Notes for Math 122
Logic and Foundations

Gary MacGillivray
University of Victoria

Contents

1 Propositional Logic **9**

1.1 Statements 9

1.2 Compound Statements and Logical Connectives 10

1.3 Negation of Statements 11

1.4 Truth Tables 12

1.5 Tautologies and Contradictions 14

1.6 Logical Equivalence 15

1.7 Converse and Contrapositive of an Implication 17

1.8 Necessary and Sufficient Conditions 18

1.9 The Laws of Logic 20

1.10 Using Only And, Or, and Not 23

1.11 Logical Implication 25

1.12 Valid Arguments and Inference Rules 26

1.13 Proving Implications 32

1.14 Exercises 33

2 Quantifiers and Written Proofs **39**

2.1 Open Statements 39

2.2 Quantifiers 40

2.3 Negating Statements Involving Quantifiers 46

2.4 Some Examples of Written Proofs 50
2.5 Exercises 52

3 Set Theory 59
3.1 What is a Set? 59
3.2 Describing Sets 60
3.3 Special Sets 62
3.4 Set Membership Set Equality, and Set Complement 62
3.5 The Empty Set 63
3.6 Subsets 64
3.7 Proper Subsets 67
3.8 The Power Set 68
3.9 Venn Diagrams 69
3.10 Set Operations 70
3.11 The Laws of Set Theory 72
3.12 Investigating Set Relationships with Venn Diagrams 75
3.13 Counting sets and subsets 79
3.14 Inclusion - Exclusion 80
3.15 Exercises 85

4 Induction and Recursion 89
4.1 Recursive definitions 89
4.2 Induction: An introduction 92
4.3 PMI – The Principle of Mathematical Induction 96
4.4 PMI and the Well Ordering Principle 100
4.5 Examples Involving Multi-term Recursively Defined Sequences 101
4.6 The Weak Form of Induction 103
4.7 Examples Involving Summations 104

4.8 Examples Involving Inequalities 107
4.9 Formulas for 1-Term Recurrences 108
4.10 A subtraction game 111
4.11 Induction Analogies and Fallacies 113
4.12 Exercises 115

5 Number Theory 119
5.1 Floors and Ceilings 119
5.2 The Division Algorithm 120
5.3 Representing Numbers in Base *b* 122
5.4 The number of digits 125
5.5 Divisibility 126
5.6 Prime numbers and unique factorization 128
5.7 Using the FTA in Proofs of Irrationality 130
5.8 There are Infinitely Many Primes 132
5.9 The Sieve of Eratosthenes 132
5.10 The *gcd* 133
5.11 The *lcm* 135
5.12 The Euclidean Algorithm 136
5.13 Integer Linear Combinations 138
5.14 Relatively prime integers 140
5.15 Modular Arithmetic (Congruences) 141
5.16 Testing for divisibility by 3 and by 9 145
5.17 Exercises 146

6 Cartesian Products and Relations 151
6.1 Cartesian Products 151
6.2 The Definition of a Relation 154
6.3 Properties of Relations: An Introduction 156

6.4 Reflexive Relations 158
6.5 Symmetric Relations 159
6.6 Transitive Relations 160
6.7 Anti-symmetric Relations 161
6.8 Relations and Matrices 163
6.9 Equivalence Relations 164
6.10 Equivalence Relations and Partitions 166
6.11 Exercises 170

7 Functions 175
7.1 The Definition of a Function and Some Related Terminology . 176
7.2 Equality of functions 178
7.3 1-1 Functions 179
7.4 Onto Functions 181
7.5 Bijections 183
7.6 Function composition 184
7.7 The identity function 186
7.8 Inverse functions 187
7.9 Exercises 188

8 Cardinality of sets 191
8.1 1-1 Correspondences and Cardinality 191
8.2 Cardinality of finite sets 192
8.3 Cardinality of infinite sets 193
8.4 Countable Sets and Sequences 194
8.5 Examples of Countably Infinite Sets 196
8.6 Proving Sets are Countable 198
8.7 Uncountable Sets 199
8.8 Proving Sets are Uncountable 200

8.9 Other cardinalities 201
8.10 Exercises 202

Chapter 1

Propositional Logic

1.1 Statements

A *statement* or *proposition* is an assertion which is either true or false, though you may not know which. That is, a statement is something that has a *truth value.*

Example 1.1.1 *Each of the following is a statement.*

1. *There are no integers* a *and* b *so that* $\sqrt{2} = \frac{a}{b}$*. (True.)*
2. *For all integers* $n \geq 0$*, the number* $n^2 + n + 41$ *is prime. (False.)*
3. *Every even positive integer except* 2 *is the sum of two prime numbers. (Goldbach's Conjecture: unknown.)*

Question 1.1.2 *Why does each of the following fail to be a statement?*

1. *Have a good day.*
2. *Are the Canucks a good team?*
3. $x > 100$.

We usually use (lower case) letters to denote statements. A good way to think of these letters is as variables that can take the values "true" and "false". Variables that can take two possible values are sometimes called *Boolean variables*, after the British logician George Boole.

1.2 Compound Statements and Logical Connectives

A *compound statement* is formed by joining other statements together with *logical connectives*, several of which are defined below. The statements that are joined together can themselves be compound statements.

Let p and q be statements.

- The *conjunction of* p *and* q is the statement denoted by $p \wedge q$, and read as “p and q”, which asserts that p and q are both true. Notice that the wedge symbol looks vaguely like the letter “n” in and.
- The *disjunction of* p *and* q is the statement denoted by $p \vee q$, and read as “p or q”, which asserts that either p is true or q is true, or both. Notice that this is the inclusive sense of the word “or”. Also, the vee symbol looks vaguely like the letter “r” in or.
- An *implication* is the statement denoted by $p \to q$, and read as “p implies q” or “if p then q”, which asserts that *if* p is true, *then* q is also true. We define that statement $p \to q$ to be true when p is false.
- A *biconditional*, or *double implication*, is the statement denoted by $p \leftrightarrow q$, and read “ p if and only if q”, which asserts that p and q have the same truth value. Notice that the assertion being made can also be phrased as “if p is true then q is true, and if q is true then p is true.”

Example 1.2.1 *The following are compound statements.*

1. $(e < \pi) \wedge (57$ *is prime*$)$ *(False because “*$(57$ *is prime*$)$*” is false.)*
2. $(\sqrt{2}$ *is rational*$) \vee (\frac{1+\sqrt{5}}{2} < 2)$ *(True because “*$(\frac{1+\sqrt{5}}{2} < 2)$*” is true).*
3. $(5^2 < 0) \to (1 < 2)$ *(True because “*$(5^2 < 0)$*” is false.)*
4. $(1 < 2) \to (5^2 < 0)$ *(False because “*$1 < 2$*” is true and “*$5^2 < 0$*” is false.*
5. $(1 = 2) \leftrightarrow ($the number of primes is finite*) (True because both “*$(1 = 2)$*” and “*(the number of primes is finite)*” are false.)*

The third and fourth points in the example demonstrate that *the statements* $p \to q$ *and* $q \to p$ *are different.* That is, for given truth values of p and q, the two statements can have different truth values.

In the algebra of real numbers, the order of operations is brackets, exponents, multiply and divide, add and subtract. Thus $-3^2(4 \times 2 + 5^2) = -9(8+25) = -9(33) = -297$. That is, exponents have precedence over multiplication and division, which in turn have precedence over addition and subtraction. Brackets are used for clarity, or to force operations to occur in a particular order.

In propositional logic there is no precedence among logical connectives. Expressions are interpreted from left to right. Brackets are used for clarity, or to force certain connectives to be applied in a particular order. The statement $p \vee q \to r$ is actually $(p \vee q) \to r$, though it is far better to simply regard the unbracketed statement as ambiguous and insist on proper bracketing. *It is good practice to always use brackets for clarity instead of assuming that the reader is able to interpret the meaning you intend.*

1.3 Negation of Statements

The *negation* of p is the statement denoted by $\neg p$, and read as "*not p,*" which asserts that p is not true. Sometimes it is helpful to think of $\neg p$ as asserting "*it is not the case that p is true*". Thus, $\neg p$ is false when p is true, and true when p is false.

The negation of $\neg p$ is the statement with the opposite truth value as $\neg p$. Thus $\neg(\neg p)$ is just another name for p.

Notice that "$\neg$" is not a logical connective. It does not join two statements together. Instead, it applies to a single (possibly compound) statement.

Negation has precedence over logical connectives. This means that $p \vee \neg q$ is $p \vee (\neg q)$, although it is more common to write $p \vee \neg q$ than it is to write $p \vee (\neg q)$. It is common practice only use brackets for negation when it is a compound statement being negated, and not when an individual statement is being negated, as in $\neg(a \to b) \wedge \neg(c \vee \neg d)$.

1.4 Truth Tables

A *truth table* gives the truth values of a statement for all possible combinations of truth values of the other statements from which it is made. Here and elsewhere, 0 and 1 will represent the truth values “false” and “true”, respectively.

The following is a truth table for the compound statements defined in the Section 1.2.

p	q	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1

And here is a truth table for negation.

p	$\neg p$
0	1
1	0

The truth table below demonstrates that *the statements $p \to q$ and $q \to p$ are different.* Since the corresponding entries in the columns under these statements are not identical, sometimes the two statements can have different truth values.

p	q	$p \to q$	$q \to p$
0	0	1	1
0	1	1	0
1	0	0	1
1	1	1	1

To make a truth table, start with k columns corresponding to the most basic statements (usually represented by letters). As we will argue below, if there are k of these you will need 2^k rows to list all possible combinations of truth values for these statements. After listing all 2^k possible combinations of truth values of the k most basic statements (how to do this is also described below) then, working with what’s inside the brackets first (just like algebra!), add a new column for each connective in the expression, and fill in the truth values using the definitions from before.

Here is how to see that *a truth table that involves k basic statements needs 2^k rows*. It is clear that two rows are needed when $k = 1$: one for when the statement is true and one for when it is false. Now consider the case when $k = 2$. When the first statement is true, the second can be true or false, and when the first statement is false, the second can be true or false. Thus, when $k = 2$ there are four rows needed in the truth table. The same sort of argument applies when $k = 3$: eight rows are needed. Four rows are needed to cover the situations where the first statement is true, as (from before) there are four combinations of truth values for the other two statements, and four more rows are needed to cover the situations where the first statement is false. Continuing in this way, the numbers of rows needed doubles for each additional statement, so if there are k statements you will need 2^k rows to list all possible combinations of truth values.

Notice that the argument above tells you *how to list all possible truth values for a collection of statements*. A different perspective is to list the rows in the order they would on a car's odometer if it had only the digits 0 and 1. These correspond to the three digit binary (base 2) representations of the numbers 0 through 7, in order.

Example 1.4.1 *Make the truth table for $(\neg p \to r) \to (q \vee \neg r)$.*

Solution

Our table will have 8 rows. Starting with the collection of truth possible values for p, q and r, we add columns to obtain the truth values of $\neg p$, $(\neg p \to r)$, $\neg r$, $(q \vee \neg r)$, and then, finally, the entire statement we want.

p	q	r	$\neg p$	$\neg p \to r$	$\neg r$	$q \vee \neg r$	$(\neg p \to r) \to (q \vee \neg r)$
0	0	0	1	0	1	1	1
0	0	1	1	1	0	0	0
0	1	0	1	0	1	1	1
0	1	1	1	1	0	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	0	0	0
1	1	0	0	1	1	1	1
1	1	1	0	1	0	1	1

Sometimes only part of the truth table needs to be made. For example, suppose it is given a and b are false, and c is true. Then the truth value of

$\neg a \vee (b \vee \neg c)$ can be found by completing the single row of the truth table where a, b and c have the given truth values.

If we are given that p is false and q is true, then we can find all possible truth values of $\neg(p \leftrightarrow r) \rightarrow (q \rightarrow s)$ by completing the four rows of the truth table where p and q have the truth values given, and all possible truth values for r and s occur.

Sometimes information about truth values can be given a more indirectly, as in the next example.

Example 1.4.2 *Given that $\neg a \rightarrow (b \leftrightarrow \neg c)$ is false, determine all possible truth values of $(a \vee b) \wedge (\neg b \vee \neg c)$.*

Solution
The information that given implication is false, lets us conclude that its hypothesis, $\neg a$, is true (so a is false), and its conclusion, $(b \leftrightarrow \neg c)$, is false (so b and $\neg c$ have different truth values, that is, b and c have the same truth value. Hence we need a truth table with only two rows:

a	b	c	$\neg b$	$\neg c$	$a \vee b$	$\neg b \vee \neg c$	$(a \vee b) \wedge (\neg b \vee \neg c)$
0	0	0	1	1	0	1	0
0	1	1	0	0	1	0	0

Therefore, if $\neg a \rightarrow (b \leftrightarrow \neg c)$ is false, so is $(a \vee b) \wedge (\neg b \vee \neg c)$.

1.5 Tautologies and Contradictions

A statement which is always true is called a *tautology.* A statement which is always false is called a *contradiction.*

For example, $p \wedge \neg p$ is a contradiction, while $p \vee \neg p$ is a tautology. Most statements are neither tautologies nor contradictions.

One way to determine if a statement is a tautology is to make its truth table and see if the statement is always true.

Example 1.5.1 *Show that $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$ is a tautology.*

Solution
Since the column of the truth table shown below corresponding to $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$ contains only the truth value 1, the statement is a tautology.

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg p \vee q$	$(p \to q) \leftrightarrow (\neg p \vee q)$
0	0	1	1	1	1	1
0	1	1	0	1	1	1
1	0	0	1	0	0	1
1	1	0	0	1	1	1

Similarly, you can determine if a statement is a contradiction by making its truth table and seeing if it is always false.

1.6 Logical Equivalence

Two statements s_1 and s_2 are *logically equivalent* if $s_1 \leftrightarrow s_2$ is a tautology.

Informally, two statements s_1 and s_2 are logically equivalent if they have the same truth table (up to the order of the rows). This happens exactly when the statement $s_1 \leftrightarrow s_2$ is a tautology.

We use the notation $s_1 \Leftrightarrow s_2$ to denote the *fact* (theorem) that $s_1 \leftrightarrow s_2$ is a tautology, that is, that s_1 and s_2 are logically equivalent. Notice that $s_1 \leftrightarrow s_2$ is a statement and can in general be true or false, and $s_1 \Leftrightarrow s_2$ indicates the (higher level) fact that s_1 and s_2 always have the same truth value as each other. It is reasonable to regard logically equivalent statements as being "the same" in a similar way as we regard 0.25 and 2/8 as being the same.

Logical equivalence plays the same role in logic that equals does in algebra: it specifies when two expressions are "the same". In the same way that equal expressions can be freely substituted for each other without changing the meaning of an expression, logically equivalent statements can be freely substituted for each other without changing the meaning of a compound statement. And, if two statements are each equivalent to the same statement, they are equivalent to each other.

Since logical equivalence is defined in terms of a statement being a tautology, *a truth table can be used to check if (prove that) two statements are logically equivalent.* Soon we will have other methods to do this as well.

It follows from the work in Example 1.5.1 that $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$.

Example 1.6.1 *Use the definition to argue that $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$ and check your reasoning using a truth table.*

Solution

The negation of $p \wedge q$ asserts "it is not the case that p and q are both true". Thus, $\neg(p \wedge q)$ is true exactly when one or both of p and q is false, that is, when $\neg p$ is true or $\neg q$ is true. Therefore $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$.

Our reasoning is confirmed by the truth table below which shows that $\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$ is a tautology.

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$
0	0	1	1	0	1	1	1
0	1	1	0	0	1	1	1
1	0	0	1	0	1	1	1
1	1	0	0	1	0	0	1

Question 1.6.2 *Use the definition to argue that $\neg(p \vee q)$ is logically equivalent to $\neg p \wedge \neg q$ and check your reasoning using a truth table.*

Example 1.6.3 *Use the definition to argue that $p \to q$ is logically equivalent to $\neg p \vee q$, and check your work using a truth table.*

Solution

From the truth table for implies, the statement $p \to q$ is true precisely when p is false, or p and q are both true. Thus it is true precisely when $\neg p$ is true or q is true. Therefore, $p \to q \Leftrightarrow \neg p \vee q$.

Our reasoning is confirmed in the truth table below. Since the columns of the truth table under the statements $p \to q$ and $\neg p \vee q$ are identical, the double implication between these statements is a tautology. (Since this is clear, we have chosen not to show that column).

p	q	$\neg p$	$p \to q$	$\neg p \vee q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

Example 1.6.4 *Use the definition to argue that $\neg(p \to q)$ is logically equivalent to $p \wedge \neg q$, and check your work using a truth table.*

Solution

From the definition of implication, the statement $p \to q$ is false only in the *case that p is true and q is false. Thus $\neg(p \to q)$ is true only in the case that p is true and q is false, that is, when $p \wedge \neg q$ is true.*

Our reasoning is confirmed in the truth table below where, again, the column corresponding to $[\neg(p \to q)] \leftrightarrow [p \wedge \neg q]$ is omitted.

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg(p \to q)$	$p \wedge \neg q$
0	0	1	1	1	0	0
0	1	1	0	1	0	0
1	0	0	1	0	1	1
1	1	0	0	1	0	0

Example 1.6.4 can be approached in a different way, using logical equivalences. Since locally equivalent expressions can be freely substituted for each other,

$$\neg(p \to q) \Leftrightarrow \neg(\neg p \vee q) \Leftrightarrow \neg(\neg p) \wedge \neg q \Leftrightarrow p \wedge \neg q$$

where we have used the results of Example 1.6.3 and Question 1.6.2. Using known logical equivalences to establish new logical equivalences is preferable to making truth tables, especially if the number of statements involves is larger that 2. We will develop methods for doing this in Section 1.9

Question 1.6.5 *Use the definition to argue that $\neg(p \leftrightarrow q)$ is logically equivalent to $(p \wedge \neg q) \vee (\neg p \wedge q)$, and check your work using a truth table.*

1.7 Converse and Contrapositive of an Implication

The *converse* of the implication $p \to q$ is $q \to p$.

The converse of the statement "*if it is raining, then I don't go golfing*" is "*if I don't go golfing, then it is raining*". The first statement is true for the people I play with, while the second one isn't; there can be many other reasons to not go golfing, for example work commitments or extreme cold.

