdots \\ P_Z &= \{\text{presidents with last names beginning with Z}\} \end{aligned}$$

Possibly, you remember the number corresponding to each letter of the alphabet better than we do. If that were the case, and we were to use $\{1, 2, ..., 26\}$ as the index set, you would automatically know that P_{17} is really P_Q. However, most people would not make that immediate association, so using the alphabet itself is easier and more natural.

Example 2.36

For each $x \in \mathbb{R}$ we want to define a subset of $\mathbb{R}$, say $\{w \in \mathbb{R} \,|\, w \geq x\}$. Surely the natural index set to use is $\mathbb{R}$ itself and then $S_x = \{w \in \mathbb{R} \,|\, w \geq x\}$. That is, $\left\{w \in \mathbb{R} \,|\, w \geq \frac{2}{3}\right\}$ and $\left\{w \in \mathbb{R} \,|\, w \geq -\sqrt{3}\right\}$ could be designated by $S_{\frac{2}{3}}$ and $S_{-\sqrt{3}}$, respectively.

The second example also leads us to the second major reason for using index sets other than subsets of $\mathbb{N}$. Though it is beyond the scope of this text, the reader will have to accept our statement that there are not enough integers to give distinct labels to each of the sets in Example 2.4.3 above. The student who continues far enough in mathematics will find that there are different sizes of infinity and the "size" of the set of real numbers is larger than the "size" of the set of integers.

When we are considering a set of sets, we use the terminology a ***family*** of sets rather than a set of sets. We also use a different notation when we are dealing with indexed families.

In Example 2.34 the family of sets $A_1, A_2, \ldots, A_{400}$ would notationally be written $\{A_i\}_{i=1}^{400}$. In Example 2.35 the family would be written $\{A_\alpha\}_{\alpha \in A}$ where $A = \{A, B, C, \ldots, Z\}$. The family in Example 2.36 would be denoted $\{S_w\}_{w \in \mathbb{R}}$. In general, if we have a family of sets A_i with index set I, we would write $\{A_i\}_{i \in I}$.

The student should note that the definitions of union and intersection are easily extended to indexed families.

Definition 2.37

Let $\{A_\alpha\}_{\alpha \in I}$ be a family of sets, each a subset of a universal set U. Then

$$\bigcap_{\alpha \in I} A_\alpha = \{x \in U \,|\, x \in A_\alpha \text{ for each } \alpha \in I\}$$

$$\bigcup_{\alpha \in I} A_\alpha = \{x \in U \,|\, x \in A_\alpha \text{ for some } \alpha \in I\}$$

Some comments are in order and are best noted by the following four statements, each of which is a consequence of the definitions above. It might also be helpful to refer back to our discussion of quantifiers in Chapter 1.

1. If $x \in \bigcup\limits_{\alpha \in I} A_\alpha$, then $\exists \alpha \in I$ with $x \in A_\alpha$.
2. If $x \notin \bigcup\limits_{\alpha \in I} A_\alpha$, then $\forall \alpha \in I$, $x \notin A_\alpha$.
3. If $x \in \bigcap\limits_{\alpha \in I} A_\alpha$, then $\forall \alpha \in I$, $x \in A_\alpha$.
4. If $x \notin \bigcap\limits_{\alpha \in I} A_\alpha$, then $\exists \alpha \in I$ with $x \notin A_\alpha$.

Another notational device is frequently used. Consider $\{A_i\}_{i=1}^{100}$; then for the intersection and union of these sets we may write

$$\bigcap_{i=1}^{400} A_i \qquad \text{(instead of } \bigcap_{i \in I} A_i \text{ where } I = \{1, 2, 3, \ldots, 400\}\text{), and}$$

$$\bigcup_{i=1}^{400} A_i \qquad \text{(instead of } \bigcup_{i \in I} A_i \text{ where } I = \{1, 2, 3, \ldots, 400\}\text{).}$$

We conclude this section with a statement of the generalization of DeMorgan's Laws (see Fact 2.16, parts 15 and 16).

Theorem 2.38: DeMorgan's Laws

Let $\{A_\alpha\}_{\alpha\in I}$ be an indexed family of sets.

$$(1)\ \overline{\bigcap_{\alpha\in I} A_\alpha} = \bigcup_{\alpha\in I} \overline{A_\alpha} \qquad\qquad (2)\ \overline{\bigcup_{\alpha\in I} A_\alpha} = \bigcap_{\alpha\in I} \overline{A_\alpha}$$

Proof. We prove part (1), leaving part (2) for the reader.

($\subseteq$): Let $x \in \overline{\bigcap_{\alpha\in I} A_\alpha}$

$\Rightarrow x \notin \bigcap_{\alpha\in I} A_\alpha$ (Definition of complement)

$\Rightarrow \exists\alpha \in I$ with $x \notin A_\alpha$ (Definition of generalized $\cap$)

$\Rightarrow \exists\alpha \in I$ with $x \in \overline{A_\alpha}$ (Definition of complement)

$\Rightarrow x \in \bigcup_{\alpha\in I} \overline{A_\alpha}$ (Defintion of union)

$\therefore \overline{\bigcap_{\alpha\in I} A_\alpha} \subseteq \bigcup_{\alpha\in I} \overline{A_\alpha}$ (Definition of $\subseteq$)

($\supseteq$): Let $y \in \bigcup_{\alpha\in I} \overline{A_\alpha}$

$\Rightarrow \exists\beta \in I$ with $y \in \overline{A_\beta}$ (Definition of generalized $\cup$)

$\Rightarrow \exists\beta \in I$ with $y \notin A_\beta$ (Definition of complement)

$\Rightarrow y \notin \bigcap_{\alpha\in I} A_\alpha$ (Definition of generalized $\cap$)

$\Rightarrow y \in \overline{\bigcap_{\alpha\in I} A_\alpha}$ (Definition of complement)

$\therefore \bigcup_{\alpha\in I} \overline{A_\alpha} \subseteq \overline{\bigcap_{\alpha\in I} A_\alpha}$ (Definition of $\subseteq$)

Now by Fact 2.13, since we have shown that $\overline{\bigcap_{\alpha\in I} A_\alpha} \subseteq \bigcup_{\alpha\in I} \overline{A_\alpha}$ and $\bigcup_{\alpha\in I} \overline{A_\alpha} \subseteq \overline{\bigcap_{\alpha\in I} A_\alpha}$, we can conclude equality. □

2.4 Exercises

1. Let $I = \{1, 2, 3, \ldots, 10\}$. For each $n \in I$, define $A_n = \{t \in \mathbb{N} \,|\, -2 < t < n\}$.
   (a) What is the smallest value of n?
   (b) What is the largest value of n?
   (c) Find A_1, A_2, A_3, and A_4.
   (d) Find $\displaystyle\bigcup_{n \in I} A_n$ and $\displaystyle\bigcap_{n \in I} A_n$.

2. Let $S = \{1, 2, 3, \ldots, 100\}$ and $T = \{12, 20, 32, 60, 105\}$. For each $n \in T$, define $A_n = \left\{s \in S \,|\, \frac{s}{n} \in \mathbb{Z}\right\}$.
   (a) Write the sets A_{12}, A_{20}, A_{32}, A_{60}, and A_{105}?
   (b) Find $\displaystyle\bigcup_{n \in T} A_n$ and $\displaystyle\bigcap_{n \in T} A_n$.

3. Let $S = \{1, 2, 3, 4\}$ and consider $\mathcal{P}(S)$. For each $n \in S$, define $A_n = \{T \in \mathcal{P}(S) \,|\, n \in T\}$.
   (a) Write the sets A_1, A_2, A_3, A_4.
   (b) Find $\displaystyle\bigcup_{n \in S} A_n$ and $\displaystyle\bigcap_{n \in S} A_n$.

4. Let $S \neq \emptyset$ and consider $\mathcal{P}(S)$. For each $i \in S$, define $A_i = \{C \in \mathcal{P}(S) \,|\, i \in C\}$.
   (a) Find $\displaystyle\bigcup_{i \in S} A_i$.
   (b) Find $\displaystyle\bigcap_{i \in S} A_i$.

5. For each $n \in \mathbb{N}$, define $A_n = \{m \in \mathbb{N} \,|\, m > n\}$.
   (a) Write A_5.
   (b) Prove $\displaystyle\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N} \setminus \{1\}$.
   (c) Prove $\displaystyle\bigcap_{n \in \mathbb{N}} A_n = \emptyset$.

6. Prove part (2) of Theorem 2.38.

7. For each of the following, let the index set I and the family of sets $\{A_i\}_{i\in I}$ be defined as given. Find $\bigcup\limits_{i\in I} A_i$ and $\bigcap\limits_{i\in I} A_i$.

   (a) $I = \{1, 2, 3, \ldots 100\}$, $A_i = \{-i, -i+1, \ldots, i\}$.

   (b) $I = \mathbb{N}$, $A_i = \left\{\frac{m}{i} \,|\, m \in \mathbb{Z}\right\}$.

   (c) $I = \mathbb{N}$, $A_i = \{-i, -i+1, \ldots, i^2\}$.

   (d) $I = \mathbb{N}$, $A_i = \{s \cdot i \,|\, s \in \mathbb{Z}\}$.

   (e) $I = \mathbb{N}$, $A_1 = \mathbb{N}$ and, for $n \geq 2$, $A_i = \left\{m \in \mathbb{N} \,|\, m \geq i \text{ and } \frac{m}{i} \notin \mathbb{N}\right\}$.

   (f) $I = \mathbb{N}$, $A_i = \{k \in \mathbb{Z} \,|\, -i \leq k \leq 2i\}$.

   (g) $I = \mathbb{N}$, $A_i = \left\{x \in \mathbb{R} \,|\, 0 \leq x \leq \frac{1}{i}\right\}$.

   (h) $I = \mathbb{N}$, $A_i = \left\{x \in \mathbb{R} \,|\, 0 \leq x < \frac{1}{i}\right\}$.

   (i) $I = \{x \in \mathbb{R} \,|\, 0 < x < 1\}$, $A_i = \left\{x \in \mathbb{R} \,|\, 1 - i \leq x \leq \frac{1}{i}\right\}$.

   (j) $I = \mathbb{N}$, $A_i = \left\{x \in \mathbb{R} \,|\, -\frac{1}{i} < x < \frac{2i-1}{i}\right\}$.

8. Suppose $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_k$. Find $\bigcup\limits_{n=1}^{k} A_n$ and $\bigcap\limits_{n=1}^{k} A_n$ and prove your answers.

3 Relations

3.1 Basic Definitions

In our everyday lives we encounter many circumstances which necessitate relating objects, sets, or people. Hiring is determined by comparing abilities of applicants and purchases are made based on relative prices. Descriptions such as "is faster than", "is the brother of", and "is smaller than" are heard countless times each day.

This concept of relating objects is used extensively in mathematics and leads us to the formal definition of a *relation*. Chapter 2 gave us the relation "is a subset of" which we will study in greater detail in this chapter. Special kinds of relations called *functions* will be considered in depth in next chapter.

Definition 3.1

A ***relation from a set*** A ***to a set*** B is a subset of $A \times B$. If R is a relation from A to A, we say R is a ***relation on*** A.

Thus, a relation is really just a set of ordered pairs.

Example 3.2

Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$. Consider the following sets.

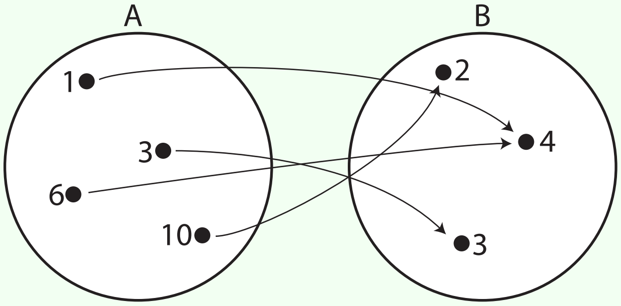
1. $R_1 = \{(a, 2), (b, 3), (c, 2), (d, 3)\}$
2. $R_2 = \{(a, 1), (a, 2), (b, 3)\}$
3. $R_3 = \{(a, 1), (b, 3), (c, 2)\}$
4. $R_4 = \{(a, a), (b, b), (c, c), (d, d)\}$
5. $R_5 = \{(d, a), (c, a), (d, d)\}$

R_1, R_2, and R_3 are relations from A to B, while R_4 and R_5 are relations on A.

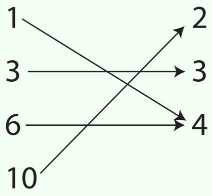
Relations may be given in many forms. Notice that a relation is essentially a pairing of elements according to some critera. Sometimes relations are specified simply by listing these pairs in set form as in the example above. When relations are given in this form, the rules or criteria for the pairing are often not known. For instance, in R_1 of Example 3.2, we know that b and d are both related to 3, but we do not know why. Similarly, relations may be indicated in table or graphical form as in Example 3.3 below.

Example 3.3

The relation $R = \{(1,4),(6,4),(3,3),(10,2)\}$ from $A = \{1,3,6,10\}$ to $B = \{2,3,4\}$ can be represented in graphical or tabular form as shown below.



Or more simply:



Or in table form:

a	b
1	4
3	3
6	4
10	2

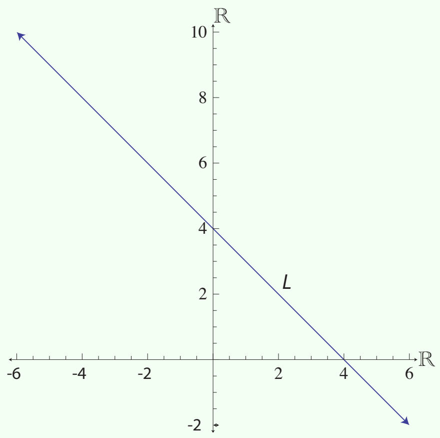
Just as with sets, listing all the ordered pairs in a relation could be tedious or impossible. In that case the relation may be described in many different ways and the associated ordered pairs are given by specifying a defining rule.

Example 3.4

The linear equation $x + y = 4$ describes a relation L on $\mathbb{R}$ consisting of an infinite set of ordered pairs whose components will satisfy the equation. Hence, the ordered pairs $(2, 2)$, $\left(\frac{3}{2}, 52\right)$, $(-7, 11)$, and $(0, 4)$ are a few of the elements in the relation. Precisely stated,

$$L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x + y = 4\}\,.$$

In the following figure, we have indicated all the ordered pairs which satisfy the equation; this is usually called the ***graph of the equation***.



Example 3.5

Let $A = \{1, 2, 3, 4\}$ and $R = \{(x, y) \in A \times A \,|\, x \leq y\}$. In this case we could enumerate R as follows:

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

Notice in Example 3.5 that it is merely inconvenient to have to list all the ordered pairs implied by the rule given. However, if the same rule were applied to the set of integers instead of the finite set A, it would be impossible to list all the associated ordered pairs.

It is often convenient notationally to refer to the relation by the criteria used for comparison. For example, in Example 3.4, we could refer to R by its defining rule "≤" so that the following to statements would be considered to be equivalent:

$$(a, b) \in R \quad \longleftrightarrow \quad (a, b) \in \leq \quad \longleftrightarrow \quad a \leq b$$

Of course, for this particular relation, the rightmost version of this statement is prefered. In general, we often use the rightmost version of the following equivalent notation:

$$(a, b) \in R \quad \longleftrightarrow \quad a\,R\,b.$$

Similarly, just as we would use the notation $a \nleq b$ when a is *not* related to b by the relation $\leq$, we will use the following notation interchangeably:

$$(a,b) \notin R \qquad \longleftrightarrow \qquad a \not R b$$

In considering each of the examples given in this section, it is clear that a relation between sets A and B need not "use up" all of both sets. This idea leads us to consider those subsets of A and B whose elements are paired by the relation, namely the ***domain*** and ***range***.

Definition 3.6

If R is a relation from A to B, then the ***domain*** of R, $\text{Dom}(R)$, is defined by

$$\text{Dom}(R) = \{a \in A \,|\, (a,b) \in R \text{ for some } b \in B\} = \{a \in A \,|\, b \in B \text{ with } (a,b) \in R\}\,.$$

The ***range*** of R, $\text{Ran}(R)$, is defined by

$$\text{Ran}(R) = \{b \in B \,|\, (a,b) \in R \text{ for some } a \in A\} = \{b \in B \,|\, a \in A \text{ with } (a,b) \in R\}\,.$$

By these definitions it is clear that $\text{Dom}(R) \subseteq A$ and $\text{Ran}(R) \subseteq B$.

Example 3.7

Consider R_1, R_2, ..., R_5 from Example 3.2. There we see

1. $\text{Dom}(R_1) = A$ and $\text{Ran}(R_1) = \{2,3\}$.
2. $\text{Dom}(R_2) = \{a,b\}$ and $\text{Ran}(R_2) = B$.
3. $\text{Dom}(R_3) = \{a,b,c\}$ and $\text{Ran}(R_3) = B$.
4. $\text{Dom}(R_4) = A$ and $\text{Ran}(R_4) = A$.
5. $\text{Dom}(R_5) = \{c,d\}$ and $\text{Ran}(R_5) = \{a,d\}$.

Example 3.8

Consider the equation $x^2 + y^2 = 1$ defined on $\mathbb{R}$. Let

$$C = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, x^2 + y^2 = 1\right\}.$$

Recall that the graph of this relation is a circle of radius 1 centered at the origin. Observe that

$$\mathrm{Dom}(C) = \{x \in \mathbb{R} \,|\, -1 \leq x \leq 1\}$$

and

$$\mathrm{Ran}(C) = \{y \in \mathbb{R} \,|\, -1 \leq y \leq 1\}$$

since substituting numbers whose squares are greater than 1 for either variable yields an equation with only complex solutions.

We will study the concepts of domain and range in more detail in the chapter on functions. However, the reader may suspect that although these sets are sometimes easily found, often they will require some insight and work to determine!

Earlier we considered the relation "$\leq$." If we were to consider the associated pairs in reverse order, we might describe this new list of ordered pairs by the relation "$\geq$." Thus we see that relations are in some sense reversible, and we formalize this concept in the definition that follows.

Definition 3.9

If R is a relation from A to B, then the ***inverse relation*** of R, denoted by R^{-1}, is defined by

$$R^{-1} = \{(b, a) \,|\, (a, b) \in R\}.$$

Notice that R^{-1} is a new relation from B to A and consists of ordered pairs from R with components reversed. Thus, the inverse of the relation

$$R = \{(2, 3), (4, 7), (2, 9), (6, 9)\}$$

is the relation

$$R^{-1} = \{(3, 2), (7, 4), (9, 2), (9, 6)\}.$$

Consider the relation R indicated in Figure 5 below.

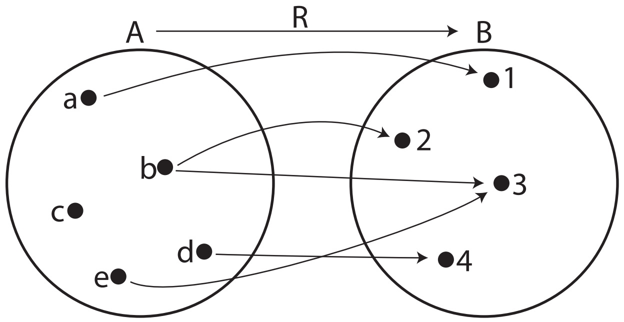


Figure 5

The inverse of R is the relation from B to A that can be found simply by reversing the direction of the arrows, as in Figure 6.

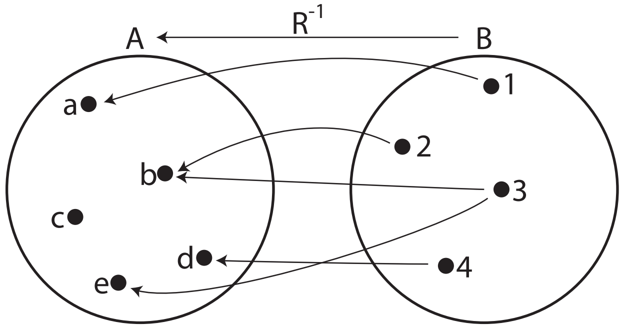


Figure 6

It should be noticed that $\mathrm{Dom}(R^{-1}) = \mathrm{Ran}(R)$ and $\mathrm{Ran}(R^{-1}) = \mathrm{Dom}(R)$. This is not an accident, as we see in the following fact, where part of the proof is left for the reader.

Fact 3.10

Let R be a relation from A to B. Then $\mathrm{Dom}(R^{-1}) = \mathrm{Ran}(R)$ and $\mathrm{Ran}(R^{-1}) = \mathrm{Dom}(R)$.

Proof. The proof of the first equality is left for the reader. To see that $\mathrm{Ran}(R^{-1}) = \mathrm{Dom}(R)$, note that by definition,

$$\mathrm{Dom}(R) = \{x \in A \,|\, (x, b) \in R \text{ for some } b \in B\},$$

and

$$\mathrm{Ran}(R^{-1}) = \big\{y \in A \,|\, (t, y) \in R^{-1} \text{ for some } t \in B\big\} = \{y \in A \,|\, (y, t) \in R \text{ for some } t \in B\}.$$

Since the sets representing $\mathrm{Ran}(R^{-1})$ and $\mathrm{Dom}(R)$ are equivalent, we have shown $\mathrm{Ran}(R^{-1}) = \mathrm{Dom}(R)$. □

Having studied the basic definitions and parts of a relation from A to B, we will now consider more special subsets of A and B.

Definition 3.11

If R is a relation from A to B and $S \subseteq A$, then the ***image*** of S, denoted by $R(S)$, is defined by

$$R(S) = \{b \in B \,|\, (s, b) \in R \text{ for some } s \in S\}\,.$$

From Figure 7 and Definition 3.11 it is clear that $R(S) \subseteq \text{Ran}(R) \subseteq B$.

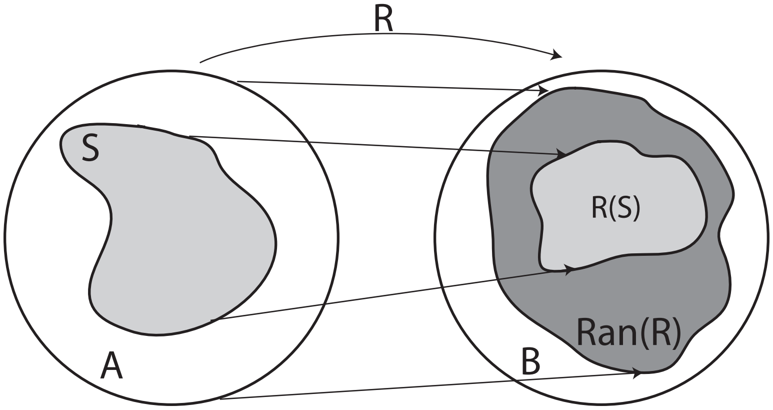


Figure 7

Example 3.12

Let $A = \{1, 2, 3, ..., 10\}$ and $B = \{2, 4, 6, 8\}$. Define the relation R from A to B by

$$R = \{(2, 2), (3, 2), (4, 6), (5, 6), (8, 8)\}\,.$$

Then $\text{Dom}(R) = \{2, 3, 4, 5, 8\}$ and $\text{Ran}(R) = \{2, 6, 8\}$.

If $S = \{2, 3, 5\}$, then $S \subseteq A$ and $R(S) = \{2, 6\}$.

If $T = \{1, 3, 5\}$, then $T \subseteq A$ and $R(T) = \{2, 6\}$.

If $V = \{6, 10\}$, then $V \subset A$ and $R(V) = \emptyset$ since there do not exist any elements $b \in B$ such that $(6, b) \in R$ or $(10, b) \in R$ because neither 6 nor 10 is in $\text{Dom}(R)$.

Definition 3.13

If R is a relation from A to B and $T \subseteq B$, then the ***preimage*** of T, denoted by $R^{-1}(T)$, is defined by

$$R^{-1}(T) = \{a \in A \,|\, (a,t) \in R \text{ for some } t \in T\}\,.$$

Then the preimage of any set is a subset of the domain of the relation. Without getting confused, the reader should carefully note that the preimage of T with respect to R is really the image of T with respect to R^{-1}, as in Figure 8. Similarly, the image of S under R is the preimage of S with respect to R^{-1}.

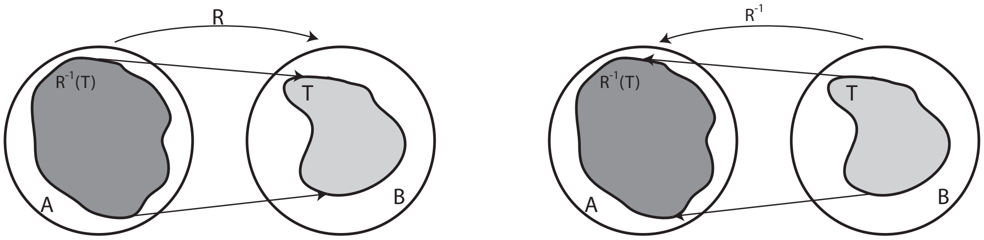


Figure 8: In the left figure, the dark grey region inside A is thought of as a preimage, but in the right figure, the dark grey region inside A is thought of as an image.

Example 3.14

Using the sets and relation of Example 3.12, we have

- $R^{-1}(\{6,8\} = \{4,5,8\}$,
- $R^{-1}(\{2\} = \{2,3\}$, and
- $R^{-1}(\{4\} = \emptyset$.

At this point we comment that since relations are just special kinds of sets, we may "operate" on relations using any set operations. For example, by taking the intersection or union of different relations, we can produce new ones. In Fact 3.15 below we make some statements concerning the domain and range of relations resulting from common set operations.

Fact 3.15

Let R_1 and R_2 be relations from A to B. Then the relations $R_1 \cup R_2$ and $R_1 \cap R_2$ from A to B have the properties that

1. $\mathrm{Dom}(R_1 \cup R_2) = \mathrm{Dom}(R_1) \cup \mathrm{Dom}(R_2)$
2. $\mathrm{Ran}(R_1 \cup R_2) = \mathrm{Ran}(R_1) \cup \mathrm{Ran}(R_2)$
3. $\mathrm{Dom}(R_1 \cap R_2) \subseteq \mathrm{Dom}(R_1) \cap \mathrm{Dom}(R_2)$
4. $\mathrm{Ran}(R_1 \cap R_2) \subseteq \mathrm{Ran}(R_1) \cap \mathrm{Ran}(R_2)$

Proof. First note that simply by definitions of relation, intersection, and union, the sets $R_1 \cup R_2$ and $R_1 \cap R_2$ are relations from A to B. We will prove part (1) by double inclusion. The student should supply the necessary reasons and proof of the remaining parts.
($\subseteq$): Let $x \in \mathrm{Dom}(R_1 \cup R_2)$
$\Rightarrow \exists y \in B$ such that $(x, y) \in R_1 \cup R_2$
$\Rightarrow y \in B$ where $(x, y) \in R_1$ or $(x, y) \in R_2$
$\Rightarrow x \in \mathrm{Dom}(R_1)$ or $x \in \mathrm{Dom} R_2$
$\Rightarrow x \in \mathrm{Dom}(R_1) \cup \mathrm{Dom} R_2$
$\therefore \mathrm{Dom}(R_1 \cup R_2) \subseteq \mathrm{Dom}(R_1) \cup \mathrm{Dom}(R_2)$

($\subseteq$): Let $x \in \mathrm{Dom}(R_1) \cup \mathrm{Dom}(R_2)$
$\Rightarrow x \in \mathrm{Dom}(R_1)$ or $x \in \mathrm{Dom}(R_2)$
$\Rightarrow \exists y_1 \in B$ where $(x, y_1) \in R_1$ or $\exists y_2 \in B$ where $(x, y_2) \in R_2$
$\Rightarrow (x, y_1) \in R_1 \cup R_2$ or $(x, y_2) \in R_1 \cup R_2$
$\Rightarrow x \in \mathrm{Dom}(R_1 \cup R_2)$
$\therefore \mathrm{Dom}(R_1) \cup \mathrm{Dom}(R_2) \subseteq \mathrm{Dom}(R_1 \cup R_2)$

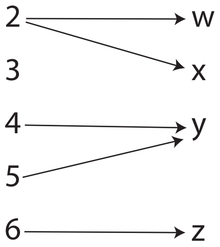
Therefore, equality holds by double inclusion. □

3.1 Exercises

1. Represent each of the relations given in Example 3.7 in table form and give a graphical representation.

2. Write in set form each of the relations indicated below.

a	b
2	5
3	6
4	7
5	5
5	8
6	



3. Complete the proof of Fact 3.10

4. Let $S = \{a, b, c, d\}$, $T = \{1, 2, 3, 4\}$, and $R = \{(a, 1), (a, 3), (b, 2), (c, 3)\}$.

   (a) Find $R(\{a, b\})$.

   (b) Find $R(\{a, c, d\})$.

   (c) Find $R^{-1}(\{1, 4\})$.

   (d) Find $R^{-1}(\{2, 3\})$.

   (e) Find $R(R^{-1}(\{1, 4\}))$. Does it relate to $\{1, 4\}$ in some way?

   (f) Find $R^{-1}(R(\{a, b\}))$. Does it relate to $\{a, b\}$ in any way?

5. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{\alpha, \beta, \gamma, \delta, \epsilon\}$, and $R = \{(1, \beta), (2, \beta), (3, \gamma), (4, \epsilon)\}$. Find the following.

   (a) $\text{Dom}(R)$

   (b) $\text{Ran}(R)$

   (c) R^{-1}

   (d) $\text{Dom}(R^{-1})$

   (e) $\text{Ran}(R^{-1})$

(f) $R(\{1,3,5\})$

(g) $R(\{5\})$

(h) $R^{-1}(\{\beta,\gamma\})$

(i) $R^{-1}(\{\alpha,\delta\})$

6. Define R on $\mathbb{R}$ by $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, y = x^2\}$. Find the following.

   (a) $\mathrm{Dom}(R)$

   (b) $\mathrm{Ran}(R)$

   (c) $R([0,2))$

   (d) $R^{-1}(\{-1\})$

   (e) $R^{-1}([1,4])$

   Hint: Think about the graph of R.

7. Let R be a relation from A to B with $S \subseteq \mathrm{Dom}(R)$ and $T \subseteq \mathrm{Ran}(R)$.

   (a) Prove $S \subseteq R^{-1}(R(S))$.

   (b) Give an example which shows that $S \neq R^{-1}(R(S))$.

   (c) Prove $T \subseteq R(R^{-1}(T))$.

   (d) Give an example that shows that $T \neq R(R^{-1}(T))$.

8. Let R be a relation from A to B with $S \subseteq \mathrm{Dom}(R)$ and $T \subseteq \mathrm{Ran}(R)$.

   (a) Prove $S \subseteq R^{-1}(R(S))$.

   (b) Give an example where $S \subset R^{-1}(R(S))$.

   (c) Prove $T \subseteq R(R^{-1}(T))$.

   (d) Give an example where $T \subset R(R^{-1}(T))$.

9. Give examples showing parts (a) and (c) of the previous problem do not hold if we delete the hypotheses $S \subseteq \mathrm{Dom}(R)$ and $T \subseteq \mathrm{Ran}(R)$.

10. (a) Prove part (2) of Fact 3.15.

    (b) Prove part (3) of Fact 3.15 and give an example showing that equality may not hold.

    (c) Prove part (4) of Fact 3.15 and give an example showing that equality may not hold.

11. Let R_1 and R_2 be relations from A to B and observe $R_1 \setminus R_2$ is a relation from A to B. What, if anything, can be said about $\mathrm{Dom}(R_1 \setminus R_2)$? $\mathrm{Ran}(R_1 \setminus R_2)$? Give examples and justify conclusions.

12. Let R be a relation from A to B and observe $\overline{R}$ is a relation from A to B. Is there a relationship between $\mathrm{Dom}(\overline{R})$ and $\overline{\mathrm{Dom}(R)}$? $\mathrm{Ran}(\overline{R})$ and $\overline{\mathrm{Ran}(R)}$? Give examples and justify conclusions

3.2 Equivalence Relations

One particular kind of relation that plays a vital role in mathematics is an equivalence relation. Before defining an equivalence relation, we will consider definitions and examples of each of the properties involved.

Definition 3.16

A relation R on a set A is ***reflexive*** if $(a, a) \in R$ for every $a \in A$; that is, for each $a \in A$, $a \, R \, a$

It is important to realize that this definition involves the universal quantifier "for every $a \in A$." Recall from Fact 1.30, part (1), that when such an expression is negated, the quantifier changes. Hence, it follows that a relation is *not reflexive* if there exists even one element in A that is not related to itself.

Example 3.17

The relation "$\leq$" on $\mathbb{Z}$ has the reflexive property since every integer n satisfies $n \leq n$.

Example 3.18

The relation "$=$" on $\mathbb{R}$ is reflexive since every real number is equal to itself.

Example 3.19

The relation $R = \{(2, 3), (2, 2), (3, 2), (3, 3)\}$ is *not* a reflexive relation on the set $A = \{1, 2, 3\}$ since $(1, 1) \notin R$. On the other hand, R *is* reflexive when considered as a relation on the set $B = \{2, 3\}$.

Example 3.20

Let S be a nonempty set and consider $\mathcal{P}(S)$, the power set of S. Then the relation "$\subseteq$" is a reflexive relation on $\mathcal{P}(S)$ since every set is a subset of itself.

Definition 3.21

A relation R on A is ***symmetric*** if whenever $(a, b) \in R$, then $(b, a) \in R$. Alternately, if $a \, R \, b$, then $b \, R \, a$.

The student should notice a major distinction between the definitions of reflexive and symmetric. The definition of reflexive is universally quantified, and so it must be true for all members of the set upon which it is defined. In contrast, the definition for the symmetric property is stated in the form of a conditional. Remember from Chapter 1 that a conditional, $p \to q$, is false only when p is true and q is false. So to show a relation R is *not symmetric* we must be able to find an ordered pair $(a, b) \in R$ such that $(b, a) \notin R$.

Example 3.22

Let $A = \{1, 2, 3, 4\}$ and consider the given relations on A. The relations

$$R = \{(1, 2), (2, 1), (3, 4), (4, 3)\} \text{ and } S = \{(1, 1)\}$$

have the symmetric property. But

$$T = \{(3, 3), (2, 4), (4, 2), (1, 2)\}$$

is *not* symmetric since $(1, 2) \in T$ and $(2, 1) \notin T$.

It is important to remember that to show a relation does not have a certain property, we need only provide a single counterexample.

Example 3.23

The relation "$\geq$" is *not* symmetric on $\mathbb{R}$ since $5 \geq 2$ but $2 \ngeq 5$.

Example 3.24

Let $A = \{\text{rectangles in the Cartesian plane}\}$ and let elements of A be related if they have the same area. Then this relation is symmetric.

Definition 3.25

A relation R on A is ***transitive*** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

Then a relation is *not transitive* if there exist $a, b, c \in A$ such that $(a, b) \in R$ and $(b, c) \in R$, but $(a, c) \notin R$.

Example 3.26

The relation "$<$" is transitive on $\mathbb{R}$.

Example 3.27

Let $R = \{(1, 1), (2, 2), (3, 3)\}$ on $\mathbb{Z}$. Then R is transitive since there do not exist $a, b, c \in \mathbb{Z}$ such that $(a, b) \in R$ and $(b, c) \in R$, but $(a, c) \notin R$.

Example 3.28

Let $R = \{(1, 2), (2, 3)\}$ on $\mathbb{Z}$. Then R is *not* transitive since $1 \, R \, 2$ and $2 \, R \, 3$ but $1 \not{R} 3$.

Definition 3.29

A relation R on a set A that is reflexive, symmetric, and transitive is called an ***equivalence relation on*** A.

A general equivalence relation on a set A is often denoted by the symbol "$\sim$," and when two elements $a, b \in A$ are related by the equivalence relation $\sim$, we write $a \sim b$ and say a and b are ***equivalent***.

Example 3.30

The equality relation "$=$" is clearly an equivalence relation on $\mathbb{R}$.

Example 3.31

Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (2, 2)\}$. Then R is *not* an equivalence relation on A because, while R is symmetric and transitive, it is not reflexive since $3 \not R 3$.

Example 3.32

Let $A = \{1, 2, 3\}$ and $S = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$. S is *not* an equivalence relation on A: S is reflexive and symmetric but not transitive, since $1\,S\,2$ and $2\,S\,3$, but $1 \not S\, 3$.

Example 3.33

Let $A = \{a, b\}$ and consider $\mathcal{P}(A)$. Then the relation $\subseteq$ on $\mathcal{P}(A)$ is reflexive and transitive but not symmetric since $\{a\} \subseteq \{a, b\}$, but $\{a, b\} \not\subseteq \{a\}$. So we see that $\subseteq$ is *not* an equivalence relation on $\mathcal{P}(S)$.

Example 3.34: Congruence Modulo n

Recall from Definition 0.11 the concept of congruence modulo n where $n \in \mathbb{N} \setminus \{1\}$. It turns out that $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. It is left as an exercise to the reader to verify this fact.

Example 3.35

Some other equivalence relations are "is the same age as" on the set of all people, "has the same area as" on the set of all rectangles in the Cartesian plane, and "lives on the same street as" on the set of all people living in a given city.

Consider the relation "is the same age as" on the set of all students in a given class. This relation groups the people in the class according to age. Each person in the class is in some group, even if it is a single member group. In addition, no person is in more than one group and all people in a specific group are the same age. These qualities are common to all equivalence relations, leading us to the following formal definition.

Definition 3.36

Let $\sim$ be an equivalence relation on A. If $x \in A$, then the ***equivalence class of*** x, denoted $\overline{x}$, is defined by

$$\overline{x} = \{y \in A \,|\, x \sim y\} .$$

$[x]$ is another common notation for the equivalence class of x.

Example 3.37

Suppose $A = \{6, 7, 8, 9, 10\}$ and let the relation R on A be defined by

$$a\,R\,b \quad \text{if} \quad a \text{ and } b \text{ have the same remainder when divided by 2.}$$

This relation is an equivalence relation since it is reflexive, symmetric, and transitive. (Verification is left for the student!) Then by Definition 3.36,

$$\overline{6} = \{6, 8, 10\},$$

$$\overline{7} = \{7, 9\},$$

$$\overline{8} = \{6, 8, 10\},$$

$$\overline{9} = \{7, 9\}, \text{ and}$$

$$\overline{10} = \{6, 8, 10\}.$$

Hence, we see $\overline{6} = \overline{8} = \overline{10}$ and $\overline{7} = \overline{9}$ so that $\overline{6}$, $\overline{8}$, and $\overline{10}$ are just different names for the same set, as are $\overline{7}$ and $\overline{9}$. Furthermore, $\overline{6}$ and $\overline{7}$ are disjoint and their union is all of A. So, the equivalence relation R has just "split" A into disjoint pieces where each piece can have different names.

The observations for the specific relation considered in Example 3.37 lead us to generalize these concepts to any equivalence relation defined on an arbitrary set.

Theorem 3.38

Let $\sim$ be an equivalence relation on A, and let $x, y \in A$. Then

1. $x \in \overline{x}$; thus, each equivalence class is non-void,
2. for $x, y \in A$, either $\overline{x} = \overline{y}$ or $\overline{x} \cap \overline{y} = \emptyset$, and
3. $\displaystyle\bigcup_{x\in A} \overline{x} = A$.

Proof.
(1): Since $x \sim x$ by the reflexive property, we have $x \in \overline{x}$ and $\overline{x} \neq \emptyset$.

(2): Let $x, y \in A$. If $\overline{x} \cap \overline{y} = \emptyset$, we are done. So suppose $\overline{x} \cap \overline{y} \neq \emptyset$ and let $z \in \overline{x} \cap \overline{y}$. We will show $\overline{x} = \overline{y}$ by double-containment.

($\subseteq$): Let $w \in \overline{x}$.

$$\begin{aligned}
&w \in \overline{x} \text{ and } z \in \overline{x} \Rightarrow x \sim w \text{ and } x \sim z \\
&\Rightarrow w \sim x \text{ and } x \sim z && \text{(by symmetry of } \sim\text{)} \\
&\Rightarrow w \sim z && \text{(by transitivity of } \sim\text{)}
\end{aligned}$$

But $z \in \overline{y}$, so $y \sim z$. Recall that we also have that $w \sim z$.

$$\begin{aligned}
&\Rightarrow y \sim z \text{ and } z \sim w && \text{(by symmetry of } \sim\text{)} \\
&\Rightarrow y \sim w && \text{(by transitivity of } \sim\text{)} \\
&\Rightarrow w \in \overline{y} \\
&\therefore \overline{x} \subseteq \overline{y}
\end{aligned}$$

($\supseteq$): The proof of this containment is identical to the proof of the previous containment (just interchange the role of x and y).

(3): To see $\displaystyle\bigcup_{a\in A} \overline{x} = A$, note that we have $\overline{x} \subseteq A$ by definition of equivalence class, so clearly $\displaystyle\bigcup_{a\in A} \overline{x} \subseteq A$. To show the reverse containment, let $w \in A$. By part (1), $w \in \overline{w}$, so $w \in \displaystyle\bigcup_{x\in A} \overline{x}$ since w is one of the elements of A. □

As stated early in the text, one of the main goals of a foundation level course in mathematics is for the student to learn to dissect and digest definitions and theorems. That is, it does little good for a student to be able to state and prove a theorem such as the previous one if he fails to truly understand and make it his own. In order to illustrate how a student might accomplish this task for himself, we will consider some of the implications of Theorem 3.38. Each time a new definition or theorem is encountered, the student should study it in a similar manner until he absorbs the concept for himself.

The first part of Theorem 3.38 tells us that any element in a set may be used to generate an equivalence class. Thus, when given an equivalence relation on a set, we may find the classes generated by that relation by choosing elements at random from the set. For example, suppose $A = \left\{\frac{2}{3}, -\frac{1}{2}, -1, 0, \frac{4}{6}, \frac{0}{3}, -\frac{4}{8}, \frac{10}{15}\right\}$ and let the equivalence relation on A be "=". Then to find the equivalence classes determined by the relation, we may choose any element in A, say $\frac{4}{6}$. Then $\frac{4}{6} \in \overline{\frac{4}{6}}$ since $\frac{4}{6} = \frac{4}{6}$. The other elements of $\overline{\frac{4}{6}}$ are $\frac{2}{3}$ and $\frac{10}{15}$ since they are the only other elements of A which are equal to $\frac{2}{3}$. Thus $\overline{\frac{4}{6}} = \left\{\frac{4}{6}, \frac{2}{3}, \frac{10}{15}\right\}$. Part (2) of this theorem implies we might just as easily have chosen $\frac{2}{3}$ or $\frac{10}{15}$ and we would have arrived at the same equivalence class. That is, since $\frac{2}{3} \in \overline{\frac{4}{6}}$, and $\frac{10}{15} \in \overline{\frac{4}{6}}$, then $\overline{\frac{4}{6}} = \overline{\frac{2}{3}} = \overline{\frac{10}{15}}$. So we conclude that we may designate an equivalence class completely using any of its elements! Furthermore, part (2) of this theorem tells us that any two equivalence classes are either identical or disjoint. Part (3) assures us that by combining all equivalence classes we will get A itself and that every element of A is in some equivalence class. Notice that $\overline{\frac{4}{6}} \cup \overline{0} \cup \overline{-\frac{1}{2}} \cup \overline{-1} = A$. We will pursue this observation shortly.

Example 3.39

Let A be the set of all ordered pairs of real numbers, and define

$$(a, b) \sim (c, d) \qquad \text{if} \qquad a^2 + b^2 = c^2 + d^2.$$

Before proceeding further, the student should find some ordered pairs that are related and then verify that this indeed defines an equivalence relation. Then for any $(x, y) \in \mathbb{R} \times \mathbb{R}$, we have

$$\overline{(x, y)} = \left\{(s, t) \,|\, x^2 + y^2 = s^2 + t^2\right\}.$$

These equivalence classes are represented geometrically by circles centered at the origin. For example,

$$\overline{(3, 4)} = \left\{(s, t) \,|\, s^2 + t^2 = 3^2 + 4^2 = 25\right\},$$

and the graph of this set of points is a circle of radius 5 centered at the origin.

As promised in the preceding paragraph, we are now going to further study some of our earlier observations concerning equivalence classes. We have noticed by example that not only are unequal equivalence classes disjoint, but that their union is equal to the set from which their elements are chosen. Thus, the equivalence classes "split" or partitioned the set.

Definition 3.40

Let A be a set and let $\{B_\alpha\}_{\alpha \in I}$ be a family of subsets of A satisfying the following three properties.

1. For each $\alpha \in I$ we have $B_\alpha \neq \emptyset$.
2. For all $\alpha, \beta \in I$, either $B_\alpha \cap B_\beta = \emptyset$ or $B_\alpha = B_\beta$.
3. $\displaystyle\bigcup_{\alpha \in I} B_\alpha = A$.

Then $\{B_\alpha\}_{\alpha \in I}$ is said to be a ***partition*** of A.

In fact, we see a very important relationship between equivalence classes and partitions which is stated in the following theorem.

Theorem 3.41

[Equivalence Class Theorem]

1. Let $\sim$ be an equivalence relation defined on a nonempty set A. Then $\mathcal{C} = \{\overline{x}\}_{x \in A}$ forms a partition of A.
2. Conversely, let $\mathcal{P} = \{B_\alpha\}_{\alpha \in I}$ be any partition of a set A and define the relation $\sim$ on A by

$$a \sim b \text{ if there exists some } \alpha \in I \text{ such that } a \in B_\alpha \text{ and } b \in B_\alpha.$$

   Then $\sim$ is an equivalence relation on A.

Proof.
(1): The fact that $\mathcal{C}$ forms a partition of A is a direct result of Theorem 3.38.

(2): If $\mathcal{P}$ is any partition of a set A, define the relation $\sim$ on A as stated in the theorem. To see $\sim$ is an equivalence relation we show it is reflexive, symmetric, and transitive.

reflexivity: Let $a \in A$. Since $\{B_\alpha\}_{\alpha \in I}$ is a partition of A, then $A = \bigcup_{\alpha \in I} B_\alpha$. Thus, $a \in \bigcup_{\alpha \in I} B_\alpha$. This implies there exists $\alpha \in I$ with $a \in B_\alpha$. However, obviously $a, a \in B_\alpha$ and by definition of α we then have $a \sim a$, and so $\sim$ is reflexive.

symmetry: Suppose $a \sim b$. Then $\exists \alpha \in I$ with $a \in B_\alpha$ and $b \in B_\alpha$. Since the logical connective "and" is symmetric, we have $b \in B_\alpha$ and $a \in B_\alpha$, so $b \sim a$ and $\sim$ is symmetric.

transitivity: Suppose $a \sim b$ and $b \sim c$. Then $\exists \alpha \in I$ with $a, b \in B_\alpha$ and $\exists \beta \in I$ with $b, c \in B_\beta$. Since $\{B_\alpha\}_{\alpha \in I}$ is a partition, any two of the subsets are either equal or disjoint; but note that $b \in B_\alpha \cap B_\beta$, so it must be the case that $B_\alpha = B_\beta$. Now it is seen that $a, b, c \in B_\alpha$, and by definition of $\sim$, we have $a \sim c$.

It remains to show that the family $\{B_\alpha\}_{\alpha \in I}$ are exactly the equivalence classes of $\sim$; that is, $\{B_\alpha\}_{\alpha \in I} = \{\overline{x}\}_{x \in A}$. The proof of this is left as an exercise. □

Example 3.42

Consider the partition $\{\{1\}, \{2, 4\}, \{3\}\}$ of the set $\{1, 2, 3, 4\}$. Then the equivalence relation induced by the partition is

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

Example 3.43

Let

$$R = \{(a,a),(a,b),(b,a),(a,c),(c,a),(b,c),(c,b),(b,b),(c,c),(d,d)\}$$

be an equivalence relation on the set $\{a,b,c,d\}$ (verify R is an equivalence relation!). Then the partition associated with R is

$$\mathcal{P} = \{\{a,b,c\},\{d\}\}.$$

In closing, it is interesting to consider the consequences of performing various set operations on relations possessing the properties defined in this section. Two such results are noted in Fact 3.44 below.

Fact 3.44

Let R_1 and R_2 be equivalence relations on A. Then the following statements are true:

1. $R_1 \cap R_2$ is an equivalence relation on A.
2. $R_1 \cup R_2$ is reflexive and symmetric.

Proof.
(1): We prove $R_1 \cap R_2$ is reflexive, symmetric, and transitive.
reflexivity: Let $a \in A$. Then $(a,a) \in R_1$ and $(a,a) \in R_2$ since R_1 and R_2 are both reflexive on A. By definition of intersection, $(a,a) \in R_1 \cap R_2$, and so $R_1 \cap R_2$ is reflexive.

symmetry: Let $(a,b) \in R_1 \cap R_2$. Then $(a,b) \in R_1$ and $(a,b) \in R_2$. Since R_1 and R_2 are both symmetric, we see that $(b,a) \in R_1$ and $(b,a) \in R_2$. Thus, $(b,a) \in R_1 \cap R_2$ and we see that $R_1 \cap R_2$ is symmetric.

transitivity: Let $(a,b),(c,d) \in R_1 \cap R_2$. Then by defintion of intersection, $(a,b),(b,c) \in R_1$ and $(a,b),(b,c) \in R_2$. The transitivity of R_1 provides that $(a,c) \in R_1$ and the transitivity of R_2 gives us $(a,c) \in R_2$. Therefore, $(a,c) \in R_1 \cap R_2$ and so $R_1 \cap R_2$ is transitive.

(2): We prove $R_1 \cup R_2$ is symmetric, leaving the proof that $R_1 \cup R_2$ is reflexive to the reader. To see that $R_1 \cup R_2$ is symmetric, let $(a,b) \in R_1 \cup R_2$. Then, by defintion of union, $(a,b) \in R_1$ or $(a,b) \in R_2$. Both relations are symmetric, so $(b,a) \in R_1$ or $(b,a) \in R_2$. Thus, $(b,a) \in R_1 \cup R_2$. □

3.2 Exercises

1. Determine whether or not the following relations are equivalence relations on the given sets. Give reasons for your answers.

   (a) $R = \{(1,1),(2,2),(3,3)\}$ on $A = \{1,2,3\}$

   (b) $R = \{(1,1),(2,2),(3,3)\}$ on $A = \{1,2,3,4\}$

   (c) $R = \{(1,3),(3,1),(1,1),(3,3)\}$ on $A = \{1,3\}$

   (d) $R = \{(1,3),(3,1),(1,1),(3,3)\}$ on $A = \{1,2,3\}$

2. Consider $\equiv_5$ on $\mathbb{Z}$. Note that

   $\overline{0} = \{n \in \mathbb{Z} \,|\, 5|n\} = \{\ldots,-10,-5,0,5,10,\ldots\}$, and
   $\overline{1} = \{n \in \mathbb{Z} \,|$ the remainder upon division of n by 5 is $1\} = \{\ldots,-9,-4,1,6,11,\ldots\}$.

   Find $\overline{2}$, $\overline{3}$, and $\overline{4}$. Considering Theorem 3.38, what is $\overline{93}$? $\overline{121}$? $\overline{-17}$?

3. (Congruence modulo n)

   (a) Prove that $\equiv_n$ is an equivalence relation.

   (b) For $n = 12$, find $\bar{5}$. How many distinct equivalence classes are there with respect to this relation? What are they?

4. Verify the relation defined in Example 3.37 is an equivalence relation.

5. Define $\sim$ on $\mathbb{R}$ by $a \sim b$ if and only if $|a| = |b|$. Prove $\sim$ is an equivalence relation on $\mathbb{R}$ and for an arbitrary element $t \in \mathbb{R}$, find $\bar{t}$.

6. For each of the following, a relation R is defined on a given set. For each, prove or disprove:
   i) R is reflexive   ii) R is symmetric   iii) R is transitive.
   In each problem where R is an equivalence relation, find $\bar{a}$, where a is any element in the set on which the relation is defined.

   (a) Define R on $\mathbb{N}$ by $a\,R\,b$ iff $a = b \cdot 10^k$ for some $k \in \mathbb{Z}$.

   (b) Define R on $\mathbb{R}$ by $x\,R\,y$ iff $x - y \in \mathbb{Z}$.

   (c) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, xy = 0\}$

   (d) Define$R$ on $\mathbb{N}$ by $x\,R\,y$ iff $2|(x+y)$.

   (e) Define R on $\mathbb{N}$ by $x\,R\,y$ iff $3|(x+y)$.

   (f) Define R on $\mathbb{R} \times \mathbb{R}$ by $(a,b)\,R\,(c,d)$ iff $(a-c) \in \mathbb{Z}$.

   (g) Define R on $\mathbb{R} \times \mathbb{R}$ by $(a,b)\,R\,(c,d)$ iff $(a-c) \in \mathbb{Z}$ and $(b-d) \in \mathbb{Z}$.

7. For the set $A = \{1,2,3,\ldots,8\}$. consider

   $$P = \{\{1,2,3\},\{4,5\},\{6\},\{7,8\}\}.$$

   Show P is a partition of A and define the induced equivalence relation (ala the Equivalence Class Theorem). Find $\bar{1}$, $\bar{2}$, $\bar{3}$, …, $\bar{8}$.

8. Consider $A = \mathbb{R} \times (\mathbb{R} \setminus \{0\})$ and define $(a,b) \sim (c,d)$ if $a \cdot d = b \cdot c$.

   (a) Show $\sim$ is an equivalence relation on A.

   (b) Prove $\overline{(1,2)} = \left\{(x,y) \in A \mid \frac{x}{y} = \frac{1}{2}\right\}$.

   (c) Give a geometric description of an arbitrary equivalance class $\overline{(a,b)}$.

9. Let R be a relation on A which is symmetric and transitive. If $\operatorname{Dom}(R) = A$, prove R is reflexive. Can this be proven without $\operatorname{Dom} = A$?

10. Construct examples of equivalence relations R_1 and R_2 such that $R_1 \cup R_2$ is not transitive. (See Fact 3.44.)

3.3 Properties of Relations on a Set

Now that we have considered relations in general and equivalence relations in particular, we would like to study some interesting properties and other special types of relations. For convenience, Definitions 3.16, 3.21, and 3.25 are repeated for completeness, though the student should recognize them from the material on equivalence relations.

Definition 3.45

A relation R on a set A is ***reflexive*** if $(a, a) \in R$ for every $a \in A$; that is, for each $a \in A$, $a \, R \, a$

Definition 3.46

A relation R on A is ***symmetric*** if whenever $(a, b) \in R$, then $(b, a) \in R$. Alternately, if $a \, R \, b$, then $b \, R \, a$.

Definition 3.47

A relation R on A is ***transitive*** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

The following definitions are new.

Definition 3.48

A relation R on a set A is ***irreflexive*** if $(a, a) \notin R$ for every $a \in A$; that is, $\forall a \in A$, $a \not R \, a$

Notice that as with the reflexive property, the definition of irreflexive involves a quantified expression. So to show a relation does not possess the irreflexive property, it suffices to find one element in A that is related to itself.

Example 3.49

The relation "$\leq$" is clearly *not* irreflexive on $\mathbb{Z}$. However, the relation "$<$" is irreflexive on any nonempty subset of $\mathbb{Z}$ since no real number is less than itself.

Example 3.50

If $A = \{\text{females in the U.S.}\}$ and R is the relation on A described by "is the mother of", then R is an irreflexive relation.

Definition 3.51

A relation R is ***asymmetric*** on A if, whenever $(a, b) \in R$, then $(b, a) \notin R$.

It follows that R is *not* asymmetric if there exists $(a,b) \in R$ such that $(b,a) \in R$.

Definition 3.52

A relation R is ***antisymmetric*** on A if, whenever $(a,b) \in R$ and $(b,a) \in R$, then $a = b$.

Recalling that contraposition of a conditional yields an equivalent statement, we may restate the definition of the antisymmetric property:

$$\text{If whenever } a \neq b, \text{ it follows that } (a,b) \notin R \text{ or } (b,a) \notin R, \text{ then } R \text{ is antisymmetric.}$$

Also, recall from Theorem 1.22, part 1g, that the negation of $[(p \wedge q) \to r]$ is equivalent to $[(p \wedge q) \wedge (\sim r)]$. Thus, "not antisymmetric" means

$$\exists a, b \in A \text{ such that } (a,b) \in R \text{ and } (b,a) \in R, \text{ but } a \neq b.$$

Example 3.53

Consider the relation "<" defined on $\mathbb{Z}$. Then this relation is asymmetric since whenever $a < b$, it follows that $b \not< a$. Also, whenever $a \neq b$, we have $a < b$ or $b < a$, but not both; thus, this relation is antisymmetric.

Example 3.54

Consider the relation "$\subseteq$" defined on $\mathcal{P}(S)$. This relation is not asymmetric, since for sets A and B such that $A = B$, it follows that both $A \subseteq B$ and $B \subseteq A$. It is antisymmetric since whenever $A \subseteq B$ and $B \subseteq A$, we have $A = B$.

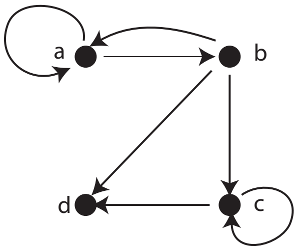
Before leaving this section, we introduce a visual method for representing finite relations. For rather small finite relations, these visual representations, called ***digraphs***, can be very helpful in conceptualizing a relation and its properties. It will be introduced briefly here and explored in more detail in the exercises and in Section 3.5.

In general, consider a finite set A and a relation R defined on it. Digraphs are constructed by drawing a small dot representing each element of A and labeling that dot appropriately. These dots are called the ***vertices*** of the graph. At each dot, say x, draw a directed line segment from it to any other dot, labeled y, if and only if $x \, R \, y$. These directed line segments are called ***edges***. Then notice that the dots represent A and the edges represent the ordered pairs in R.

Example 3.55

Consider the set $A = \{a, b, c, d\}$ and the relation

$$R = \{(a,a), (c,c), (a,b), (b,a), (b,d), (c,d), (b,c)\}.$$



Digraph of R

Notice that there is an edge representing every ordered pair in R. For those elements in A that are related to themselves, there is an edge that looks like a loop. In this relation there are only two loops since only a and c are related to themselves. Then we can quickly see from the digraph that R is not reflexive. It is also easy to conclude from the picture that R is not symmetric, not transitive, not irreflexive, not asymmetric, and not antisymmetric! Why?