Following Example 1.2.1 (and immediately above) we noted that an implication and its converse can have different truth values. This assertion is re-confirmed in the truth table below our discussion of the contrapositive.

Therefore *an implication and its converse are not logically equivalent.* One of them can not be used in place of the other.

The *contrapositive* of the implication $p \to q$ is $\neg q \to \neg p$.

For example, when a and b are given integers, the contrapositive of "*if a and b are odd integers then the integer ab is odd*" is "*if the integer ab is even then it is not the case that the integers a and b are odd*", or equivalently "*if the integer ab is even then the integer a is even or the integer b is even*".

An implication and its contrapositive are logically equivalent. This assertion is confirmed by the truth table below.

				implication	contrapositive	converse
p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$	$q \to p$
0	0	1	1	1	1	1
0	1	1	0	1	1	0
1	0	0	1	0	0	1
1	1	0	0	1	1	1

For completeness, we note that the *inverse* of $p \to q$ is the statement $\neg p \to \neg q$. It is the contrapositive of the converse of $p \to q$ (or the other way around).

1.8 Necessary and Sufficient Conditions

Suppose you say "*if it is sunny outside, then I will go cycling*", intending that it be a true statement. (Possibly you will also go cycling if it cloudy but not windy, but are not saying that.) Then you are saying that the truth of the statement "*it is sunny outside*" is enough to guarantee the truth of the statement "*I will go cycling*". Most people would go cycling even if it were not sunny (maybe you are one of them), so the two statements are not logically equivalent.

The phrase *p is a sufficient condition for q*, or more briefly *p is sufficient for q*, is translated into symbols as the implication $p \to q$. The same is true of any equivalent phrasing that that suggests that doing p is enough to guarantee that q is also done, that is, if p happens, then q happens.

Now consider the (true) statement "*In order to get a Math degree, you must take Math 122*". It says that taking Math 122 is necessary for getting a

Math degree, that is, you need to do it. This is equivalent to the implication "*if you get a Math degree, then you have taken Math 122*". Most people take Math 122 and don't get a Math degree so the two statements are not logically equivalent.

The phrase *a is necessary for b* is translated into symbols as $b \to a$ (note which is the hypothesis of the implication and which is the conclusion!). The same is true of any equivalent phrasing that that suggests if you are going to to b, then you need to do a along the way, or that b happens only if a happens.

Example 1.8.1 *Write the following statements in symbols:*

1. *you must be at least four feet tall in order to ride the roller-coaster*
2. *a square is a rectangle*

Solution

1. *Let f be the statement "you are at least 4 feet tall", and let r be the statement "you can ride the roller-coaster". The given statement is saying that being at least 4 feet tall is a necessary condition for being able to ride the roller-coaster. Hence the statement is $r \to f$. (If you rode the roller-coaster, then you must have been at least 4 feet tall. Note that being 4 feet tall is definitely not a sufficient condition for being able to ride the roller-coaster, for example you also need to not be afraid of heights.)*
2. *Let s is the statement "this shape is a square" and c is the statement "this shape is a rectangle". The given statement is saying that being a square is a sufficient condition to guarantee. That is, if a shape is a square, then it is a rectangle. Hence the statement is $s \to c$. (Note that there are plenty of rectangles that are not squares, so being a square is not necessary for being a rectangle.)*

Combining the above, what does it mean to say that p is a necessary and sufficient condition for q? The statement "p is sufficient for q" is rendered symbolically as $p \to q$. The statement "p is necessary for q" is rendered symbolically as $q \to p$. Thus, "p is a necessary and sufficient condition for

q" is the same as $(q \to p) \land (p \to q)$, which (as we have seen) is logically equivalent to $p \leftrightarrow q$, or "p if and only if q".

Example 1.8.2 *The statement "this triangle is equilateral" it is necessary and sufficient for the statement "this triangle has three equal interior angles". Every equilateral triangle has three equal interior angles, so that the condition is sufficient. And every triangle with three equal interior angles is equilateral, so that the condition is necessary. Thus, the statements "this triangle has 3 equal interior angles" and "this triangle is equilateral" are logically equivalent and can be used interchangeably.*

1.9 The Laws of Logic

We now set out to develop an algebra of propositions. To do so, we need some basic operations (logical equivalences) that can be used. Each of the following can be verified (proved) with a truth table. In some cases we have already done that. It is a good idea to memorize them, so that they are at your fingertips when needed.

In what follows, **1** denotes a statement that is always true (i.e., a tautology), and **0** denotes a statement that is always false (i.e., a contradiction).

When we refer to "*The Laws of Logic*", we are referring to the following collection of logical equivalences.

- Idempotence: $p \lor p \Leftrightarrow p, \quad p \land p \Leftrightarrow p$
- Commutative: $p \land q \Leftrightarrow q \land p, \quad p \lor q \Leftrightarrow q \lor p$
- Associative: $(p \land q) \land r \Leftrightarrow p \land (q \land r), \quad (p \lor q) \lor r \Leftrightarrow p \lor (q \lor r)$
- Distributive: $p \lor (q \land r) \Leftrightarrow (p \lor q) \land (p \lor r), \quad p \land (q \lor r) \Leftrightarrow (p \land q) \lor (p \land r)$
- Double Negation: $\neg(\neg p) \Leftrightarrow p$
- DeMorgan's Laws: $\neg(p \lor q) \Leftrightarrow \neg p \land \neg q, \quad \neg(p \land q) \Leftrightarrow \neg p \lor \neg q$
- Identity: $p \land \mathbf{1} \Leftrightarrow p, \quad p \lor \mathbf{0} \Leftrightarrow p$
- Dominance: $p \land \mathbf{0} \Leftrightarrow \mathbf{0}, \quad p \lor \mathbf{1} \Leftrightarrow \mathbf{1}$

The following are some other useful logical equivalences.

- $p \to q \Leftrightarrow \neg p \vee q$
- $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p) \Leftrightarrow (\neg p \vee q) \wedge (p \vee \neg q)$

It is apparent that the Laws of Logic come in pairs. The *dual* of a statement is obtained by replacing $\vee$ by $\wedge$; $\wedge$ by $\vee$; **0** by **1**; and **1** by **0**, wherever they occur. It is a theorem of logic that if s_1 is logically equivalent to s_2, then the dual of s_1 is logically equivalent to the dual of s_2.

Example 1.9.1 *Use the Laws of Logic and other known logical equivalences to show that*

$$p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$$

Solution.

$$\begin{array}{lll}
p \leftrightarrow q & & \\
\quad \Leftrightarrow & (\neg p \vee q) \wedge (p \vee \neg q) & \text{Known L.E.} \\
\quad \Leftrightarrow & (\neg p \wedge (p \vee \neg q)) \vee (q \wedge (p \vee \neg q)) & \text{Distributive} \\
\quad \Leftrightarrow & [(\neg p \wedge p) \vee (\neg p \wedge \neg q)] \vee [(q \wedge p) \vee (q \wedge \neg q)] & \text{Distributive (twice)} \\
\quad \Leftrightarrow & [\mathbf{0} \vee (\neg p \wedge \neg q)] \vee [(q \wedge p) \vee \mathbf{0}] & \text{Known contradictions} \\
\quad \Leftrightarrow & (\neg p \wedge \neg q) \vee (q \wedge p) & \text{Identity} \\
\quad \Leftrightarrow & (p \wedge q) \vee (\neg p \wedge \neg q) & \text{Commutative } (2\times)
\end{array}$$

There are two other forms of the Distributive Laws. These can be derived from the versions given above.

Example 1.9.2 *Use the Laws of Logic and other known logical equivalences to show that*

$$(q \wedge r) \vee p \Leftrightarrow (q \vee p) \wedge (r \vee p)$$

Solution.

$$\begin{array}{lll}
(q \wedge r) \vee p & & \\
\quad \Leftrightarrow & p \vee (q \wedge r) & \text{Commutative} \\
\quad \Leftrightarrow & (p \vee q) \wedge (p \vee r) & \text{Distributive} \\
\quad \Leftrightarrow & (q \vee p) \wedge (r \vee p) & \text{Commutative (twice)}
\end{array}$$

Question 1.9.3 *Use the Laws of Logic and other known logical equivalences to show that*

$$(q \vee r) \wedge p \Leftrightarrow (q \wedge p) \vee (r \wedge p)$$

The Laws of Logic can be used in several other ways. One of them is to prove that a statement is a tautology without resorting to a truth table. This amounts to showing it is logically equivalent to **1**.

Example 1.9.4 *Use the Laws of Logic and other known logical equivalences to show that* $\neg q \vee (p \to q)$ *is a tautology.*

Solution.

$$\begin{array}{lllr}
\neg q \vee (p \to q) & & & \\
 & \Leftrightarrow & \neg q \vee (\neg p \vee q) & \text{Known L.E.} \\
 & \Leftrightarrow & \neg q \vee (q \vee \neg p) & \text{Commutative} \\
 & \Leftrightarrow & (\neg q \vee q) \vee \neg p & \text{Associative} \\
 & \Leftrightarrow & \mathbf{1} \vee \neg p & \text{Known tautology} \\
 & \Leftrightarrow & \mathbf{1} & \text{Dominance}
\end{array}$$

Therefore $\neg q \vee (p \to q)$ *is a tautology.*

Similarly, a statement is proved to be a contradiction when it is shown to be logically equivalent to **0**.

Another use of the Laws of Logic is to "simplify" statements. While the term "simplify" needs to be explained (quantified somehow) to be meaningful, or so we know when we are done, sometimes it is clear that an equivalent expression found is simpler than the one that was started with.

Example 1.9.5 *Use the Laws of Logic and other known logical equivalences to simplify the expression* $\neg(\neg p \to q) \vee (p \wedge \neg q)$.

Solution.

$$\begin{array}{lllr}
\neg(\neg p \to q) \vee (p \wedge \neg q) & & & \\
 & \Leftrightarrow & \neg(\neg\neg p \vee q) \vee (p \wedge \neg q) & \text{Known L.E.} \\
 & \Leftrightarrow & \neg(p \vee q) \vee (p \wedge \neg q) & \text{Double Negation} \\
 & \Leftrightarrow & (\neg p \wedge \neg q) \vee (p \wedge \neg q) & \text{DeMorgan} \\
 & \Leftrightarrow & (p \vee \neg p) \wedge \neg q & \text{Dist've (from right to left)} \\
 & \Leftrightarrow & \mathbf{1} \wedge \neg q & \text{Known tautology} \\
 & \Leftrightarrow & \neg q & \text{Identity}
\end{array}$$

Thus $\neg q$ *is a simpler form of* $\neg(\neg p \to q) \vee (p \wedge \neg q)$ *which is logically equivalent to it.*

Example 1.9.6 *Use the Laws of Logic and other known logical equivalences to show that*

$$(p \wedge q) \wedge [(q \wedge \neg r) \vee (p \wedge r)] \Leftrightarrow \neg(p \to \neg q)$$

Solution.
Use LHS *to denote the expression on the left hand side. Then*

$$\begin{array}{lll}
LHS & & \\
\Leftrightarrow & [(p \wedge q) \wedge (q \wedge \neg r)] \vee (p \wedge q) \wedge (p \wedge r)] & \text{Distributive} \\
\Leftrightarrow & [((p \wedge q) \wedge q) \wedge \neg r) \vee [((p \wedge q) \wedge p) \wedge r)] & \text{Associative} \\
\Leftrightarrow & [(p \wedge (q \wedge q)) \wedge \neg r) \vee [((p \wedge p) \wedge q) \wedge r)] & \text{Commutative, Associative} \\
\Leftrightarrow & [(p \wedge q) \wedge \neg r) \vee [(p \wedge q) \wedge r)] & \text{Idempotence} \\
\Leftrightarrow & (p \wedge q) \wedge (\neg r \vee r) & \text{Distributive} \\
\Leftrightarrow & (p \wedge q) \wedge \mathbf{1} & \text{Known tautology} \\
\Leftrightarrow & (p \wedge q) & \text{Identity} \\
\Leftrightarrow & \neg\neg(p \wedge q) & \text{Double Negation} \\
\Leftrightarrow & \neg(\neg p \vee \neg q) & \text{DeMorgan} \\
\Leftrightarrow & \neg(p \to \neg q) & \text{Known L.E.}
\end{array}$$

1.10 Using Only And, Or, and Not

It turns out that any statement is logically equivalent to one that uses only $\neg$ and the connectives $\wedge, \vee$. The logical equivalences above allow statements involving the logical connectives $\to$ and $\leftrightarrow$ to be replaced by equivalent statements that use only $\wedge, \vee$, and $\neg$.

It is also possible to do this directly from the truth table, as will now be demonstrated.

Example 1.10.1 *Let* s *be the statement involving* p *and* q *for which the truth table is given below.*

p	q	s
0	0	1
0	1	1
1	0	0
1	1	1

Find a statement logically equivalent to s that uses only $\neg$ and the connectives $\wedge, \vee$.

Solution.
First, for each row of the truth table where the statement s is true, write a statement that's true only when p and q have the truth values in that row. This statement will involve the logical connective "and". For the truth table above:

- *Row 1:* $\neg p \wedge \neg q$
- *Row 2:* $\neg p \wedge q$
- *Row 4:* $p \wedge q$

Now, to get an expression that's logically equivalent to s, take the disjunction of these statements: it will be true exactly when the truth values of p and q correspond to a row of the truth table where s is true (row 1 or row 2 or row 4). Thus $s \Leftrightarrow (\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q)$.

The process is exactly the same for any statement given by a truth table, if there are more than two statements involved.

There is some terminology and an important fact (important in computer science) associated with what we have done. The expression associated with each row of the truth table – a conjunction of variables or their negations – is called a *minterm.* The compound statement derived using the process consists of the disjunction of a collection of minterms (that is, they are all joined together using "or"). It is called the *disjunctive normal form* of the statement s. Since every statement has a truth table, and every truth table leads to a statement constructed as above, a consequence of the procedure just described is the theorem that *every statement is logically equivalent to one that is in disjunctive normal form.*

It can be observed directly from the truth table that

$$\begin{array}{rcll} s & \Leftrightarrow & p \to q & \\ & \Leftrightarrow & \neg p \vee q & \text{Known L.E.} \end{array}$$

The principle that things that are logically equivalent to the same statement are logically equivalent to each other now implies it should be true that that

$(\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q) \Leftrightarrow \neg p \vee q$. This can be shown with the Laws of Logic.

Question 1.10.2 *Use the Laws of Logic and other known logical equivalences to show that*

$$(\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q) \Leftrightarrow \neg p \vee q$$

It is possible to go beyond writing statements so they involve only $\wedge, \vee$, and $\neg$. With careful use of DeMorgan's Laws, really only $\vee$ and $\neg$, or $\wedge$ and $\neg$, are needed.

Example 1.10.3 *Find an expression logically equivalent to $p \leftrightarrow q$ that uses only $\vee$ and $\neg$.*

Solution.. *We know $p \leftrightarrow q \Leftrightarrow (\neg p \vee q) \wedge (\neg q \vee p)$. By DeMorgan's Law, $(\neg p \vee q) \wedge (\neg q \vee p) \Leftrightarrow \neg\big(\neg(\neg p \vee q) \vee \neg(\neg q \vee p)\big)$, so $p \leftrightarrow q \Leftrightarrow \neg\big(\neg(\neg p \vee q) \vee \neg(\neg q \vee p)\big)$. The latter statement uses only $\vee$ and $\neg$.*

If you use DeMorgan's Law in a different way, then you can get an expression for $p \leftrightarrow q$ than involves only $\wedge$ and $\neg$.

Question 1.10.4 *Find an expression logically equivalent to $p \leftrightarrow q$ that uses only $\wedge$ and $\neg$.*

One can go a bit farther and introduce the logical connective "nand" (not and), so that "p nand q" is the statement $\neg(p \wedge q)$. It transpires that any proposition can be expressed (in a possibly complicated way) using only "nand". The same thing applies to "nor", where "p nor q" is the statement $\neg(p \vee q)$.

1.11 Logical Implication

We say p *logically implies* q when $p \rightarrow q$ is a tautology.

Informally, a statement p logically implies a statement q if the truth of p guarantees the truth of q. This happens exactly when $p \rightarrow q$ is a tautology. Note that we are not concerned about what happens if p is false. This is because of the truth table for implies: $p \to q$ is true (by definition) when p is false.

We use the notation $p \Rightarrow q$ to denote the fact (theorem) that $p \to q$ is a tautology, that is, that p logically implies q. Notice that $p \to q$ is a statement and can in general be true or false, and $p \Rightarrow q$ indicates the (higher level) fact that the truth of p guarantees the truth of q.

Example 1.11.1 *Argue that* $(a \wedge b) \Rightarrow a$.

Solution.
We need to argue that $(a \wedge b) \to a$ *is a tautology. By the definition of implication, the statement is true whenever the hypothesis* $a \wedge b$ *is false. Suppose that* $a \wedge b$ *is true. Then* a *and* b *are both true. Therefore,* $(a \wedge b) \to a$ *is true. It follows that* $(a \wedge b) \to a$ *is a tautology.*

The example above could have also been done by making a truth table to verify that $(a \wedge b) \to a$ is a tautology.

By the example above, if in the midst of an argument, we were to discover that $a \wedge b$ is true, we would be entitled to conclude (infer, or deduce) that a is true (and the same for b). In the next section we will develop a collection of basic rules for making inferences.

In what follows we argue that *the logical equivalence* $p \Leftrightarrow q$ *is the same as the two logical implications* $p \Rightarrow q$ *and* $q \Rightarrow p$. Suppose $p \Leftrightarrow q$. Then $p \leftrightarrow q$ is a tautology. Since $p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$, the latter statement is also a tautology. By Example 1.11.1, each of $(p \to q)$ and $(q \to p)$ is a tautology. Therefore $p \Rightarrow q$ and $q \Rightarrow p$ (the latter could also be written as $p \Leftarrow q$; the intended meaning of the notation is obvious). In the same way, if both $p \Rightarrow q$ and $p \Leftarrow q$, then $p \Leftrightarrow q$.