From the previous example it is reasonable to conclude that for an arbitrary finite relation R defined on A, the relation will have the reflexive property if and only if each vertex has a loop. Claims were also made regarding other conclusions that could be drawn from the digraph. The student is asked to explore the general case in the exercises below.

3.3 Exercises

1. Consider the following relations and determine whether they are reflexive, irreflexive, symmetric, asymmetric, antisymmetric, or transitive.

   (a) $R = \{(1,1),(3,3),(5,5)\}$ on $A = \{1,3,5\}$

   (b) $R = \{(1,1),(2,2),(1,2)\}$ on $A = \{1,2\}$

   (c) $R = \{(1,2),(2,1),(1,1)\}$ on $A = \{1,2\}$

   (d) $R = \{(1,3),(2,3),(3,2),(3,1)\}$ on $A = \{1,2,3\}$

   (e) $R = \{(1,1),(2,2),(3,3),(4,4),(1,3),(2,4)\}$ on $A = \{1,2,3,4\}$

   (f) $R = \{(3,4)\}$ on $A = \{3,4\}$

   (g) $R = \{(3,3)\}$ on $A = \{3,4\}$

2. Let $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \,|\, a < b+5\}$. Is R reflexive, irreflexive, symmetric, asymmetric, antisymmetric, or transitive? Justify your answer.

3. Let $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \,|\, |a-b| < 5\}$. Is R reflexive, irreflexive, symmetric, asymmetric, antisymmetric, or transitive? Justify your answer.

4. Let R_1 and R_2 be relations on A.

   (a) If R_1 and R_2 are both irreflexive, prove $R_1 \cap R_2$ and $R_1 \cup R_2$ are irreflexive.

   (b) If R_1 and R_2 are both antisymmetric, is $R_1 \cup R_2$ antisymmetric? Justify your answer.

   (c) If R_1 and R_2 are both asymmetric, is $R_1 \cup R_2$ asymmetric? Justify your answer.

   (d) If R_1 and R_2 are both asymmetric, prove $R_1 \cap R_2$ is asymmetric. Justify your answer.

   (e) If R_1 and R_2 are both antisymmetric, is $R_1 \cap R_2$ antisymmetric? Justify your answer.

5. Let R be a relation on a finite nonempty set A. Justify your claims in each part below. What can be said about the digraph of R if the relation

   (a) is irreflexive? (b) is not irreflexive?
   (c) is symmetric? (d) is not symmetric?
   (e) is asymmetric? (f) is not asymmetric?
   (g) is antisymmetric? (h) is not antisymmetric?
   (i) is transitive? (j) is not transitive?

6. Let $A = \{1,2,3,4,5\}$ and $R = \{(2,3),(2,4),(3,5),(2,5),(5,5)\}$

   (a) Draw a digraph of this relation.

   (b) Determine which properties are possessed by R, explaining in each case how you can tell from your digraph.

7. (a) Draw a digraph of the relation $<$ on the set $A = \{1, 2, 3, 4\}$.

   (b) Draw a digraph of the relation $\leq$ on the set $A = \{1, 2, 3, 4\}$.

8. Draw a digraph of $\mathcal{P}(S)$ under the relation $\subseteq$ where $S = \{a, b\}$.

3.4 Orderings

Besides equivalence relations, there are some combinations of the properties of relations in Section 3.3 that are of special interest. In this section we will study various types of orderings.

Definition 3.56

A relation R on A is called a ***partial order*** of A if R is reflexive, antisymmetric, and transitive. The symbol $\prec$ will be used to denote a general partial order. A set A together with a partial order $\prec$ on A is called a ***partially ordered set*** (or simply a ***poset***) and will be denoted $(A, \prec)$.

It is important to remember that if we change the set upon which a partial order is defined, $(A, \prec)$ may cease to be a partially ordered set.

Example 3.57

Let $R = \{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$ be a relation defined on the set $A = \{1,2,3\}$. Then (A, R) is a partially ordered set since R is reflexive, antisymmetric, and transitive. However, if we enlarge the set A in any way (say, $A = \{1,2,3,4\}$), then R will fail to be reflexive, making (A, R) no longer partially ordered.

Example 3.58

The relation "$\leq$" is a partial order of $\mathbb{Z}$.

Example 3.59

For any set A, the subset relation "$\subseteq$" is a partial order of $\mathcal{P}(A)$.

Example 3.60

Let the relation R be defined on $\mathbb{Z}$ by

$$a\,R\,b \qquad \text{iff} \qquad a|b.$$

R is not a partial order of A since $2\,R\,(-2)$ and $(-2)\,R\,2$, but $2 \neq -2$, making R not antisymmetric. However, if we restrict R to $\mathbb{N}$, the set of positive integers, then R becomes a partial order. This relation of "divisibility" will be used so often as an example of an ordering that we will use the special symbol $\ll$ to denote it in the context of orderings. That is, we will say $3 \ll 12$ since $3|12$.

The term partial is used in defining this type of relation because it indicates that there might be some "gaps" in our ordering. That is, in many partially ordered sets there are elements which are not comparable. For example, in the partially ordered set $(\mathcal{P}(A), \subseteq)$, there could be elements B and C in $\mathcal{P}(A)$ such that neither $B \subseteq C$ nor $C \subseteq B$. Of special interest are partially ordered sets in which *all* elements are related.

Definition 3.61

Let $\prec$ be a partial order of a set A. Then $\prec$ is a ***linear order*** (or ***total order***) of A if for all elements $a, b \in A$, it follows that $a \prec b$ or $b \prec a$.

Example 3.62

The partial order $\leq$ on $\mathbb{Z}$ is a linear order since for any integers a and b, it follows that $a \leq b$ or $b \leq a$.

Example 3.63

The partial order $\ll$ on $\mathbb{Z}$ given in Example 3.60 fails to be a linear order since integers 3 and 5 are not related under $\ll$; that is, $3 \not\ll 5$ and $5 \not\ll 3$.

The third type of ordering we will consider is a ***well-ordering*** of a set. However, we must first introduce some preliminary concepts.

Definition 3.64

Let $\prec$ be a partial ordering of a nonempty set A.

- An element $\alpha \in A$ is a ***maximal element*** if $\nexists\, a \in A \setminus \{a\}$ with $\alpha \prec a$.
- An element $\alpha \in A$ is a ***maximum element*** if $\forall\, a \in A$ we have $a \prec \alpha$.
- An element $\alpha \in A$ is a ***minimal element*** if $\nexists\, a \in A \setminus \{a\}$ with $a \prec \alpha$.
- An element $\alpha \in A$ is a ***minimum element*** if $\forall\, a \in A$ we have $\alpha \prec a$.

Some comments seem to be in order here. A maximal element is just an element for which there is no "larger" element in the set. (The same type of thinking applies for minimal.) However, a maximum element is in fact "larger" than every other element of the set. (Again, the same type of thinking applies for minimum.) Sometimes we call a maximum element the ***last*** or ***largest*** element of the set and a minimum element is called the ***least*** or ***first*** element of the set. Note that the terms "largest" and "least" are used loosely since we are not necessarily using them in the sense of comparing sizes of numbers.

Example 3.65

Consider the relation $\ll$ on the set $A = \{1, 2, 3, 4, 5, 6\}$.

- 1 is a minimal element of A since no other element of A divides 1. We can also say that 1 is a minimum or first element of A since 1 divides every element of A.
- 4, 5, and 6 are each maximal elements since in each case no other element of A can be divided by them.
- This set has no maximum element under $\ll$.
- 2 and 3 are neither maximal nor minimal.

Example 3.66

Let A be a nonempty set and consider $\mathcal{P}(A)$ with the partial order $\subseteq$. Then $\emptyset$ is a minimum element and A is a maximum element.

We can now introduce the concept of a *well ordered* set.

Definition 3.67

Let $(A, \prec)$ be a linearly ordered set. If each non-void subset of A contains a first (minimum) element, then $(A, \prec)$ is a ***well ordered*** set.

Example 3.68

Consider the set $A = \{1, 2, \ldots, 10\}$ with the linear order the natural $\leq$ on A. Then $(A, \leq)$ is a well ordered set since one can just examine any nonempty subset and find its first element. For example, $B = \{2, 4, 6, 8, 10\}$ is a non-void subset of A and its first element is 2.

One of the most useful well ordered sets in mathematics is the set of natural numbers $\mathbb{N}$ with the linear ordering $\leq$. However, the fact that this ordering is a well-ordering, though intuitively reasonable, is assured by the **Well-Ordering Axiom**. That is, the fact that $(\mathbb{N}, \leq)$ is a well ordered set is a basic axiom (assumption) which will be discussed further in a later chapter.

Another concept which plays an important role in mathematics is the concept of *bounds* for a set.

Definition 3.69

Let $(A, \prec)$ be a partially ordered set and $B \subseteq A$. An element $x \in A$ is an ***upper bound for*** B if $b \prec x$ for each $b \in B$. Similarly, an element $y \in A$ is a ***lower bound for*** B if $y \prec b$ for each $b \in B$.

The reader should note that an upper bound (lower bound) for B need not be in B itself and certainly is not unique, even if it exists.

Example 3.70

Consider $(\mathbb{Z}, \leq)$. Let $B_1 = \{1, 2, 5, 7\}$, $B_2 = \{\ldots, -5, -4, -3, -2, -1\}$, and $B_3 = \{1, 2, 3, \ldots\}$.

- Observe B_2 has no lower bound, and x is an upper bound for B for each x with $-1 \leq x$.
- Similarly, B_3 has no upper bound, but each $y \in \mathbb{Z}$ with $y \leq 1$ is a lower bound.
- In considering B_1, there are plenty of upper bounds (any $x \in \mathbb{Z}$ with $7 \leq x$) and plenty of lower bounds (any $x \in \mathbb{Z}$ with $x \leq 1$).

Example 3.71

Consider the relation $\ll$ on the set $A = \{2, 3, 4, \ldots, 36\}$. Let $S = \{4, 6, 8, 36\}$. We see 2 is the only lower bound for S and there does not exist any upper bound.

In some situations, if one considers all the upper bounds for a subset, there exists a least element in the set of upper bounds, and that type of element is of interest.

Definition 3.72

Let $(A, \prec)$ be a partially ordered set and $B \subseteq A$. An element $x \in A$ is ***the least upper bound for*** B if

1. x is an upper bound for B, and
2. if y is any upper bound for B, then $x \prec y$.

The ***greatest lower bound*** is defined similarly.

The reader is cautioned that even if upper bounds exist, there may not be a least upper bound.

Example 3.73

Consider $(A, \ll)$ as in Example 3.71 and let $B = \{12, 18, 24\}$. Notice that 2, 3, and 6 are lower bounds for B and in fact, 6 is the greatest lower bound since $2 \ll 6$, $3 \ll 6$ and $6 \ll 6$.

Example 3.74

Consider $(A \setminus \{6\}, \ll)$ where A is defined as in Example 3.71. Then $B = \{12, 18, 24\}$ has 2 and 3 as lower bounds, but there does not exist a greatest lower bound (convince yourself that neither 2 nor 3 are the greatest lower bound).

Consider two posets $(A, \prec_A)$ and $(B, \prec_B)$. The Cartesian product, $A \times B$, is an important set which we have discussed previously. Are there some natural ways to use the orderings on A and B to create partial orderings on $A \times B$? The two most useful and natural of these are known as the ***product*** ordering and the ***lexicographic*** (or ***alphabetic***) ordering.

Definition 3.75

Let $(A, \prec_A)$ and $(B, \prec_B)$ be posets. We define the ***product ordering***, $\prec_P$, on $A \times B$ by

$$(a, b) \prec_P (c, d) \quad \text{iff} \quad a \prec_A c \text{ and } b \prec_B d.$$

Definition 3.76

Let $(A, \prec_A)$ and $(B, \prec_B)$ be posets. We define the ***lexicographic ordering***, $\prec_L$, on $A \times B$ by $(a, b) \prec_L (c, d)$ if and only if

1. $a \prec_A c$ and $a \neq c$, or
2. $a = c$ and $b \prec_B d$.

The student should think carefully about the lexicographic ordering and note that it is exactly like alphabetizing. The proof of the fact that these two orderings are indeed partial orderings on $A \times B$ is left to the reader.

Fact 3.77

Let $(A, \prec_A)$ and $(B, \prec_B)$ be posets.

1. The product ordering, $\prec_P$, is a partial ordering of $A \times B$.
2. The lexicographic ordering, $\prec_L$, is a partial ordering of $A \times B$.

3.4 Exercises

1. Consider $A = \{1, 2, 3, 5\}$ and $R = \{(1, 1), (2, 2), (3, 3), (5, 5), (2, 5), (1, 5)\}$.
   (a) Show R is a partial ordering of A.
   (b) Show R is not a linear ordering of A.
   (c) Show 1, 2, and 3 are each minimal elements of A.
   (d) Show 3 and 5 are maximal elements of A.

2. Consider $A = \{1, 2, 3, 5\}$ and consider $\mathcal{P}(A)$ with the partial ordering $\subseteq$. Find the minimum and maximum elements of $\mathcal{P}(A)$.

3. Consider $B = \mathcal{P}(A) \setminus \{\emptyset, A\}$ with the partial ordering $\subseteq$ and A defined as in Exercise #2. Find the four minimal and the four maximal elements of B.

4. Consider $\mathbb{N}$ with the natural linear ordering $\leq$. Prove $\mathbb{N}$ has a minimum element but not a maximal element.

5. Consider $\mathbb{N}$ and define $a\,R\,b$ iff $-a \leq -b$. Prove $\mathbb{N}$ has a maximum element but no minimal element.

6. Let (A, R) be a linearly ordered set and let $\alpha \in A$ be a maximal (minimal) element. Prove α is a maximum (minimum) element.

7. Prove that the linearly ordered set $(\mathbb{Z}, \leq)$ is not well ordered.

8. Prove that $(\mathbb{R}, \leq)$ is not a well ordered set by showing the set $\{x \in \mathbb{R} \,|\, 0 < x < 1\}$ does not have a first element.

9. Let $A = \{1, 2, \ldots, 36\}$ and consider $(A, \ll)$. Let $B_1 = \{10, 21\}$, $B_2 = \{1, 5, 25\}$, $B_3 = \{12, 24, 36\}$.
   (a) Find all lower bounds of B_1, B_2, and B_3.
   (b) Find all upper bounds of B_1, B_2, and B_3.
   (c) Find the the greatest lower bound and the least upper bound of B_1, B_2, and B_3 (if they exist).

10. Let A be a nonempty set and consider $(\mathcal{P}(A), \subseteq)$. If $\mathcal{B} \subset \mathcal{P}(A)$,
    (a) Prove $\displaystyle\bigcup_{B \in \mathcal{B}} B$ is an upper bound for $\mathcal{B}$
    (b) Prove $\displaystyle\bigcap_{B \in \mathcal{B}} B$ is a lower bound for $\mathcal{B}$.
    (c) Indeed, prove they are the least upper bound and greatest lower bound respectively.

11. Prove part 1 of Fact 3.77.

12. Prove part 2 of Fact 3.77.

3.5 Hasse Diagrams

Hasse diagrams are a useful and simple notational device for giving a geometric representation of partially ordered sets. These diagrams are really simplified versions of digraphs. The rules for interpreting or constructing a Hasse diagram of a partially ordered set $(A, \prec)$ are as follows:

1. ***All points of*** A ***must be placed in the Hasse diagram.*** That is, we begin in the same way as in the construction of a more general digraph.

2. If $x, y \in A$ and $x \prec y$ then x appears below y (vertically) and a line is drawn between x and y.

3. ***No arrows are drawn.*** Since every poset has the antisymmetric property, relationships between two different elements of A can go in only one "direction." From property (2), any such relationships will always be drawn from "bottom" to "top", thus eliminating the need for arrows.

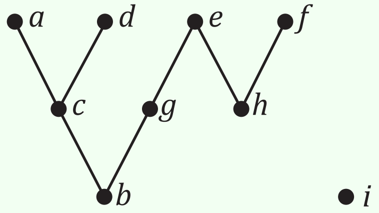
4. ***The reflexive property is not indicated.*** This is because in posets, it is known that all points are related to themselves. Thus, to indicate the reflexive property in a Hasse diagram would only clutter the picture with loops at every vertex. However, it is important to remember that each point is related to itself.

5. ***The transitive property is not indicated.*** As with the reflexive property, this is because all posets, by definition, have the transitive property. So, if there are edges from a to b and from b to c, there is no need to draw an edge from a to c because we already know a must be related to c. Again, it is important to remember transitivity.

The reader should practice drawing Hasse diagrams from a given poset. In addition, try considering a Hasse diagram and reconstructing the original set and partial ordering.

Example 3.78

Consider the Hasse diagram below



The Hasse diagram of $(A, \prec)$

In a moment we will enumerate A and $\prec$ completely, but let us first consider the Hasse diagram. Notice that the element a is above the element c and connected by a line; hence, we know $c \prec a$. Similarly, we see $c \prec d$, etc. Do you see that $b \prec a$? Note that by moving along the line from b to c and then along the line from c to a, we have an upward path connecting c to a, so $b \prec a$ because the relation is transitive. Keep in mind that the reason we did not put a direct line from b to a was to keep the diagram as uncluttered as possible. (Recall rule 2 above.) Note the c is not related to e; Although c is height-wise below e, there is not an upward sequence of lines from c to e. The element i is related only to itself (remember that lines of reflexivity are not placed on the diagram). So,

$$A = \{a, b, c, d, e, f, g, h, i\}$$

since all elements of A are in the diagram, and

$$\begin{aligned}\prec \quad = \quad & \{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),(g,g),(h,h),(i,i),(b,c),(b,a),(b,d),\\ & (b,g),(b,e),(c,a),(c,d),(g,e),(h,e),(h,f)\}\,.\end{aligned}$$

Surely, the Hasse diagram provides a clearer picture of the relationships in the poset $(A, \prec)$ than does the list of ordered pairs!

Example 3.79

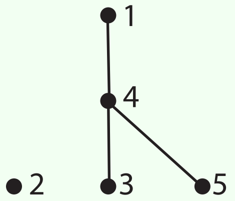
Consider the set $A = \{1, 2, 3, 4, 5\}$ and the partial ordering

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

To create the Hasse diagram, we look for "bottom" elements. Now 1 and 4 are not "bottom" elements since $5 \preceq 1$ and $3 \preceq 4$. However, 2, 3, and 5, are "bottom" elements.

What elements lie just above the bottom elements? Note that since 2 is related only to itself (which is not indicated on the diagram), 2 will not be related to any element in any row above it. Next, consider what is above 3. Now $3 \preceq 1$ and $3 \preceq 4$ so both 4 and 1 belong above 3. Further, noting that $4 \preceq 1$, we see that 4 belongs on "level two" and 1 belongs on "level three".

Finally, observe that $5 \preceq 4$, and we have the complete Hasse diagram.

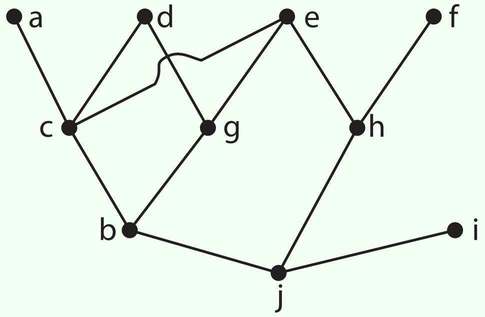


The Hasse diagram of $(A, \preceq)$

When a poset is given in Hasse diagram form it is easy to see such concepts as upper bounds for sets, lower bounds for sets, greatest lower bounds for sets, and least upper bounds for sets.

Example 3.80

Consider the poset $(A, \prec)$ given by the Hasse diagram below and the subset $B = \{c, g\}$.



The Hasse diagram of $(A, \prec)$

The reader can easily observe the following:

- j is a minimal element and, indeed, is a minimum element;
- a, d, e, and f are all maximal elements. Are these all of the maximal elements?
- In fact, i is another maximal element. (Did you find it?)
- The elements d and e are upper bounds for B and yet, B does not have a least upper bound.
- b and j are lower bounds for B, and b is the greatest lower bound.

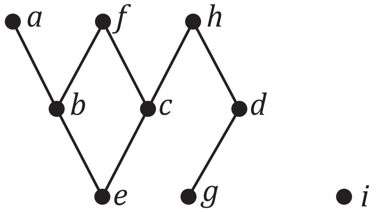
3.5 Exercises

1. Make a Hasse diagram for $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ with the ordering $\ll$.

2. From the Hasse diagram in problem 1, find all maximal, maximum, minimum, and minimal elements of A.

3. For the Hasse diagram in problem 1 and the set $B = \{2, 3\}$, find all upper bounds, lower bounds, and the glb and lub, if they exist.

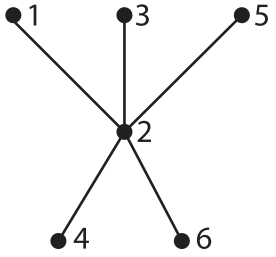
4. From the Hasse diagram below, enumerate the set and the partial ordering on that set.

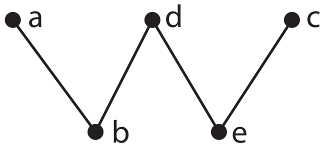


5. From the Hasse diagram in problem 4, find all maximal, maximum, minimum, and minimal elements of A.

6. For the Hasse diagram in problem 4, and the set $B = \{a, g\}$, and $D = \{a, b, c\}$, find all upper bounds, lower bounds, and the glb and lub, if they exist.

7. Consider the following Hasse diagrams of $(A, \prec_A)$ and $(B, \prec_B)$ respectively.





Questions (a) through (e) deal with $(A \times B, \prec_L)$ where is $\prec_L$ the lexicographic order.

(a) List all elements of $A \times B$ which preceed $(2, d)$.

(b) List all elements of $A \times B$ which succeed $(2, d)$.

(c) List all upper bounds for the set $D = \{(4, b), (2, d), (6, a)\}$.

(d) List all lower bounds for the set D above.

(e) If D has a lub, what is it?

Questions (f) through (j) deal with $(A \times B, \prec_P)$ where $\prec_P$ is the product order.

(f) List all elements of $A \times B$ which preceed $(2, d)$.

(g) List all elements of $A \times B$ which succeed $(2, d)$.

(h) List all upper bounds for the set $D = \{(4, b), (2, d), (6, a)\}$.

(i) List all lower bounds for the set D above.

(j) If D has a lub, what is it?

4 Functions

4.1 Basic Definitions

In Chapter 3, after defining a relation, we restricted our attention to various types of orderings and equivalence relations. We will now consider other very special and important types of relations which are called *functions*.

Definition 4.1

If A and B are sets, then the relation f from A to B is a ***function from*** A ***to*** B if whenever $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

Then a function f from A to B is a subset of $A \times B$ with the additional property that no two distinct ordered pairs in f have the same first component.

Example 4.2

Let $A = \{1, 2, 3\}$ and $B = \{6, 7, 8, 9\}$. Consider the following relations from A to B.

$$f = \{(1, 6), (2, 9), (3, 9)\}$$

$$g = \{(1, 6), (2, 7), (3, 8), (1, 9)\}$$

$$h = \{(1, 6), (2, 7)\}$$

Then f and h are functions from A to B, while g is not because $(1, 6)$ and $(1, 9)$ are elements of g, but $6 \neq 9$.

Notice in the previous example that in a function the second element in an ordered pair may repeat indefinitely. It is repetition of the first element that is not allowed. That is, each element in $\mathrm{Dom}(f)$ must be paired with a unique element of B.

4.1.1 Functional Notation

We will frequently use the following notation interchangable when studying functions.

$$f(a) = b \quad \longleftrightarrow \quad (a, b) \in f.$$

The notation on the left is a modification of the notation we previously used for images of sets under relations. Recall from Chapter 3 that if f is any relation from A to B and $\{a\} \subseteq A$, then $f(\{a\})$ is the image of $\{a\}$. When f is a function, the image of a single element set must also contain only a single element. Thus, we alter the notation slightly by omitting the brackets and write

$$f(a) = b$$

instead of

$$f(\{a\}) = \{b\}\,.$$

Since functions are sometimes called "mappings," we may say f "maps" a to b or a is "mapped" to b by f. Using this function notation, we see Definition 4.1 can be recast as:

$$f \text{ is a function from } A \text{ to } B \text{ if for } a_1, a_2 \in A,\ a_1 = a_2 \text{ implies that } f(a_1) = f(a_2);$$

that is, equal elements in A cannot map to different elements in B.

One notational device is of such convenience that we include it as a definition.

Definition 4.3

Let f be a function from A to B such that $\text{Dom}(f) = A$. Then we write $f\colon A \to B$.

Thus, when we write "$f\colon A \to B$," we are are saying three things:

1. f is a function.
2. $\text{Dom}(f) = A$
3. $\text{Ran}(f) \subseteq B$

Consider Example 4.2 and observe $f : A \to B$ is notationally correct, but $g : A \to B$ is incorrect (g is not a function) and $h\colon A \to B$ is incorrect ($\text{Dom}(h) \neq A$).

It is worth mentioning here that texts differ in their use of the notation $f\colon A \to B$ for a function. For notational purposes, we have chosen to require that a function from A to B be defined for each element of A. However, in cases where this is the only condition violated, we may correct the notation by restricting the relation to the domain. Considering h from Example 4.2, we could correctly write $h\colon \{1, 2\} \to B$.

4.1.2 Visualizing Functions

In Figures 9 and 10 below, we examine in pictorial form the implications of the definition of a function.

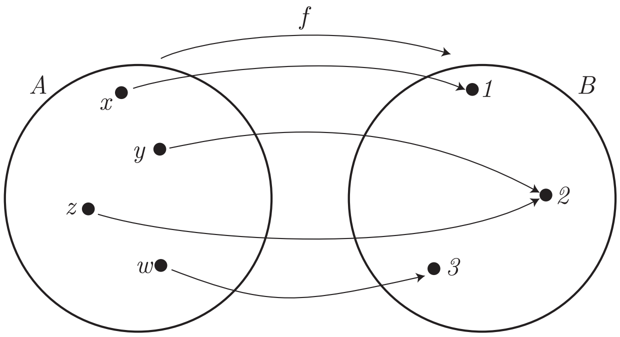


Figure 9: A function f

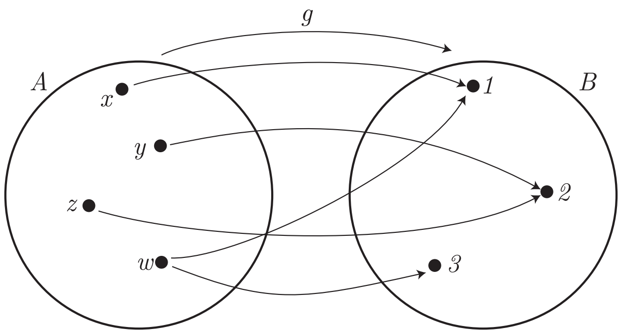


Figure 10: A non-function relation g

The relation represented in Figure 9,

$$f = \{(x,1),(y,2),(z,2),(w,3)\}\,,$$

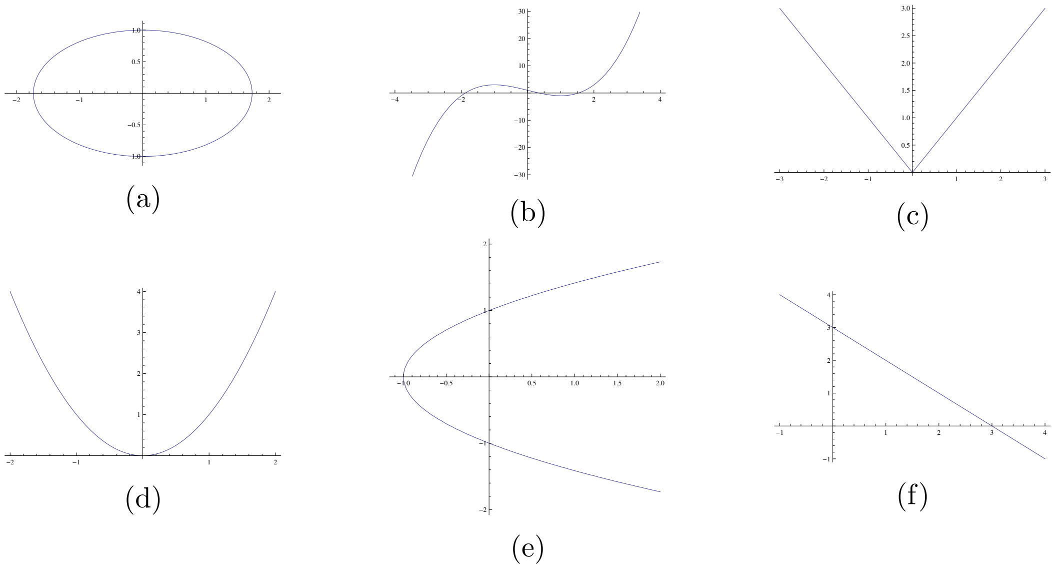
is a function since it satisfies the definition. However, the relation

$$g = \{(x,1),(y,2),(z,2),(w,1),(w,3)\}$$

is not a function since $g(\{w\}) = \{1,3\}$. In terms of the arrow diagrams above, we can make some general observations.