1.12 Valid Arguments and Inference Rules

An *argument* is an implication $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$. The statements $p_1, p_2, \ldots, p_n$ are called *premises*, and the statement q is called the *conclusion*. Put differently, an argument is an assertion. Since the truth table for implies says that an implication is true when its hypothesis is false, and since the hypothesis is the conjunction of all of the premises, the assertion being made is that *if the premises are all true, then so is the conclusion.*

An argument is called *valid* if the implication is a tautology (i.e., if the premises logically imply the conclusion, so that the conclusion is guaranteed to be true when all of the hypotheses are true), otherwise it is *invalid.*

To show that an argument is invalid, it needs to be demonstrated that the implication is not a tautology. From the truth table for implies, this amounts to describing a single row of a truth table where each premise is true and the conclusion is false. Such a collection of truth values is called a *counterexample* to the argument.

Arguments are usually presented in the tabular format shown below for the example $[(p \to \neg q) \wedge (\neg r \to p) \wedge q] \to \neg r$. The premises are listed first, and then the conclusion is listed below a separating line.

$$\begin{array}{r} p \to \neg q \\ \neg r \to p \\ q \\ \hline \therefore\ \neg r \end{array}$$

Example 1.12.1 *Show that the argument above is invalid.*

Solution. *We need to give a counterexample: a truth value assignment for p, q and r such that the premises are all true and the conclusion is false. It is best to start by determining what's needed for the conclusion to be false, and then figure out what's needed for the premises to all be true.*

In order for the conclusion to be false, $\neg r$ must be false, hence r must be true.

When $\neg r$ is false, the second premise is true no matter if p is true or false (this one is free!). The truth of third premise gives us that q must true. Finally, we want to choose a truth value for p so that the first premise is true. When p is false, the implication $p \to \neg q$ is true. (And since $\neg q$ is false, this is the only possible truth value assignment to p that makes the first premise true.) Thus, if p, q, r have the truth values $0, 1, 1$, respectively, the premises are all true and the conclusion is false. Therefore, the argument is not valid.

A truth table can, in principle, be used to show an argument is valid or invalid. But, if the number of premises involved is large, so is the table. A better way is to give a *proof*: a chain of logical equivalences and implications involving the premises (which are assumed to be true because an implication is true when its hypothesis is false). The idea is that *every statement you write down is true, and is either a premise, or an allowed additional hypothesis, or is derived from statements known to be true via logical equivalences and implications.*

Our ultimate goal is to write mathematical proofs in words. Proving logical implications using inference rules and logical equivalences is a step towards that goal. When we write proofs in words we will use the same basic framework: write down the premises, and then make a sequence of true statements which are either known from before, allowed additional hypotheses. or derived from statements known to be true via logical equivalences and implications, until the desired conclusion is finally reached.

The two following *inference rules* are each a logical implication. They are just common sense, but can be formally proved with a truth table. These will get used frequently in arguments and hence need to be at your fingertips, so they should be memorized.

- Modus Ponens: $(p \to q) \wedge p \Rightarrow q$
- Chain Rule (Law of Syllogism): $(p \to q) \wedge (q \to r) \Rightarrow p \to r$

We use these inference rules to prove some other rules. The rules above are worth memorizing. The rules in the examples and question below are easy consequences of them and need not be remembered.

Example 1.12.2 *Prove the rule Modus Tollens:* $[(p \to q) \wedge \neg q] \Rightarrow \neg p$.

Proof.

1.	$p \to q$	Premise
2.	$\neg q \to \neg p$	L.E. to 1
3.	$\neg q$	Premise
4.	$\therefore\ \neg p$	$2, 3,$ M.P.

Question 1.12.3 *Prove the rule Disjunctive Syllogism:* $[(p \vee q) \wedge \neg p] \Rightarrow q$.

Example 1.12.4 *Prove the rule Resolution:* $[(p \vee r) \wedge (q \vee \neg r)] \Rightarrow p \vee q$.

Proof.

1.	$p \vee r$	Premise
2.	$\neg p \rightarrow r$	L.E. to 1
3.	$q \vee \neg r$	Premise
4.	$\neg r \vee q$	3, Commutative
5.	$r \rightarrow q$	L.E. to 4
6.	$\neg p \rightarrow q$	2, 5, Chain Rule
7.	$p \vee q$	L.E. to 6

Here are two more inference rules which are clearly true, and which can be formally proved with a truth table.

- Disjunctive Amplification: $p \Rightarrow p \vee q$
- Conjunctive Simplification: $p \wedge q \Rightarrow p$

Question 1.12.5 *Argue in words that the rules Disjunctive Amplification and Conjunctive Simplification hold (i.e., that the corresponding implications are tautologies), and then verify your work with a truth table.*

Example 1.12.6 *Use inference rules and logical equivalences to establish the validity of the argument:*

$$\begin{array}{r} \neg p \leftrightarrow q \\ \neg q \rightarrow r \\ p \\ \hline \therefore\ r \end{array}$$

Proof.

1.	$\neg p \leftrightarrow q$	Premise
2.	$(\neg p \rightarrow q) \wedge (q \rightarrow \neg p)$	L.E. to 1
3.	$q \rightarrow \neg p$	2, Conjunctive Simplification
4.	$p \rightarrow \neg q$	3, Contrapositive
5.	$\neg q \rightarrow r$	Premise
6.	$p \rightarrow r$	4, 5, Chain Rule
7.	p	Premise
8.	r	6, 7, M.P.

The validity or invalidity of argument which is given in words can established as before. Before doing that, the argument needs to be translated into symbolic form.

Example 1.12.7 *Determine whether the argument below is valid or invalid, and give a proof or counterexample as appropriate.*

If I run, then my ankle does not hurt
If I am not injured, then I run
My ankle hurts

∴ *I am injured*

Solution. *Let p, q, and r denote the statements "I run", "My ankle hurts", and "I am injured", respectively. Then the argument is:*

$$\begin{array}{r} p \to \neg q \\ \neg r \to p \\ q \\ \hline \therefore\ r \end{array}$$

If we try to construct a counterexample in the same way as in Example 1.12.1, then we will not be able to find a way to assign truth values so that the conclusion is false and all premises are true. This suggests that the argument is valid (unlike most stories about sports injuries). We can prove it using inference rules.

1.	$p \to \neg q$	Premise
2.	$\neg r \to p$	Premise
3.	$\neg r \to \neg q$	2, 1, Chain Rule
4.	$q \to r$	3, Contrapositive
5.	q	Premise
6.	$\therefore\ r$	4, 5, M.P.

We conclude this section with two more inference rules that can be proved with a truth table, and then some discussion about them.

- Proof by Contradiction: $(\neg p \to \mathbf{0}) \Rightarrow p$
- Proof by Cases: $(p \to r) \wedge (q \to r) \Rightarrow (p \vee q) \to r$

Question 1.12.8 *Argue in words that the rules Proof by Contradiction and Proof by Cases hold (i.e., that the corresponding implications are tautologies), and then verify your work with a truth table.*

The idea behind "Proof by Contradiction" is that one should only be able to obtain true statements when starting with true statements, and using logical equivalences and logical implications. Hence, if falsity of the desired conclusion leads to a statement that is never true (that is, a contradiction), then the conclusion can not be false. Here, we illustrate the use of this rule in a proof of the type above by giving a second proof of the rule "Resolution".

Example 1.12.9 *Use Proof by Contradiction to establish the validity of the rule Resolution.*

Proof.

1.	$\neg(p \vee q)$	Negation of conclusion, for proof by contradiction
2.	$\neg p \wedge \neg q$	1, DeMorgan
3.	$\neg p$	2, Conjunctive Simplification
4.	$\neg q$	2, Conjunctive Simplification
5.	$p \vee r$	Premise
6.	$\neg p \to r$	L.E. to 5
7.	r	3, 6, M.P.
8.	$q \vee \neg r$	Premise
9	$\neg q \to \neg r$	L.E. to 8
10.	$\neg r$	4, 9, M.P.
11.	$r \wedge \neg r \quad (\Leftrightarrow \mathbf{0})$	Known contradiction from 7, 10
12.	$p \vee q$	1, 11, Proof by Contradiction

The rule "Proof by Contradiction" is better illustrated by a proof in words. An example will be given in Section 2.4.

The intuition behind "Proof by Cases" is simple enough. If the truth of p guarantees the truth of a conclusion, r, and the truth of q guarantees the truth of r, and one of p and q must be true, then r must be true. The way this rule is applied is that *if one of several cases must arise, and the desired conclusion holds in each case, then the premises logically imply the conclusion.* This rule is also best illustrated by by a proof in words. An example will be given in Section 2.4.

1.13 Proving Implications

Consider the following (valid) argument

$$\begin{array}{rl} & u \to r \\ & (r \wedge s) \to (p \vee t) \\ & q \to (u \wedge s) \\ & \neg t \\ \hline \therefore & q \to p \end{array}$$

If you go about trying to prove the validity of this argument using the inference rules in the previous section, then it is quite likely to end in frustration. The question is *how do we establish the validity of an argument whose conclusion is an implication?*.

When the conclusion is an implication like $q \to p$, we can approach proving validity of the validity of the argument using proof by cases. The statement q is either false or true. When q is false, the desired conclusion $q \to p$ is true by the definition of implication (we don't even need to use the premises!). Thus it remains to show the desired conclusion holds when q is true. That means we can add the additional premise that q is true. And if we do that, then proving that $q \to p$ is true is equivalent to proving p is true because if q is true and p is true, then $q \to p$ is true. Once we've shown that $q \to p$ is true in the two possible cases that can arise, then we can use Proof By Cases to conclude that the argument is valid. It is common in mathematics to not even mention the case where q is false, and simply take q as an addition premise (i.e., assume it is true), and then argue that p must be true.

The discussion in the previous paragraph comes down to the logical equivalence $a \to (b \to c) \Leftrightarrow (a \wedge b) \to c$.

Question 1.13.1 *Use known logical equivalences to show that* $a \to (b \to c) \Leftrightarrow (a \wedge b) \to c$.

With respect to the argument given at the start of the section, let a be the conjunction of its premises. Then the argument is $a \to (q \to p)$. By Question 1.13.1, this statement is locally equivalent to $(a \wedge b) \to c$. Therefore, the argument $a \to (q \to p)$ is valid (i.e., the implication is a tautology) precisely when the argument $(a \wedge b) \to c$ is valid. Hence the validity of the given argument can be established by establishing the validity of the argument:

$$\begin{array}{ll} & u \to r \\ & (r \wedge s) \to (p \vee t) \\ & q \to (u \wedge s) \\ & \neg t \\ & q \\ \hline \therefore & p \end{array}$$

Question 1.13.2 *Establish the validity of the argument immediately above.*

1.14 Exercises

1. If the statement $q \wedge r$ is true, determine all combinations of truth values for p and s such that the statement $(q \to [\neg p \vee s]) \wedge [\neg s \to r]$ is true.

2. Suppose $\neg[(p \to q) \leftrightarrow (q \to p)]$ is false. Can $p \leftrightarrow q$ have both possible truth values? Explain.

3. Is $(p \to q) \to [(p \to q) \to q]$ a tautology? Why or why not?

4. Show that $[(p \vee q) \wedge (r \vee \neg q)] \to (p \vee r)]$ is a tautology by making a truth table, and then again by using an argument in words that considers the two cases "q is true" and "q is false".

5. Show that the two statements $(p \wedge q) \to r$ and $(p \to r) \wedge (q \to r)$ are not logically equivalent.

6. Consider the statement "if the goods are unsatisfactory, then your money will be refunded". This was an advertising slogan of the T. Eaton Company. Is the given statement logically equivalent to "goods satisfactory or money refunded"? What about to "if your money is not refunded, then the goods are satisfactory"? And what about to "if the goods are satisfactory, then your money will not be refunded".

7. Write each of the following statements, in English, in the form “if p, then q”.

   (a) I go swimming on Mondays.

   (b) In order to be able to go motorcycling on Sunday, the weather must be good.

   (c) Eat your vegetables or you can’t have dessert.

   (d) You can ride a bicycle only if you wear a helmet.

   (e) Polynomials are continuous functions.

   (f) A number n that is a multiple of 2 and also a multiple of 3 is a multiple of 6.

   (g) You can’t have any pudding unless you eat your meat.

8. Write in English the converse, contrapositive and negation of each statement.

   (a) If I had \$1,000,000, I’d buy you a fur coat.

   (b) If it is not raining and not windy, then I will go running or cycling.

   (c) A day that’s sunny and not too windy is a good day for walking on the waterfront.

   (d) If 11 pigeons live in 10 birdhouses, then there are two pigeons that live in the same birdhouse.

   (e) If every domino covers a black square and a white square, then the number of black squares equals the number of white squares.

9. Determine if each statement below is true or false, and explain your reasoning.

   (a) It is possible for an implication and its contrapositive to have different truth values.

   (b) If the statement q is true, then, for any statement p, the statement $p \to q$ is true.

   (c) If $s_1 \to s_2$ is a contradiction, then so is its contrapositive.

   (d) There are truth values for p and q such that $p \to q$ and $q \to p$ are both false.

(e) $(\neg p \vee q) \wedge \neg(\neg p \vee q)$ is a contradiction.

(f) If the statement $\mathcal{P}$ is a contradiction, then, for any statement q, the statement $\mathcal{P} \to q$ is a tautology.

(g) If two statements are logically equivalent, then so are their negations.

10. A sign posted outside of Tokyo says "*In order to attack the city, you must be green and related to Godzilla. If you are not green and not related to Godzilla, then you can not attack the city*".

    (a) Render the two statements on the sign in symbols. Start with: *Let a be the assertion "you can attack the city"*, and carry on from there.

    (b) Argue that the two statements on the sign are not logically equivalent, contrary to what the author probably intended. Which is more restrictive on who can attack Tokyo?

    (c) Correct the second statement so that it is logically equivalent to the first one.

11. Use known logical equivalences to show that $(\neg a \to b) \wedge (\neg b \vee (\neg a \vee \neg b))$ is logically equivalent to $\neg(a \leftrightarrow b)$.

12. Use known logical equivalences to show that $\neg(p \leftrightarrow q)$ is logically equivalent to $(p \vee q) \wedge (p \to \neg q)$.

13. Find an expression logically equivalent to $\neg(p \leftrightarrow q)$ that involves only $\neg$ and $\vee$.

14. Let s be the statement whose truth table is given below.

p	q	r	s
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

(a) Express the statement s in terms of p, q and r in such a way that only negation ($\neg$) and the logical connectives $\vee$ and $\wedge$ are used.

(b) Find an equivalent formulation of s that uses only $\neg$ and $\vee$.

(c) Find an equivalent formulation of s that uses only $\neg$ and $\wedge$.

15. Define the logical connective "nand" (not and) by $p \overline{\wedge} q \Leftrightarrow \neg(p \wedge q)$.

    (a) Find a representation of each of the following statements using only the logical connective nand.

    i. $\neg p$

    ii. $p \wedge q$

    iii. $p \vee q$

    iv. $p \rightarrow q$

    v. $p \leftrightarrow q$

    (b) Explain why every statement has a representation using only the logical connective nand.

16. (a) Argue that "logically implies" has the property (called *transitivity*) that if a, b and c are statements such that $a \Rightarrow b$ and $b \Rightarrow c$, then $a \Rightarrow c$.

    (b) Suppose a, b, c and d are statements such that $a \Rightarrow b$, $b \Rightarrow c$, $c \Rightarrow d$, and $d \Rightarrow a$. Argue that any two of these statements are logically equivalent.

17. Determine whether each statement is true or false, and briefly explain your reasoning.

    (a) If an argument is valid then it is possible the conclusion to be false when all premises are true.

    (b) If the premises can't all be true, then the argument is valid.

    (c) If $p \Leftrightarrow q$ and $q \Leftrightarrow r$, then $p \Leftrightarrow r$.

18. Show that the argument

$$\begin{array}{rl} & p \leftrightarrow q \\ & q \rightarrow r \\ & r \vee \neg s \\ & \neg s \rightarrow q \\ \hline \therefore & s \end{array}$$

is invalid by providing a counterexample.

19. Use basic inference rules to establish the validity of the argument

$$\begin{array}{lr} & p \to \neg q \\ & q \lor r \\ & p \lor u \\ & \neg r \\ \hline \therefore & u \end{array}$$

20. Use any method to show the following argument is valid.

$$\begin{array}{lr} & p \\ & \neg q \leftrightarrow \neg p \\ \hline \therefore & q \end{array}$$

21. Show that the following argument is not valid.

$$\begin{array}{lr} & p \lor r \\ & p \lor q \\ \hline \therefore & q \lor r \end{array}$$

22. Write the argument below in symbolic form. If the argument is valid, prove it. If the argument is not valid, give a counterexample:

$$\begin{array}{ll} & \text{If I watch football, then I don't do mathematics} \\ & \text{If I do mathematics, then I watch hockey} \\ \hline \therefore & \text{If I don't watch hockey, then I watch football} \end{array}$$

23. Write the argument below in symbolic form. If the argument is valid, prove it. If the argument is not valid, give a counterexample:

$$\begin{array}{ll} & \text{If you are pregnant or have a heart condition,} \\ & \quad \text{then you can not use the hot tub} \\ & \text{You do not have a heart condition} \\ & \text{You can use the hot tub.} \\ \hline \therefore & \text{You are not pregnant} \end{array}$$

24. If the argument below is valid, then use any method to prove it. Otherwise, give a counterexample to show that the argument is invalid.

$$\begin{array}{rr} & \neg r \rightarrow p \\ & q \rightarrow \neg p \\ \hline \therefore & \neg(r \vee t) \rightarrow \neg q \end{array}$$

Chapter 2

Quantifiers and Written Proofs

In this chapter we make the transition from writing symbolic proofs to writing convincing arguments (i.e. proofs) in English. A number of tools for proving mathematical statements will be introduced, and then others will be added to our toolkit as time goes by. (Note: no one gets to know for sure which tool will work in a given situation, but experience can help make it possible to know which ones are likely to work, and in which order various methods should be tried.) Each proof strategy will make use of the logic and structure developed in the previous chapter.

2.1 Open Statements

An *open statement* is an assertion that contains one or more variables. When the context is clear, we will drop the qualifier "open", and refer to assertions that contain one or more variables as *statements*.

An example of an open statement is "x *is a root of* $x^2 - 5x + 6$". It is not possible to know the truth value of this statement until you know the value of x. This statement is true if $x = 3$, and false if $x = 1$. It is never true if x is required to be a negative real number, and (as we've seen) can be true if x is required to be a positive real number.

The *universe of a variable* is the collection of allowed replacements for the variable.

Depending on the universe, a statement could be true sometimes and false sometimes, or always true, or never true. An example is $x^2 = 2$. If x can be any real number, then this statement is true when $x = \sqrt{2}$ and when $x = -\sqrt{2}$. If x must be an integer, then it is never true.

It is also possible that a statement does not make sense for a given universe. For example the statement "$n < 5$" does not make sense if n is a complex number. We will assume that statements make sense for the universe under consideration.

The point to remember about open statements is that *once the variables are assigned values (from the universe), then the resulting statement has a truth value.*

Before the variables have values, we only have a chance to know if an open statement is (i) always true (no matter which allowed values are assigned to the variables), (ii) always false (no matter which allowed values are assigned to the variables), or (iii) sometimes true and sometimes false (depending on which of the allowed values are assigned to the variables).

The Laws of Logic and other logical equivalences apply to open statements involving variables because they apply in exactly the same way each time allowed values are given to the variables. Thus, for example, if $p(x)$ and $q(x)$ are open statements involving the variable x, then for every allowed replacement x_0 for x, $p(x_0)$ and $q(x_0)$ are statements as in Chapter 1 – each of them is either true or false – and $\neg(p(x_0) \vee q(x_0))$ has the same truth value as $\neg p(x_0) \wedge \neg q(x_0)$. Thus we say the open statement $\neg(p(x) \vee q(x)$ is logically equivalent to the open statement $\neg p(x) \wedge \neg q(x)$. Similarly, the contrapositive of the open statement $p(x) \to q(x)$ is the open statement $\neg q(x) \to \neg p(x)$, and so on.

Question 2.1.1 *Let $p(x)$ and $q(x)$ be open statements involving the variable x, with respect to some given universe. Use the Laws of Logic and other known logical equivalences to show that $\neg(p(x) \to q(x))$ is logically equivalent to $p(x) \wedge \neg q(x)$.*

2.2 Quantifiers

When we make an assertions like "*if* $x^2+3x+2 = 0$ *then* $x = -1$ *or* $x = -2$", the intention is to convey that the assertion holds for every real number x.

That is, a complete specification of the assertion is "*For every real number x, if $x^2 + 3x + 2 = 0$ then $x = -1$ or $x = -2$.*" Notice that this statement has a truth value.

Similarly, an assertion like "*some rectangles are squares*" is intended to convey that at least one rectangle is a square. Thus a more precise specification of the assertion is "*There exist rectangles which are squares.*" Again, notice that this statement has a truth value.

The *existential quantifier*, $\exists$, asserts that *there exists* at least one allowed replacement for a variable for which the given statement is true. Think of the backwards "E" as representing "exists". Synonyms for "*there exists*" include "*there is*", "*there are*", "*some*", and "*at least one*".

Example 2.2.1 *Express the statement* "there exists an integer n such that n squared minus n plus one equals zero" *using an existential quantifier, and determine its truth value.*

Solution.
A symbolic representation of this statement is $\exists n, n^2 - n + 1 = 0$, where the universe of n is the integers.

This statement is false. The equation $n^2 - n + 1 = 0$ has no solutions in the real numbers, so it has no integer solutions.

The comma following an existential quantifier is best read as "such that", as in the textual representation of the statement in the example above.

Question 2.2.2 *Express the statement* "there exists an integer n such that 2 to the power of n is greater than n cubed" *using an existential quantifier, and determine its truth value.*

Example 2.2.3 *Suppose the universe of x is the real numbers. Express that statement $\exists x, x^2 > x^3$ in English, without symbols except for x, and determine its truth value.*

Solution.
The statement is "There exists a real number x such that x squared is greater than x cubed.".

This statement is true. When $x = -2$ we have $(-2)^2 = 4 > (-2)^3 = -8$.

Question 2.2.4 *Suppose the universe of* n *is the integers. Express the statement* $\exists n, 2n > 3n$ *in English, without symbols except for* n*, and determine its truth value.*

Question 2.2.5 *Suppose the universe is the integers. Explain why the statement* $\exists n, (n > 10) \to (0 = 1)$ *is true.*

An existential quantifier is like the logical connective "or". For example, if the universe of n is the positive integers and $p(n)$ is an open statement, then $\exists n, p(n)$ is asserting that $p(n)$ is true when $n = 1$, or it is true when $n = 2$ or when $n = 3$, and so on.

Example 2.2.6 *Suppose the universe consists of the integers 1, 2, 3. Write a statement logically equivalent to* $\exists x, x < 3$ *which does not involve a quantifier, and determine its truth value.*

Solution.
The quantified statement is logically equivalent to

$$(1 < 3) \vee (2 < 3) \vee (3 < 3)$$

which is true because (for example) $1 < 3$ *is true.*

Question 2.2.7 *Suppose the universe consists of the integers 1, 2, 3. Write a statement logically equivalent to* $\exists x, x^2 = 2x + 3$ *which does not involve a quantifier, and determine its truth value.*

The *universal quantifier*, $\forall$, asserts that the given statement is true *for all* allowed replacements for a variable. Think of the upside-down "A" as representing "All". Synonyms for "*for all*", include "*all*", "*every*" and "*for each*".

Example 2.2.8 *Express the statement "for all positive integers n, the integer 10n is greater than n" using a universal quantifier, and determine its truth value.*

Solution.
A symbolic representation of this statement is $\forall n, 10n > n$*, where the universe of* n *is the positive integers.*

The statement is true. If n *is a positive integer, then so is* $10n$*, and* $10n - n = 9n > 0$ *since* $n > 0$*.*

The comma following a universal quantifier is best read as a pause, as it is in the textual representation of the statement.

Question 2.2.9 *Express the statement "for all real numbers x, 2 times x is greater than or equal to x " using a universal quantifier, and determine its truth value.*

Example 2.2.10 *Suppose the universe of x is the non-zero real numbers. Express the statement $\forall x, \frac{1}{x} < x$ in English, without symbols except for numbers and x, and determine its truth value.*

Solution.
The statement is "For every non-zero real number x, the fraction 1 over x is less that x." *The statement is false. If $x = \frac{1}{2}$ then $\frac{1}{x} = 2$, and 2 is not less than $\frac{1}{2}$.*

Question 2.2.11 *Suppose the universe is the integers. Express the statement $\forall x, x^2 \neq x$ in English, without symbols except for numbers and x and without using the word "not", and determine its truth value.*

A universal quantifier is like the logical connective "and". For example, if the universe of n is the positive integers and $p(n)$ is an open statement, then $\forall n, p(n)$ is asserting that $p(n)$ is true when $n = 1$, and when $n = 2$, and when $n = 3$, and so on.

Example 2.2.12 *Suppose the universe of x consists of the integers 1, 2, 3. Write a statement logically equivalent to $\forall x, x > 1$ which does not involve a quantifier, and determine its truth value.*

Solution.
The quantified statement is logically equivalent to

$$(1 > 1) \wedge (2 > 1) \wedge (3 > 1),$$

which is false because $1 > 1$ is false.

Question 2.2.13 *Suppose the universe of x consists of the integers 1, 2, 3. Write a statement logically equivalent to $\forall x, 2x \neq 8$ which does not involve a quantifier, and determine its truth value.*

When quantifiers are nested, they are read in order from left to right. For example, if x and y are understood to be real numbers, "$\forall x, \exists y, x + y = 0$" is read as follows: *for all x, the statement "$\exists y, x + y = 0$" is true.* It is saying that no matter which real number x is chosen, once it is known there is a real number y such that $x + y = 0$. This is true because the number y can be chosen to be the negative of x. Hence, $\exists y, x + y = 0$ is true for any x. Consequently, $\forall x, \exists y, x + y = 0$ is true.

By contrast, $\exists y, \forall x, x + y = 0$ is saying that there is a number y such that for every number x, the sum $x + y$ is zero. This is false. One of the options for x is $y^2 + 1$. For this choice of x, we have $x + y = y^2 + y + 1$, so that $x + y = 0$ if and only if $y^2 + y + 1 = 0$. The latter equation has no solutions in the real numbers.

The lesson to be learned is that *the order of quantifiers is important.* Reversing the order of the quantifiers completely changes the assertion being made.

Question 2.2.14 *Suppose the universe is the non-zero real numbers. Translate each of the statements $\forall x, \exists y, xy = 1$ and $\exists y, \forall x, xy = 1$ into English, and determine the truth value of each one.*

Example 2.2.15 *Use quantifiers to express the statement "for all integers n, the integer $n(n + 1)$ is even" symbolically.*

Solution.
We need the precise definition of an even integer. An integer k is even *when there is an integer t such that $k = 2t$. Symbolically, k is even when $\exists t, k = 2t$, where the universe of t is the integers. With this in mind, the statement to be translated becomes "$\forall n, \exists t, n(n + 1) = 2t$".*

Example 2.2.16 *Suppose the universe consists of the integers 1, 2. Write a statement logically equivalent to $\forall x, \exists y, xy = 2$ that does not involve quantifiers, and determine its truth value.*

Solution.
When $x = 1$, the statement $\exists y, xy = 2$ is precisely $(1 \cdot 1 = 2) \vee (1 \cdot 2 = 2)$, which is true. When $x = 2$, the statement $\exists y, xy = 2$ is precisely $(2 \cdot 1 = 2) \vee (2 \cdot 2 = 2)$, which is true. Thus, $\forall x, \exists y, xy = 2$ is precisely the statement

$$[(1 \cdot 1 = 2) \vee (1 \cdot 2 = 2)] \wedge [(2 \cdot 1 = 2) \vee (2 \cdot 2 = 2)].$$

The first expression in square brackets corresponds to the statement $\exists y, xy = 2$ *when* $x = 1$*, the second one corresponds to this statement when* $x = 2$*, and we are taking the conjunction of these statements because of the universal quantifier. The given statement is true.*

Question 2.2.17 *Suppose the universe consists of the integers 1, 2. Write a statement logically equivalent to* $\exists y, \forall x, xy = 2$ *that does not involve quantifiers, and determine its truth value.*

Example 2.2.18 *Suppose the universe is the integers. Determine the truth value of the statement* $\forall x, \exists y, x + y < 10$*.*

Solution.
The first quantifier is "for all", and it applies to x*. Thus, the quantified statement is going to be true only if the statement that follows,* $\exists y, x+y < 10$*, is true no matter what* x *in the universe is used. The next quantifier is "there exists', and it applies to* y *This quantified statement is going to be true only if there is at least one* y *in the universe so that* $x + y < 10$ *is true.*

Given any integer x*, if we choose* y *to be* $-x$ *then* $x + y = x + (-x) = 0$*. Therefore, for any* x*, there exists* y *such that* $x+y < 10$*. Thus, the statement* $\forall x, \exists y, x + y < 10$ *is true.*

Question 2.2.19 *Suppose the universe is the integers. Determine the truth value of the statement* $\exists x, \exists y, xy = 4$*.*

Question 2.2.20 *Suppose the universe is the integers. Determine the truth value of the statement* $\exists x, \forall y, x + y < 10$*.*

Let $s(x)$ denote a statement involving the variable x. Observe that if $\forall x, s(x)$ is true, then so is $\exists x, s(x)$, provided the universe contains a non-zero number of elements: if an assertion is true for every element of the universe, then it is true for at least one element of the unverse (provided there is one). If the universe contains no elements, then $\forall x, s(x)$ is true, and $\exists x, s(x)$ is never true (why?). Of course, the truth of $\exists x, s(x)$ tells us nothing about the truth of $\forall x, s(x)$. Why?

Both universal and existential quantifiers can be (unintentionally) hidden. An example is the statement "if $(a \neq 0)$ and $(ax^2 + bx + c = 0)$ then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

which is meant to apply to all real numbers x. If the universal quantifier were made explicit, it would read "for all real numbers $x \ldots$". Similarly, the statement "a real number can have more than one decimal expansion" is intended to assert the existence of one or more such numbers. If the existential quantifier were made explicit, it would read "there is a real number x such that x has more than one decimal expansion".

Question 2.2.21 *According to Robert Plant, the original first line of the Led Zepplin song* Stairway to Heaven *was* "There's a lady who knows all is glitters, is gold, and she is buying a stairway to heaven." *Explain why, when this statement is written in symbols, either $\exists$ or $\forall$ quantifier appears, and the two formulations are logically equivalent.*

Logical equivalence of open statements was discussed towards the end of Section 2.1. For example, $\neg(p(x) \vee q(x))$ is logically equivalent to $\neg p(x) \wedge \neg q(x)$, the contrapositive of $p(x) \to q(x)$ is $\neg q(x) \to \neg p(x)$, and the converse of $p(x) \to q(x)$ is $q(x) \to p(x)$. Recall that logically equivalent statements can be freely substituted for each other without changing the truth value of any expression in which they are involved. This reasoning also applies to statements involving quantifiers. In particular, *the contrapositive of* $\forall x, p(x) \to q(x)$ is $\forall x, \neg q(x) \to \neg p(x)$ because the contrapositive of $p(x) \to q(x)$ is $\neg q(x) \to \neg p(x)$. Similarly, *the converse of* $\exists x, p(x) \to q(x)$ is $\exists x, q(x) \to p(x)$ because converse of $p(x) \to q(x)$ is $q(x) \to p(x)$.

Question 2.2.22 *What is the contrapositive of $\exists x, p(x) \to q(x)$? Why? What is the converse of $\forall x, p(x) \to q(x)$? Why?*

2.3 Negating Statements Involving Quantifiers

Being able to read and write statements involving quantifiers, especially nested quantifiers, is an important skill. Another important skill is to be able to figure out what is needed for a quantified statement to be true, or to be false. A related skill which is crucial in mathematics is to be able to properly negate a quantified statement.

Intuitively, the negation of an existentially quantified statement should be an universally quantified statement because if it is not the case that a statement is true for at least one allowed replacement from the universe, then it is false for all allowed replacements. Similarly, the negation of a universally quantified statement should be an existentially quantified statement because if it is not the case that a statement is true for all allowed replacements from the universe, then it is false for at least one allowed replacement. Let's formalize this intuition.

We first determine the negation of an existentially quantified statement.

Proposition 2.3.1 *For any universe, the negation of $\exists x, p(x)$ is $\forall x, \neg p(x)$.*

Proof. We need to argue that $\forall x, \neg p(x)$ has the opposite truth value as $\exists x, p(x)$. We consider two cases, depending on the truth value of $\exists x, p(x)$.

Suppose first that $\exists x, p(x)$ true. Then there is some element x_0 in the universe such that $p(x_0)$ is true, and so $\forall x, \neg p(x)$ is false.

Now suppose $\exists x, p(x)$ is false. Then there is no x_0 in the universe for which $p(x_0)$ is true, and so $\forall x, \neg p(x)$ is true.

Therefore $\neg\exists x, p(x) \Leftrightarrow \forall x, \neg p(x)$. □

Example 2.3.2 *Suppose the universe is the integers. Write the negation of the statement $\exists n, (2n = 6) \to (n = 0)$ in symbols, without any negated quantifiers and without any negated mathematical symbols, and determine its truth value.*

<u>Solution</u>.
By Proposition 2.3.1 we have

$$\begin{aligned} \neg\exists n, (2n = 6) \to (n = 0) &\Leftrightarrow \forall n, \neg((2n = 6) \to (n = 0)) \\ &\Leftrightarrow \forall n, (2n = 6) \wedge (n \neq 0) \\ &\Leftrightarrow \forall n, (2n = 6) \wedge ((n < 0) \vee (n > 0)) \end{aligned}$$

since $n \neq 0 \Leftrightarrow (n < 0) \vee (n > 0)$. Thus the desired statement is $\forall n, (2n = 6) \wedge ((n < 0) \vee (n > 0))$. It is false because, for example, when $n = 0$ the statement $(2n = 6) \wedge ((n < 0) \vee (n > 0))$ is false. (Note: we could have seen *that the statement is false by noting that the statement* $(2n = 6) \to (n = 0)$ *is true when* $n = 0$*, for example, because* $2n = 6$ *is false for that replacement for* n*, and hence* $\exists n, (2n = 6) \to (n = 0)$ *is true.)*

Question 2.3.3 *Suppose the universe is the real numbers. Write the negation of the statement* $\exists x, x, x^2 - 10 < 9$ *in symbols, without any negated quantifiers and without any negated mathematical symbols, and determine its truth value.*

We now determine the negation of a universally quantified statement.

Proposition 2.3.4 *For any universe. the negation of* $\forall x, q(x)$ *is* $\exists x, \neg q(x)$*.*

Proof. We need to argue that $\exists x, \neg q(x)$ has the opposite truth value as $\forall x, q(x)$. We consider two cases, depending on the truth value of $\forall x, q(x)$.

Suppose first that $\forall x, q(x)$ is true. Then $q(x_0)$ is true for every x_0 in the universe. Thus $\neg q(x_0)$ is false for every element x_0 of the universe, and so $\exists x, \neg q(x)$ is false.

Now suppose $\forall x, q(x)$ is false. Then $q(x_0)$ is false for some element x_0 of the universe. That means $\neg q(x_0)$ is true, and so $\exists x, \neg q(x)$ is true.

Therefore, $\neg \forall x, q(x) \Leftrightarrow \exists x, \neg q(x)$. □

A different proof of Proposition 2.3.4 uses Proposition 2.3.1. We have

$$\exists x, \neg q(x) \Leftrightarrow \neg\neg\exists x, \neg q(x) \Leftrightarrow \neg\forall x, \neg\neg q(x) \Leftrightarrow \neg\forall x, q(x).$$

Example 2.3.5 *Suppose the universe is the real numbers. Write the negation of the statement* $\forall x, \sqrt{x^2} = x$ *in symbols, without any negated quantifiers and without any negated mathematical symbols, and determine its truth value.*

Solution.
By Proposition 2.3.4 we have

$$\begin{aligned} \neg\forall x, \sqrt{x^2} = x &\Leftrightarrow \exists x, \neg(\sqrt{x^2} = x) \\ &\Leftrightarrow \exists x, \sqrt{x^2} \neq x \\ &\Leftrightarrow \exists x (\sqrt{x^2} < x) \vee (\sqrt{x^2} > x) \end{aligned}$$

This the desired statement is $\exists x(\sqrt{x^2} < x) \vee (\sqrt{x^2} > x)$. It is true because, for example, when $x = -2$ we have $\sqrt{x^2} = \sqrt{(-2)^2} = 2 > -2$ (since $\sqrt{\cdot}$ denotes the positive square root of its argument).