- A function is characterized by having the property that each element in the domain has only one exiting arrow.
- Furthermore, for function f of Figure 9, we may correctly state $f\colon A \to B$ since each element of A has an exiting arrow (so $\mathrm{Dom}(f) = A$).
- A non-function such as g can be spotted easily by looking for an element with two or more exiting arrows.

In Examples 3.4 and 3.8 we were reminded that the kinds of relations that are defined by equations relating two real numbers can be represented by a graph G: A point (a,b) being on the graph G indicates that a is related to b according to the equation defining the relation (i.e. (a,b) satisfies the defining equation of the relation). Geometrically, we may determine if a relation is a function by imagining a vertical line passing through the graph of the relation. If such a line would at any time pass through two distinct points of the graph, the relation fails to be a function since distinct points on any vertical line have the same first component but different second components. This criteria is called the ***vertical line test*** for a function. In Figure 11 all graphs except (a) and (e) represent functions.



(a) (b) (c) (d) (e) (f)

Figure 11: Which relations are functions?

It should be noted that the vertical line test is not a substitute for a proof, which we will consider shortly.

4.1.3 Relaxing Notation

If we adhered strictly to the notation of the definitions we would quickly tire of repeating things, and so we become "sloppier" notationally. However, the reader should recognize and work hard in developing the confidence to be mathematically correct in dealing with and understanding the ideas communicated. The type of relaxation we mention here is shown in the following example.

Example 4.4

Let $A = B = \mathbb{R}$ and consider

$$f = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} \,|\, y = x^2 + 1\right\}.$$

Here we have carefully specified A, B, and the relation f we wish to consider using set builder notation (since, after all, a function is a relation which is a set of ordered pairs). However, we often specify a function by simply stating its defining equation. For example, in defining f, we could simply said the following.

Consider the function $f\colon\mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 1$.

Notice that in stating $f\colon\mathbb{R} \to \mathbb{R}$, we were declaring that f is a function whose domain is $\mathbb{R}$ and whose range is contained in $\mathbb{R}$. In certain contexts where the domain is always understood to be a certain set, we may often drop stating "$f\colon\mathbb{R} \to \mathbb{R}$" and just define the function by saying

Consider the function defined by $f(x) = x^2 + 1$.

For example, in single variable calculus class, it is understood that the domain of all functions will be the largest subset of real numbers for which the function is defined. We will adopt that convention for the remainder of this textbook. That is, if we state something like

Let $f(x) = \sqrt{x^2 + 1}$,

we are declaring that f is a function whose domain is the largest subset of $\mathbb{R}$ for which the f is defined (all of $\mathbb{R}$ in this case) and whose range lies in $\mathbb{R}$.

4.1.4 Proofs that relations are or are not functions

Let us now consider some relations defined in algebraic form.

Example 4.5

Let $f(x) = 3x - 2$. Clearly $\mathrm{Dom}(f) = \mathbb{R}$. To verify f is a function, we show that if $x_1, x_2 \in \mathrm{Dom}(f)$ with $x_1 = x_2$, then $f(x_1) = f(x_2)$. Clearly, for any $x_1 = x_2$, it follows that $3x_1 - 2 = 3x_2 - 2$, so that $f(x_1) = f(x_2)$. Since this argument is valid for any choice of x_1 and x_2, it follows that f is a function. Since $\mathrm{Dom}(f) = \mathbb{R}$, we can correctly write $f\colon\mathbb{R} \to \mathbb{R}$.

Example 4.6

Let $g(x) = \dfrac{1}{x-2}$. Then

$$\mathrm{Dom}(g) = \{x \in \mathbb{R} \mid x \neq 2\} = \mathbb{R} \setminus \{2\}\,,$$

since letting $x = 2$ make the expression $\dfrac{1}{x-2}$ undefined. To verify that g is a function, suppose $x_1, x_2 \in \mathrm{Dom}(g)$ with $x_1 = x_2$. Then simple arithmetic shows us that $\dfrac{1}{x_1 - 2} = \dfrac{1}{x_2 - 2}$, and therefore $g(x_1) = g(x_2)$ as required by the definition of function. Further, we can state $g \colon \mathbb{R} \setminus \{2\} \to \mathbb{R}$.

We must emphasize that just any equation involving real numbers x and y does not define a function (or even a relation). Consider the following example.

Example 4.7

Consider the relation R defined by the equation $y^2 = x$. Since the ordered pairs $(9, 3)$ and $(9, -3)$ both satisfy the given equation (and are thus in R), but $3 \neq -3$, we conclude this relation is not a function.
Graphing the equation $y^2 = x$ would have given you some insight that it does not define a function, for it would have failed the vertical line test. However, the vertical line test is just a heuristic that can guide you to a precise explanation as to why a given relation is not a function.

4.1 Exercises

1. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 6, 9, 12, 15\}$ and consider the following relations.

$$\begin{aligned} f &= \{(1, 9), (2, 6), (3, 12), (4, 3)\} \\ g &= \{(1, 9), (2, 9), (3, 9), (4, 9), (5, 9)\} \\ h &= \{(1, 3), (2, 6), (4, 12), (5, 3)\} \\ k &= \{(x, y) \in A \times B \mid y = 3x\}. \end{aligned}$$

   Which of the relations are functions from A to B? If $D = \{3, 6, 9, 12\}$, which are functions from A to D?

2. Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{4, 6, 10, 12, 16\}$ and consider the following relations from A to B.

   - $f = \{(2, 10), (4, 12), (6, 4), (1, 10), (2, 6), (5, 16)\}$
   - $g = \{(2, 6), (4, 4), (3, 10), (1, 16), (5, 12)\}$
   - $h = \{(1, 16), (2, 12), (3, 10), (4, 6), (5, 4), (6, 16)\}$
   - $k = \{(6, 12), (5, 16), (1, 12)\}$

   (a) Which of the relations above is a function from A to B?

   (b) For which of the functions above is the notation $f : A \to B$ appropriate?

3. Let $A = \mathbb{R}$ and $B = \mathbb{R}$. Define the relation f from A to B by $f(x) = \dfrac{1}{(1-x)^2}$.

   (a) Prove that f is a function from A to B.

   (b) Is the notation $f : A \to B$ correct? If not, how could A be changed to make the notation correct?

4. Consider the following relations defined from A to B, where A and B are defined as indicated. In each case, prove or disprove that f is a function from A to B. If f is a function from A to B, determine whether or not the notation $f : A \to B$ can be used. If not, how could A be changed to make the notation correct?

   (a) $A = \mathbb{N}$, $B = \mathbb{N}$, and $f(x) = 2x$

   (b) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = \sqrt{x}$.

   (c) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = |x - 2|$.

   (d) $A = \mathbb{N}$, $B = \mathbb{N}$, and $f(n) = 7n + 5$.

   (e) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = 7x + 5$.

   (f) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = \frac{3}{1+x^2}$.

   (g) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = \sqrt{x - 3}$.

   (h) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = x^{2/3}$.

(i) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = \begin{cases} 0 & \text{if } x \in \mathbb{Q} \\ 1 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases}$

(j) $A = \mathbb{R}$, $B = \mathbb{R}$, and $f(x) = \begin{cases} 0 & \text{if } x \in \mathbb{Q} \\ 1 & \text{if } x^2 \in \mathbb{R} \setminus \mathbb{Q} \end{cases}$

5. It is usually obvious whether or not a proposed real-valued function is actually a function (e.g. $f(x) = x^2$ is well defined, but $g(x) = \pm\sqrt{1 - x^2}$ is not). Sometimes, however, it is not so obvious due to the proposed function's definition being sensitive to multiple representations of domain elements (e.g. 1/2 and 2/4 and 0.5 are multiple representations of the same real number), and so it is critical that one checks if the proposed function is "well defined" in the sense that different representations of domain elements produce the same range element. That is, you must check if $x_1, x_2 \in \text{Dom}(f)$ and $x_1 = x_2$, then $f(x_1) = f(x_2)$. With that in mind, decide whether or not the following proposed functions are well defined and prove your answer.

   (a) Define $p : \mathbb{Q} \to \mathbb{Z}$ by $p\left(\frac{a}{b}\right) = ab$.

   (b) For integer $n > 1$, define $\mathbb{Z}_n = \{\overline{a} \,|\, \overline{a} \text{ is an equivalence class with respect to } \equiv_n\}$. That is, $\mathbb{Z}_n$ is the set of equivalence classes of congruence modulo n on $\mathbb{Z}$. Recall that in $\mathbb{Z}_n$, elements may have multiple representations (e.g. in $\mathbb{Z}_5$, $\overline{2} = \overline{7}$). Next, define $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by
   $$f(\overline{a}) = \overline{a^3 - a}.$$

6. Let $f : A \to B$. Define a relation $\sim$ on A by $a_1 \sim a_2$ if and only if $f(a_1) = f(a_2)$. Show $\sim$ is an equivalence relation on A.

4.2 Properties of Functions

We will now consider some special properties of functions. Again, it is important that these definitions not only be memorized but also digested. Furthermore, the student should only proceed with the section after carefully understanding the definitions and notation from Section 4.1.

4.2.1 One-to-One Functions

Definition 4.8

A function $f : A \to B$ is ***one-to-one*** (or ***injective***), denoted ***1-1***, if for $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

That is, no distinct elements of the domain may be mapped to the same element in the range. Hence, in Example 4.2 the function f fails to be one-to-one since $f(2) = 9$ and $f(3) = 9$, but $2 \neq 3$. In Figure 11 the functions represented by the graphs in parts (b), (c), and (d) are not one-to-one since we can find distinct values in the domain which map to the same value in the range. Geometrically, such points can be found using a ***horizontal line test*** similar to the vertical line test for functions.

Example 4.9

Consider the relation defined by $f(x) = 2x^2$. Since f is defined for all real numbers and $x_1 = x_2$ implies $f(x_1) = 2x_1^2 = 2x_2^2 = f(x_2)$, we conclude f is a function. However, f is *not* one-to-one since $f(1) = 2 = f(-1)$, but $1 \neq -1$.

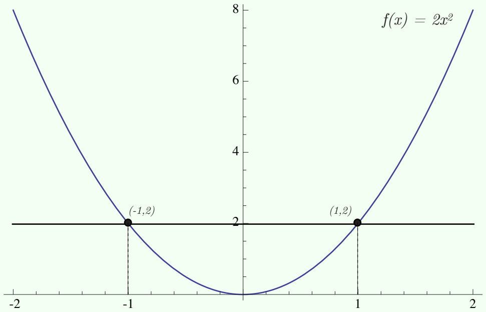


Figure 12: f is not 1-1 since it fails the horizontal line test.

Example 4.10

Let $g(x) = \sqrt{x-1}$. Then g is a function with $\mathrm{Dom}(g) = \{x \in \mathbb{R} \mid x \geq 1\}$. We prove that g is one-to-one.

Proof. Let $x_1, x_2 \in \mathrm{Dom}(g)$ and suppose that $g(x_1) = g(x_2)$.

$\Rightarrow \sqrt{x_1 - 1} = \sqrt{x_2 - 1}$

$\Rightarrow x_1 - 1 = x_2 - 1$ (Arithmetic: If $a = b$, then $a^2 = b^2$)

$\Rightarrow x_1 = x_2$ □

4.2.2 Onto Functions

Definition 4.11

A function $f\colon A \to B$ is an ***onto*** (or ***surjective***) function if $\mathrm{Ran}(f) = B$.

The idea here is that the image of A under f is all of B. That is, after mapping every element of A into B, there will be no elements of B left out. Referring to Figure 11 we note that (b) and (f) represent onto functions. Given $f : A \to B$, we already know that $\mathrm{Ran}(f) \subset B$ by definition of the notation "$f\colon A \to B$," so to prove that f is onto, one only needs to check that $B \subset \mathrm{Ran}(f)$. Equivalently,

$$f \text{ is onto} \qquad \text{iff} \qquad \forall b \in B, \exists a \in A \text{ such that } f(a) = b.$$

Example 4.12

We prove that the function $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x^3 - 5$ is onto.

Proof. Let $y \in \mathbb{R}$. Consider $x = \sqrt[3]{\dfrac{y+5}{2}} \in \mathbb{R}$. Then

$$f(x) = f\left(\sqrt[3]{\frac{y+5}{2}}\right) = 2\left(\sqrt[3]{\frac{y+5}{2}}\right)^3 - 5 = 2 \cdot \frac{y+5}{2} - 5 = (y+5) - 5 = y.$$

Therefore, f is onto. □

Example 4.13

Define $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2$. g is *not* onto because $\mathrm{Ran}(g) = [0, \infty) = \{y \in \mathbb{R} \mid y \geq 0\} \subset \mathbb{R}$. Indeed, for any $y < 0$, there does not exist $x \in \mathbb{R}$ such that $f(x) = y$ since $f(x) = x^2 \geq 0$ for all $x \in \mathbb{R}$.

Example 4.14

Define $h\colon\mathbb{R} \to [0,\infty)$ by $g(x) = x^2$. Then g is onto:

Proof. Let $y \in [0,\infty)$. Choose $x = \sqrt{y}$ and note that $x \in \mathbb{R}$ sinch $y \geq 0$. Now

$$h(x) = x^2 = (\sqrt{y})^2 = y,$$

and so h is onto. □

Note that the only difference between the previous two examples was in the specification of the set B, which is often called the "codomain." Indeed, any function $f\colon A \to B$ can be made to be onto by specifying $B = f(A)$.

4.2.3 One-to-One Correspondences (or Bijections)

Definition 4.15

A function $f\colon A \to B$ that is both one-to-one and onto is a ***one-to-one correspondence*** (or ***bijection***).

Definition 4.16

Let A be any nonempty set and define $I_A(x) = x$ for all $x \in A$. This function is a one-to-one correspondence and is called the ***identity function*** on A.

We will take the opportunity here to introduce some notation that will be studied in greater detail in Chapter 5. $\mathcal{F}(A)$ will represent the set of all functions from a nonempty set A to itself. $\mathcal{S}(A)$ will be used to represent the subset of $\mathcal{F}(A)$ whose elements are one-to-one and onto. $\mathcal{S}(A)$ is always nonempty since the identity function on A is an element of the set (since $A \neq \emptyset$).

Example 4.17

Let $A = \{a, b\}$. Define all functions on A as follows:

$\to$	I	f	g	h
a	a	a	b	b
b	b	a	b	a

Table 7: $\mathcal{F}(A)$ where $A = \{a, b\}$

We have $\mathcal{F}(A) = \{I, f, g, h\}$ and $\mathcal{S}(A) = \{I, h\}$ (Here, the table is read that $f = \{(a,a),(b,a)\}$, etc.)

4.2.4 Inverse Functions

When studying relations, we considered the idea of an inverse relation. We must be more careful when looking for inverses of functions because of the additional requirement involved.

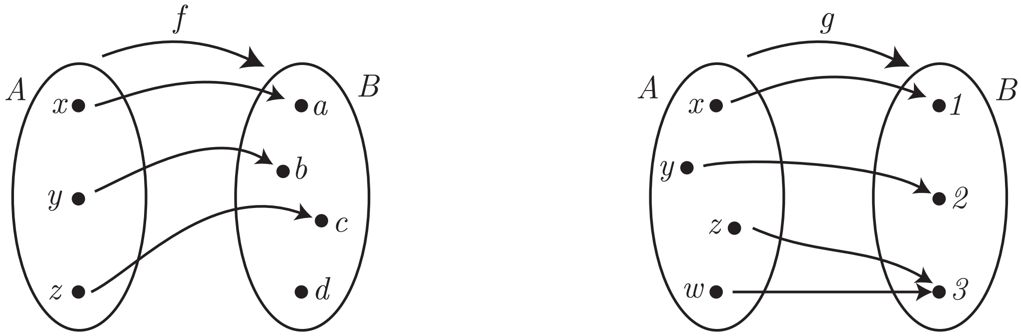


Figure 13

In Figure 13 we see that $f : A \to B$ and the arrows of f can be reversed so that f^{-1} is a function from B to A; however, f^{-1} is not defined for all values of B and so we could not write $f^{-1} : B \to A$. If we restrict the domain, we could write $f^{-1} : \{a, b, c\} \to A$ or $f^{-1}\!:\!\mathrm{Ran}(f) \to A$.

With the function g indicated in 13 we encounter a more serious problem. Notice that z and w are both mapped to 3 by the function g. Therefore, reversing the direction of the arrows would map 3 to both z and w, a violation of the definition of a function. ***Thus it is clear that while all functions have inverses, the inverses may not be functions.*** We will consider the properties a function must have to possess an inverse function. We will call such a function ***invertible***.

Theorem 4.18

Let $f\!:\!A \to B$. Then $f^{-1}\!:\!\mathrm{Ran}(f) \to A$ if and only if f is one-to-one.

Proof. Suppose $f : A \to B$ and recall that this means f is a function, $\mathrm{Dom}(f) = A$, and $\mathrm{Ran}(f) \subseteq B$.

($\Leftarrow$): Assume f is one-to-one. To prove that $f^{-1}\!:\!\mathrm{Ran}(f) \to A$, we must establish that f^{-1} is a function, $\mathrm{Dom}(f^{-1}) = \mathrm{Ran}(f)$, and $\mathrm{Ran}(f^{-1}) \subseteq B$.

- First, to show that f^{-1} is a function, suppose (b, a_1) and (b, a_2) are elements of f^{-1}. Then (a_1, b) and (a_2, b) are elements of f. Since f is one-to-one, $a_1 = a_2$. Therefore f^{-1} is a function.
- Note that since f is a relation we have $\mathrm{Dom}(f^{-1}) = \mathrm{Ran}(f)$ (by Fact 3.10).
- Finally, since f is a relation, we have $\mathrm{Ran}(f^{-1}) = \mathrm{Dom}(f) = A$, so $\mathrm{Ran}(f^{-1}) \subseteq A$ (also by Fact 3.10).

(⇒): Left as an exercise to the reader.

□

Theorem 4.19

If $f\colon A \to B$ and f is one-to-one and onto, then $f^{-1}\colon B \to A$ is one-to-one and onto.

Proof. Suppose $f\colon A \to B$ and f is one-to-one and onto. Then we must prove three things. (1) $f^{-1}\colon B \to A$, (2) f^{-1} is one-to-one, and (3) f^{-1} is onto.

1. To see that $f^{-1}\colon B \to A$, just note that since f is one-to-one, then by Theorem 4.18, $f^{-1}\colon \mathrm{Ran}(f) \to A$. Further, since f is onto, $\mathrm{Ran}(f) = B$, so now we have $f^{-1}\colon B \to A$.
2. To prove that f^{-1} is one-to-one, let $(b_1, a), (b_2, a) \in f^{-1}$. Then $(a, b_1), (a, b_2) \in f$, and since f is a function, $b_1 = b_2$.
3. To prove that f^{-1} is onto, let a be an arbitrary element of A. Consider the element $b = f(a)$ in B. That is, consider $(a, b) \in f$. Then $(b, a) \in f^{-1}$. That is, $f^{-1}(b) = a$. We have shown that an arbitrary element $a \in A$ is the image under f^{-1} of the element $b = f(a)$ in B, so f^{-1} is onto.

□

4.2 Exercises

1. Let $A = \{1,2,3,4,5\}$, $B = \{1,3,5,7,11\}$ and define

$$\begin{aligned} f &= \{(1,3),(2,5),(3,7),(4,1),(5,5)\}, \\ g &= \{(1,1),(2,3),(3,3),(4,3),(5,5)\}, \\ h &= \{(1,11),(2,7),(3,5),(4,3),(5,1)\}. \end{aligned}$$

   Which are 1-1 and onto? Give reasons.

2. For each of the functions in Exercise #1, write the inverse and decide which inverses are functions.

3. Define $f\colon \mathbb{N} \to \mathbb{N}$ by $f(n) = 2n$. Prove f is 1-1 but not onto.

4. Define $f\colon \mathbb{N} \to \mathbb{N}$ by $f(n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even} \end{cases}$. Prove f is onto but not 1-1.

5. Define $f\colon \mathbb{Z} \to \mathbb{Z}$ by $f(n) = -n$. Prove f is a bijection.

6. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = e^{3x-2}$.

   (a) Prove that f is one-to-one but not onto.

   (b) Using theorems discussed in class, what can you say about the relation f^{-1}?

7. Define $g : (0, \infty) \to \mathbb{R}$ by $g(x) = \ln x$.

   (a) Prove that g is a bijection.

   (b) Using theorems discussed in class, what can you say about the relation g^{-1}?

8. Define $h : \mathbb{R} \setminus \{2\} \to \mathbb{R} \setminus \{3\}$ by $h(x) = \dfrac{3x}{x-2}$. Prove that h is a bijection.

9. For each of the functions in 4.1 Exercises #4, prove or disprove that the function is:

   (a) 1-1,

   (b) onto.

10. Let $A = \{1,2,3\}$ and write all elements in $\mathcal{S}(A)$ in table form as in Example 4.17.

11. Consider the portion of Theorem 4.18 which states:

    Let $f\colon A \to B$. Then $f^{-1}\colon \mathrm{Ran}(f) \to A$ implies f is one-to-one.

    Prove this statement by contradiction.

12. Define $s : \mathbb{Z}_4 \to \mathbb{Z}_4$ by $s(\overline{a}) = \overline{2a}$. Decide whether or not s is 1-1 and onto and prove your answers.

13. Repeat the previous problem, but replace $\mathbb{Z}_4$ with $\mathbb{Z}_5$.

14. Let $f : \mathbb{R} \to \mathbb{R}$. We say f is *strictly increasing* if $a < b$ implies $f(a) < f(b)$. Prove that if f is strictly increasing, then f is one-to-one and f^{-1} is strictly increasing.

4.3 Compositions and Algebraic Combinations of Functions and Relations

There are numerous ways of combining functions in special cases which will be considered at the end of this section. However, the most general method involves the concept of composition. Indeed, this concept also applies to combining relations, and we will give the definition in that general context before refocusing on functions.

4.3.1 Composition of Relations

If one considers a relation R as a number of paths from the points of the set A to the points of the set B, and the relation S a number of paths from the points of the set B to the points of the set C, it is natural to attempt to connect these paths to obtain paths from the points of A to the points of C. That is precisely what the composition does.

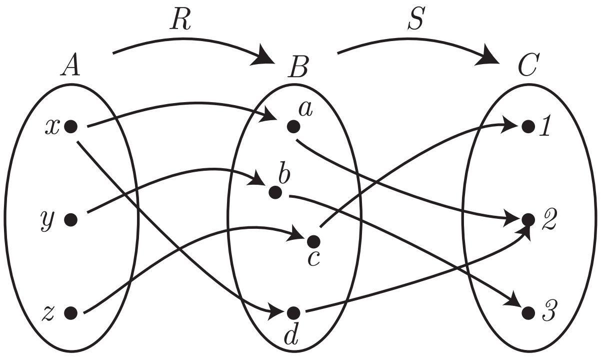


Figure 14: R is a relation from A to B and S is a relation from B to C.

Definition 4.20

Let R be a relation from A to B and S be a relation from B to C. Then the ***composition*** of R and S, denoted $S \circ R$, is defined by

$$S \circ R = \{(a, c) \in A \times C \,|\, \exists b \in B \text{ with } (a, b) \in R \text{ and } (b, c) \in S\}\,.$$

Example 4.21

Consider the relations R and S defined by the arrow diagram of Figure 14. By following the arrows from elements of A to B and then from B to C, we determine the following.

- $(x,2) \in S \circ R$ since $a \in B$ with $(x,a) \in R$ and $(a,2) \in S$.
- $(y,3) \in S \circ R$ since $b \in B$ with $(y,b) \in R$ and $(b,3) \in S$.
- $(z,1) \in S \circ R$ since $c \in C$ with $(z,c) \in R$ and $(c,1) \in S$.
- $S \circ R = \{(x,2),(y,3),(z,1)\}$

Example 4.22

Let $A = \{a,b,c,d,e\}$, $B = \{1,2,3,4,5\}$, $C = \{\alpha,\beta,\gamma\}$, with $R = \{(a,1),(a,3),(b,5),(c,4),(d,4)\}$ and $S = \{(2,\alpha),(3,\gamma),(4,\alpha),(4,\beta)\}$. Now we see from the definition that $(a,\gamma) \in S \circ R$ since $3 \in B$ with $(a,3) \in R$ and $(3,\gamma) \in S$. Checking all the possibilities, we have

$$S \circ R = \{(a,\gamma),(c,\alpha),(c,\beta),(d,\alpha),(d,\beta)\}.$$

Example 4.23

Let $A = \{a,b,c\}$, $B = \{1,2,3\}$, $C = \{\alpha,\beta,\gamma\}$ with $R = \{(a,1),(b,1),(c,1)\}$ and $S = \{(2,\beta),(2,\gamma)\}$. Using the definition we see $S \circ R = \emptyset$.

Surely, Example 4.23 is less interesting than Example 4.22, and the student, after a moment's reflection, should observe that the problem with the second example was caused by the fact that $\operatorname{Ran}(R) \cap \operatorname{Dom}(S) = \emptyset$.

That is, none of the terminal points of R were initial points of S. The desirability for starting the definition of composition in the general context of relations is two fold. First, the simplistic reason is that it is possible to do so and yields a more general framework. Secondly, there are some rather important relations which are related to functions but are not necessarily functions themselves, for example, the inverse of a function is always a relation but may not be a function.

4.3.2 Composition of Functions

Fact 4.24

If $f : A \to B$ and $g : B \to C$, then $g \circ f : A \to C$.

Proof. There are three things we must prove.

1. $\mathrm{Dom}(g \circ f) = A$.

   From the definition of $g \circ f$, it is apparent that $\mathrm{Dom}(g \circ f) \subseteq A$. To see the reverse containment, consider an arbitrary element $a \in A$. Since $\mathrm{Dom}(f) = A$, there exists $b \in B$ with $(a, b) \in f$, and since $b \in B$ and $\mathrm{Dom}(g) = B$, there exists $c \in C$ with $(b, c) \in g$. Now again, by definition of $g \circ f$, we see $(a, c) \in g \circ f$ and so $a \in \mathrm{Dom}(g \circ f)$.

2. $\mathrm{Ran}(g \circ f) \subseteq C$.

   The validity of this statement is apparent from the definition of $g \circ f$.

3. $g \circ f$ is a function.

   To verify this, suppose $(a, c_1), (a, c_2) \in g \circ f$ (we must prove $c_1 = c_2$). By definition of $g \circ f$, there exists $b_1 \in B$ with $(a, b_1) \in f$ and $(b_1, c_1) \in g$, and similarly, there exists $b_2 \in B$ with $(a, b_2) \in f$ and $(b_2, c_2) \in g$. However, $(a, b_1), (a, b_2) \in f$ implies that $b_1 = b_2$ since f is a function. Then since $(b_1, c_1) \in g$ and $(b_2, c_2) \in g$ (remember $b_1 = b_2$ and g is a function), we see $c_1 = c_2$. Thus, $g \circ f$ is a function.

□

Notation for Composition of Functions

Suppose $f\colon A \to B$, $g\colon B \to C$, and $(a, c) \in g \circ f$. Then, by definition of composition, there exists $b \in B$ such that $(a, b) \in f$ and $(b, c) \in g$. If we convert the ordered pair notation to functional notation, we have

$$(g \circ f)(a) = c. \tag{1}$$

On the other hand, we have

$$f(a) = b \text{ and } g(b) = c,$$

and by substitution we arrive at

$$g(f(a)) = c. \tag{2}$$

Thus, from Equations 1 and 2, we see

$$(g \circ f)(a) = g(f(a)). \tag{3}$$

Equation 3 gives us an iterative way to evaluate values of compositions of functions.

Example 4.25

Define $f\colon\mathbb{R} \to \mathbb{R}$ by $f(x) = 3x$ and $g\colon\mathbb{R} \to \mathbb{R}$ by $g(x) = x^2$. Then $g \circ f\colon\mathbb{R} \to \mathbb{R}$ is the new function given by

$$(g \circ f)(x) = g(f(x)) = g(3x) = (3x)^2 = 9x^2.$$

Also, $f \circ g\colon\mathbb{R} \to \mathbb{R}$ is given by

$$(f \circ g)(x) = f(g(x)) = f(x^2) = 3(x^2) = 3x^2.$$

This example points out clearly that in general, $g \circ f \neq f \circ g$. The reader should also verify that although f is a bijection, neither $f \circ g$ nor $g \circ f$ is one-to-one or onto.

Example 4.26

Define $f\colon\mathbb{R}\to\mathbb{R}$ by $f(x)=x^3$ and $g\colon\mathbb{R}\to\mathbb{R}$ by $g(x)=2x$. Then $g\circ f\colon\mathbb{R}\to\mathbb{R}$ is given by

$$(g\circ f)(x)=g(f(x))=g(x^3)=2(x^3)=2x^3$$

and $f\circ g\colon\mathbb{R}\to\mathbb{R}$ is given by

$$(f\circ g)(x)=f(g(x))=f(2x)=(2x)^3=8x^3.$$

Here, both f and g are bijections, as are $g\circ f$ and $f\circ g$.

If the student thoughtfully considers the two preceding examples, he or she is led to the following theorem.