Question 2.3.6 *Suppose the universe is the integers. Write the negation of the statement $\forall n, (2^n = 2n) \leftrightarrow (n = 2)$ in symbols, without any negated quantifiers and without any negated mathematical symbols, and determine its truth value.*

It is important to note that the statements $p(x)$ and $q(x)$ in Propositions 2.3.1 and 2.3.4, respectively, may themselves be quantified statements, and so the process of replacing negated quantifiers may need to be repeated over and over.

Example 2.3.7 *Write the statement $\neg[\exists a, \exists b, \frac{a}{b} = \sqrt{2}]$ in symbols without any negated quantifiers.*

Solution.
By Proposition 2.3.1,

$$\begin{aligned}
\neg[\exists a, \exists b, \frac{a}{b} = \sqrt{2}] &\Leftrightarrow \forall a, \neg[\exists b, \frac{a}{b} = \sqrt{2}] \\
&\Leftrightarrow \forall a, \forall b, \neg[\frac{a}{b} = \sqrt{2}] \\
&\Leftrightarrow \forall a, \forall b, \frac{a}{b} \neq \sqrt{2}
\end{aligned}$$

Therefore the desired statement is $\forall a, \forall b, \frac{a}{b} \neq \sqrt{2}$.

(Notes: (1.) We will prove in the next section that this statement is true when the universe is the integers, that is, $\sqrt{2}$ is irrational.
(2.) To reinforce that the truth value of a quantified statement can depend on the universe, note that if the universe is the real numbers, then the statement $\forall a, \forall b, \frac{a}{b} \neq \sqrt{2}$ is false. That's demonstrated by taking $a = \sqrt{2}$ and $b = 1$.)

Question 2.3.8 *Suppose the universe is the real numbers. Write the statement $\neg[\exists x, \forall y, xy \neq 1]$ in symbols without any negated quantifiers, and determine its truth value. Is the truth value different when the universe is the non-zero real numbers?*

2.4 Some Examples of Written Proofs

Suppose you want to write a proof in words for a statement of the form "if p then q". That is, you wish to establish the theorem $p \Rightarrow q$. There are many techniques (methods) that can be tried. There is no guarantee of which method will work best in any given situation. Experience is a good guide, however. Once a person has written a few proofs, they get a sense of the best thing to try first in any given situation.

To use the method of *direct proof* to show p logically implies q, *assume p is true* and then *use definitions, known implications, and known logical equivalences to argue that q must be true.* The reason for assuming p is true comes from the definition of logical implication. In this case the first line of the proof is "*Assume p.*" and the last says, essentially, "*q is true*". What comes in between depends on p and q.

In the following example of a direct proof, we use the definition of an even integer: An integer n is *even* if there exists an integer k so that $n = 2k$. Put differently, the integer n is even if it leaves remainder 0 on division by 2. An integer n is *odd* if it leaves remainder 1 on division by 2, that is, if $n = 2k+1$ for some integer k. Every integer is either even or odd, and not both.

Proposition 2.4.1 *If the integer n is even, then n^2 is even.*

Proof. Suppose that the integer n is even. Hence, there exists an an integer k so that $n = 2k$. Then, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, n^2 is even. □

It is customary in mathematics to use a box to indicate the end (or absence) of an argument.

Another proof technique is to *prove the contrapositive.* That is, assume q is false, and argue using the same things as above that p must also be false. This works since $p \to q \Leftrightarrow \neg q \to \neg p$. In this case the first line of the proof is "*Assume $\neg q$.*" and the last is, essentially, "*$\neg p$ is true*". This method is sometimes called giving an *indirect proof.* The motivation for the name comes from the fact that the logical implication is proved indirectly, by its contrapositive.

Proposition 2.4.2 *If the integer n^2 is even, then n is even.*

Proof. We will prove the contrapositive that if n is not even, then n^2 is not even.

Suppose that the integer n is not even, that is, it is odd. We want to show that n^2 is odd. Since n is odd, there exists an an integer k so that $n = 2k+1$. Then, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, n^2 is odd. □

Yet another technique is *proof by contradiction*. The method comes from the inference rule with the same name in Section 1.12. A proof by contradiction that p implies q begins by assuming q is false and proceeding as above until deriving a statement which is a (logical) contradiction. Doing so enables you to conclude that q is true. In such a situation, the first line of the proof is "Suppose $\neg q$." and the proof ends with "We have obtained a contradiction. Therefore q."

Here is a classic example of proof by contradiction. It uses the definition of a rational number: a number x is *rational* if there exist integers a and b so that $x = a/b$. A number is *irrational* if it is not rational.

Put slightly differently, x is rational if it is a ratio of two integers. There are many ratios of integers that equal a given number. In particular, there is always one where the fraction a/b is in *lowest terms*, meaning that a and b have no common factors other than one.

Proposition 2.4.3 *$\sqrt{2}$ is not rational.*

Proof. Suppose $\sqrt{2}$ is rational. Then there exist integers a and b so that $\sqrt{2} = a/b$. The integers a and b can be chosen so that the fraction a/b is in lowest terms, so that a and b have no common factor other than 1. In particular, a and b are not both even.

Since $\sqrt{2} = a/b$, we have that $2 = (a/b)^2 = a^2/b^2$. By algebra, $2b^2 = a^2$. Therefore a^2 is even. By Proposition 2.4.2, a is even. Thus there exists an integer k so that $a = 2k$. It now follows that $2b^2 = a^2 = (2k)^2 = 4k^2$, so that $b^2 = 2k^2$. Therefore b^2 is even. By Proposition 2.4.2, b is even.

We have now derived the contradiction (a and b are not both even) and (a and b are both even). Therefore, $\sqrt{2}$ is not rational. □

Sometimes the hypotheses lead to a number of possible situations, and it is easier to consider each possibility in turn. In the method of *proof by cases*, one lists the cases that could arise (being careful to argue that all possibilities are taken into account), and then shows that the desired result holds in each case. It could be that different cases are treated with different proof methods. For example, one could be handled directly, and another by contradiction.

In the following example we make use the fact that every integer n can be uniquely written in the form $3k + r$, where k is an integer and r equals 0, 1, or 2. When the remainder, r, equals 0 we have $n = 3k$, so that n is a multiple of 3.

Proposition 2.4.4 *If the integer n^2 is a multiple of 3, then n is a multiple of 3.*

Proof. We prove the contrapositive: if n is not a multiple of 3, then n^2 is not a multiple of 3. Suppose n is not a multiple of 3. Then the remainder when n is divided by 3 equals 1 or 2. This leads to two cases:

Case 1. The remainder on dividing n by 3 equals 1.

Then, there exists an integer k so that $n = 3k + 1$. Hence $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. Since $(3k^2 + 2k)$ is an integer, the remainder on dividing n^2 by 3 equals 1. Therefore n^2 is not a multiple of 3.

Case 2. The remainder on dividing n by 3 equals 2.

Then, there exists an integer k so that $n = 3k + 2$. Hence $n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$. Since $(3k^2 + 4k + 1)$ is an integer, the remainder on dividing n^2 by 3 equals 1. Therefore n^2 is not a multiple of 3.

Both cases have now been considered. In each of them, we have shown that n^2 is not a multiple of 3. It now follows that if n is not a multiple of 3, then n^2 is not a multiple of 3. This completes the proof. □

2.5 Exercises

1. Suppose the universe for the variables is the integers. Let $p(n)$ be "*n is even*" and $q(n)$ be "*n is odd*". Determine the truth value of each statement and provide a brief explanation of your reasoning.

(a) $\forall n, p(n) \vee q(n)$

(b) $[\exists n, p(n)] \wedge [\exists n, q(n)]$

(c) $\exists n, p(n) \to q(n)$

(d) $[\forall n, p(n)] \wedge [\forall n, q(n)]$

(e) $\forall n, \exists m, n + m = 0$

(f) $\exists n, \forall m, n + m = 0$

2. Suppose the universe contains at least one element.

   (a) Explain why $\forall x, p(x) \wedge q(x)$ is logically equivalent to $[\forall x, p(x) \ \wedge$ $[\forall x, q(x)]$.

   (b) Explain why $\exists x, p(x) \vee q(x)$ is logically equivalent to $[\exists x, p(x) \ \vee$ $[\exists x, q(x)]$.

3. Use the example where the universe is the integers, and the statements in Question 1 to:

   (a) Explain why $\forall x, p(x) \vee q(x)$ is not logically equivalent to $[\forall x, p(x)] \vee$ $[\forall x, q(x)]$.

   (b) Explain why $\exists x, p(x) \wedge q(x)$ is not logically equivalent to $[\exists x, p(x)] \wedge$ $[\exists x, q(x)]$.

4. Write each statement in plain English. Do not use any symbols except the letters that denote elements of the universe.

   (a) $\forall x, \forall y, (x \neq -y) \to (x + y) \neq 0$, where the universe is the real numbers.

   (b) $\exists s, \forall t, p(s) \wedge [(t \neq s) \to \neg p(t)]$, where the universe of s and t is the collection of all students who completed Math 122 last fall, and $p(s)$ is the assertion "s got 100% on the final exam".

5. Suppose that the collection of allowed replacements for the variable p is {*Gary*, *Christi*} and the collection of allowed replacements for the variable c is {*Whitehorse*, *Ottawa*, *Halifax*}. Let $v(p, c)$ be the statement "p has visited c". Write each statement in symbolic form without quantifiers.

   (a) Christi has visited every city.

(b) There is a city Gary has not visited.

(c) For every person there is a city which they have visited.

6. Determine if each statement below is true or false, and explain your reasoning.

   (a) The negation of "*Every golf shot is a hook or a slice*" is "*Some golf shots are hooks and slices*".

   (b) The negation of "*All enforcers skate slowly and pass badly*" is "*Some enforcers skate fast and pass well*".

7. Suppose the universe of m and n is $\{-1, 0, 1\}$. For each of the following statements,

   (i) write a compound statement involving neither quantifiers nor variables that is logically equivalent to the given quantified statement,

   (ii) determine the truth value, and

   (iii) write the negation of the quantified statement in symbols, with quantifiers, and without using negation ($\neg$) or any negated mathematical symbols like $\neq$ or $\not<$.

   (a) $\forall n, n^3 - n = 0$

   (b) $\exists n, \forall m, n + m < 1$.

8. Determine if each statement below is true or false, and explain your reasoning.

   (a) When the statement "*There is no largest integer.*" is written is symbols, both of the quantifiers $\forall$ and $\exists$ appear.

   (b) For the universe of real numbers, $\forall x, \exists y, xy = 1$ is false.

   (c) For the universe of integers, $\exists x, (x^2 < 0) \to (x > 10)$ is true.

   (d) For the universe of real numbers, the contrapositive of "$\exists y, \forall x.(xy < x + y) \to (y = 0)$" is "$\forall y, \exists x.(y \neq 0) \to (xy \geq x + y)$."

9. Let L be a given real number. We say that a sequence $a_1, a_2, \ldots$ of real numbers has *limit* L if, for every real number $\epsilon > 0$ there exists an integer N such that $|L - a_n| < \epsilon$ for all $n \geq N$.

(a) Write the criteria above for a sequence $a_1, a_2, \ldots$ of real numbers to have limit L in symbols. Don't forget to specify the universe for each variable.

(b) Write the negation of the criteria in symbols.

(c) Explain in words how the negation of the criteria tells you when you can conclude a sequence $a_1, a_2, \ldots$ of real numbers does not have limit L.

(d) Apply the negation of the criteria to show that the sequence $a_1, a_2, \ldots$, where $a_n = (-1)^n$, does not have limit 0.

10. Consider the following (correct) argument in which all variables represent integers.

    Suppose n and k are odd.
    Then $n = 2t + 1$ for some integer t, and $k = 2\ell + 1$ for some integer ℓ.
    Hence, $nk = (2t + 1)(2\ell + 1) = 4t\ell + 2t + 2\ell + 1$.
    Therefore, nk is odd.

    (a) Write the implication proved by the argument in plain English.

    (b) Write the contrapositive of the implication in plain English. Is it also proved by the argument?

    (c) Write the converse of your statement in (a). Is it also proved by the argument?

11. Consider the following. All variables represent integers.

    Proposition: If n^2 is a multiple of 8, then n is a multiple of 8.
    Proof: Let $n = 8m$. Then $n^2 = 64m^2 = 8(8m^2)$, which is a multiple of 8, as desired. □

    Why does the given argument not prove the proposition? Either give a correct proof, or give an example to show that the proposition is false.

12. (a) Let n be in integer. Explain what is wrong with the following argument which "shows" that *if n is a multiple of 2 and a multiple of 3, then n is a multiple of 6.*

    Suppose n is a multiple of 6. Then $n = 6k$ for some integer k. Since $6 = 2 \times 3$, we have that $n = 2 \times (3k)$, so it is a multiple of 2, and $n = 3 \times (2k)$, so it is a multiple of 3. □

(b) Give a correct proof of the assertion.

13. Suppose that m and n are integers. It is claimed that the argument below proves that *if mn is odd, then m and n are both odd.* Does it? Explain your reasoning.

    Suppose that the integers m and n are both even. Then there exists an integer k such that $m = 2k$, and there exists an integer ℓ such that $n = 2\ell$. Thus,

    $$mn = (2k)(2\ell) = 2(2k\ell).$$

    Since $2k\ell$ is an integer, mn is even.

14. Suppose that the integer a is a multiple of 3, and the integer b is a multiple of 4. Give a direct proof that ab is a multiple of 12.

15. Prove that:

    (a) The sum of two even inters is even.

    (b) The sum of an even integer and an odd integer is odd.

    (c) The sum of two odd integers is even.

    (d) The product of two even integers is even. Further, it is a multiple of 4.

    (e) The product of an even integer and an odd integer is even.

    (f) The product of two odd integers is odd.

    (g) If a and b are integers such that $a + b$ is even, then a and b are both even or both odd.

    (h) If a and b are integers such that $a + b$ is odd, then a is even and b is odd, or a is odd and b is even.

    (i) If a and b are integers such that ab is even, then a is even or b is even.

    (j) If a and b are integers such that ab is odd, then a and b are both odd.

16. Prove that $\sqrt{3}$ is irrational. (Hints. Use Proposition 2.4.4, and, in the proof that $\sqrt{2}$ is irrational, read the phrase "*is even*" as "*is a multiple of 2*", and then try using the same argument with 2 replaced by 3.)

17. Prove that if the integer n^2 is a multiple of 5, then the integer n is a multiple of 5. (Hint: prove the contrapositive using a proof by cases; there are 4 cases.)

18. Prove that $\sqrt{5}$ is irrational. (See the hint for Question 16, and also use the result in Question 17.)

Chapter 3

Set Theory

3.1 What is a Set?

A *set* is a well-defined collection of objects called *elements* or *members* of the set.

Here, *well-defined* means accurately and unambiguously stated or described. Any given object must either be an element of the set or not be an element of the set. There is no concept of partial membership and there is no possibility of being a member more than once.

The *barber paradox* gives an example of a set that is not well-defined: *There is only one barber in a certain town. He is male. He lives in the town. All of the men in the town are clean-shaven. The barber shaves all and only the men in the town who do not shave themselves. Who shaves the barber?* Now, if the barber shaves himself, then since the barber only the men who do not shave themselves, he does not shave himself. Furthermore, if he does not shave himself, then since he shaves all of the men who don't shave themselves, he shaves himself. Hmmm. One explanation for this paradox is that the set, S, of men in the town who are shaved by the barber is not well-defined, as the barber must simultaneously be a member of the set and not be a member of the set.

The collection of objects that are not members of a given set X is itself a set. It is called the *complement* of X and denoted by X^c. However, the set X^c is only well-defined if we know which objects are allowed to be members of the sets we're talking about.

The *universe* (of discourse) is the set of objects that are allowed to be members of the sets we are talking about. The universe is itself a set and is typically denoted by $\mathcal{U}$.

We may not always explicitly mention the universe – for example, what we're talking about might make sense no matter what the universe is – but we will always assume it exists.

3.2 Describing Sets

Sets can be described in several ways. One way to describe a set is to write a description of the set in words, as in "the set of all integers that can be written as the sum of two squares". There are three main ways of describing a set using mathematical notation.

1. *Explicit listing*: list the elements between braces (i.e. curly brackets), as in $\{2, 3, 5, 7\}$. The elements of a set that's described by explicit listing are exactly the (different) objects in the list obtained when the outer brackets are erased.

Example 3.2.1 *What are the elements of* $\{\text{car}, \pi, \{X\}\}$*?*

Solution.
They are $\text{car}, \pi,$ *and* $\{X\}$.

Question 3.2.2 *What are the elements of* $\{-1, \{3\}\}$*?*

2. *Implicit listing*: list enough its elements to establish a pattern and use an ellipsis "$\ldots$".

Proper use of the ellipsis requires that at least two elements be listed so that the pattern is established. (It could be that more elements must be listed before the pattern is apparent.) The elements of a set that's described by implicit listing are those that follow the pattern, and respect any limits set.

Example 3.2.3 *Use the method of implicit listing to describe the set of non-negative even integers less than or equal to 120, and the set of odd integers.*

Solution.
The two sets are $\{0, 2, 4, \ldots, 120\}$ *and* $\{\ldots - 3, -1, 1, 3, \ldots\}$. *(Note: there is more than one way to describe the set of of integers using this method.)*

Question 3.2.4 *Use the method of implicit listing to describe the set of integers which are multiples of 7, and the set of integers between* -5 *and 30, inclusive.*

3. *Set-builder notation*: specify the set of the collection of all objects of a particular type that satisfy a given condition. The elements of a set described using set-builder notation are those objects of the given type that make the stated condition true for the universe $\mathcal{U}$.

Example 3.2.5 *Use set-builder notation to describe the (i) set of prime numbers less that 10, and (ii) the set of all positive even integers.*

Solution.
The two sets are $\{x : (x \text{ is prime}) \ \wedge \ (x < 10)\}$ *and* $\{2k : k = 1, 2, \ldots\}$.

Question 3.2.6 *Use set-builder notation to describe the set of even positive integers less than 100.*

Example 3.2.7 *Describe the elements of the set*

$$\{a/b : a \text{ and } b \text{ are integers, and } a/b = 0.25\}$$

in plain English.