Theorem 4.27

Let $f\colon A\to B$ and $g\colon B\to C$. Then

1. If f and g are one-to-one, then $g\circ f$ is one-to-one.
2. If f and g are onto, then $g\circ f$ is onto.

Proof.

1. Assume f and g are one-to-one. To see $g\circ f$ is one-to-one, suppose $(g\circ f)(a_1)=(g\circ f)(a_2)$. Then $g(f(a_1))=g(f(a_2))$. Since g is one-to-one, we have $f(a_1)=f(a_2)$. But f is also one-to-one, so $a_1=a_2$.
2. Assume f and g are onto. To see that $g\circ f$ is onto, let $c\in C$. We need to find some $a\in A$ such that $(g\circ f)(a)=c$. Since $c\in C$ and g is onto, there exists $b\in B$ with $g(b)=c$. Similarly, since $b\in B$ and f is onto, there exists some $a\in A$ such that $f(a)=b$. Thus we see that $(g\circ f)(a)=g(f(a))=g(b)=c$, and hence $g\circ f$ is onto.

□

To see that the converse of this theorem is not necessarily true, consider the following example.

Example 4.28

Suppose $A=\{1\}$, $B=\{x,y\}$, and $C=\{8\}$. Define $f\colon A\to B$ by $f=\{(1,x)\}$ and $g: B\to C$ by $g=\{(x,8),(y,8)\}$. Then f is one-to-one but not onto and g is onto but not one-to-one. Also, $g\circ f: A\to C$ is given by $g\circ f=\{(1,8)\}$ which is both one-to-one and onto.

This example, though extremely simple, contains much information and as such, is worth understanding and remembering. For that reason, without labeling the points, let's draw a picture of it and consider it again.

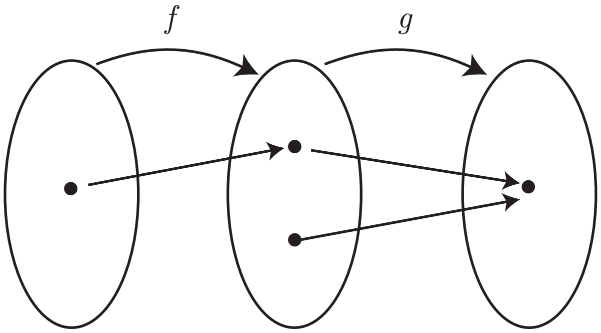


Figure 15: A simple but revealing composition of functions.

Notice that f is 1-1, g is not 1-1, $g \circ f$ is 1-1, f is not onto, g is onto, and $g \circ f$ is onto.

Although this example proves the total converse of Theorem 4.27 is not true, we can surprisingly prove a partial converse, to which we are lead by the example above.

Theorem 4.29

Let $f\colon A \to B$ and $g\colon B \to C$.

1. If $g \circ f$ is one-to-one, then f is one-to-one.
2. If $g \circ f$ is onto, then g is onto.

Proof.

1. Assume $g \circ f$ is one-to-one. To see f is one-to-one, let $f(a_1) = f(a_2)$. Then since g is a function, we have $g(f(a_1)) = g(f(a_2))$. This implies $(g \circ f)(a_1) = (g \circ f)(a_2)$. Since $g \circ f$ is one-to-one, we have $a_1 = a_2$. Therefore, f is one-to-one.
2. Assume $g \circ f$ is onto. To see g is onto, let $c \in C$. Since $g \circ f$is onto, there exists some $a \in A$ such that $(g \circ f)(a) = c$, and $(g \circ f)(a) = g(f(a))$. But $f(a) = b$ for some $b \in B$ and for that b we have $g(b) = c$. Therefore, g is onto

□

Figure 15 even indicates some additional truths. Why, in considering the 1-1 properties, was it possible for $g \circ f$ to be 1-1 and yet g is not necessarily 1-1? Recall we have proved f must be 1-1. Since f was not onto, the other element of B was "not seen" by $g \circ f$. Consider the next fact. (The proof is left as an exercise.)

Fact 4.30

Let $f\colon A \to B$ and $g\colon B \to C$. If $g \circ f$ is 1-1 and f is onto, then g must be 1-1.

Similarily, considering the onto property, the fact that $g \circ f$ is onto forces g to be onto, but not f. In Figure 15, this is possible because g is not 1-1. Again, the proof of the following fact is left for the reader.

Fact 4.31

Let $f\colon A \to B$ and $g\colon B \to C$. If $g \circ f$ is onto and g is 1-1, then f must be onto.

If the reader is not aware of the importance of examples in mathematics, surely Example 4.28 and the related Figure 15 must be impressive. Not only did the provide a counterexample of the converse of Theorem 4.27, but they also led us to a partial converse and two other additional facts. Such gems are to be saved and cherished.

The following fact, whose proof is left as an exercise, is the associative law for composition of functions (and can clearly be extended to an associative law for composition of relations).

Fact 4.32

Let $f\colon A \to B$, $g\colon B \to C$, and $h\colon C \to D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$.

Before reading the next theorem, the student should recall that $\mathcal{S}(A)$ is the set of bijections on a nonempty set A, and I_A is the identity function on A defined by $I_A(x) = x$ for all $x \in A$.

Theorem 4.33

Let A be a nonempty set and let $f \in \mathcal{S}(A)$. Then

1. $I_A \circ f = f \circ I_A = f$.
2. $f \circ f^{-1} = f^{-1} \circ f = I_A$.

The importance of the preceding theorem has to do with its connection to the subject of *abstract algebra*. Let is make note of some of the features of the set $\mathcal{S}(A)$ together with composition of functions (verify that each are true).

1. An "operation" (composition) is defined on $\mathcal{S}$: Given any two functions $f, g \in \mathcal{S}(A)$, the composition $f \circ g$ is also an element of $\mathcal{S}(A)$. That is, $\circ$ is a *binary operation* on $\mathcal{S}(A)$ (see Chapter 5).

2. Composition is *associative* by Fact 4.32.

3. There is a special function $I_A \in \mathcal{S}(A)$ called an *identity element* that, when composed with any other function $f \in \mathcal{S}(A)$, leaves f unchanged.

4. Every function $f \in \mathcal{S}(A)$ has an inverse f^{-1} that is also in $\mathcal{S}(A)$.

In abstract algebra, any set with these four properties is called a *group*. Groups are the object of much study in abstract algebra.

4.3.3 Arithmetic Combinations of Real-Valued Functions

Let us briefly consider some other possibilities for combining functions. Surely the student is aware of such things as $f+g$, $f-g$, $f\cdot g$, and f/g. What must be a setting in which these concepts make sense?

Definition 4.34

Let $f\colon A\to\mathbb{R}$ and $g\colon\mathbb{R}\to\mathbb{R}$ where $A\subseteq\mathbb{R}$. Define

$$(f+g)(x) := f(x)+g(x)$$

$$(f-g)(x) := f(x)-g(x)$$

$$(f\cdot g)(x) := f(x)\cdot g(x)$$

$$(f/g)(x) := f(x)/g(x) \text{ (provided } g(x)\neq 0)$$

(Here, ":=" reads "is definitionally equal to.") Then each of these is a function from A to $\mathbb{R}$. Consider $f+g$ and notice that to "add" functions we must have a common domain and the ability to add points in the range of the functions. Similar comments can be made about the other functions described above.

4.3 Exercises

1. Let $A = \{1, 2, 3, 4\}$, $B = \{5, 6, 7\}$, $C = \{11, 12, 13, 14, 15\}$, $R = \{(1, 6), (1, 7), (2, 5), (3, 7)\}$, and $S = \{(5, 12), (5, 15), (6, 13), (7, 13)\}$. Find $S \circ R$, R^{-1}, S^{-1}, $(S \circ R)^{-1}$, and $R^{-1} \circ S^{-1}$.

2. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = 1 - 2x$ and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^3$. Find

   (a) $(f \circ g)(0)$
   (b) $(g \circ f)(0)$
   (c) $(f \circ g)(2)$
   (d) $(g \circ f)(2)$
   (e) $(f \circ g)(x^2)$
   (f) $(g \circ f)(x + 1)$
   (g) $(f \circ g)(x)$
   (h) $(g \circ f)(x)$

3. Define $g : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 1$ and $h : [0, \infty) \to \mathbb{R}$ by $h(x) = \sqrt{x}$. Find the formula for $h \circ g$ and find $\mathrm{Dom}(h \circ g)$.

4. Let $A = \{a, b, c, d, e\}$, $B = \{1, 2, 3, 4\}$, and $C = \{\alpha, \beta, \gamma, \delta\}$ and define $f : A \to B$ and $g : B \to C$ as follows.

$$f = \{(a, 2), (b, 1), (c, 4), (d, 4), (e, 3)\} \qquad g = \{(1, \delta), (2, \alpha), (3, \gamma), (4, \beta)\}$$

   (a) Find $g \circ f$.

   (b) Is $g \circ f$ one-to-one? If so, which of f and g must be one-to-one? If not, which function is to blame for $g \circ f$ not being one-to-one? Either way, what fact from the textbook applies to this situation?

   (c) Is $g \circ f$ onto? If so, which of f and g must be onto? If not, which function is to blame for $g \circ f$ not being onto? Either way, what fact from the textbook applies to this situation?

5. Let $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4\}$, and $C = \{\alpha, \beta, \gamma, \delta, \epsilon\}$ and define $f : A \to B$ and $g : B \to C$ as follows.

$$f = \{(a, 2), (b, 1), (c, 4), (d, 3)\} \qquad g = \{(1, \delta), (2, \alpha), (3, \beta), (4, \gamma)\}$$

   (a) Find $g \circ f$.

   (b) Is $g \circ f$ one-to-one? If so, which of f and g must be one-to-one? If not, which function is to blame for $g \circ f$ not being one-to-one? Either way, what fact from the textbook applies to this situation?

   (c) Is $g \circ f$ onto? If so, which of f and g must be onto? If not, which function is to blame for $g \circ f$ not being onto? Either way, what fact from the textbook applies to this situation?

6. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 1$ and $g : [0, \infty) \to \mathbb{R}$ by $g(x) = \sqrt{x}$.

   (a) Find the formulas $f \circ g$ and $g \circ f$.

   (b) How can you tell, just from consideration of the component functions f and g, that neither $f \circ g : [0, \infty) \to \mathbb{R}$ nor $g \circ f : \mathbb{R} \to \mathbb{R}$ is onto?

(c) Just from consideration of f and g separately, can you conclude whether or not $f \circ g$ and $g \circ f$ are one-to-one?

7. Prove Fact 4.30

8. Prove Fact 4.31

9. Prove Fact 4.32.

10. Prove Theorem 4.33

4.4 Properties Functions and Relations

In Chapter 2 we developed many ways to combine subsets (union, intersection, minus, etc.). Recognizing that functions and relations just "move" sets, it is natural to ask a large number of questions about how these concepts interrelate. In this section we will state several facts (in general, leaving the proofs to the reader) which indicate some of these interrelationships. Because these facts are used frequently throughout mathematics, they deserve more attention than just being listed as problems.

Fact 4.35

Let R be a relation from A to B and S a relation from B to C. Then $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Fact 4.36

Let R be a relation on A.

1. R is symmetric if and only if $R = R^{-1}$.
2. R is transitive if and only if $R \circ R \subseteq R$.

Fact 4.37

Let $f : A \to B$ with $S_1, S_2 \subseteq A$ and $T_1, T_2 \subseteq B$. Then the following statements are true.

1. $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$.
2. $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$.
3. $f^{-1}(T_1 \setminus T_2) = f^{-1}(T_1) \setminus f^{-1}(T_2)$.
4. $f^{-1}(\overline{T_1}) = \overline{f^{-1}(T_1)}$.
5. $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$.
6. $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$.
7. If f is one-to-one, then $f(S_1 \cap S_2) = f(S_1) \cap f(S_2)$.
8. $(f^{-1} \circ f)(S_1) \supseteq S_1$.
9. If f is one-to-one, then $(f^{-1} \circ f)(S_1) = S_1$.
10. $(f \circ f^{-1})(T_1) \subseteq T_1$.
11. If f is onto (or more generally, if $T_1 \subseteq \text{Ran}(f)$), then $(f \circ f^{-1})(T_1) = T_1$.

Proof. We provide a sample proof of part (5) and leave the rest for the student.

($\subseteq$): To see $f(S_1 \cup S_2) \subseteq f(S_1) \cup f(S_2)$, let $b \in f(S_1 \cup S_2)$. Then $(a, b) \in f$ for some $a \in S_1 \cup S_2$. By definition of union, $a \in S_1$ or $a \in S_2$. Then either $b \in f(S_1)$ or $b \in f(S_2)$. In either case, $b \in f(S_1) \cup f(S_2)$, and we have shown that $f(S_1 \cup S_2) \subseteq f(S_1) \cup f(S_2)$.

($\supseteq$): If $b \in f(S_1) \cup f(S_2)$, then $b \in f(S_1)$ or $b \in f(S_2)$. This implies $(a_1, b) \in f$ for some $a_1 \in S_1$, or $(a_2, b) \in f$ for some $a_2 \in S_2$. So we must have $a_1 \in S_1 \cup S_2$ or $a_2 \in S_1 \cup S_2$. Therefore, $(a_1, b) \in f$ for some $a_1 \in S_1 \cup S_2$ or $(a_2, b) \in f$ for some $a_2 \in S_1 \cup S_2$. Either way, $b \in f(S_1 \cup S_2)$ and we have proven that $f(S_1 \cup S_2) \supseteq f(S_1) \cup f(S_2)$.

Thus, we have established the desired equality by double inclusion. □

Fact 4.38

Let $f : A \to B$ and let $\{S_\alpha\}_{\alpha \in I}$ be a family of subsets of A.

1. $f\left(\bigcup_{\alpha \in I} S_\alpha\right) = \bigcup_{\alpha \in I} f(S_\alpha)$
2. $f\left(\bigcap_{\alpha \in I} S_\alpha\right) \subseteq \bigcap_{\alpha \in I} f(S_\alpha)$

Fact 4.39

Let $f : A \to B$ and let $\{T_\alpha\}_{\alpha \in I}$ be a family of subsets of B.

1. $f^{-1}\left(\bigcup_{\alpha \in I} T_\alpha\right) = \bigcup_{\alpha \in I} f^{-1}(T_\alpha)$
2. $f^{-1}\left(\bigcap_{\alpha \in I} T_\alpha\right) = \bigcap_{\alpha \in I} f^{-1}(T_\alpha)$

4.4 Exercises

1. Prove Fact 4.35.
2. Prove part (1) of Fact 4.36
3. Prove part (2) of Fact 4.36.
4. Prove part (1) of Fact 4.37.
5. Prove part (2) of Fact 4.37.
6. Prove part (3) of Fact 4.37.
7. Prove part (4) of Fact 4.37.
8. Prove part (6) of Fact 4.37.
9. Give a counterexample for equality in part (6) of Fact 4.37. (Hint: Look at part (7).)
10. Prove part (7) of Fact 4.37.
11. Prove part (8) of Fact 4.37.
12. Give a counterexample for equality in part (8) of Fact 4.37. (Hint: Look at part (9).)
13. Prove part (9) of Fact 4.37.
14. Prove part (10) of Fact 4.37.
15. Give a counterexample for equality in part (10) of Fact 4.37.. (Hint: Look at part (11).)
16. Prove part (11) of Fact 4.37.
17. Prove Fact 4.38
18. Prove Fact 4.39

5 Binary Operations

5.1 Basic Definitions

The concept of functions is extremely important throughout all branches of mathematics and the student has been strongly encouraged to understand functions well since they are such an important building block. One type of function which the student has encountered throughout mathematics (possibly without recognizing it as such) is the binary operation.

Definition 5.1

Let S be a nonempty set. If $*: S \times S \to S$, then $*$ is called a ***binary operation*** on S. Notationally, we usually write $s_1 * s_2 = s_3$ instead of the more cumbersome $*((s_1, s_2)) = s_3$, or the even more cumbersome (but technically correct) $((s_1, s_2), s_3) \in *$.

If the reader examines the definition of binary operation he will see it assigns to each ordered pair in $S \times S$ another point of S. A host of examples should rush into your mind, but before listing a few of these many examples, let us investigate this definition carefully.

If we wish to show $*: S \times S \to S$, what things must we show? We must show $*$ is a function with the appropriate range and domain.

We first consider the problem of showing $*$ is a function. Recall that this means each element of $S \times S$ has a unique image. Technically we must show if two ordered pairs of $*$ have the same first components, then they must have the same second component. Caution: the ordered pairs of $*$ look like $((s_1, s_2), s_3)$; that is, they are ordered pairs where first components are themselves ordered pairs. In this light, suppose $((s_1, s_2), s_3)$, and $((t_1, t_2), t_3)$ are elements of $*$ with the same first components. Since they have the same first components, we have $(s_1, s_2) = (t_1, t_2)$, which means $s_1 = t_1$ and $s_2 = t_2$. Based on that assumption we must show $s_3 = t_3$ to prove $*$ is a function. Restating this in less cumbersome notation,we must show that if $s_1 = t_1$ and $s_2 = t_2$, then $s_1 * s_2 = t_1 * t_2$.

The problem of checking range and domain require we show any two elements of S can be starred ($\text{Dom}(*) = S \times S$) and will yield an element of S ($\text{Ran}(*) = S$). Usually these properties are apparent and follow from the definition of $*$ but must be checked.

Example 5.2

If $+$ is usual addition of integers, then $+$ is a binary operation on $\mathbb{Z}$. Though we have not defined "usual addition," the student certainly is willing to believe equals added to equals are equal (i.e. $+$ is a function), that any two integers can be added (i.e. the domain of $+$ is $\mathbb{Z} \times \mathbb{Z}$), and the result will yield an integer (i.e. the range of $+$ is $\mathbb{Z}$).

Example 5.3

If $\div$ is usual division of real numbers, then $\div$ is not a binary operation on $\mathbb{R}$. Why? We are all aware we cannot divide by zero. But if we eliminate that problem we do have a binary operation on $\mathbb{R} \setminus \{0\}$?

Example 5.4

Define $*$ on $\mathbb{Q}$ by $\frac{a}{b} * \frac{c}{d} = \frac{a+c}{b}$. Is $*$ a binary operation on $\mathbb{Q}$? Surely two rationals can be starred and will yield a rational number (so the domain and range of $*$ are as required for a binary operation on $\mathbb{Q}$), so this is not our problem. But is $*$ a function? No, since we see

$$\frac{1}{2} * \frac{2}{3} = \frac{3}{2}, \qquad \text{but} \qquad \frac{1}{2} = \frac{2}{4} \text{ and } \frac{2}{3} = \frac{6}{9} \qquad \text{and yet} \qquad \frac{2}{4} * \frac{6}{9} = \frac{8}{4}.$$

If the student is not precisely clear on this discussion, please start reading this chapter again carefully, noting the subtleties involved, considering more examples, and asking questions. The following fact enumerates a number of examples of binary operations familiar to the reader. Although the reader probably understands and agrees with most of these, the proofs would require rigorous definitions of the binary operations listed which we have not given except for $\cap$, $\cup$, and set difference, $\setminus$.

Fact 5.5

Each of the following is true.

1. $+$ is a binary operation on $\mathbb{Z}$; that is, $+ \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
2. $\cdot$ is a binary operation on $\mathbb{Z}$; that is, $\cdot \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
3. $-$ is a binary operation on $\mathbb{Z}$; that is, $- \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
4. $+$, $-$, and $\cdot$ are a binary operations on $\mathbb{Q}$.
5. $+$, $-$, and $\cdot$ are a binary operations on $\mathbb{R}$.
6. $\div$ is a binary operation on $\mathbb{Q} \setminus \{0\}$.
7. $\div$ is a binary operation on $\mathbb{R} \setminus \{0\}$.
8. $\cup$ is a binary operation on $\mathcal{P}(S)$.
9. $\cap$ is a binary operation on $\mathcal{P}(S)$.
10. $\setminus$ is a binary operation on $\mathcal{P}(S)$.

Before investigating properties of binary operations, one more example is needed. As we will see, this example has some very interesting properties and will be extremely important in later mathematics courses.

Definition 5.6

If A is a nonempty set,

$$\mathcal{S}(A) = \{f : A \to A \mid f \text{ is a bijection}\}$$

is called the ***symmetric group*** on A. The elements of $\mathcal{S}(A)$ are called ***permutations*** of A. In the special case where $A = \{1, 2, \dots, n\}$, $\mathcal{S}(A)$ is denoted S_n.

Fact 5.7

$\circ$ is a binary operation on $\mathcal{F}(A)$ and on $\mathcal{S}(A)$.

Proof. Surely any two functions from A to A can be composed and will yield a function from A to A, so the range and domain of $\circ$ are appropriate. Let $f, g, h, k \in \mathcal{F}(A)$ with $f = h$ and $g = k$, which means $f(x) = h(x)$ and $g(x) = k(x)$ for all $x \in A$. Surely then, for any $x \in A$, we have $(g \circ f)(x) = g(f(x)) = g(h(x)) = k(h(x)) = (k \circ h)(x)$. Hence, equals composed with equals are equal and we can conclude $\circ$ is a binary operation on $\mathcal{F}(A)$.

Since Theorem 4.29 assures us that the composition of bijections from A to A is a bijection from A to A, we can conclude $\circ$ is a binary operation on $\mathcal{S}(A)$. □

Permutations play a significant role in many diverse areas of mathematics. It will be useful for the student to become adept at manipulating permutations and increasing understanding of some of their properties. The remainder of this section will focus on elements of S_n . Consider the following permutations $f, g, h \in S_6$.

f	g	h
$1 \mapsto 4$	$1 \mapsto 2$	$1 \mapsto 6$
$2 \mapsto 3$	$2 \mapsto 4$	$2 \mapsto 5$
$3 \mapsto 1$	$3 \mapsto 3$	$3 \mapsto 2$
$4 \mapsto 6$	$4 \mapsto 1$	$4 \mapsto 3$
$5 \mapsto 2$	$5 \mapsto 6$	$5 \mapsto 1$
$6 \mapsto 5$	$6 \mapsto 5$	$6 \mapsto 4$

A much simplier way to write permutations is to use "double line" notation, a notation in which the domain elements are written on the first line and the corresponding images are written below. For example, f, g, and h from above would be written

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}, \; g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}, \text{ and } h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 3 & 1 & 4 \end{pmatrix}.$$

Not only is it easier to write permutations this way, but certainly doing manipulations is easier. For example,

$$[(f \circ g) \circ h](5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 3 & 1 & 4 \end{pmatrix} (5) = 3.$$

Here, as each function is applied, the current result is "fed" into the top and the new result "falls out" the bottom. The process is continued until the final image is determined. Indeed, by allowing the functions to operate in a similar manner in each of the domain elements 1, 2, 3, 4, 5, and 6, we see that

$$(f \circ g) \circ h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 1 & 3 & 4 \end{pmatrix}$$

This double line notation easily deals with the concept of inverses since we need only interchange the lines to indicate the reversed roles of domain and range elements. Of course, if for esthetic reasons we want to sort the new first row into some other order, we can.

$$f^{-1} = \begin{pmatrix} 4 & 3 & 1 & 6 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 1 & 6 & 4 \end{pmatrix}$$

If one simply remembers that the inverse is just the "flip," then calculations are easy, as seen in the next example.

Example 5.8

Consider the following calculation in S_5.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$$

Notice that in the second and third factors we "fed" the resulting current value in the bottom row and got the next "current value" in the top row because those factors were inverses. Thus, we accomplished the "flip" without actually physically interchanging rows.

Some permutations are particularly nice. Before defining this type of permutation formally, let us make sure the reader understands some notation. Let $f \in S_n$ and $k \in \mathbb{N}$. Then by f^k, we mean f composed with f, k times; i.e.,

$$f^k = \underbrace{f \circ f \circ \cdots \circ f}_{k \text{ times}}.$$

Example 5.9

Consider $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 4 & 2 & 3 & 6 & 7 & 8 \end{pmatrix} \in S_8$

Observe $f(1) = 1$, $f(6) = 6$, $f(7) = 7$, and $f(8) = 8$. So 1, 6, 7, and 8 are fixed by f. Thus, we see that $f^k(1) = 1$ for every $k \in \mathbb{N}$. Similary, f^k fixes 6, 7, and 8. But what about the elements that are not fixed by f?

$$f(2) = 5, f^2(2) = 3, f^3(2) = 4, \text{ and } f^4(2) = 2.$$

So we see that 2 has cycled back to itself with four applications of f. Also note that four applications of f to 3, 4, and 5 also cycle back to 3, 4, and 5, respectively. This example motivates the next definition.

Definition 5.10

Let $f \in S_n$ and $A = \{1, 2, 3, \ldots, n\}$. If there exists an element $x \in A$ such that

$$A = \left\{f^1(x), f^2(x), f^3(x), \ldots\right\} \cup \{a \in A \,|\, f(a) = a\},$$

then f is called a ***cycle***. If $k > 1$ is the smallest integer such that $f^k(x) = x$, then f is called a cycle of ***length*** k.

Cycles can be represented using "single-line" notation as follows: If f is a cycle of length k, we write

$$f = (x, f(x), f^2(x), f^3(x), \ldots, f^{k-1}(x)).$$

Here, all elements of A that do not appear in the single line notation for f are fixed by f. Any number appearing in the single line notation for a cycle f is mapped to the number appearing immediately to its right, with the exception of the last number which maps to the first number. This notation is made clear by the next example.

Example 5.11

The permutation of Example 5.9 is a cycle of length 4, and we write

$$f = (2, 5, 3, 4).$$

This notation means

$$\begin{aligned} f(2) &= 5 \\ f(5) &= 3 \\ f(3) &= 4 \\ f(4) &= 2 \\ f(1) &= 1 \\ f(6) &= 6 \\ f(7) &= 7 \\ f(8) &= 8 \end{aligned}$$

Thus, the very simple notation (2, 5, 3, 4) thus communicates a great deal of information in a really compact form. Finally, the reader should note that $f = (2, 5, 3, 4) = (5, 3, 4, 2) = (3, 4, 2, 5) = (4, 2, 5, 3)$.

How does this new single line notation handle the concept of inverses? Instead of moving right, simply move left. Using the cycle f from the preceeding example, we see that $f^{-1} = (2, 5, 3, 4)^{-1}$, which takes 5 to 2, 3 to 5, 4 to 3, and 2 to 4. (Here we hit the left most element, and so we looped to the far right end). Of course, if we wanted to, we could rewrite f^{-1} as

$$f^{-1} = (2, 5, 3, 4)^{-1} = (4, 3, 5, 2) = (3, 5, 2, 4) = (5, 2, 4, 3) = (2, 4, 3, 5).$$

Fortunately, as we will see in Theorem 5.14, this single line notation is useful in dealing with any permutation. But first we introduce a new definition and theorem.

Definition 5.12

Let $f = (a_1, a_2, \ldots, a_k)$ and $g = (b_1, b_2, \ldots, b_m)$ be cycles in S_n. Then f and g are called ***disjoint cycles*** if $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_m\} = \emptyset$ are disjoint sets. That is, f and g do not move (map to something different) any of the same elements.

Example 5.13

Consider $f, g, h \in S_9$ defined by $f = (2,4,5,3,7)$, $g = (1,6,8)$, and $h = (4,5,9,6)$. Now f and g are disjoint cycles, but h is not disjoint from f since both map 4 other than to itself. Similarly, g and h are not disjoint since both map 6 other than to itself.

Theorem 5.14

If $f = (a_1, a_2, \ldots, a_k)$ and $g = (b_1, b_2, \ldots, b_m)$ are disjoint cycles in S_n, then $f \circ g = g \circ f$. That is, disjoint cycles commute.

Proof. To see $f \circ g = g \circ f$, we must show that these two functions do the same thing to each $x \in \{1, 2, 3, \ldots, n\}$. So let $x \in \{1, 2, 3, \ldots, n\}$.

Case 1: $x \in \{1, 2, 3, \ldots, n\} \setminus (\{a_1, a_2, \ldots, a_k\} \cup \{b_1, b_2, \ldots, b_m\})$. In this case x is fixed by both f and g, so,

$$(f \circ g)(x) = f(g(x)) = f(x) = x = g(x) = g(f(x) = (g \circ f)(x).$$

Case 2: $x \in \{a_1, a_2, \ldots, a_k\}$. Since f and g are disjoint, $x \notin \{b_1, b_2, \ldots, b_m\}$, so x is fixed by g. Thus,

$$(f \circ g)(x) = f(g(x)) = f(x) = g(f(x)) = (g \circ f)(x)$$

since $f(x) \in \{a_1, a_2, \ldots, a_k\}$ and so is fixed by g.

Case 3: $x \in \{b_1, b_2, \ldots, b_m\}$. Since f and g are disjoint cycles, $x \notin \{a_1, a_2, \ldots, a_k\}$, so x is fixed by f. Now

$$(f \circ g)(x) = f(g(x)) = g(x) = g(f(x)) = (g \circ f)(x)$$

since $g(x) \in \{b_1, b_2, \ldots, b_m\}$ and so is fixed by f. □

We are now ready to see how this single line notation impacts all permutations.

Theorem 5.15

Every permutation in S_n can be expressed as a product of disjoint cycles.

A rigorous proof of Theorem 5.15 requires the use of mathematical induction (see Chapter 6), so such a proof will not be given here. However, we can describe the procedure for expression a permutation as a product of disjoint cycles.

Step 1: Let x be any element not fixed by f (if no such element exists, then f fixes all elements of $\{1, 2, \ldots, n\}$ and can be expressed as $f = (1)$, the trivial cycle). Then consider the sequence of elements $x, f(x), f^2(x), \ldots$. Since there are only a finite number of elements in $\{1, 2, ..., n\}$, this list must eventually repeat some element. Assume that the first element which repeats is $f^{k_1}(x)$. Since $f^{k_1}(x)$ is a repeat of some element appearing earlier in the list, we claim that, in fact, $f^{k_1}(x) = x$, since if not, $f^{k_1}(x) = f^j(x)$ where $j \in \{1, 2, \ldots, k_1 - 1\}$ and so $f(f^{k_1-1}(x)) = f^{k_1}(x) = f^j(x) = f(f^{j-1}(x))$. But note that $f^{k_1-1}(x) \neq f^{j-1}(x)$ since f^{k_1} was the first element in the list to repeat. That is, $f^{k_1}(x) = f^j(x)$ would contradict the fact that f is 1-1. Therefore, the cycle $(x, f(x), f^2(x), \ldots, f^{k_1-1}(x))$ is part of f.

Step 2: Let y be any element not in $\left\{x, f(x), f^2(x), \ldots, f^{k_1-1}(x)\right\}$ that is not fixed by f (if no such element exists, $f = (x, f(x), f^2(x), \ldots, f^{k_1-1}(x))$ and we are done). Then using the same logic as in Step 1, we identify a cycle $(y, f(y), f^2(y), \ldots, f^{k_2-1}(y))$ that is disjoint from $(x, f(x), f^2(x), \ldots, f^{k_1}(x))$ and is also a part of f.

If we repeat Step 2 until no non-fixed elements of $\{1, 2, \ldots, n\}$ remain, then the resulting cycles constitute the required product of disjoint cycles that equals f.

Example 5.16

Consider

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 5 & 4 & 3 & 8 & 7 & 6 & 2 & 9 & 14 & 12 & 13 & 10 & 11 \end{pmatrix} \in S_{14}.$$

Starting with 1, we have the cycle (1). Recalling that in single line notation we usually do not even write elements which map to themselves, we will disregard this cycle. Then starting with 2, we get the cycle $(2, 5, 8)$. We see that 3 is the smallest integer not checked so far; starting with 3, we obtain the cycle $(3, 4)$. Next, 6 is the smallest integer not found in any of the cycles created to this point; starting with 6, we get $(6, 7)$. Noting that 9 is fixed by f, we will next start with 10. The result is the cycle $(10, 14, 11, 12, 13)$. All the elements having been used, the final result is

$$f = (2, 5, 8) \circ (3, 4) \circ (6, 7) \circ (10, 14, 11, 12, 13).$$

Since disjoint cycles commute and cycles can notationally be started any place in the loop, we could write many other equivalent forms of the result. For example,

$$f = (3, 4) \circ (10, 14, 11, 12, 13) \circ (6, 7) \circ (2, 5, 8) = (3, 4) \circ (8, 2, 5) \circ (6, 7) \circ (14, 11, 12, 13, 10).$$

The next example shows how any composition of non-disjoint cycles can be expressed as a product of disjoint cycles.

Example 5.17

Consider the product $(3,2)\circ(4,2,1,9,7)\circ(6,5,4)\circ(9,5,6,7)\circ(1,3,5,9,4)$ in S_9. The simplest form of this product can be calculated as follows.

$$(3,2)\circ(4,2,1,9,7)\circ(6,5,4)\circ(9,5,6,7)\circ(1,3,5,9,4)=(1,2)\circ(3,5)\circ(4,9,6).$$

If you are not following the calculation above, be sure to remember that you feed an element in from the right, apply each function to the current domain element, and proceed with that result to the next function on the left. For example, to see where this product maps 1, you would do the following calculation.

$$\begin{aligned}
&((3,2)\circ(4,2,1,9,7)\circ(6,5,4)\circ(9,5,6,7)\circ(1,3,5,9,4))\,(1)=\\
&((3,2)\circ(4,2,1,9,7)\circ(6,5,4)\circ(9,5,6,7))\,(3)=\\
&((3,2)\circ(4,2,1,9,7)\circ(6,5,4))\,(3)=\\
&((3,2)\circ(4,2,1,9,7))\,(3)=\\
&(3,2)(3)=\\
&2
\end{aligned}$$

So the composition takes 1 to 2 as indicated in the result above. Of course, one can determine that that the composition takes 1 to 2 by visually "chasing" the images of 1, moving from right to left across the product of cycles. In a similar way, you can see the composition takes 2 to 1, creating the first cycle above.

5.1 Exercises

1. Determine whether $*$ as defined below is a binary operation on the given set.

   (a) $a * b = a^b$ on $\mathbb{N}$.

   (b) $a * b = a^b$ on $\mathbb{Z}$.

   (c) $a * b = b$ on $\mathbb{N}$.

   (d) $a * b = |a| \cdot b$ on $\mathbb{R}$.

   (e) $a * b = a\sqrt{b}$ on $\mathbb{R}$.

   (f) $a * b = ab + 1$ on $\mathbb{Z}$.

   (g) $a * b = a^2 + b^2$ on $\mathbb{Z}$.

   (h) $a * b = ab + b^2$ on $\mathbb{Z}$.

   (i) $a * b = 3$ on $\mathbb{Z}$.

   (j) $a * b = a + \frac{b}{2}$ on $\mathbb{Z}$.

   (k) $a * b = a^2 b$ on $\mathbb{Z}$.

   (l) $a * b = \sqrt{ab}$ on $\mathbb{Z}$.

   (m) $a * b = a + b - 3$ on $\mathbb{Z}$.

2. Define $*$ on $\mathbb{Z}$ by $a * b = a + 2b$. Prove $*$ is a binary operation on $\mathbb{Z}$.

3. Prove part (8) of Fact 5.5.

4. Prove part (9) of Fact 5.5.

5. Prove part (10) of Fact 5.5.

6. Define $\triangle$ on $\mathcal{P}(S)$ by $A \triangle B = (A \setminus B) \cup (B \setminus A)$ for all $A, B \in \mathcal{P}(S)$. Prove $\triangle$ is a binary operation on $\mathcal{P}(S)$.

7. Let

   $$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}, \text{ and } h = (4, 3, 5, 7, 8)$$

   be permutations in S_9.

   (a) Express f and g in single line notation.

   (b) Find the single line form as a product of disjoint cycles of $f \circ g \circ h^{-1}$.

   (c) Use the double line notation to express g^{-1}. Using that result, write g^{-1} as a product of disjoint cycles.

   (d) Use the expression of g in single line notation and write g^{-1} . Compare the answers from this problem the previous problem.

8. Express

   $$(2, 4, 6, 5) \circ (9, 1, 7) \circ (8, 4, 3) \circ (2, 5, 7, 9) \circ (5, 4, 9, 7, 6, 8)$$

   as a product of disjoint cycles.

5.2 Properties of Binary Operations

In studying binary operations and their impact on mathematics we need to introduce some of their properties.

Definition 5.18

Let $*$ be a binary operation on S. We say $*$ is ***commutative*** if and only if for all $s, t \in S$ we have $s * t = t * s$. We say $*$ is ***associative*** if and only if for all $r, s, t \in S$ we have $(r * s) * t = r * (s * t)$.

Example 5.19

Of the binary operations enumerated in Fact 5.5 we see $+$ and $\cdot$ on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are commutative, while $-$ and $\div$ fail to be commutative. For example, $2 + 3 = 3 + 2$; in general $m + n = n + m$ for all $m, n \in \mathbb{Z}$, and $2 \cdot 3 = 3 \cdot 2$; in general, $m \cdot n = n \cdot m$ for all $m, n \in \mathbb{Z}$, and yet $2 - 3 \neq 3 - 2$ and $6 \div 2 \neq 2 \div 6$.

Example 5.20

A rather important class of noncommutative examples is given by considering $(\mathcal{S}(A), \circ)$. Specifically, if $A = \{1, 2, 3\}$ with $f, g \in S_3$ defined by

$$f = (1, 2, 3) \text{ and } g = (2, 3),$$

then

$$g \circ f = (1, 3) \text{ while } f \circ g = (1, 2),$$

so $g \circ f \neq f \circ g$.

Example 5.21

Of the binary operations in Fact 5.5 we have $+$, $\cdot$, $\cup$, and $\cap$ are associative, while $-$ and $\div$ are not associative. For example,

- $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{Z}$,
- $A \cup (B \cup C) = (A \cup B) \cup C$ for all $A, B, C \in \mathcal{P}(S)$,
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{R}$, and
- $A \cap (B \cap C) = (A \cap B) \cap C$ for all $A, B, C \in \mathcal{P}(S)$.

Yet,

- $(1 - 3) - 5 = -7 \neq 3 = 1 - (3 - 5)$ and
- $\frac{1}{2} \div \left(\frac{1}{3} \div \frac{1}{4}\right) = \frac{3}{8} \neq 6 = \left(\frac{1}{2} \div \frac{1}{3}\right) \div \frac{1}{4}$.

We should comment that on $\mathcal{S}(A)$, $\circ$ is an associative (see Fact 4.32) though, in general, noncommutative binary operation.

The reader is aware of some rather special elements in various sets as related to a binary operation on these sets. The definition below introduces those concepts in a general context.

Definition 5.22

Let $*$ be a binary operation on S. If $e \in S$ and $e * s = s * e = s$ for all $s \in S$, then e is called an ***identity*** of S with respect to (or under) $*$.

Example 5.23

- 0 is an identity under $+$ on $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$),
- 1 is an identity under $\cdot$ on $\mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$),
- $\emptyset$ is an identity under $\cup$ on $\mathcal{P}(S)$, and
- S is an identity under $\cap$ on $\mathcal{P}(S)$.

A moment's reflection convinces us that $-$ and $\div$ on $\mathbb{Q}$ and $\mathbb{Q}\setminus\{0\}$ respectively do not have an identity since $\nexists a \in \mathbb{Q}$ with $a - x = x - a = x$ for all $x \in \mathbb{Q}$, and $\nexists b \in \mathbb{Q} \setminus \{0\}$ with $b \div x = x \div b = x$ for all $x \in \mathbb{Q} \setminus \{0\}$.

One habit the student should be attempting to develop is that of asking reasonable questions and at least attempting to answer them. For example, might there be more than one identity for a binary operation $*$ on S? In that vein, after searching the examples at hand (a good first step in understanding any problem), we find at most one identity in each case. So we begin to believe that maybe there is always at most one. One natural approach to convincing ourselves would be to assume there are two identities, say e_1 and e_2, for a set S under $*$. Now

$e_1 * e_2 = e_1$ since e_2 is an identity, and yet

$e_1 * e_2 = e_2$ since e_1 is an identity,

so we see that $e_1 = e_2$ since $*$ is a function. Thus, we have answered this question and in so doing proven the following theorem.

Theorem 5.24

Let $*$ be a binary operation on a set S. If there exists an identity for S under $*$, then it is unique.

A word of caution: 0 and 1 are both identities for the set $\mathbb{Z}$, but with respect to different binary operations.

Now that we are aware of identities and binary operations on sets, another related concept should enter the reader's mind.

Definition 5.25

Let $*$ be a binary operation on a set S with identity e under $*$, and let $s \in S$. If there exists $t \in S$ with $s * t = t * s = e$, then t is said to be an ***inverse*** for s under $*$. We use the notation s^{-1} to denote the inverse of s.

Note: At times, alternative notation is used for the inverse of an element with respect to a specific operation. For example, -2 denotes the inverse of 2 with respect to $+$.

Example 5.26

For $\mathbb{Z}$ under $+$ we see 0 is the identity and each element $m \in \mathbb{Z}$ has an inverse $-m$ under addition. For example, $2 + (-2) = (-2) + 2 = 0$, and in general, $m + (-m) = (-m) + m = 0$ for $m \in \mathbb{Z}$.

Example 5.27

For $\mathbb{Q}$ under $\cdot$ we see 1 is the identity, but not every element has an inverse. Why? Don't forget 0! Surely every nonzero element has an inverse. To see this, consider $\frac{a}{b} \in \mathbb{Q}$ with $\frac{a}{b} \neq 0$. Recall b is never 0 in a rational number $\frac{a}{b}$, and since $\frac{a}{b} \neq 0$, we have $a \neq 0$, so and $\frac{b}{a} \in \mathbb{Q}$ and

$$\frac{b}{a} \cdot \frac{a}{b} = 1.$$

However, since $0 \cdot x = x \cdot 0 = 0$ we note 0 cannot have an inverse under multiplication.

Again the question of uniqueness arises and is answered in the following theorem.

Theorem 5.28

Let $*$ be an associative binary operation on S with identity e. If $s \in S$ has an inverse, then it is unique.

Proof. Assume there are two inverses for s, say b and c. Now

$$\begin{aligned}
b =& e * b && \text{since } e \text{ is the identity} \\
=& (c * s) * b && \text{since } c * s = e \\
=& c * (s * b) && \text{since } * \text{ is associative} \\
=& c * e && \text{since } s * b = e \\
=& c && \text{since } e \text{ is the identity.}
\end{aligned}$$

□

Fact 5.29

Consider $\mathcal{S}(A)$ under $\circ$.

1. $\circ$ is commutative on $\mathcal{S}(A)$ if and only if A has fewer than three elements.
2. $\circ$ is associative on $\mathcal{S}(A)$.
3. I_A is the identity for $\mathcal{S}(A)$ under $\circ$ where $I_A(x) = x$ for all $x \in A$.
4. For each $f \in \mathcal{S}(A)$, there exists an inverse, $f^{-1} \in \mathcal{S}(A)$.

This proof is left as an exercise for the student.

Another word frequently used when speaking of binary operations is the term closed. Consider $*\colon S \times S \to X$ and recall this means $*$ is a function which assigns an element of X to each pair of elements of S. In this situation, is $*$ a binary operation on S? The answer is yes, if $X \subseteq S$, because the product of two elements of S would be in S. That is, S is "closed" under $*$. This concept seems almost pointless when applied to S itself but becomes very useful when one is considering subsets of S. After the following definition we will consider some examples.

Definition 5.30

Let $*$ be a binary operation on a set S and $T \subseteq S$. We say T is ***closed*** under $*$ if $t_1 * t_2 \in T$ for all $t_1, t_2 \in T$.

Fact 5.31

Let $*$ be a binary operation on S and $T \subseteq S$. Then T is closed under $*$ if and only if $*$ is a binary operation on T.

Proof.
($\Rightarrow$): Assume $*$ is a binary operation on T. Then surely $*\colon T \times T \to T$ means $t_1 * t_2$ for all $t_1, t_2 \in T$, so T is closed under $*$.

($\Leftarrow$): Assume T is closed under $*$. Then since $*$ is a function from $S \times S$ to S and $T \times T \subseteq S \times S$, $*$ is a function from $T \times T$. So when one restricts the domain of $*$ to $T \times T$, the range of $*$ is a subset of T because T is closed under $*$. Hence, $*\colon T \times T \to T$ and so $*$ is a binary operation on T. □

The essence of this concept of closed is that in showing a binary operation already defined on a larger set is in fact a binary operation on a subset, we must simply show closure.

One final concept deals with the situation where we have two binary operations, $*$ and $\triangle$ on a set S.

Definition 5.32

Let $*$ and $\triangle$ be binary operations on a set S.

- We say $*$ ***distributes on the left*** with respect to $\triangle$ if $a*(b\triangle c) = (a*b)\triangle(a*c)$ for all $a, b, c \in S$.
- We say $*$ ***distributes on the right*** with respect to $\triangle$ if $(b\triangle c)*a = (b*a)\triangle(c*a)$ for all $a, b, c \in S$.
- In the case that $*$ is both left and right distributive with respect to $\triangle$, we drop the adjective left or right and state $*$ ***distributes*** with respect to $\triangle$.

Example 5.33

Consider usual $+$ and $\cdot$ on $\mathbb{Z}$. Now $+$ is not distributive with respect to $\cdot$ since

$$17 = 2 + (3 \cdot 5) \neq (2+3) \cdot (2+5) = 35.$$

However, $\cdot$ does distribute with respect to $+$ since

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

and

$$(b+c) \cdot a = b \cdot a + c \cdot a$$

for all $a, b, c \in \mathbb{Z}$.

The following fact is a restatement of Parts (11) and (12) of Fact 2.16.

Fact 5.34

Consider $\cup$ and $\cap$ as binary operations on $\mathcal{P}(S)$. Then $\cup$ distributes with respect to $\cap$ and $\cap$ distributes with respect to $\cup$.

5.2 Exercises

1. Prove $\cup$ and $\cap$ are commutative binary operations on $\mathcal{P}(S)$.

2. Prove $\div$ is not commutative on $\mathbb{Q} \setminus \{0\}$.

3. Prove $\cap$ is associative on $\mathcal{P}(S)$.

4. Prove $\setminus$ is not associative on $\mathcal{P}(S)$.

5. For each legitimate binary operation $*$ in Section 5.1, Exercise #1, decide whether or not $*$ is commutative and associative and prove your answer.

6. For each legitimate binary operation $*$ in Section 5.1, Exercise #1, decide if there is an identity element and find it if there is one.

7. Define $*$ on $\mathbb{Z}$ by $a * b = a + b + 2$.

   (a) Prove that $*$ is a binary operation on $\mathbb{Z}$.

   (b) Find the identity element and prove that it is an identity for $*$.

   (c) For an arbitrary element $a \in \mathbb{Z}$, find a^{-1} and prove that a^{-1} is an inverse of a with respect to $*$.

8. Prove case (1) of Fact 5.29.

9. Prove case (2) of Fact 5.29.

10. Prove case (3) of Fact 5.29.

11. Prove case (4) of Fact 5.29.

12. Prove $\nexists$ an identity for $\mathcal{P}(S)$ with the binary operation $\setminus$.

13. Consider $\cdot$ on $\mathbb{Z}$ and recall 1 is the multiplicative identity. Which elements have inverses under multiplication?

14. Does $\div$ distribute on the left with respect to addition on $\mathbb{Q} \setminus \{0\}$?

15. Does $\div$ distribute on the right with respect to addition on $\mathbb{Q} \setminus \{0\}$?

6 Properties of the Integers

6.1 Fundamentals

This section is devoted to summarizing many properties of the integers which the student has encountered throughout his mathematics studies. In Chapter 2 we defined $\mathbb{Z}$ and $\mathbb{N}$ to be the sets of integers and natural numbers (positive integers) respectively. Although we have not, nor do we intend to do so now, defined addition, subtraction, multiplication, or division, we assume that the student is familiar with those concepts. (Note: In this chapter, all variables, unless otherwise indicated, will represent integers.)

Furthermore, in Chapter 5 we commented on some of the other properties those binary operations satisfy on $\mathbb{Z}$. For the sake of clarity we will summarize those properties in the following theorem which we will assume lies in the base of knowledge of the reader.

Theorem 6.1

Addition ($+$) and multiplication ($\cdot$) are both binary operations on the set of integers ($\mathbb{Z}$) and satisfy the following properties.

1. Both are commutative binary operations; that is, $a + b = b + a$ and $ab = ba$ for all $a, b \in \mathbb{Z}$.

2. Both are associative binary operations; that is, $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{Z}$.

3. Both operations have identities. That is, 0 is an identity under addition because $0 + a = a + 0 = a$ for all $a \in \mathbb{Z}$, and 1 is an identity under multiplication because $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}$.

4. Under addition each element has an inverse; that is, for $a \in \mathbb{Z}$, there exists $(-a) \in \mathbb{Z}$ such that $a + (-a) = 0 = (-a) + a$.

5. Multiplication distributes with respect to addition. That is, for all $a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = ab + ac$ and $(a + b) \cdot c = ac + bc$.

It should be noted that the only elements of $\mathbb{Z}$ which have inverses under multiplication are 1 and -1. Although subtraction is also a binary operation on $\mathbb{Z}$, it certainly is not commutative or associative and there does not exist an identity under subtraction. Certainly, the situation for division is even worse. Indeed, division is not even a binary operation on $\mathbb{Z}$ since, for example, 2 divided by 5 is not an integer. However, in some cases we do have that "a" divided by "b" is an integer and we have denoted those cases by "$b|a$". The use of the vertical line is intended to be distinct from "a/b" which is the commonly used notation for rational numbers where, in fact, any two integers (divisor $\neq 0$) can be divided.

Another important property of $\mathbb{Z}$ is the fact that it is ordered with the usual concept of order which is familiar to the reader. We will denote that usual order by $<$. There is, however, another ordering of $\mathbb{Z}$ which we used several times in earlier chapters. It is the ordering defined by $a \ll b$ if $a|b$. For the purpose of understanding the material in this chapter, a rigorous knowledge of "ordering" is not required. However, such a careful presentation is found in Sections 3.4 and 3.3. With these thoughts in mind we can carefully investigate some old friends.

Definition 6.2

For $x, y \in \mathbb{Z}$, $x \neq 0$, suppose there exists $n \in \mathbb{Z}$ with $x \cdot n = y$. Then we say x is a ***divisor*** of y or that y is a ***multiple*** of x. Furthermore, if x is a divisor of both y and z we say x is a ***common divisor*** of y and z, and similarily, if k is a multiple of x and y we say k is a ***common multiple***. Clearly, these concepts apply to common divisors (or multiples) of more than two integers.

Comment: Another way to see the concepts in the definition above is to note that $n \ll x$ means n is a divisor of x or that x is a multiple of n. Thus if $n \ll x$ and $n \ll y$, then n is a common divisor of x and y. Similarily, if $x \ll y$ and $z \ll y$, then y is a common multiple of x and z.

Example 6.3

It is a simple observation that 4 is a common divisor of 12, 28, 36, and 44, and that 140 is a common multiple of 2, 5, and 7. Using the notation of the preceding comment we could write $4 \ll 12$, $4 \ll 28$, $4 \ll 36$, and $4 \ll 44$ to denote that 4 is a common divisor of 12, 28, 36, and 44. Similarly, we could write $2 \ll 140$, $5 \ll 140$, and $7 \ll 140$ to denote that 140 is a common multiple of 2, 5, and 7.

We now state a fact listing some familiar applications of these concepts. The proofs are left to the student.

Fact 6.4

Let $a, b, c, d, e \in \mathbb{Z}$ with $a, b \neq 0$. Then each of the following statements is true.

1. If $a|c$ and $a|d$, then $a|(c+d)$.
2. If $a|c$, then $a|(cd)$
3. If $a|b$ and $b|c$, then $a|c$.

Two concepts that the reader has encountered earlier are the concepts of the *greatest common divisor* and that of the *least common multiple*. In attempting to define those concepts the obvious first thought is to choose amongst the common divisors the greatest and that would be the greatest common divisor. But which concept of greatest do we want to use, $<$ or $\ll$? In fact, it doesn't really matter, since both yield the same result. However, the student will see later that the concept is a more easily used tool if one uses $\ll$ to pick the greatest.

Definition 6.5

Let $m, n \in \mathbb{Z}$ (not both zero). An integer k is said to be the ***greatest common divisor*** (gcd) of n and m if

1. $k > 0$,
2. k is a common divisor of n and m, and
3. if s is any common divisor of n and m, then $s|k$.

Notationally, we will write $k = (n, m)$ or $k = \gcd\{m, n\}$. Clearly, this definition can be applied to more than two integers. If $(m, n) = 1$, m and n are said to be ***relatively prime***.

A few comments are necessary.

1. Restating this definition using the notation $\ll$ we have that $k = \gcd\{m, n\}$ if
   (a) $k > 0$,
   (b) $k \ll m$ and $k \ll n$, and
   (c) if s is any common divisor of m and n then $s \ll k$.

2. In the definition we talked about "the" gcd and indeed, that was intentional. If, in fact, there were two integers s and t which both satisfied the properties of being a gcd, then each would divide the other and both are positive. Hence, they would have to be equal. Another way to think of this is that $s \ll t$ and $t \ll s$, and since $\ll$ is a partial ordering, the antisymmetric property guarantees that $s = t$. Thus, the gcd is unique if it exists.

3. The ultimate answer as to the existence of the gcd is provided in Section 6.3. However, the student should note that the restriction that not both n and m are zero was necessary. To see this, observe that if both m and n are zero, then every positive integer divides them; hence, there can be no greatest.

Example 6.6

Consider each of the following sets of integers and its gcd.

- $\gcd\{0, -14\} = 14$.
- $\gcd\{28, 35\} = 7$.
- $\gcd\{60, -378, 396\} = 6$.
- 6 and 35 are relatively prime since $\gcd\{6, 35\} = 1$.

Definition 6.7

Let $m, n \in \mathbb{Z}$ with $m, n \neq 0$. An integer k is said to be the ***least common multiple*** (lcm) of m and n if

1. $k > 0$,
2. k is a common multiple of m and n, and
3. if s is any common multiple of m and n, then $k|s$.

Notationally, we will write $k = \operatorname{lcm}\{m, n\}$. Clearly, this definition can be applied to more than two integers.

A set of comments paralleling those made for gcd could be made about the lcm; however, we will leave it to the reader do so.

Example 6.8

Consider each of the following sets of integers and its corresponding lcm.

- $\operatorname{lcm}\{21, 28\} = 84$.
- $\operatorname{lcm}\{6, 17, -15\} = 510$.

Definition 6.9

A positive integer $p > 1$ is said to be ***prime*** if its only positive integer divisors are 1 and p.

As usual we should observe several things. First, note that 1 is a special integer when one considers multiplication. Indeed, it is the multiplicative identity. While it is positive and its only positive divisor is 1, it is excluded from being a prime by the requirement that a prime number must be greater than 1. Another viewpoint of a prime is obtained by considering the ordering $\ll$. In that light, a positive integer $p > 1$ is a prime if $n \in \mathbb{Z}$, $n > 1$, and $n \ll p$ implies $n = p$.

Example 6.10

Each of the integers 2, 5, 7, 11, 13 are primes, while each of the integers 4, 6, 8 fails to be prime since each is divisible by 2. The integers -2, -3, -19 fail to be prime since they are not positive.

6.1 Exercises

1. Find three common divisors and three common multiples for each of the following sets and then find the gcd and the lcm of each set.

   (a) $\{-42, 14, 64, 36\}$

   (b) $\{18, -10, -6\}$

   (c) $\{-48, 54, 15, 6\}$

2. Show that if $n = 0$ or $m = 0$, then there does not exist a common multiple of m and n, and so certainly not an lcm.

3. Find all primes less than 100.

4. Write the numbers 2, 62, 89, 1002, and 975 as products of positive powers of primes. (For example, $60 = 2^2 \cdot 3 \cdot 5$.)

5. Prove part (1) of Fact 6.4. Hint: Distributive law.

6. Prove part (2) of Fact 6.4.

7. Prove part (3) of Fact 6.4.

8. Prove that if the $\operatorname{lcm}\{m, n\}$ exists, it is unique.

9. Consider $(\mathbb{N} \setminus \{1\}, \ll)$ and let $x \in \mathbb{N} \setminus \{1\}$. Prove that x is prime if and only if x is a minimal element of $\mathbb{N} \setminus \{1\}$.

6.2 Mathematical Induction

The usual order $\leq$ of $\mathbb{N}$ has the property that each non-void subset has a first or least element. Such orders are called "well-orderings" and though the reader does not need a rigorous knowledge of well-orderings to understand this section, such a careful presentation is available in Section 3.4. We mentioned that $\mathbb{N}$ is a well ordered set and although that fact is intuitively reasonable, it must be assumed as a basic axiom.

Axiom 6.11: Well Ordering Axiom

$(\mathbb{N}, \leq)$ is a well ordered set.

The following is not a proof of the Well Ordering Axiom but rather an attempt to indicate its intuitive reasonableness. Consider a nonempty subset, A, of $\mathbb{N}$. Since $A \neq \emptyset$, there exists some integer $n \in A$. Now either n is the first element of A (and we are finished) or there exists some element of A which is less than n. Continuing this process at most n times we must find the first element of A. Why this argument fails to prove the Well Ordering Axiom is very subtle and lies in the ability to choose an element from a nonempty set. For our purposes it is sufficient that the Well Ordering Axiom seems reasonable and is one of our basic assumptions.

We can prove the WOA applies to some slightly more general sets.

Fact 6.12

Let r be a fixed integer and let $A_r = \{n \in \mathbb{Z} \,|\, n \geq r\}$. Then A_r is a well ordered set under the natural ordering.

Proof.
Case 1: If $r > 0$, then A_r itself is a non-void subset of $\mathbb{N}$ and so well ordered by the Well Ordering Axiom.

Case 2: If $r \leq 0$, then to see that A_r is well ordered we must consider an arbitrary nonempty subset of A_r, say B. Now let us define

$$D_r = \{b - r + 1 \,|\, b \in B\}\,.$$

Then $B \neq \emptyset$ implies $D \neq \emptyset$. Now $b - r + 1 \geq r - r + 1 = 1$ for all $b \in B$, making D_r a nonempty subset of $\mathbb{N}$. Hence, by the Well Ordering Axiom, D_r has a first element, say x, and the proof is easily completed by showing that $x + r - 1$ is the first element of B. (See problem 4 in Exercises 6.2.) □

There are many statements which are consequences of the Well Ordering Axiom. In this section, we prove two of the most useful, the two principles of mathematical induction.