Solution.
The members of this set are exactly the fractions whose numerical value is 0.25. (There are infinitely many of these including $1/4, 3/12$, *and* $-5/(-20)$.*)*

Question 3.2.8 *Describe the elements of the set*

$$\{n : n \textit{ is an integer and is a multiple of 2 and a multiple of 3}\}$$

in plain English.

3.3 Special Sets

Some sets are well-known, and are denoted by special symbols.

- The set of *natural numbers* is $\mathbb{N} = \{1, 2, 3, \ldots\}$. Some people include 0 as an element of this set. It is always wise to check the definition that a particular author is using.
- The set of *integers* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, The use of the symbol $\mathbb{Z}$ can be traced back to the German word *zählen*.
- The set of *rational numbers* is $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, \text{ and } b \neq 0\}$. The symbol $\mathbb{Q}$ is used because these are *quotients* of integers.
- The set of *real numbers*, denoted by $\mathbb{R}$, has as elements all numbers that have a decimal expansion.
- The set of *complex numbers* is $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, \text{ and } i^2 = -1\}$.

3.4 Set Membership Set Equality, and Set Complement

If x is a member of the set S, we write $x \in S$, and if x is not a member of the set S, we write $x \notin S$.

Example 3.4.1 *Let* $X = \{1, \{2\}, \{1, \{2\}\}\}$. *Is* $2 \in X$*? What about* $\{1, 2\}$*? And what about* $\{1\}$*?*

Solution.
The elements of X *are exactly* $1, \{2\}\}$, *and* $\{1, \{2\}$. *Thus none of 2,* $\{1, 2\}$ *and* $\{1\}$ *is an element of* X*: an element of* X *must be identical to one of the objects in the list of elements of* X. *None of these are.*

Question 3.4.2 *Let* $A = \{\{a, b\}, c, \{a, b, c\}\}$. *Is* $a \in A$*? What about* $\{a, c\}$*?*

Sets are defined in terms of the objects they contain. We say sets A and B are *equal*, and write $A = B$ if they have exactly the same elements. That is, $A = B$ when $x \in A \Leftrightarrow x \in B$ for all $x \in \mathcal{U}$.

By the definition of equality of sets, it does not matter how a set is described; what matters is which elements it contains. Any particular object either belongs to the collection or it doesn't. All of $\{1, 2, 2, 3\}, \{1, 2, 3, 3\}$ $\{3, 2, 3, 1\}$ and $\{1, 2, 3\}$ all describe the same set because they all have the same three elements: 1, 2, and 3.

Throughout mathematics, vertical bars are used to denote a measure of size. For instance, when x is a real number, the absolute value, $|x|$, measures the size of x in terms of its distance from 0 on the number line.

When a set X has a finite number of elements, *we use the symbol $|A|$ to denote the number of elements of the set A.* For example, $|\{1, 2, 2, 3, 3, 3\}| = 3$.

As mentioned in Section 3.1, the *complement* of the set X is the set $X^c = \{x : x \notin X\}$. It is clear that the set X^c depends on the universe $\mathcal{U}$. If $\mathcal{U} = \{1, 2, 3\}$, then $\{1\}^c = \{2, 3\}$, whereas if $\mathcal{U} = \mathbb{Z}$, then $\{1\}^c = \{\ldots, -1, 0, 2, 3, \ldots\}$.

Proposition 3.4.3 *Let A and B be sets. Then $A = B$ if and only if $A^c = B^c$.*

Proof. ($\Rightarrow$) Suppose $A = B$. Then, for all $x \in \mathcal{U}$ we have $(x \in A) \Leftrightarrow (x \in B)$. Therefore, for all $x \in \mathcal{U}$ we have $(x \notin A) \Leftrightarrow (x \notin B)$. Therefore $A^c = B^c$.

($\Leftarrow$) Suppose $A^c = B^c$. Then, for all $x \in \mathcal{U}$ we have $(x \notin A) \Leftrightarrow (x \notin B)$. Therefore, for all $x \in \mathcal{U}$ we have $(x \notin A) \Leftrightarrow (x \notin B)$. Therefore $A = B$.

The proof is now complete. □

Note: mathematicians usually indicate the end of a proof with a hollow box, as in "□", or a filled black box. Other indicators have been used, and continue to be used. Euclid used the letters QED (*quod erat demonstrandum* – that which was to be demonstrated) for proofs, and QEF (*quod erat faciendum* – which was to be done) for constructions.

3.5 The Empty Set

It is certainly possible for a collection to have nothing in it. A good example would be the collection of years after 1967 in which the Toronto Maple Leafs have won the Stanley Cup.

The *empty set* is the set that has no elements, that is $\{\}$. It is commonly denoted by $\emptyset$.

The following sets are all equal to $\emptyset$: $\{x \in \mathbb{R} : x^2+1 = 0\}$, $\{n \in \mathbb{Z} : n^2-1 = 7\}$ and $\{a/b \in \mathbb{Q} : a/b = \sqrt{2}\}$.

The empty set is a perfectly legitimate object, and as such can occur as an element of a set. Notice that $\emptyset$ is different from $\{\emptyset\}$. The former set has no elements, while the latter set has one element, $\emptyset$. The set $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}, \emptyset\}\}$ has three elements: $\emptyset, \{\emptyset\}$, and $\{\{\emptyset\}, \emptyset\}\}$.

3.6 Subsets

We say that a set A is a *subset* of a set B if every element of A is an element of B (i.e., $x \in A \Rightarrow x \in B$). If A is a subset of B we write $A \subseteq B$, and otherwise we write $A \not\subseteq B$.

Example 3.6.1 $\mathbb{N} \subseteq \mathbb{Z}$*,* $\mathbb{Z} \subseteq \mathbb{Q}$*, and* $\mathbb{Q} \subseteq \mathbb{R}$*. Also,* $\{1, 3, 5\} \subseteq \{1, 3, 5\}$*, and* $\{2, 4\} \not\subseteq \{4, 5, 6\}$.

Sometimes confusion arises in making the distinction between $\in$ and $\subseteq$. The first one makes the assertion that *a particular object belongs* to a set; the second one says that *every element of one set is an element of another set.*

Notice that every set is a subset of itself (why?), that is $X \subseteq X$ for every set X.

A more subtle point is that $\emptyset$ *is a subset of every set.* To see this, let A be an arbitrary set. According to the definition, the statement $\emptyset$ is the same as the logical implication $x \in \emptyset \Rightarrow x \in A$. In turn, this statement is the same as the implication $(x \in \emptyset) \to (x \in A)$ being a tautology. The implication has only the truth value "true" because its hypothesis, $x \in \emptyset$, is false for any x. A different way to say it is that every element in the collection of members of the empty set – there aren't any – is a member of A.

Example 3.6.2 *Let* $A = \{1, 2, \{1, 2\}\}$*. Answer each question true or false, and briefly explain your reasoning.*

1. $\{2\} \in A$

2. $\{2, \{1, 2\}\} \subseteq A$

3. $\emptyset \in A$

4. $\emptyset \subseteq A$

5. $|A| = 2.$

Solution.
The elements of A are $1, 2,$ and $\{1, 2\}$. Therefore:

1. *False, $\{2\}$ is not among the list of elements of A.*

2. *True, both 2 and $\{1, 2\}$ are elements of A.*

3. *False, $\emptyset$ is not among the list of elements of A.*

4. *True, $\emptyset$ is a subset of every set.*

5. *False, A is 3 elements so $|A| = 3$.*

Question 3.6.3 *Let $A = \{a, c, \{a, b\}, \{a, c\}\}$. Answer each question true or false, and briefly explain your reasoning.*

1. $\emptyset \subseteq A.$

2. $\emptyset \in A$

3. $b \in A$

4. $\{a, c\} \in A$

5. $\{a, c\} \subseteq A$

6. $|A| = 3$

7. $\{a, b, c\} \subseteq A$

How many subsets does $\{a, b\}$ have? Let's count the options. Any particular subset either contains a or it does not. In both situations, there are two further options: the subset either contains b or it does not. Thus there are four possibilities $\{a, b\}, \{a\}, \{b\}, \{\}$.

The above reasoning can be extended to show that *a set with n elements has exactly 2^n subsets.*

In the following we show that the subset relation is *transitive*, that is, if A is a subset of B, and B is a subset of C, then A is a subset of C. (There is a more general meaning for the word "transitive". It will arise later in the course.) Before beginning the proof, it is useful to identify the statement to be proved, and the hypotheses that can be used in the argument. The statement to be proved is "A is a subset of C". That is, it needs to be argued that every element of A is an element of C. Equivalently, it needs to be argued that an arbitrary element of A is an element of C. The hypotheses that can be used in the argument are: "A is a subset of B", and "B is a subset of C". Constructing the proof involves using these to help argue that an arbitrary element of A must be an element of C.

Proposition 3.6.4 *Let A, B and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Proof. Take any $x \in A$. Since $A \subseteq B$, the element $x \in B$. Since $B \subseteq C$, the element $x \in C$. Therefore, if $x \in A$ then $x \in C$. That is, $A \subseteq C$. □

Recall that if p and q are statements, then the logical equivalence $p \Leftrightarrow q$ is the same as the two logical implications $p \Rightarrow q$ and $q \Rightarrow p$. The logical equivalence is proved once the two logical implications are proved.

Proposition 3.6.5 *Let A and B be sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Proof. ($\Rightarrow$) Suppose $A = B$. Then every element of A is an element of B, and every element of B is an element of A. Thus, $A \subseteq B$ and $B \subseteq A$.

($\Leftarrow$) Suppose $A \subseteq B$ and $B \subseteq A$. Then every element of A is an element of B (because $A \subseteq B$), and every element of B is an element of A. This means A and B have exactly the same elements, so $A = B$. □

3.7 Proper Subsets

The word "proper" occurs frequently in mathematics. Each time it has essentially the same meaning, roughly "*and not equal to the whole thing*".

A set A is a *proper subset* of a set B if $A \subseteq B$ and $A \neq B$. That is, A is a proper subset of B when every element of A belongs to B (so $A \subseteq B$) and there is an element in B which is not in A (so $A \neq B$).

Three common ways to denote that A is a proper subset of B are $A \subset B$, $A \subsetneq B$, and $A \subsetneqq B$. The last two of these are clear. The first one is, unfortunately, used by some authors to denote that A is a subset of B. While we we not do that, this is yet another reminder that it is always wise to check what the notation means instead of assuming.

Example 3.7.1 *We know that $\mathbb{Z} \subsetneqq \mathbb{Q}$ because $\mathbb{Z} \subseteq \mathbb{Q}$, and $1/2 \in \mathbb{Q}$ but $1/2 \notin \mathbb{Z}$.*

Question 3.7.2 *Explain how we know that $\mathbb{Q} \subsetneqq \mathbb{R}$.*

From above, a set X with n elements has 2^n subsets. All but one of them is a proper subset.

Proposition 3.7.3 *Let A, B and C be sets. If $A \subseteq B$ and $B \subsetneqq C$, then $A \subsetneqq C$.*

Proof. Two things need to be shown: (i) $A \subseteq C$, and (ii) $A \neq C$. Since $B \subsetneqq C$ implies that $B \subseteq C$, statement (i) is true by Proposition 3.6.4.

To show statement (ii) we must find an element C which is not an element of A. Since $B \subsetneqq C$, there exists $x \in C$ such that $x \notin B$. Since every element of A is an element of B, x can not be an element of A. Therefore $A \neq C$.

Both statements have been shown, and the proof is now complete. □

Question 3.7.4 *Prove that if $A \subsetneqq B$ and $B \subseteq C$, then $A \subsetneqq C$. (The argument is essentially the same as the one above.)*

3.8 The Power Set

The *power set* of a set A is the set whose elements are the subsets of A. The notation $\mathcal{P}(A)$ is commonly used to denote the power set of A.

The name "power set" comes from the fact that a set with n elements has exactly 2^n subsets. Thus, there are 2^n elements in the power set of a set with n elements.

Example 3.8.1 *Let $A = \{a, b\}$. What set is $\mathcal{P}(A)$?*

<u>Solution</u>.
We know that A has four subsets, $\{a, b\}, \{a\}, \{b\}, \{\}$, so that $\mathcal{P}(A) = \big\{\{a, b\}, \{a\}, \{b\}, \{\}\big\}$.

Question 3.8.2 *Explain why $\mathcal{P}(\emptyset) = \{\emptyset\}$. Is $\mathcal{P}(\emptyset)$ non-empty?*

The following facts are important to remember. For any set X:

- $\mathcal{P}(X)$ is a set.
- The elements of $\mathcal{P}(X)$ are sets (too).
- $A \in \mathcal{P}(X) \Leftrightarrow A \subseteq X$ (this is the definition of the power set).
- By the previous point, $\emptyset \in \mathcal{P}(X)$ and $X \in \mathcal{P}(X)$.

The following proposition is included because its proof forces us to think about power sets and their elements.

Proposition 3.8.3 *Let A and B be sets. Then $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.*

Proof. ($\Rightarrow$) Suppose $A \subseteq B$. We need to show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Take any $X \in \mathcal{P}(A)$. Then $X \subseteq A$. Since $A \subseteq B$, we have by Proposition 3.6.4 that $X \subseteq B$. Therefore $X \in \mathcal{P}(B)$. Therefore $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

($\Leftarrow$) Suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. We need to show that $A \subseteq B$.

Since $A \subseteq A$, $A \in \mathcal{P}(A)$. Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, $A \in \mathcal{P}(B)$. By definition of $\mathcal{P}(B)$, $A \subseteq B$. □

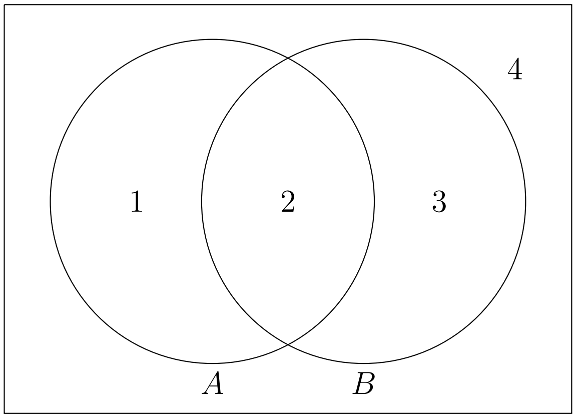
3.9 Venn Diagrams

Informally, a Venn diagram is a picture that shows all possible memberships between elements of the universe and a finite collection of sets. They are named after the British mathematician John Venn.

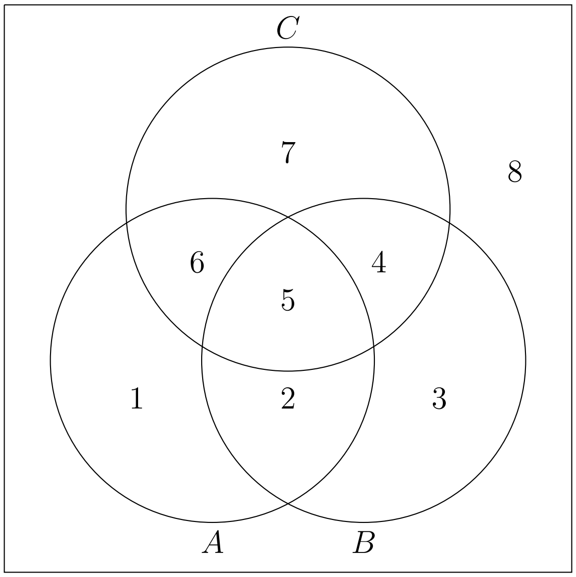
Let A and B be sets. For any element of the universe, there are four mutually-exclusive possibilities, where *mutually exclusive* means only one possibility can hold at a time.

1. it belongs to A and not to B;
2. it belongs to both A and B;
3. it belongs to B and not to A;
4. it belongs to neither A nor B.

Notice how these four possibilities correspond to the four rows of a truth table for the statements $x \in A$ and $x \in B$. They also correspond to the four regions in the Venn diagram below (the region number matches the statement number).



It is possible to draw a Venn diagram for any number of sets. If there are n sets, $A_1, A_2, \ldots, A_n$, then there will be 2^n regions, one corresponding to each collection of truth values for the n statements $x \in A_1, x \in A_2, \ldots, x \in A_n$. A Venn diagram for the three sets A, B, C is shown below.



Question 3.9.1 *Match each region on the Venn diagram above to the corresponding truth values for the statements $x \in A, x \in B, x \in C$.*

3.10 Set Operations

Let A and B be sets.

- The *union* of A and B is the set $A \cup B = \{x : (x \in A) \vee (x \in B)\}$. This is the set of elements that belong to A or to B.

- The *intersection* of A and B is the set $A \cap B = \{x : (x \in A) \wedge (x \in B)\}$. This is the set of elements that belong to A and to B.

- The *set difference of A and B* is the set $A \backslash B = \{x : x \in A \text{ and } x \notin B\}$. This is the subset of A obtained by deleting from A all of the elements that are also in B. For this reason, the notation $A - B$ is also commonly used.

- The *symmetric difference* of A and B is the set $A \oplus B = (A \backslash B) \cup (B \backslash A)$. This is the set of elements that belong to exactly one of the sets A and B, Set union and intersection correspond to the logical operations $\vee$ and $\wedge$, respectively. Notice that the set union symbol looks vaguely like the symbol for the logical connective "or", and the set intersection symbol looks vaguely like the symbol for the logical connective 'and". Indeed, union is defined using "or", and intersection is defined using "and".

The operation of set difference can be seen to correspond to the logical connective implication. We know $x \in A \setminus B \Leftrightarrow (x \in A) \rightarrow (x \notin B)$.

The operation of symmetric difference corresponds to the logical connective "exclusive or". If p and q are statements, then p *exclusive or* q is the statement $p \veebar q$ which is true when exactly one of p and q is true. That is $p \veebar q \Leftrightarrow \neg(p \leftrightarrow q)$.

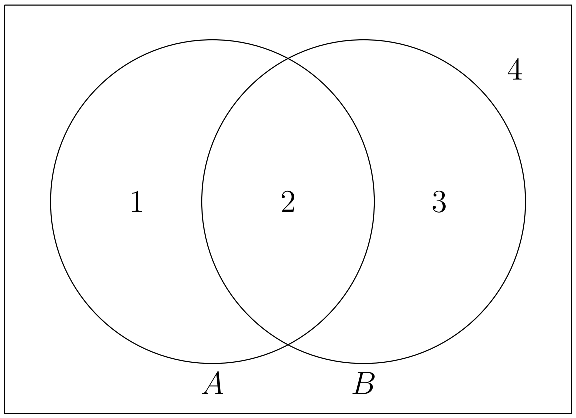
By definition $x \in A \oplus B$ if and only if $(x \in A) \veebar (x \in B)$ is true.