Theorem 6.13: The First Principle of Mathematical Induction (FPMI)

Let r be a fixed integer and let $P(n)$ be a statement for each integer $n \geq r$. If

1. $P(r)$ is true, and
2. for integer $k \geq r$, $P(k)$ implies $P(k+1)$,

then $P(n)$ is true for all $n \geq r$.

Proof. Let $r \in \mathbb{Z}$ be a fixed integer and suppose

1. $P(n)$ is a statement for each integer $n \geq r$,
2. $P(r)$ is true, and
3. for each integer $k \geq r$, $P(k)$ implies $P(k+1)$.

Define

$$S = \{n \in \mathbb{Z} \,|\, n \geq r \text{ and } P(n) \text{ is false}\}.$$

If S can be shown to be void, then the proof is complete. Suppose $S \neq \emptyset$; then it is a nonempty subset of the well ordered set $A_r = \{n \in \mathbb{Z} \,|\, n \geq r\}$ (see Fact 6.12). As such, S has a first element, say k. Now $k \in S$, and since $P(r)$ is true, we must have $k > r$. So $r \leq k - 1 < k$. Remember, k was the first element of S, so $k \in S$ and $P(k-1)$ is true. So by supposition 3 above, we are assured that $P(k) = P((k-1)+1)$ is true, which is a contradiction to our choice of k. Then our assumption that $S \neq \emptyset$ must be false, forcing S to be void. Thus, $P(n)$ is true for all integers $n \geq r$. □

The student should pause for a moment to reflect on the power of this theorem. The First Principle of Mathematical Induction (FPMI) allows one to prove infinitely many statements are true by proving only that two statements are true! We will provide examples that show how to use FPMI to prove an infinite sequence of statements $P(r), P(r+1), P(r+2), \ldots$ are all true, but first we state and prove an equivalent formulation of FMPI that is often useful.

Theorem 6.14: The Second Principle of Mathematical Induction (SPMI)

Let r be a fixed integer and let $P(n)$ be a statement for each integer $n \geq r$. If

1. $P(r)$ is true, and
2. $P(m)$ being true for all integers m satisfying $r \leq m < k$ implies that $P(k)$ is true,

then $P(n)$ is true for all $n \geq r$.

Proof. Let $r \in \mathbb{Z}$ be a fixed integer and suppose

1. $P(n)$ is a statement for each integer $n \geq r$,
2. $P(r)$ is true, and
3. $P(m)$ being true for all integers m satisfying $r \leq m < k$ implies that $P(k)$ is true.

Define

$$S = \{n \in \mathbb{Z} \,|\, n \geq r \text{ and } P(n) \text{ is false}\}\,.$$

If S can be shown to be void, then the proof is complete. Suppose $S \neq \emptyset$; then it is a nonempty subset of the well ordered set $A_r = \{n \in \mathbb{Z} \,|\, n \geq r\}$ (see Fact 6.12). As such, S has a first element, say k. Now $k \in S$, and since $P(r)$ is true, we must have $k > r$. So $P(m)$ must be true for all m such that $r \leq m < k$ (recall k was the first element of S). Part (3) of our assumption guarantees that $P(k)$ is true, and this contradiction forces S to be empty. Thus, we have proven $P(n)$ is true for all $n \geq r$. □

Before we consider some proofs using the induction principles, we should observe a few things. In both principles, the choice of r (the *base case*) is up to the student subject to two restrictions. Of course, we must have $P(n)$ be a statement for every $n \geq r$ and we must choose r such that $P(r)$ is true. For example, if we consider the propositional function $P(n)$ which states $n^2 > 8$, then in fact, $P(n)$ is a statement for each $n \in \mathbb{N}$. However, the first value of $n \in \mathbb{N}$ for which $P(n)$ is true is $r = 3$. Now we have $P(3)$ is true and that $P(n)$ is a statement for each $n \geq r = 3$.

The main difference between FPMI and SPMI lies in the condition 2; in FPMI, one must show that the truth of $P(k)$ implies the truth of $P(k+1)$, whereas in SPMI, one must show that the truth of $P(r)$, $P(r+1)$, …, and $P(k-1)$ implies the truth of $P(k)$. So, in SPMI, condition 2 simply has more hypotheses. These additional hypotheses are often not needed or used, and in these cases FPMI is the prefered method. Below, we will demonstrate proofs using both principles, and it is hoped that through these examples and further practice, the student will learn how to choose the appropriate method for particular proofs.

Example 6.15

Prove that $n^2 > 8$ for all integers $n \geq 3$.

Proof. (by induction on n) Let $P(n)$ be the sentence "$n^2 > 8$." Clearly $P(n)$ is a statement for all $n \in \mathbb{Z}$, and in particular for $n \geq 3$.

base case: $n = 3$. $P(3)$ is the statement "$3^2 > 8$," which is clearly true.

inductive step: Suppose k is an integer such that $k \geq 3$. We wish to prove that if $P(k)$ is true, then $P(k+1)$ must be true as well. To prove this conditional statement, suppose $P(k)$ is true; that is, suppose $k^2 > 8$ (this is called the *inductive hypothesis*). Now observe that

$$\begin{aligned}(k+1)^2 &= k^2 + 2k + 1 \\ &> 8 + 2k + 1 && \text{(Since } k^2 > 8 \text{ by our inductive hypothesis)} \\ &> 8 && \text{(Since } k \geq 3 \text{ implies } 2k+1 > 0\text{)}\end{aligned}$$

We have demonstrated that if $P(k)$ is true (i.e. $k^2 > 8$ is true), then $P(k+1)$ is true (i.e. $(k+1)^2 > 8$ is true).

Therefore by FPMI, $n^2 > 8$ for all integers $n \geq 3$. □

If the proposition function $P(n)$ is clear from the context of the problem, we can shorten our exposition in our proofs somewhat by avoiding explicitly labeling this statement by "$P(n)$," as in the following example.

Example 6.16

Prove that for all integers $n \geq 1$,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. (by induction on n)

base case: $n = 1$. If $n = 1$, the statement to be proven is the statement

$$1 = \frac{1(1+1)}{2},$$

which is evidently true.

inductive step. Suppose $k \geq 1$ and that the statement is true for $n = k$. That is, suppose

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

We wish to prove on the basis of this assumption that the equation is true for $n = k+1$. Observe that

$$\begin{aligned} 1 + 2 + 3 + \cdots + (k+1) &= (1 + 2 + 3 + \cdots + k) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \qquad \text{(by the inductive hypothesis)} \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{k^2 + 3k + 2}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)[(k+1)+1]}{2} \end{aligned}$$

Thus, if the statement is true for $n = k$, then it is also true for $n = k+1$, and by FPMI, the equation is true for all integers $n \geq 1$. □

For the next two example, we use SPMI, which is also known as the *strong form of induction.*

Example 6.17

Prove that for every $n \in \mathbb{N}$,

$$24|(2 \cdot 7^n + 3 \cdot 5^n - 5).$$

Proof. As with proofs using FPMI, proofs using strong induction have a base case and an inductive step. The main difference is that in the inductive step, the inductive hypothesis includes more assumptions.

base cases: $n = 1$ and $n = 2$. In strong induction proofs, it is often helpful to establish a few base cases (it will become clear why in the inductive step). First, let us note that when $n = 1$, then $2 \cdot 7^n + 3 \cdot 5^n - 5 = 24$ and it is clear that 24 divides this quantity. Additionally, if $n = 2$, $2 \cdot 7^n + 3 \cdot 5^n - 5 = 168 = 24 \cdot 7$, and 24 divides the quantity.

inductive step. Let $k > 2$ and suppose that for every integer m satisfying $1 \leq m < k$, we have $24|(2 \cdot 7^m + 3 \cdot 5^m - 5)$. Then

$$\begin{aligned}
2 \cdot 7^k + 3 \cdot 5^k - 5 &= 2 \cdot 7^2 \cdot 7^{k-2} + 3 \cdot 5^2 \cdot 5^{k-2} - 5 \\
&= 98 \cdot 7^{k-2} + 75 \cdot 5^{k-2} - 5 \\
&= (24 \cdot 4 + 2)7^{k-2} + (24 \cdot 3 + 3)5^{k-2} - 5] \\
&= 24(4 \cdot 7^{k-2} + 3 \cdot 5^{k-2}) + [2 \cdot 7^{k-2} + 3 \cdot 5^{k-2} - 5]
\end{aligned}$$

Clearly 24 divides the first term of this last sum, and $24|(2 \cdot 7^{k-2} + 3 \cdot 5^{k-2} - 5)$ by the inductive hypothesis since $k > 2$ implies $1 \leq k - 2 < k$. Thus, by part 1 of Fact 6.4, $24|(2 \cdot 7^k + 3 \cdot 5^k - 5)$.

Thus, by SPMI, $24|(2 \cdot 7^n + 3 \cdot 5^n - 5)$ for all $n \in \mathbb{N}$. □

Example 6.18

Define a sequence of natural numbers $\{a_n\}$ as follows:

$$\begin{aligned} a_1 =& 1, \\ a_2 =& 3, \text{ and} \\ a_n =& a_{n-2} + 2a_{n-1} \text{ for } n > 2. \end{aligned}$$

Definitions such as this are called *recursive definitions*, or we would say the a_n's are *defined recursively*. We prove that a_n is odd for every $n \in \mathbb{N}$.

Proof.

base cases: $n = 1$ and $n = 2$. Clearly the statement is true for $n = 1$ and $n = 2$.

inductive step Let $k > 2$ and suppose a_m is odd for all integers m such that $1 \leq m < k$. Now $a_k = a_{k-2} + 2a_{k-1}$, and since $1 \leq k - 2 < k - 1 < k$, a_{k-1} and a_{k-2} fall under the inductive hypothesis, we know that a_{k-1} and a_{k-2} are both odd. Thus, there exist integers i and j such that $a_{k-1} = 2i + 1$ and $a_{k-2} = 2j + 1$. Now

$$a_k = a_{k-2} + 2a_{k-1} = 2j + 1 + 2(2i + 1) = 2(j + i + 1) + 1,$$

which is odd.

Thus, SPMI assures that a_n is odd for all $n \in \mathbb{N}$. □

6.2 Exercises

1. Use mathematical induction to prove each of the following propositional functions is true for all $n \geq r$, where r is the smallest nonnegative integer for which the statement is true.

   (a) $2 + 4 + 6 + \cdots + 2n = n(n+1)$

   (b) $1 + 3 + 5 + \cdots + (2n-1) = n^2$

   (c) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

   (d) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$

   (e) $1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}\dfrac{n(n+1)}{2}$

   (f) $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$

   (g) $3|(n^3 - n)\ \forall n \geq 1$.

   (h) $3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = \dfrac{3(5^{n+1}-1)}{4}$

   (i) $3|(n^3 + 2n)$

   (j) $5|(n^5 - n)$

   (k) $6|(n^3 - n)$

   (l) $21|(4^{n+1} + 5^{2n-1})$

   (m) $9|(10^n + 3 \cdot 4^{n+2} + 5)$

   (n) $64|(9^n - 8n - 1)$

   (o) $8|(3^{2n} - 1)$

2. A sequence is defined recursively by

$$\begin{aligned} &x_1 = 1, \\ &x_2 = 2, \text{ and} \\ &x_n = x_{n-1} + 2x_{n-2} \text{ for } n \geq 3. \end{aligned}$$

   Conjecture a formula for x_n and use the 2nd Principle of Mathematical Induction to prove your conjecture is correct.

3. Recall that the definition of a^n where $n \in \mathbb{N}$ is $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ times}}$. Prove the following exponent laws by induction.

   (a) $a^n a^m = a^{m+n}$ Hint: Fix arbitrary $m \in \mathbb{N}$ and induct on n.

   (b) $(a^n)^m = a^{nm}$

4. Consider the algebraic expression

$$(x+y)^n = \sum_{r=0}^{n} a_r x^{n-r} y^r,$$

where $a_r = \frac{n!}{(n-r)!r!}$. Prove that this formula is true for $n \in \mathbb{N}$.

5. Complete the proof of Fact 6.12 by showing that $x + r - 1$ is the first element of B.

6. For finite set A, define $n(A)$ to be the number of elements of A. Prove that if $n(A) = 1$ and $n(B) = n$, then $n(A \times B) = 1 \cdot n$.

7. Having completed the previous problem, use induction on the number of elements of A to prove that if $n(A) = m$ and $n(B) = n$, then $n(A \times B) = m \cdot n$.

8. Use mathematical induction to prove the following.

   (a) $(n+1)(n!) = (n+1)!$ for $n \geq 0$

   (b) $2^n < n!$ for all $n \geq 4$.

   (c) $(n+1)! > 2^{n+3}$ for all $n \geq 5$

   (d) $n! < n^n$ for all $n \geq 2$.

   (e) $\dfrac{n!}{0!n!} + \dfrac{(n+1)!}{1!n!} + \dfrac{(n+2)!}{2!n!} + \dfrac{(n+3)!}{3!n!} + \cdots \dfrac{(n+s)!}{s!n!} = \dfrac{(n+s+1)!}{s!(n+1)!}$ for all integers $s \geq 0$.

   (f) $\dfrac{2!}{1!1!} + \dfrac{4!}{2!2!} + \dfrac{6!}{3!3!} + \cdots + \dfrac{(2n)!}{n!n!} = \dfrac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} \cdot 2n$ for all $n \in \mathbb{N}$

9. Use mathematical induction to prove that

$$\frac{n^3}{3} + \frac{n^5}{5} + \frac{7n}{15}$$

is an integer for all integers $n \geq 0$.

10. For each of the following, discover a formula and, using induction, prove the resulting propositional statement is true.

    (a) $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! =$

    (b) $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{n(n+1)} =$

11. Use mathematical induction to prove that

    (a) $n^2 - 7n + 12 \geq 0$ for all integers $n \geq 3$.

    (b) $8|(n^2 - 1)$ for all positive odd integers n.

12. For what nonnegative values of n is it true that $n^3 < 2^n$? Using induction, prove that the statement is true for all $n \geq r$, where r is the least postive integer possible.

13. The *Fibonacci sequence* is defined recursively by

$$\begin{aligned} &f_1 = 1 \\ &f_2 = 1 \\ &f_n = f_{n-2} + f_{n-1} \text{ for all integers } n \geq 3. \end{aligned}$$

Using this recursive formula, we can easily list the first several numbers in the sequence:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

Use the Second Principle of Mathematical Induction to prove that the n-th term of the Fibonacci sequence is given by the (nonrecursive) formula

$$f_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$$

for all integers $n \geq 1$.

14. Use the Second Principle of Mathematical Induction to prove that postage of 12¢ or greater can be made from 4¢ and 5¢ stamps.

Hint: Mathematically, the problem is to show that for all integers $n \geq 12$,

$$n = 4p_n + 5q_n$$

for some $p_n, q_n \in \mathbb{N}$.

7 Selected Solutions

Section 0

1. (a) 48 is even since $48 = 2 \cdot 24$ and 24 is an integer.

   (c) $12|60$ since $60 = 12 \cdot 5$ and 5 is an integer.

   (b) $17 \equiv_{12} 53$ since $12|(17-53)$. We can see that $12|(17-53)$ since $17-53 = -36 = 12(-3)$ and -3 is an integer.

3. (a) $142 = 15 \cdot 9 + 7$, so $q = 9$ and $r = 7$

5. (a) 9

   (c) 0

6. (a) 6

7. *Proof.* Let m be an even integer and let n be an odd integer. Then there exist integers j and k such that $m = 2j$ and $n = 2k+1$. Now we see that

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

Since $j+k$ is an integer, then by definition of odd integer, $m+n$ is odd. □

Section 1.1

1. (a) Is a false statement. It is false because $4 \not| (8-99)$.

   (c) Is not a statement. Its truth is dependent upon the particular class to which it refers.

   (e) Is not a statement. It is subjective opinion, and its truth varies depending on who says it.

Section 1.2

1. If p is true and q is true, the person saying this statement has followed through on their promise and so are being truthful. If p is true and q is false, the person has told a falsehood since they did not follow through on their promose. If p is false, the condition of the promise is not "activated," so the person has not lied, and so their statement is true.

2. (b) $p =$ "I study", $q =$ "I pass"
   Logical structure: $(\sim p) \to (\sim q)$.

   (d) $p =$ "I was well qualified", $q =$ "I got the job"
   Logical structure: $p \wedge (\sim q)$.

3. (a) Hint: It helps to reword this as a conditional expression: "If a is a positive number, then $a > 0$."

(c) Dogs cannot bark or cats cannot climb trees.

4. (d)
   - Converse: If I eat 2 cheeseburgers and a chocolate cake, then my weight will drop below 170 pounds.
   - Inverse: If my weight does not drop below 170 pounds, then I will not eat 2 cheeseburgers or I will not eat a chocolate cake.
   - Contrapositive: If I do not eat 2 cheeseburgers or a chocolate cake, then my weight will not drop below 170 pounds.

6. (d)

p	q	r	$\sim r$	$p \vee (\sim r)$	$\sim (p \vee (\sim r))$	$q \vee p$	$\sim (p \vee (\sim r)) \wedge (q \vee p)$	$[\sim (p \vee \sim r) \wedge (q \vee p)] \to p$
T	T	T	F	T	F	T	F	T
T	T	F	T	T	F	T	F	T
T	F	T	F	T	F	T	F	T
T	F	F	T	T	F	T	F	T
F	T	T	F	F	T	T	T	F
F	T	F	T	T	F	T	F	T
F	F	T	F	F	T	F	F	T
F	F	F	T	T	F	F	F	T

7. (c)
   - Converse: If xy is even, then x is odd and y is even.
   - Inverse: If x is even or y is odd, then xy is odd.
   - Contrapositive: If xy is odd, then x is even or y is odd.

Section 1.3

1.

p	q	$\sim q$	$\sim p$	$p \to q$	$(p \to q) \wedge (\sim q)$	$[(p \to q) \wedge (\sim q)] \to (\sim p)$
T	T	F	F	T	F	T
T	F	T	F	F	F	T
F	T	F	T	T	F	T
F	F	T	T	T	T	T

Since $[(p \to q) \wedge (\sim q)] \to (\sim p)$ is true for all possible truth values of p and q, then it is a tautology.

3.

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Since $[(p \to q) \wedge (q \to r)] \to (p \to r)$ is true for all possible truth values for p, q, and r, then it is a tautology.

5. (a) A foot does not have 12 inches or a yard does not have three feet.

   (c) I study and I do poorly in this course.

6. (a)

p	q	$\sim p$	$p \vee q$	$\sim (p) \wedge (p \vee q)$	$\sim (p) \wedge (p \vee q) \to q$
T	T	F	T	F	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	F	F	F	T

Since $\sim (p) \wedge (p \vee q) \to q$ is true for all possible truth values of p and q, then it is a tautology.

Section 1.4

1. (a) Some cows do not eat grass.
   (c) Every car is not blue or weighs at least 4000 pounds.
   (h) Some math books are not white and are easy to read.
   (j) There is a real number x such that x is positive and $-x$ is nonnegative.
   (l) There exists a real number x such that $x^2 = -1$.

3. (a) There exists a black sheep.
   (b) For all integers m and n, $m + n$ is even if and only if m and n are both odd or both even.

4. (a) i. $\exists a \in G, \forall g \in G, \exists n \in \mathbb{Z}, a^n = g$
   ii. $\forall a \in G, \exists g \in G, \forall n \in \mathbb{Z}, a^n = g$, or in English: For all $a \in G$, there exists some $g \in G$ such that for all integers n, $a^n \neq g$.
   (b) i. $\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall m, n \in \mathbb{N}, m, n > N \to |x_n - x_m| < \epsilon$
   ii. There exists a real number $\epsilon > 0$ such that for all $N \in \mathbb{N}$, there exist natural numbers m and n such that $m, n > N$ and $|x_n - x_m| \geq \epsilon$.

Section 1.5

1. (c) *Proof.* Let m and n be integers such that m is even and n is odd. Then there exist integers k and l such that $m = 2k$ and $n = 2l + 1$. Now we see that

$$m + n = 2k + (2l + 1) = 2(k + l) + 1,$$

and since $k + l$ is an integer, we have shown that $m + n$ is odd. □

2. *Proof.* (by contraposition) Let n be an integer and suppose n is even. Then there is some integer k such that $n = 2k$. Now we see that $5n - 7 = 5(2k) - 7 = 10k - 7 = 10k - 8 + 1 = 2(5k - 4) + 1$. Since $5k - 4 \in \mathbb{Z}$, we see that $5n - 7$ is odd. □

3. *Proof.* Suppose n^2 is even. Then by a previously proven fact, we may conclude that n is even as well. Thus, $n = 2k$ for some integer k. Now $n^2 = (2k)^2 = 4k^2$ and k^2 is an integer. Therefore, $4|n^2$. □

5. This statement is false. Consider $n = 3$: In this case, it is true that $4|(n^2 - 1)$ (i.e. $4|8$), but it is not true that $4|(n - 1)$ (i.e. $4 \not| \, 2$).

6. *Proof.* Suppose that $m, n \in \mathbb{Z}$ and that $3 \nmid m$ and $3 \nmid n$. Since 3 does not divide either m or n, then the remainder upon division of either m or n by 3 will be either 1 or 2. So, there are three cases to consider: both remainders are 1, both remainders are 2, and one remainder is 1 while the other is 2.

Case: Both remainders are 1. In this case, by the Division Algorithm, there exist $q_1, q_2 \in \mathbb{Z}$ such that $m = 3q_1 + 1$ and $n = 3q_2 + 1$. Consequently,

$$m^2 - n^2 = (3q_1+1)^2 + (3q_2+1)^2 = 9q_1^2 + 6q_1 + 1 - (9q_2^2 + 6q_2 + 1) = 3(3q_1^2 + 2q_1 - 3q_2^2 - 2q_2),$$

and from this last expression it is evident that $3|(m^2 - n^2)$.

Case: Both remainders are 2. The argument here is similar to the previous case - you provide the details!

Case: One remainder is 1 and the other is 2. The argument here is similar to the first case - you provide the details! □

8. (b) In a proof of this fact using the method of contradiction, one would start by assuming that f and g are both one-to-one and $g \circ f$ is not one-to-one.

9. (b) *Proof.* (By contraposition) Let m and n are integers and suppose that n is even. Since n is even, there exists an integer k such that $n = 2k$. Next, to prove that either $m + n$ is odd or m is even, we use Theorem 1.22(i), and argue that if m is not even (i.e. m is odd), then $m + n$ is odd. To that end, suppose that m is odd. Since m is odd, there exists some integer l such that $m = 2l + 1$. Now we have

$$m + n = 2k + (2l + 1) = 2(k + l) + 1,$$

and since $k + l$ is an integer, we see that $m + n$ is odd. □

Section 2.1

1. False because $3/2 \notin \mathbb{Z}$.

3. True because $5 = 4 + 1$ where 4 is an even integer.

5. False because 5 is not a perfect square of an integer (i.e. $\sqrt{5} \notin \mathbb{Z}$).

7. False - 1/2 is simply not in the list of elements, even as an unreduced fraction such as 2/4.

9. True - Since $n \in \mathbb{N}$, then $n \geq 1$. Thus, the set in question consists of the integers that are greater than or equal to 1 and less than or equal to 5, or in other words, it is the set $\{1, 2, 3, 4, 5\}$.

11. True - all of the sets in question consist of exactly the same elements (order doesn't matter).

13. True - the conditions that $n \in \mathbb{Z}$ and $n > 0$ amounts to specifying the set of positive integers, which is the set of natural numbers.

15. False - the definition of the set is ambiguous since the elements of the set may differ depending on the choice of universal set. If the universal set is $\mathbb{N}$, the set in question is just $\{1\}$, but if the universal set is $\mathbb{Z}$, then the set is $\{-1, 1\}$.

Section 2.2

1. (a) True - D consists of odd elements and E consists of even elements, so the two sets are disjoint (i.e. $D \cap E = \emptyset$).

   (c) True - by inspection, we see that each element of B is also an element of A.

   (e) True - It is certainly true that $A \cap D \subseteq A$ (by Fact 2.16, Part 2). Additionally, we see that $A \cap D \neq A$ since $2 \in A$ but $2 \notin (A \cap D)$. Thus, $A \cap D \subset A$.

   (g) False - we see that $D \cup E = U$.

   (i) False

   (k) True - $\emptyset$ is a subset of any set by Fact 2.14.

   (m) False - "5" is not a set, it is a naked element, and as such, it cannot be a subset of any set. Note: the reason that this is false is NOT because $5 \notin B$!

   (o) True - this is verified by direct computation of $\bar{D}$.

2. Solutions in blue.

   (a) $\overline{B} \ = \{1, 4, 6, 7, 8, 9, 10\}$
   (b) $D \setminus A \ = \{7, 9\}$
   (c) $\overline{D} \cap \overline{A} \ = \{6, 8, 10\}$
   (d) $\overline{D \cup A} \ = \{6, 8, 10\}$

   (e) $E \cap (B \cup D) \ = \{2\}$
   (f) $\overline{A} \cup (B \setminus D) \ = \{2, 6, 7, 8, 9, 10\}$
   (g) $\overline{D \cap E} \ = U$
   (h) $\overline{D \setminus E} \ = E$

3. (a) False. $\{\{1\}\}$ has only one element - namely, $\{1\}$.

   (c) False. "1" is not a set, and so cannot be a subset of any set.

   (e) False. $\{\{1\}\}$ has only one element - namely, $\{1\}$.

   (g) True. $\emptyset$ is a subset of any set by Fact 2.14.

4. Prove: $A \subseteq A \cup B$.

   Proof. Suppose it is true that $a \in A$. Then it is certainly true that $a \in A$ or $a \in B$ (since only one of the two statements connected by "or" must be true for the whole statement to be true). Thus, be definition of union, $a \in A \cup B$. □

7. Prove: A and $\bar{A}$ are disjoint.

   Proof. To prove that A and $\bar{A}$ are disjoint, we must argue that $A \cap \bar{A} = \emptyset$. Suppose to the contrary that $A \cap \bar{A} \neq \emptyset$. Then there must exist some element a in $A \cap \bar{A}$. Now $a \in A \cap \bar{A}$ implies (by definition of intersection) that $a \in A$ and $a \in \bar{A}$. But $a \in \bar{A}$ implies (by definition of set complement) that $a \notin A$. Now we have $a \in A$ and $a \notin A$, which is a contradiction. □

17. Prove: $\overline{\overline{A}} = A$.

Proof.

$$\begin{aligned}\overline{\overline{A}} &= \big\{x \in U \,|\, x \notin \overline{A}\big\} && \text{(definition of set complement)}\\ &= \big\{x \in U \,|\, \sim(x \in \overline{A})\big\} && \text{(definition of } \notin\text{)}\\ &= \{x \in U \,|\, \sim(x \notin A)\} && \text{(definition of set complement)}\\ &= \{x \in U \,|\, \sim[\sim(x \in A)]\} && \text{(definition of } \notin\text{)}\\ &= \{x \in U \,|\, x \in A\} && \text{(Theorem 1.22(b))}\\ &= A.\end{aligned}$$

□

21. (i) Prove that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Proof.
($\subseteq$) Let $x \in A - (B \cup C)$. Then $x \in A$ and $x \notin (B \cup C)$. Thus, by definition of complement, $x \in A$ and $x \in \overline{B \cup C}$. By DeMorgan's Law for sets, we can say that $x \in A$ and $x \in \overline{B} \cap \overline{C}$. Now, by definition of intersection, $x \in A$ and $x \in \overline{B}$ and $x \in \overline{C}$. From this we can conclude that $x \in A$ and $x \in \overline{B}$, and $x \in A$ and $x \in \overline{C}$ (it is easily seen that $[p \wedge (q \wedge r)] \leftrightarrow [(p \wedge q) \wedge (p \wedge r)]$ is a tautology). Thus, we have $x \in A$ and $x \notin B$, and $x \in A$ and $x \notin C$, and it follows that $x \in A - B$ and $x \in A - C$. Therefore, $x \in (A - B) \cap (A - C)$.
($\supseteq$) This containment can be proven by reversing the steps of the previous argument. □

23. (f) Prove or disprove: $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

Proof.
($\subseteq$): Let $x \in A \cap (B \triangle C)$. Then $x \in A$ and $x \in B \triangle C$. By definition of symmetric difference, we now have $x \in A$, and $x \in B - C$ or $x \in C - B$. If it is the case that $x \in A$ and $x \in B - C$, then according to the definition of set difference we see that $x \in A$, and $x \in B$ and $x \notin C$. Thus, $\underline{x \in A \cap B}$ and, since $x \notin C$, we have $\underline{x \notin A \cap C}$. Thus,

$$x \in (A \cap B) - (A \cap C) \subseteq [(A \cap B) - (A \cap C)] \cup [(A \cap C) - (A \cap B)] = (A \cap B) \triangle (A \cap C).$$

The case in which $x \in A$ and $x \in C - B$ is handled similarly.
($\supseteq$): The reverse containment is done by reversing the logic of the preceding argument. □

Section 2.3

4. (a) False. The elements of $A \times B$ are all ordered pairs, not naked elements like "5."