The set operation that corresponds to the logical operation negation is complement. We have $\neg(x \in A) \Leftrightarrow (x \in A^c)$.

As in the situation for logical connectives, *there is no precedence among set operations, except that complements are done first.* The moral of the story is that one should always use brackets for clarity.

With reference to the Venn diagram below,

- $A \cup B$ is represented by regions 1, 2, and 3;
- $A \cap B$ is represented by region 2;
- $A \setminus B$ is represented by region 1;
- $B \setminus A$ is represented by region 3;
- $A \oplus B$ is represented by regions 1 and 3;
- A^c is represented by regions 3 and 4;
- B^c is represented by regions 1 and 4;



Notice that the diagram suggests various set relationships. For example, it suggests $A \setminus B = A \cap B^c$, and $A = (A \setminus B) \cup (A \cap B)$. Both of these are true. We will see how to prove them, and other relationships between sets, in the next section.

3.11 The Laws of Set Theory

For each Law of Logic there is a corresponding Law of Set Theory.

- Commutative: $A \cup B = B \cup A, \quad A \cap B = B \cap A.$
- Associative: $A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C$
- Distributive: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  and also on the right: $(B \cap C) \cup A = (B \cup A) \cap (C \cup A), \quad (B \cup C) \cap A = (B \cap A) \cup (C \cap A)$
- Double Complement: $(A^c)^c = A$
- DeMorgan's Laws: $(A \cup B)^c = A^c \cap B^c, \quad (A \cap B)^c = A^c \cup B^c$
- Identity: $\emptyset \cup A = A, \quad \mathcal{U} \cap A = A$
- Idempotence: $A \cup A = A, \quad A \cap A = A$
- Dominance: $A \cup \mathcal{U} = \mathcal{U}, \quad A \cap \emptyset = \emptyset$

Arguments that prove logical equivalences can be directly translated into arguments that prove set equalities. As an example, we prove one of the associative laws. The proof amounts to using set builder notation and demonstrating that the sets on each side of the equals sign are described by logically equivalent conditions.

Proposition 3.11.1 *Let A, B and C be sets. Then $(A \cup B) \cup C = A \cup (B \cup C)$.*

Proof.

$$\begin{aligned}
(A \cup B) \cup C &= \{x : (x \in A \cup B) \vee (x \in C)\} && \text{Definition} \\
&= \{x : ((x \in A) \vee (x \in B)) \vee (x \in C)\} && \text{Definition} \\
&= \{x : (x \in A) \vee ((x \in B) \vee (x \in C))\} && \text{Associative} \\
&= \{x : (x \in A) \vee (x \in B \cup C)\} && \text{Definition} \\
&= A \cup (B \cup C) && \text{Definition}
\end{aligned}$$

□

A proof for each of the Laws of Set Theory can be carried out similarly to the above. (Exercise: do some!)

Question 3.11.2 *Prove that $A \setminus B = A \cap B^c$.*

DeMorgan's Laws for set theory can be proved using the same method is Proposition 3.11.1. They can also be proved by showing that $LHS \subseteq RHS$ and $RHS \subseteq LHS$. For the purposes of illustration, we choose the latter method.

Proposition 3.11.3 (DeMorgan's Laws) *Let A and B be sets. Then*

- $(A \cup B)^c = A^c \cap B^c$*; and*
- $(A \cap B)^c = A^c \cup B^c$*.*

Proof. We prove only the first statement. The proof of the second statement can be done in a similar way.

$(LHS \subseteq RHS)$ Let $x \in (A \cup B)^c$. Then $x \notin A \cup B$. Thus, $x \notin A$ and $x \notin B$. That is, $x \in A^c$ and $x \in B^c$. Therefore $x \in A^c \cap B^c$, and so $(A \cup B)^c \subseteq A^c \cap B^c$.

$(RHS \subseteq LHS)$. Let $x \in A^c \cap B^c$. Then $x \in A^c$ and $x \in B^c$. Thus, $x \notin A$ and $x \notin B$. Therefore, $x \notin A \cup B$, that is, $x \in (A \cup B)^c$. Hence, $A^c \cap B^c \subseteq (A \cup B)^c$. □

A careful look at the argument reveals that the second part of the proof, $(RHS \subseteq LHS)$, is really the same steps as in the first part in the reverse order. That's because each step is actually an equivalence rather than (just) an implication. These are the same equivalences that would be used if the statement were proved using the Laws of Logic. The same thing happens frequently proofs about set equality. Once half of a proof is constructed, it pays to think about whether the other half is already in hand.

Each of the Laws of Set Theory can (also) be proved using the method in the proof of Proposition 3.11.3. (Exercise: do some!). Most mathematicians would regard this as the "go to" method for proving set equalities.

There are ways in which the universe plays a similar role in set theory as a tautology does in logic. Similarly, the empty set can be seen to play a similar role in set theory as a contradiction does in logic. The following proposition is the set theory version of the logical equivalences:

- $p \vee \neg p \Leftrightarrow \mathbf{1}$;
- $p \wedge \neg p \Leftrightarrow \mathbf{0}$;

Proposition 3.11.4 *Let A be a set. Then*

- $A \cup A^c = \mathcal{U}$*;*
- $A \cap A^c = \emptyset$*;*

Proof. To see the first statement, recall that every element x is either in A or in A^c, so that $A \cup A^c = \mathcal{U}$. To see the second statement, note that, by definition, no element x can be in both A and A^c, so that $A \cap A^c = \emptyset$. □

The proposition below corresponds to the logical equivalence $p \veebar q \Leftrightarrow (p \vee q) \wedge \neg(p \wedge q)$. The proof of the set equality looks a lot like the proof of the corresponding logical equivalence. We now have enough Laws of Set Theory to write the proof using them.

Proposition 3.11.5 *Let A and B be sets. Then $A \oplus B = (A \cup B) \setminus (A \cap B)$*

Proof.

$$\begin{array}{rcll}
A \oplus B & = & (A \setminus B) \cup (B \setminus A) & \text{Definition} \\
& = & (A \cap B^c) \cup (B \cap A^c) & \text{Known equality} \\
& = & ((A \cap B^c) \cup B) \cap ((A \cap B^c) \cup A^c) & \text{Distributive} \\
& = & [(A \cup B) \cap (B^c \cup B)] \cap [(A \cup A^c) \cap (B^c \cup A^c)] & \text{Distributive} \\
& = & [(A \cup B) \cap \mathcal{U}] \cap [\mathcal{U} \cap (B^c \cup A^c)] & \text{Known equality} \\
& = & (A \cup B) \cap (B^c \cup A^c) & \text{Identity} \\
& = & (A \cup B) \cap (A \cap B)^c & \text{DeMorgan} \\
& = & (A \cup B) \setminus (A \cap B) & \text{Known equality}
\end{array}$$

□

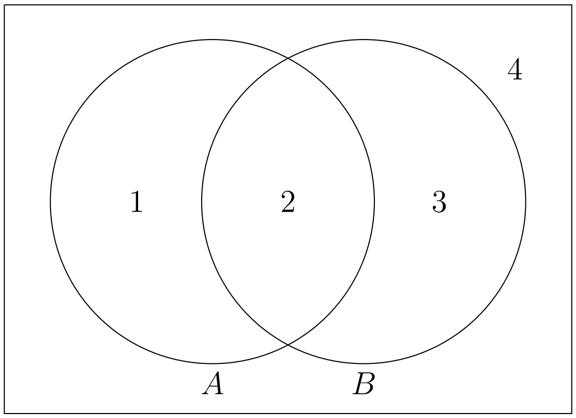
Question 3.11.6 *Use the Laws of Set Theory and other known set equalities to show that $(A \setminus B) \cup (A \cap B) = A$.*

3.12 Investigating Set Relationships with Venn Diagrams

The Venn diagram below suggests that, in general, $A \setminus B \neq B \setminus A$ because $A \setminus B$ is represented by region 1, while $B \setminus A$ is represented by region 3. (They may be equal for certain sets A and B, for instance if both sets are empty.) To confirm that these sets are not in general equal, we need to give an example of a universe and sets A and B such that $A \setminus B \neq B \setminus A$.

Fortunately, this is easy to do directly from the Venn diagram. Let the universe be the set of region numbers, and let each set be the collection of region numbers it contains in the diagram. Here, $\mathcal{U} = \{1, 2, 3, 4\}$, $A = \{1, 2\}$ and $B = \{2, 3\}$, then $A \setminus B = \{1\}$ and $B \setminus A = \{3\}$.

We thus have an important principle: *If two sets are represented by different collection of regions in a Venn diagram, then an example showing the sets are not equal can be obtained directly from the diagram.*



Venn diagrams can also provide intuition about equality between sets. As a first example, let's investigate whether $A \cup B$ is equal to $(A \setminus B) \cup B$. Using the diagram from before, we have:

Set	Represented by Regions
A	$1, 2$
B	$2, 3$
$A \cup B$	$1, 2, 3$
$A \setminus B$	1
$(A \setminus B) \cup B$	$1, 2, 3$

Since both sets are represented by the same collection of regions, we expect that they are equal. There are several different ways to construct a proof.

- Construct a truth table to show that the statement $x \in A \cup B \leftrightarrow x \in (A \setminus B) \cup B$ is a tautology. To do that, one has to express the memberships on each side in terms of compound statements, as in $[x \in A \vee x \in B] \leftrightarrow [(x \in A \wedge \neg(x \in B)) \vee x \in B]$.

- Use the definition of the two sets and show they are described by logically equivalent conditions.

- Write a proof in words, showing $LHS \subseteq RHS$ and $RHS \subseteq LHS$. The written proofs tend to follow the flow of logic used in constructing the set of regions that represent a set, except in the reverse order. In this example:

> *($LHS \subseteq RHS$) Take any $x \in A \cup B$. Then $x \in A$ or $x \in B$. We consider two cases, depending on whether $x \in B$. If $x \in B$, then $B \cup (A \setminus B) = (A \setminus B) \cup B$. If $x \notin B$, then x must be in A since it is in $A \cup B$. Thus $x \in A \setminus B$, and hence $x \in (A \setminus B) \cup B$. In either case, $x \in (A \setminus B) \cup B$. Therefore $A \cup B \subseteq (A \setminus B) \cup B$.*
>
> *($RHS \subseteq LHS$) Take any $x \in (A \setminus B) \cup B$. Then either $x \in A \setminus B$ or $x \in B$. If $x \in A \setminus B$, then $x \in A$ so $x \in A \cup B$. If $x \in B$, then $x \in B \cup A = A \cup B$. In either case, $x \in A \cup B$. Therefore $(A \setminus B) \cup B \subseteq A \cup B$.* □

Venn diagrams can also give insight into other types of relationships between. An example is the statement $A \subseteq B \Leftrightarrow A \cup B = B$. It is clear that if $A \subseteq B$ then $A \cup B = B$. What follows is not a proof, but will prove to be quite easy to turn into a proof. The condition $A \subseteq B$ says that every element of A is in B so, referring to the Venn diagram, no elements of A would be located in region 1. When region 1 contains no points of A, the set $A \cup B$ is (actually) represented by regions 2 and 3, so $A \cup B = B$. For the other logical implication, in the Venn diagram above, $A \cup B$ is represented by regions 1, 2, and 3, while B is represented by regions 2 and 3. The condition $A \cup B = B$, says that there are no elements of A that would be located in region 1 of the diagram. When this happens, A is (actually) represented by region 2 and, since B is represented by regions 2 and 3, this means $A \subseteq B$.

We now transform the observations in the preceding paragraph into a proof. There are two things so show:

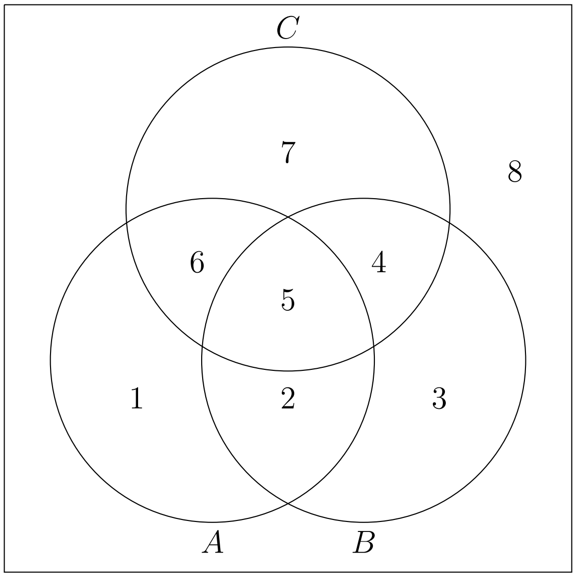
($A \subseteq B \Rightarrow A \cup B = B$) The goal is to prove that $A \cup B = B$. By definition of union, $B \subseteq A \cup B$. It remains to argue that $A \cup B \subseteq B$. Take any $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in B$ there is nothing to show. If $x \in A$, then since $A \subseteq B$, $x \in B$. This completed the proof that $A \cup B = B$.

($A \cup B = B \Rightarrow A \subseteq B$) The goal is to prove that $A \subseteq B$. Take any $x \in A$. Then, by definition of union, $x \in A \cup B$. Since $A \cup B = B$, $x \in B$. Therefore $A \subseteq B$. □

Because the definition of union involves the logical connective “or”, it is important to remember that *proofs of set relationships where one set involves the operation of union often use the method of proof by cases.*

Let’s use a diagram above to investigate whether $A \cup (B \cap C)$ equals $(A \cup$

$B) \cap C$.



Set	Represented by Regions
A	$1, 2, 5, 6$
B	$2, 3, 4, 5$
C	$4, 5, 6, 7$
$B \cap C$	$4, 5$
$A \cup (B \cap C)$	$1, 2, 4, 5, 6$
$A \cup B$	$1, 2, 3, 4, 5, 6$
$(A \cup B) \cap C$	$4, 5, 6$

As before, the regions correspond to the sets that would arise if we performed the set operations using $\mathcal{U} = \{1, 2, \ldots, 8\}, A = \{1, 2, 5, 6\}, B = \{2, 3, 4, 5\}$ and $C = \{4, 5, 6, 7\}$. Hence, when the sets in question are represented by different regions, these sets provide a counterexample. Doing so for the the example above, $A \cup (B \cap C) = \{1, 2, 4, 5, 6\}$ and $(A \cup B) \cap C = \{4, 5, 6\}$. Therefore the two expressions determine different sets in general.

The Venn diagram suggests $(A \cup B) \cap C \subseteq A \cup (B \cap C)$. Proving it would be a good exercise.

3.13 Counting sets and subsets

A set is called *finite* if it is empty, or $|X| = n$ for some positive integer n.

A set that isn't finite is called *infinite*. We will study infinite sets in a later chapter.

Recall our argument that *if X is a set and $|X| = n$, then X has exactly 2^n subsets*: Imagine constructing a subset of X. For each of the n elements of X there are two options: either it belongs to the subset or it doesn't. Each collection of n choices leads to a different subset.

Example 3.13.1 *Let $X = \{x_1, x_2, \ldots, x_n\}$. Determine the number of*

1. *subsets of X;*
2. *proper subsets of X;*
3. *non-empty subsets of X;*
4. *non-empty proper subsets of X;*
5. *subsets of X that contain x_1;*
6. *subsets of X that do not contain x_2;*
7. *subsets of X that contain x_3 and x_4, but not x_5.*

Solution.

1. *2^n, from above.*
2. *$2^n - 1$; only the set X itself is not a proper subset of X.*
3. *$2^n - 1$; all subsets of X except $\emptyset$ are non-empty.*
4. *Provided $X \neq \emptyset$, the number is $2^n - 2$, all subsets of X except X and $\emptyset$ are non-empty and proper. If $X = \emptyset$ then X has no non-empty proper subsets.*

5. *Any subset of X that contains x_1 is the union of $\{x_1\}$ and a subset of $X \setminus \{x_1\}$, so that there 2^{n-1} such subsets.*

   Another point of view is count the number of ways to construct a subset of X that contains x_1. We can do it as a sequence of n steps. First, put x_1 into the subset This choice is forced, so there is only one option of what to do. Then, for each of the remaining elements, $x_2, x_3, \dots, x_n$, decide whether it is in the subset of not. Different choices lead to different subsets. Since the outcome chosen at each step does not affect the number of options available at each subsequent step, the number of different outcomes of the construction is $1 \times 2^{n-1}$. Since each outcome leads to a different subset of X that contains x_1, the number of subsets of X that contain x_1 equals 2^{n-1}.

6. *2^{n-1}; the reasoning is as above.*

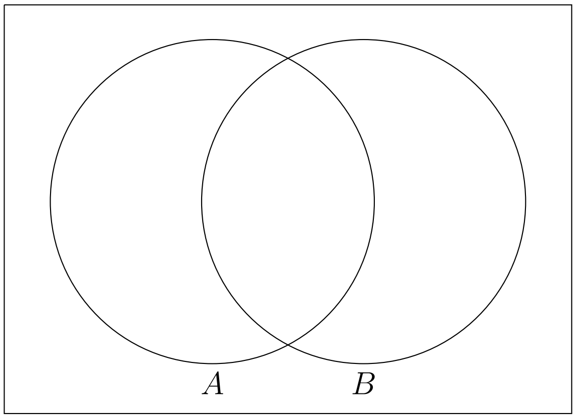
7. *2^{n-3}; there is one option for what to do with each of x_3, x_4 and x_5, and two choices for each of the other elements (it is in the subset, or not in the subset).*

3.14 Inclusion - Exclusion

It is a bit tricky to count the number of subsets of $X = \{x_1, x_2, \dots, x_n\}$ that contain x_1 or x_2. It isn't the number that contain x_1 plus the number that contains x_2 because subsets that contain both x_1 and x_2 are included twice. We could consider 3 cases: (i) subsets that contain x_1 and not x_2; (ii) subsets that contain x_2 and not x_1; and (iii) subsets that contain x_1 and x_2. This leads to the answer $2^{n-2} + 2^{n-2} + 2^{n-2} = 3 \cdot 2^{n-2}$. An alternative method uses the Principle of Inclusion and Exclusion, which is discussed below.