   (c) True. $\emptyset \subseteq B$, and so by definition of power set, we have $\emptyset \in \mathcal{P}(\mathcal{B})$.

(e) False. While it is true that $\{2\} \in \mathcal{P}(A)$, the subsets of $\mathcal{P}(A)$ are collections of subsets of A. But $\{2\}$ is not a collection of subsets of A - it is a single naked subset of A.

17. Prove $A \times (B \cap D) = (A \times B) \cap (A \times D)$.

Proof.

$$\begin{aligned}
A \times (B \cap D) &= \{(a,x) \mid a \in A, \text{ and } x \in B \cap D\} \\
&= \{(a,x) \mid a \in A, \text{ and } x \in B \text{ and } x \in D\} \\
&= \{(a,x) \mid a \in A \text{ and } x \in B, \text{ and } a \in A \text{ and } x \in D\} && ([p \wedge (q \wedge r)] \Leftrightarrow [(p \wedge q) \wedge (p \wedge r)]) \\
&= \{(a,x) \mid (a,x) \in (A \times B) \text{ and } (a,x) \in (A \times D)\} && (\text{definition of Cartesian product}) \\
&=(A \times B) \cap (A \times D) && (\text{definition of intersection})
\end{aligned}$$

□

16. This statement is false. As a counterexample, let the universal set be $U = \mathbb{R}$, and consider the intervals $A = [1,2]$, $B = [1,2]$, $D = [2,3]$, and $E = [2,3]$. Drawing a picture of the Cartesian products in question will make it clear that, for example, $(1,3) \notin (A \times B) \cup (D \times E)$ but $(1,3) \in (A \cup D) \times (B \cup E)$.

Section 2.4

3. (a) $A_1 = \{\{1\},\{1,2\},\{1,3\},\{1,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{1,2,3,4\}\}$

(b) $\displaystyle\bigcup_{n \in S} A_n = \mathcal{P}(S) \setminus \{\emptyset\}$ $\qquad$ $\displaystyle\bigcap_{n \in S} A_n = \{S\}$

7. (a) $\displaystyle\bigcup_{i \in I} A_i = A_{100}$ $\qquad$ $\displaystyle\bigcap_{i \in I} A_i = A_1$.

(i) $\displaystyle\bigcup_{i \in \mathbb{N}} A_i = (-\infty, 1]$ $\qquad$ $\displaystyle\bigcap_{i \in \mathbb{N}} A_i = \{0\}$

8. $\displaystyle\bigcup_{i=1}^{k} A_i = A_k$

Proof.

($\subseteq$): Let $x \in \displaystyle\bigcup_{i=1}^{k} A_i$. Then there is some i, $1 \leq i \leq i$, such that $x \in A_i$. But $A_i \subseteq A_k$, so $x \in A_k$.

($\supseteq$): Let $x \in A_k$. Then clearly $x \in \displaystyle\bigcup_{i=1}^{k} A_i$. □

Section 3.1

5. (a) $\{1,2,3,4\}$
   (b) $\{\beta,\gamma,\epsilon\}$
   (c) $\{(\beta,1),(\beta,2),(\gamma,3),(\epsilon,4)\}$
   (d) $\{\beta,\gamma,\epsilon\}$
   (e) $\{1,2,3,4\}$
   (f) $\{\beta,\gamma\}$. Notice that 5 doesn't really contribute to the solution since $5 \notin \text{Dom}(R)$.
   (g) $\emptyset$
   (h) $\{1,2,3\}$
   (i) $\emptyset$ (since $\alpha,\delta \notin \text{Ran}(R)$).

6. (a) $\mathbb{R}$
   (b) $[0,\infty)$
   (c) $[0,4)$
   (d) $\emptyset$ (since $-1 \notin \text{Ran}(R)$)
   (e) $[-2,1] \cup [1,2]$

7. (a) *Proof.* Suppose $S \subseteq \text{Dom}(R)$ and let $s \in S$. Then since $s \in \text{Dom}(R)$, by definition of domain, $\exists b \in B$ such that $(s,b) \in R$. Next, since $s \in S$ and $(s,b) \in R$, then the definition of image of S under R tells us that $b \in R(S)$. But now we have $b \in R(S)$ and $(s,b) \in R$, and by the definition of preimage of $R(S)$ under R, we see that $s \in R^{-1}(R(S))$. □

   (b) Give an example which shows that $S \neq R^{-1}(R(S))$.

   Let $A = \{1,2\}$ and $B = \{\alpha\}$, then define relation R from A to B by $R = \{(1,\alpha),(2,\alpha)\}$. Consider $S = \{1\} \subseteq \text{Dom}(R) = A$ and observe that

$$R^{-1}(R(S)) = R^{-1}(\{\alpha\}) = \{1,2\},$$

   so $S \neq R^{-1}(R(S))$.

10. (c) *Proof.* Let $b \in \text{Ran}(R_1 \cap R_2)$. Then $\exists a \in A$ such that $(a,b) \in R_1 \cap R_2$. Thus, $(a,b) \in R_1$ and $(a,b) \in R_2$. Since $(a,b) \in R_1$, then $b \in \text{Ran}(R_1)$, and since $(a,b) \in R_2$, then $b \in \text{Ran}(R_2)$. Thus $b \in \text{Ran}(R_1) \cap \text{Ran}(R_2)$. □

   For a counterexample of equality, consider $R_1 = \{(1,\alpha)\}$ and $R_2 = \{(2,\alpha)\}$, both relations from $A = \{1,2\}$ to $B = \{\alpha\}$. Since $R_1 \cap R_2 = \emptyset$, then $\text{Ran}(R_1 \cap R_2) = \emptyset$. On the other hand, $\text{Ran}(R_1) \cap \text{Ran}(R_2) = \{\alpha\}$.

Section 3.2

1. (a) Yes
   (b) No

(c) No

(d) No

2.
$\overline{2} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$
$\overline{3} = \{\ldots, --7, -2, 3, 8, 13, \ldots\}$
$\overline{4} = \{\ldots, -6, -1, 4, 9, 12, \ldots\}$
Notice that $\overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4} = \mathbb{Z}$ and these 5 equivalence classes form a partitiion of $\mathbb{Z}$. Thus, any other equivalence class must equal one of these 5 classes. In general, if $x \in \mathbb{Z}$, then $\overline{x} = \overline{r}$ where r is the remainder upon division of x by 5. So, in particular, $\overline{93} = \overline{3}$, $\overline{121} = \overline{1}$, and $\overline{-17} = \overline{3}$.

5.
reflexivity. Let $x \in \mathbb{R}$. Then certainly $|x| = |x|$, and thus $x \sim x$.

symmetry. Let $x, y \in \mathbb{R}$ and suppose $x \sim y$. Then $|x| = |y|$, and hence $|y| = |x|$. Thus, $y \sim x$.

transitivity. Let $x, y, z \in \mathbb{R}$ and suppose that $x \sim y$ and $y \sim z$. Then $|x| = |y|$ and $|y| = |z|$. Thus, $|x| = |z|$ and we conclude that $x \sim z$.

6. (a) Is an equivalence relation.

(b) Is an equivalence relation.

(c) Is not an equivalence relation.

(d) Is an equivalence relation.

(e) Is not an equivalence relation.

(f) Is an equivalence relation.

(g) Is an equivalence relation.

Section 4.1

1. (a) Is a function from A to B. Is a function from A to D.

(b) Is a function from A to B. Is a function from A to D.

(c) Is a function from A to B. Is a function from A to D.

(d) Is a function from A to B. Is not a function from A to D.

4. Each of these is a function from A to B. However, the notation $f : A \to B$ is appropriate as follows.

(a) Y

(b) N

(c) Y

(d) Y

(e) Y

(f) Y

(g) N

(h) Y

(i) Y

(j) N. Observe that $\sqrt{2} \notin \text{Dom}(f)$, so $\text{Dom}(f) \neq \mathbb{R}$.

5(b). This is a well-defined function. To see that this is true, let $\overline{a_1}, \overline{a_2} \in Z_n$ and suppose $\overline{a_1} = \overline{a_2}$. Then $a_1 \equiv_n a_2$, which means $n|(a_1 - a_2)$, which in turn means that $\exists k \in \mathbb{Z}$ such that $a_1 - a_2 = nk$. Now

$$\begin{aligned} a_1^3 - a_1 - (a_2^3 - a_2) =& (a_1^3 - a_2^3) - (a_1 - a_2) \\ =& (a_1 - a_2)(a_1^2 + a_1a_2 + a_2^2) - (a_1 - a_2) \\ =& (a_1 - a_2)(a_1^2 + a_1a_2 + a_2^2 - 1) \\ =& nk(a_1^2 + a_1a_2 + a_2^2 - 1) \end{aligned}$$

Thus, we see that $n|[a_1^3 - a_1 - (a_2^3 - a_2)]$, and so $\overline{a_1^3 - a_1} = \overline{a_2^3 - a_2}$. Therefore, $f(\overline{a_1}) = f(\overline{a_2})$.

Section 4.2

1. (a) Is neither 1-1 nor onto.

   (b) Is neither 1-1 nor onto.

   (c) Is 1-1 and onto.

3. f is 1-1.

   Proof. Let $n_1, n_2 \in \text{Dom}(f) = \mathbb{Z}$, and suppose that $f(n_1) = f(n_2)$. Then we have $2n_1 = 2n_2$, from which we deduce that $n_1 = n_2$. □

   f is not onto. To see this, consider $1 \in \mathbb{Z}$. Observe that $1 \notin \text{Ran}(f)$ since $\text{Ran}(f)$ consists only of even integers. Thus, $\text{Ran}(f) \neq \mathbb{Z}$, and so f is not onto.

6. Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = e^{3x-2}$.

   (a) f is 1-1: Let $x_1, x_2 \in \mathbb{R}$ and suppose $f(x_1) = f(x_2)$. Then $e^{3x_1-2} = e^{3x_2-2}$, and since ln is a a function (a reasonable assumption), we have $\ln(e^{3x_1-2}) = \ln(e^{3x_2-2})$. From known properties of ln, we see that $3x_1 - 2 = 3x_2 - 2$, and from there it is obvious that $x_1 = x_2$. To see that f is not onto $\mathbb{R}$, just observe that the range of f is $(0, \infty)$. So, for example, there is no $x \in \mathbb{R}$ such that $f(x) = 0$.

   (b) By Theorem 4.18, since f is one-to-one, we can say that $f^{-1} : \text{Ran}(f) \to \mathbb{R}$; that is, $f^{-1} : (0, \infty) \to \mathbb{R}$.

9. (a) 1-1, not onto

(b) 1-1, not onto

(c) not 1-1, not onto

(d) 1-1, not onto

(e) 1-1 and onto

(f) not 1-1, not onto

(g) 1-1, not onto

(h) not 1-1, not onto

(i) not 1-1, not onto

(j) not 1-1, not onto

12. Hint: Just make a table of the function values - there are only 4 elements of the domain! From this table, the solution is obvious.

14. To prove that if f is strictly increasing, then f is 1-1: Suppose f is strictly increasing and let $x_1, x_2 \in \mathbb{R}$ with $f(x_1) = f(x_2)$. If, for the sake of contradiction, it is the case that $x_1 \neq x_2$, then let us assume without loss of generality that $x_1 < x_2$. Since f is increasing, then $f(x_1) < f(x_2)$, contrary to our hypothesis that $f(x_1) = f(x_2)$.

Section 4.3

4. (a) $g \circ f = \{(a, \alpha), (b, \delta), (c, \beta), (d, \beta), (e, \gamma)\}$

   (b) $g \circ f$ is not 1-1 since $(c, \beta) \in g \circ f$ and $(d, \beta) \in g \circ f$, but $c \neq d$. The contrapositive of Theorem 4.29 Part 1 tells us that since f is not 1-1, then $g \circ f$ cannot be 1-1.

   (c) Yes, $g \circ f$ is onto. Theorem 4.29 Part 2 tells us that since $g \circ f$ is onto, then g is necessarily onto.

7. *Proof.* Suppose $g \circ f$ is 1-1 and f is onto. To see that g is 1-1, let $b_1, b_2 \in \text{Dom}(g) = B$ and suppose that $g(b_1) = g(b_2)$. Because f is onto B, there exist $a_1, a_2 \in \text{Dom}(f) = A$ such that $f(a_1) = b_1$ and $f(b_2) = a_2$. Now $(g \circ f)(a_1) = g(f(a_1)) = g(b_1)$ and $(g \circ f)(a_2) = g(f(a_2)) = g(b_2)$, and since $g(b_1) = g(b_2)$, we see that $(g \circ f)(a_1) = (g \circ f)(a_2)$. Because $g \circ f$ is 1-1 by hypothesis, we can conclude that $a_1 = a_2$. Finally, since $a_1 = a_2$ and f is a function, we see that $f(a_1) = f(a_2)$; that is, $b_1 = b_2$. Therefore, g is 1-1. □

Section 4.4

2. *Proof.*
   (⇒): Suppose R is a symmetric relation on a set A. To prove that $R = R^{-1}$, we will do a double containment argument.
   (⊆): Let $(a, b) \in R$. Because R is symmetric, we have $(b, a) \in R$, but this is equivalent to saying $(a, b) \in R^{-1}$.
   (⊇): Let $(a, b) \in R^{-1}$. Then $(b, a) \in R$. Because of the symmetry hypothesis, we have $(a, b) \in R$ also.

($\Leftarrow$): Suppose R is a relation on A such that $R = R^{-1}$. To prove that R is symmetric, let $(a,b) \in R$. Then since $R = R^{-1}$, we see that $(a,b) \in R^{-1}$. Thus, $(b,a) \in R$. □

6. *Proof.*
($\subseteq$): Let $a \in f^{-1}(T_1 \setminus T_2)$. Then there exists $t \in T_1 \setminus T_2$ such that $(a,t) \in f$. Since $t \in T_1 \setminus T_2$, then we can say $t \in T_1$ and $t \notin T_2$. The fact that $t \in T_1$ and $(a,t) \in f$ implies that $\underline{a \in f^{-1}(T_1)}$. Next, we wish to argue that $a \notin f^{-1}(T_2)$. To this end, suppose to the contrary that $a \in f^{-1}(T_2)$. This means that there exists $\hat{t} \in T_2$ such that $(a,\hat{t}) \in f$. Because $(a,t),(a,\hat{t}) \in f$ and f is a function, we see that $t = \hat{t}$; however, this is an impossibility since $t \notin T_2$. Therefore, we can conclude that $\underline{a \notin f^{-1}(T_2)}$. The two underscored facts then imply that $a \in f^{-1}(T_1) \setminus f^{-1}(T_2)$.

   ($\supseteq$): Let $a \in f^{-1}(T_1) \setminus f^{-1}(T_2)$. Then $a \in f^{-1}(T_1)$ and $a \notin f^{-1}(T_2)$. Because $a \in f^{-1}(T_1)$, there exists $t \in T_1$ such that $(a,t) \in f$. Observe that $t \notin T_2$, for otherwise the fact that $(a,t) \in f$ would imply that $a \in f^{-1}(T_2)$, contrary to hypothesis. Thus, we know that $t \in T_1$ and $t \notin T_2$, which in turn means that $t \in T_1 - T_2$. Finally, since $t \in T_1 - T_2$ and $(a,t) \in f$, we see that $a \in f^{-1}(T_1 - T_2)$. □

16. *Proof.* Suppose $f : A \to B$ is onto and let $T_1 \subseteq B$. We prove that $(f \circ f^{-1})(T_1) = T_1$ by double containment.
($\subseteq$): Let $b \in (f \circ f^{-1})(T_1)$. Then by definition of image, there exists $t \in T_1$ such that $(t,b) \in f \circ f^{-1}$. Next, by definition of composition, there exists some $a \in A$ such that $(t,a) \in f^{-1}$ and $(a,b) \in f$. Now see that $(a,b) \in f$, and by definition of inverse of a relation, $(a,t) \in f$. Because f is a function we must have $b = t$. Since $t \in T_1$, we now see that $b \in T_1$ as required.

    ($\supseteq$): Let $b \in T_1$. Because f is onto, we see that $T_1 \subseteq B = \operatorname{Ran}(f)$, so $b \in \operatorname{Ran}(f)$. Thus, there exists some $a \in A$ such that $(a,b) \in f$. We may also observe, then, that $(b,a) \in f^{-1}$. Because $(b,a) \in f^{-1}$ and $(a,b) \in f$, then by definition of composition we see that $(b,b) \in f \circ f^{-1}$. Finally, because $(b,b) \in f \circ f^{-1}$ and $b \in T_1$, then $b \in (f \circ f^{-1})(T_1)$. □

18. Fact 4.39, Part 2.

    Proof.
($\subseteq$): Let $a \in f^{-1}\left(\bigcap_{\alpha \in I} T_\alpha\right)$. Then there exists $t \in \bigcap T_\alpha$ such that $(a,t) \in f$. Since $t \in \bigcap T_\alpha$, we know that for every $\alpha \in I$, $t \in T_\alpha$. Thus, for every $\alpha \in I$, we have $(a,t) \in f$ and $t \in T_\alpha$. From this we see that for every $\alpha \in I$, $a \in f^{-1}(T_\alpha)$. Therefore, $a \in \bigcap f^{-1}(T_\alpha)$.

    ($\supseteq$): Let $a \in \bigcap_{\alpha \in I} f^{-1}(T_\alpha)$. Then for every $\alpha \in I$ we have $a \in f^{-1}(T_\alpha)$, and so for every $\alpha \in I$, there exists some t_α such that $(a,t_\alpha) \in f$. However, because f is a function, all of the elements t_α must be equal to some fixed element t, and we further observe that $t \in \bigcap T_\alpha$. Now $(a,t) \in f$ where $t \in \bigcap T_\alpha$, and we conclude that $a \in f^{-1}\left(\bigcap T_\alpha\right)$. □

Section 5.1

1. (a) Yes.

   i. $*$ is a function: Let $a_1, a_2, b_1, b_2 \in \mathbb{N}$ and suppose $a_1 = a_2$ and $b_1 = b_2$. Then $a_1 * b_1 = a_1^{b_1} = a_2^{b_2} = a_2 * b_2$.

   ii. $\text{Dom}(*) = \mathbb{N} \times \mathbb{N}$: Clearly $\text{Dom}(*) \subseteq \mathbb{N} \times \mathbb{N}$ from the definition of $*$. To see that $\text{Dom}(*) \supseteq \mathbb{N} \times \mathbb{N}$, just note that for every $a, b \in \mathbb{N}$, a^b is a well-defined number.

   iii. $\text{Ran}(*) \subseteq \mathbb{N}$. By axioms of integers, when $a, b \in \mathbb{N}$, then $a * b = a^b \in \mathbb{N}$.

   (b) No. The range of $*$ is not contained in $\mathbb{N}$. Consider $a = 2$ and $b = -1$.

   (g) Yes. Follow the steps in (a), modified accordingly, to verify.

   (j) No. The range of $*$ is not in $\mathbb{Z}$. Consider $a = 1$ and $b = 1$.

   (l) No. The range of $*$ is not contained in $\mathbb{R}$. Consider $a = 2$ and $b = -1$. Then $a * b \notin \mathbb{R}$ (in fact, $a * b \in \mathbb{C}$).

   (m) Yes. Follow the steps in (a), modified accordingly, to verify.

6. *Proof.* We must argue that $\triangle : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S)$.
   1. Let A_1, A_2, B_1, and B_2 be elements of $\mathcal{P}(S)$ and suppose $A_1 = A_2$ and $B_1 = B_2$. Then

$$\begin{aligned} A_1 \triangle B_1 &= (A_1 \setminus B_1) \cup (B_1 \setminus A_1) \\ &= (A_2 \setminus B_2) \cup (B_2 \setminus A_2) \qquad \text{(since } \cup \text{ and } \setminus \text{ are functions from } \mathcal{P}(S) \times \mathcal{P}(S) \text{ to } \mathcal{P}(S)) \\ &= A_2 \triangle B_2. \end{aligned}$$

   Consequently, $\triangle$ is a well-defined function on $\mathcal{P}(S) \times \mathcal{P}(S)$.

   2. Let $A, B \in \mathcal{P}(S)$. Because $\cup$ and $\setminus$ are binary operations on $\mathcal{P}(S)$, we see that $A \triangle B$, which is defined in terms of binary operations $\cup$ and $\setminus$ (Fact 5.5), is an element of $\mathcal{P}(S)$, and so is defined. Thus, $\text{Dom}(\triangle) = \mathcal{P}(S) \times \mathcal{P}(S)$.

   3. Also note that for $A, B \in \mathcal{P}(S)$, $A \triangle B \in \mathcal{P}(S)$ due do the status of $\cup$ and $\setminus$ as binary operations on $\mathcal{P}(S)$ (Fact 5.5). Thus, $\text{Ran}(\triangle) \subseteq \mathcal{P}(S)$. □

7. (a) $f = (1\ 3\ 2\ 6)(5\ 10\ 7\ 9)$, $g = (1\ 2\ 3)(4\ 7\ 8\ 9\ 10)(5\ 6)$, $h = (2\ 10\ 6\ 9\ 3\ 8)(4\ 5\ 7)$

   (b) i. $f^{-1} = \begin{pmatrix} 3 & 6 & 2 & 4 & 10 & 1 & 9 & 8 & 5 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 3 & 1 & 4 & 9 & 2 & 10 & 8 & 7 & 5 \end{pmatrix}$

   ii. $f = [(1\ 3\ 2\ 6)(5\ 10\ 7\ 9)]^{-1} = (5\ 10\ 7\ 9)^{-1}(1\ 3\ 2\ 6)^{-1} = (5\ 9\ 7\ 10)(1\ 6\ 2\ 3)$

(c) Using 2-row notation:

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 3 & 1 & 4 & 9 & 2 & 10 & 8 & 7 & 5 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 10 & 8 & 5 & 7 & 9 & 4 & 2 & 3 & 6 \end{pmatrix}$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 7 & 6 & 5 & 8 & 9 & 10 & 4 \end{pmatrix}$$

− − − − − − − − − − − − − − −

$$g \circ h \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 2 & 6 & 1 & 4 & 5 & 3 & 7 & 8 \end{pmatrix}$$

Next, using cycle notation:

$$g \circ h \circ f^{-1} = \underbrace{(1\ 2\ 3)(4\ 7\ 8\ 9\ 10)(5\ 6)}_{g}\,\underbrace{(2\ 10\ 6\ 9\ 3\ 8)(4\ 5\ 7)}_{h}\,\underbrace{(5\ 9\ 7\ 10)(1\ 6\ 2\ 3)}_{f^{-1}} = (1\ 10\ 8\ 3\ 2\ 9\ 7\ 5)(4\ 6)$$

Indeed, by inspection, we see that the two solutions agree.

Section 5.2

5. (a) not commutative, not associative
   (c) not commutative, is associative
   (d) not commutative, is associative
   (f) is commutative, not associative
   (g) is commutative, not associative
   (h) not commutative, not associative
   (i) is commutative, is associative
   (k) not commutative, not associative
   (m) is commutative, is associative

7. (b) $e = -2$
   (c) For arbitrary $a \in \mathbb{Z}$, we have $a^{-1} = -a - 4$.

12. Actually, if $S = \emptyset$, there is an identity with repsect to set difference; namely, $\emptyset$ is the identity. However, if $S \neq \emptyset$, then there is no identity in $\mathcal{P}(S)$ with respect to set difference. To see this, suppose to the contrary that such an identity $E \in \mathcal{P}(S)$ with respect to $\setminus$ exists. Then for every set $A \in \mathcal{P}(S)$, we have $E \setminus A = A \setminus E = A$. However, it $(E \setminus A) \cap (A \setminus E) = \emptyset$ by Fact 2.16 (4), and so this implies that $A = \emptyset$. But if $S \neq \emptyset$, then there exists some nonempty set $A \in \mathcal{P}(S)$, and so we have a contradiction.

Section 6.2

1. (a) Base Case, n = 1: When $n = 1$, the equation to prove reads

$$2 = 1(1+1),$$

which is clearly true.

Inductive Step: Suppose the equation is true for arbitrary $k \geq 1$. Then

$$\begin{aligned} 2+4+6+\cdots+2(k+1) =& 2+4+6+\cdots 2k+2(k+1) \\ =& k(k+1)+2(k+1) \qquad \text{(by the inductive hypothesis)} \\ =& (k+1)(k+2). \end{aligned}$$

Thus, the $(k+1)$-st version of the equation is true when the k-th version of the equation is true. Therefore, by FPMI, $2+4+6+\cdots+2n = n(n+1)$ for all integers $n \geq 1$.

(h) Base Case, n = 0: When $n = 0$, the equation to prove reads

$$3 \cdot 5^0 = \frac{3(5^1-1)}{4},$$

which is evidently true.

Inductive Step: Let $k \geq 0$ and suppose that

$$3 \cdot 5^0 + 3 \cdot 5^1 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^k = \frac{3(5^{k+1}-1)}{4}.$$

Then

$$\begin{aligned} 3 \cdot 5^0 + 3 \cdot 5^1 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^{k+1} =& 3 \cdot 5^0 + 3 \cdot 5^1 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^k + 3 \cdot 5^{k+1} \\ =& \frac{3(5^{k+1}-1)}{4} + 3 \cdot 5^{k+1} \\ =& \frac{3(5^{k+1}-1)}{4} + \frac{12 \cdot 5^{k+1}}{4} \\ =& \frac{15 \cdot 5^{k+1} - 3}{4} \\ =& \frac{3 \cdot 5^{k+2} - 3}{4} \\ =& \frac{3(5^{k+2}-1)}{4}. \end{aligned}$$

Therefore, by FPMI, $3 \cdot 5^0 + 3 \cdot 5^1 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = \frac{3(5^{n+1}-1)}{4}$ for all $n \in \mathbb{Z}$ with $n \geq 0$.

(o) Base case, $n = 0$: When $n = 0$, the statement to prove reads $8|(3^0 - 1)$, or equivalently, $8|0$, which is clearly true since $0 = 8 \cdot 0$.

Inductive step: Suppose $k \geq 0$ and suppose that $8|(3^{2k} - 1)$. Then there exists an integer j such that $3^{2k} - 1 = 8j$. Now

$$\begin{aligned} 3^{2(k+1)} - 1 =& 3^2 \cdot 3^{2k} - 1 \\ =& (8+1)3^{2k} - 1 \\ =& 8 \cdot 3^{2k} + (3^{2k} - 1) \\ =& 8 \cdot 3^{2k} + 8j \qquad \text{(by the inductive hypothesis)} \\ =& 8 \cdot (3^{2k} + j). \end{aligned}$$

Since $3^{2k} + j \in \mathbb{Z}$, we see that $8|3^{2(k+1)} - 1$. Therefore, by FPMI, $8|(3^{2n} - 1)$ for all integers $n \geq 0$.

(13) *Proof.*
Base case, $n = 1, n = 2$. By direct substitution, it is quickly verified that the formula yields $f_1 = 1$ and $f_2 = 1$.

Inductive Step. Assume $k \geq 3$ and that

$$f_m = \frac{(1+\sqrt{5})^m - (1-\sqrt{5})^m}{2^m\sqrt{5}}$$

for all integers m satisfying $1 \leq m < k$. Then

$$\begin{aligned} f_k &= f_{k-2} + f_{k-1} \\ &= \frac{(1+\sqrt{5})^{k-2} - (1-\sqrt{5})^{k-2}}{2^{k-2}\sqrt{5}} + \frac{(1+\sqrt{5})^{k-1} - (1-\sqrt{5})^{k-1}}{2^{k-1}\sqrt{5}} && \text{(by the inductive hypothesis)} \\ &= \frac{2(1+\sqrt{5})^{k-2} - 2(1-\sqrt{5})^{k-2} + (1+\sqrt{5})^{k-1} - (1-\sqrt{5})^{k-1}}{2^{k-1}\sqrt{5}} \\ &= \frac{4(1+\sqrt{5})^{k-2} - 4(1-\sqrt{5})^{k-2} + 2(1+\sqrt{5})^{k-1} - 2(1-\sqrt{5})^{k-1}}{2^{k}\sqrt{5}} \\ &= \frac{4(1+\sqrt{5})^{k-2} - 4(1-\sqrt{5})^{k-2} + 2(1+\sqrt{5})(1+\sqrt{5})^{k-2} - 2(1-\sqrt{5})(1-\sqrt{5})^{k-2}}{2^{k}\sqrt{5}} \\ &= \frac{(6+2\sqrt{5})(1+\sqrt{5})^{k-2} + (-6+2\sqrt{5})(1-\sqrt{5})^{k-2}}{2^{k}\sqrt{5}} && \text{(combining like terms)} \\ &= \frac{(1+\sqrt{5})^2(1+\sqrt{5})^{k-2} - (1-\sqrt{5})^2(1-\sqrt{5})^{k-2}}{2^{k}\sqrt{5}} && ((1+\sqrt{5})^2 = 6+2\sqrt{5} \text{ and } (1-\sqrt{5})^2 = 6-2\sqrt{5}) \\ &= \frac{(1+\sqrt{5})^k - (1-\sqrt{5})^k}{2^{k}\sqrt{5}}. \end{aligned}$$

Thus, by SPMI, we see that

$$f_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$$

for all integers $n \geq 1$. □