Let A and B be finite sets. Referring to the Venn diagram below, let's calculate $|A \cup B|$. The number $|A| + |B|$ counts each element in $A \setminus B$ exactly once, each element in $B \setminus A$ exactly once, and each element in $A \cap B$ exactly twice. *Therefore, $|A| + |B| - |A \cap B|$ counts each element of the union exactly once.*

The size of each single set is *included* and then the size of the intersection is *excluded.*



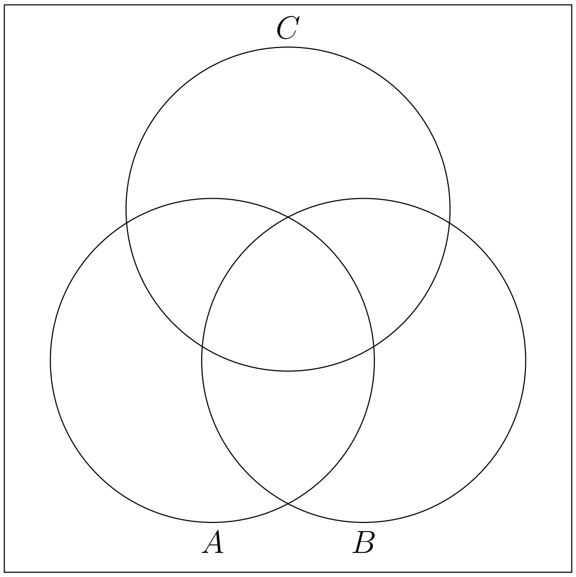
Let's go back to the example of computing the number of subsets of $S = \{x_1, x_2, \ldots, x_n\}$ that contain x_1 or x_2. Let A be the collection of subsets of S that contain x_1, and B be the collection of subsets of S that contain x_2. The subsets we want to count are exactly the elements of $A \cup B$. By the Principle of Inclusion and Exclusion, $|A \cup B| = |A| + |B| - |A \cap B| = 2^{n-1} + 2^{n-1} - 2^{n-2} = 3 \cdot 2^{n-2}$, which agrees with our previous calculation.

For sets A, B and C, a similar argument gives that

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

The size of each single set is *included*, the size of each intersection of two of the sets is *excluded*, and then the size of the intersection of all three sets is *included*.

The argument can be extended beyond three sets. The resulting theorem is called the *Principle of Inclusion and Exclusion* (PIE). It says that the number of elements of the union of n finite sets can be computed by including the number of elements in each single set, excluding the number of elements in all possible intersections of two sets, including the number of elements in all possible intersections of three sets, excluding the number of elements in all possible intersection of four sets, and so on.



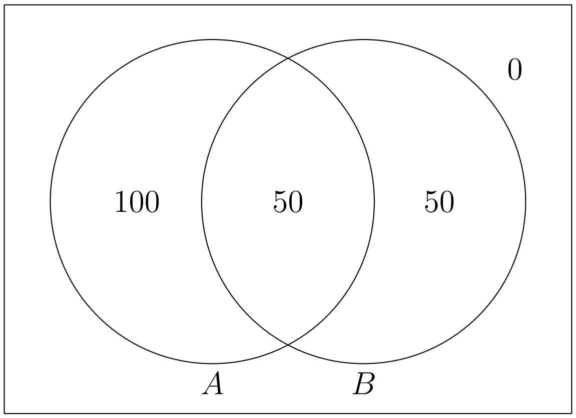
Example 3.14.1 *Suppose that in a group of 200 students, there are 150 taking Math 122, 100 taking Math 101, and 50 taking both of these classes.*

1. *How many of these students are taking neither Math 122 nor Math 101?*

2. *How many of these students are taking exactly one of Math 122 and Math 101?*

Solution.

We will use PIE. Let A be the set of students taking Math 122, and B be the set of students taking Math 101. The information given is that $\mathcal{U} = 200$, $|A| = 150$, $|B| = 100$, and $|A \cap B| = 50$. We can work backwards and fill in the number of elements in the 4 regions of the Venn Diagram: fill the diagram in starting with the region corresponding to intersection of all sets, and working "outwards" to the region corresponding to the elements not in any of the sets. It is given that $|A \cap B| = 50$. Since $|A| = 150$, and $|A \cap B| = 50$, it follows that $|A \setminus B| = 150 - 50 = 100$. Similarly, $|B \setminus A| = 100 - 50 = 50$. Therefore $|A \cup B| = 50 + 100 + 50$, the sum of the numbers in the 3 regions of the Venn Diagram that comprise $A \cup B$. Finally $|\mathcal{U} \setminus (A \cup B)| = 200 - (50 + 100 + 50) = 0$.



The answer to the questions is therefore:

1. *This is* $|(A \cup B)^c| = |\mathcal{U} \setminus (A \cup B)| = 0$.

2. *This is* $|(A \setminus B) \cup (B \setminus A)| = 100 + 50 = 150$. *Notice that the sets associated with corresponding regions of the Venn Diagram regions are disjoint (their intersection is empty), so that the number of elements in their union is just the sum of the elements in the sets.*

Question 3.14.2 *Suppose that in a group of 50 motorcyclists, 30 own a Triumph and 32 own a Honda. If 15 motorcyclists in the group own neither type of motorcycle, how many own a motorcycle of each type?*

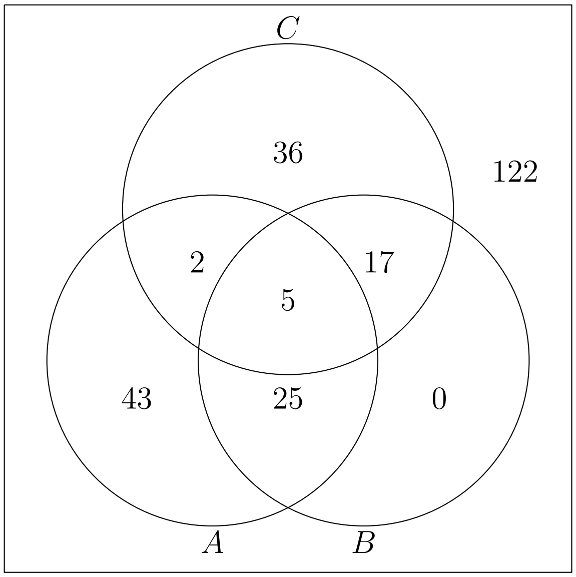
The same can be done for three (or more) sets.

Example 3.14.3 *Suppose that, of 250 programmers, 75 can program in Ada, 47 can program in Basic, and 60 can program in C++. There are 30 who can program in both Ada and Basic, 22 who can program in both Basic and C++, 7 who can program in both C++ and Ada, and 5 who can program in all three languages.*

1. *How many can program in at most one of them?*

2. *How many can program in Ada and exactly one of the other two languages?*

Solution.
Let A, B and C be the set of programmers who can program in Ada, Basic and C++, respectively. Filling in the regions of a Venn Diagram as above leads to the picture below.



The answers to the questions can then be read directly from the picture.

1. *We want* $|(A \cup B \cup C)^c| + |A \setminus (B \cup C)| + |B \setminus (A \cup C)| + |C \setminus (A \cup B)| = 122 + 43 + 0 + 36 = 201$

2. *We want* $|(A \cap B) \setminus C| + |(A \cap C) \setminus B| = 25 + 2 = 27$.

Since a Venn diagram for n sets has 2^n regions, 2^n pieces of information are needed to completely fill in the diagram. The Principle of Inclusion - Exclusion relates the number of elements in of the union of the sets corresponding to the various regions of the diagram which are "internal" to the union of the sets involved. The region corresponding to the collection of elements that belong to none of the sets is determined by subtracting the umber of elements in the union of the sets (which can be computed by PIE) from the size of the universe. (Note that this requires that the universe be a finite set. Everything else requires only that the sets involved in the union all be finite.) It follows that if a piece of information is missing, say the size of the intersection of all of the sets, then one can solve for it using PIE and / or the relationship between the size the the universe and the size of the complement of the union of the sets.

3.15 Exercises

1. Let $A = \{1, 2, \{1, 2\}\}$. Answer each question true or false, and briefly explain your reasoning.

   (a) $\{2\} \in A$

   (b) $\{1, 2\} \subsetneqq A$

   (c) $\{2, \{1, 2\}\} \subseteq A$

   (d) $\emptyset \in A$

   (e) $A \cap \mathcal{P}(A) = \emptyset$

2. Answer each question true or false, and briefly explain your reasoning.

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

   (b) If $A \cap B$ is not empty, then $A \setminus B$ is a proper subset of A.

   (c) If $x \in A$, then $\{x\} \in \mathcal{P}(A)$.

   (d) $\{\emptyset\}$ has two different subsets.

3. Let A and B be sets. Prove that any two of the following statements are (logically) equivalent.

   (a) $A \subseteq B$

   (b) $A \cup B = B$

   (c) $A \cap B = A$

   (d) $A \setminus B = \emptyset$

   (e) $A \oplus B \subseteq B$

   (f) $B^c \subseteq A^c$

Note: by a result from the Logic questions, it suffices to establish a cycle of 6 implications, for example (a) $\Rightarrow$ (b) $\Rightarrow \cdots \Rightarrow$ (f) $\Rightarrow$ (a). On the other hand, it is good practice to prove directly that any pair of statements are equivalent.

4. Let A and B be sets. Prove that $A \cup B = A \cap B \Leftrightarrow A = B$.

5. Let $A = \big\{\emptyset, \{x\}, B, \{1, \{x\}\}\big\}$, and $B = \{1, x\}$. Answer each question true or false, and briefly explain your reasoning.

   (a) $x \in A$.

   (b) $\{\emptyset\} \subseteq A$.

   (c) $B \subseteq A$.

   (d) $1 \in B \cap A$.

6. Prove that if $A \subsetneqq B$ and $B \subseteq C$, then $A \subsetneqq C$.

7. Prove or disprove each of the following statements about sets.

   (a) If $A \cap B \subseteq C$, then $\big((A \subseteq C) \wedge (B \subseteq C)\big)$.
   (b) $A \setminus B = (B \setminus A)^c$.

8. Prove that for all sets A, B and C, if $A \subseteq B$ and $B \cap C = \emptyset$, then $A \cap C = \emptyset$. Hint: Proof by contradiction.

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

10. Give a counterexample to each statement.

    (a) $(A \setminus B) \cap C = (A \cap C) \setminus B^c$, for all sets A, B, and C.
    (b) $(A \setminus B) \cup C^c = (A \cup B) \setminus C$, for all sets A, B, and C.

11. Let A, B and C be sets. Prove that $A \setminus (B \setminus C) = (A \setminus B) \cup (A \setminus C^c)$ without using set-builder notation and showing that the two sides are determined by logically equivalent expressions. Hint: an easy way uses the Laws of Set Theory.

12. Prove the same statement as in the previous question by showing LHS $\subseteq$ RHS and RHS $\subseteq$ LHS.

13. Prove or disprove: For all sets A, B and C, $(A\backslash B)\cup(B\backslash C)=A\backslash C$.

14. Let A, B, C be sets. Prove that $(A\cap B\cap C)^c=(A^c\cup B^c\cup C^c)$ by:

    (a) using the Associative Law to insert brackets and then DeMorgan's Law;

    (b) Showing LHS $\subseteq$ RHS and RHS $\subseteq$ LHS;

    (c) using set-builder notation and showing the LHS and RHS are defined by logically equivalent expressions

15. Repeat Question 14 for the equality $(A\cup B\cup C)^c=(A^c\cap B^c\cap C^c)$, and then state, but do not prove, the corresponding laws for any number of sets.

16. Let A and B be sets. Prove that the following statements are all (logically) equivalent.

    (a) $A=B$

    (b) $A\subseteq B$ and $B\subseteq A$

    (c) $A\setminus B=B\setminus A$

    (d) $A\oplus B=\emptyset$

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

    (f) $A^c=B^c$

17. Prove that for all sets A, B and C, $A\setminus(B\cup C)=(A\setminus B)\cap(A\setminus C)$ by using set-builder notation and showing the LHS and RHS are defined by logically equivalent expressions.

18. Repeat the previous question but use the Laws of Set Theory instead of set-builder notation.

19. Prove that for all sets A, B and C, if $B\cap C\subseteq A$, then

$$(C\setminus A)\cap(B\setminus A)=\emptyset.$$

    by using set-builder notation and using the fact that the hypothesis corresponds to the logical implication that for any x, $(x\in B)\wedge(x\in C)\Rightarrow(x\in A)$.

20. Repeat the previous question but use the Laws of Set Theory instead of set-builder notation.

21. Prove that for all sets A and B, if $B \subseteq A^c$, then $A \cap B = \emptyset$.

22. Let A, B, C be sets. Prove that if $A \cap B = \emptyset$, then $A \cap B \cap C = \emptyset$. Is the converse true? Explain.

23. Let $X = \{a, b, c, \ldots, z\}$. Determine the number of subsets $T \subseteq X$ that:

    (a) contain z;

    (b) do not contain a, e, i, o, u;

    (c) are such that $\{w, x, y\} \subsetneqq T$;

    (d) contain a and b but not c;

    (e) contain m or do not contain n;

    (f) contain at least one of p, q, r;

    (g) are such that $\{f, g, h\} \not\subseteq T$.

24. Determine the number of sets X such that $\{1, 2, 3\} \subseteq X \subsetneqq \{1, 2, 3, 4, 5, 6\}$. Explain your reasoning.

25. Two sets X and Y are called *disjoint* if $X \cap Y = \emptyset$.

    (a) Prove that if X and Y are disjoint finite sets, then $|X \cup Y| = |X| + |Y|$.

    (b) Prove that if A, B, C are pairwise disjoint finite sets (i.e., finite sets such that any two of them are disjoint), then $|A \cup B \cup C| = |A| + |B| + |C|$.

26. Suppose that in a group of 50 motorcyclists, 30 own a Triumph and 32 own a Honda. If 15 motorcyclists in the group own neither type of motorcycle, how many own a motorcycle of each type?

27. In a group of 35 ex-athletes, 17 play golf, 20 go cycling, and 12 do yoga. Exactly 8 play golf and go cycling, 8 play golf and do yoga, 7 go cycling and do yoga, and 4 do all three activities. How many of the ex-athletes do none of these activities?

Chapter 4

Induction and Recursion

4.1 Recursive definitions

The word "recursive" originates from the Latin word *recurs*, which means "returned", and which arises from a verb that means "go back". Informally, we will call a process "recursive" if it refers back to itself. In mathematics, a process is recursive if successive results depend on previous ones. In order to avoid an infinite regression of self-references, some basic outcomes (results, values) must be explicitly known without any self-reference.

We will start with recursively defined sequences.

A *recursive definition of a sequence* consists of two parts:

1. one or more *base cases* that explicitly state one or more terms of the sequence, and
2. a *recursion* that gives other terms of the sequence in terms of those already known.

For example, the Fibonacci numbers is the sequence $f_1, f_2, \ldots$ recursively defined by $f_1 = 1, f_2 = 1$, and $f_{n+1} = f_n + f_{n-1}$.

The definition can be applied over and over to compute as many terms of the sequence as desired. It begins $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$. The Fibonacci sequence has many wild and wonderful properties. Every third Fibonacci number is even, every fourth is a multiple of three, every fifth is a multiple of 5, every sixth is a multiple of 8. In general, every n-th Fibonacci number is a multiple of f_n. Another remarkable fact is that

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

This is even more stunning when you stop to think that f_n is an integer! Just for the sake of interest, let's look at the right hand side a bit more closely. The quantity $\frac{1-\sqrt{5}}{2}$ is less than one, so $\left(\frac{1-\sqrt{5}}{2}\right)^n$ converges to zero (quickly) as n grows. Because of this, it turns out that f_n is the nearest integer to $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$, i.e., the integer that arises from rounding.

Example 4.1.1 *Let $a_0, a_1, \ldots$ be the sequence recursively defined by $a_0 = 2$, $a_1 = 5$ and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$. Compute a_5.*

Solution.
We have $a_0 = 2$ and $a_1 = 5$. Therefore,

$$\begin{array}{rclcrcr} a_2 &=& 5a_1 - 6a_0 &=& 5\cdot 5 - 6\cdot 2 &=& 13\\ a_3 &=& 5a_2 - 6a_1 &=& 5\cdot 13 - 6\cdot 5 &=& 35\\ a_4 &=& 5a_3 - 6a_2 &=& 5\cdot 35 - 6\cdot 13 &=& 97\\ a_5 &=& 5a_4 - 6a_3 &=& 5\cdot 97 - 6\cdot 35 &=& 275 \end{array}$$

It turns out that $a_n = 2^n + 3^n$. This can be proved using methods from later in this chapter.

Question 4.1.2 *Let $b_1, b_2, \ldots$ be the sequence recursively defined by $b_1 = 2$, and $b_n = 3b_{n-1} + 5$ for $n \geq 2$. Compute b_6.*

We now turn our attention to writing recursive definitions of sequences. the key to doing this is to give the first few terms explicitly, then imagine that all terms up to the n-th are of the correct form, and then to describe how to get the $(n+1)$-st term from those already defined. How many terms should be given explicitly? It needs to be *at least as many terms as are needed to apply the recurrence.* In Example 4.1.1 the recurrence requires the previous two terms, so the first two terms of the sequence were given explicitly. For some sequences more than the minimum number of initial terms need to be given, but we won't come across any of them.

Example 4.1.3 *Give a recursive definition of:*

1. *The sequence* $1, 2, 4, 8, \ldots, 2^n, \ldots$
2. *The sequence* $-5, -2, 1, 4, \ldots, 3n-5, \ldots$
3. *The sequence* $a_1, a_2, \ldots$ *where* $a_n = 1 + 2 + \cdots + n$.

Solution.

1. $a_0 = 1$, *and* $a_{n+1} = 2a_n$, *for all* $n \geq 0$.
2. $a_0 = -5$ *and* $a_{n+1} = a_n + 3$ *for all* $n \geq 0$.
3. $a_1 = 1$, *and* $a_{n+1} = a_n + (n+1)$.

We now generalize Example 4.1.3, part 1. A *geometric progression* (or geometric sequence) is a sequence $a, ar, ar^2, ar^3, \ldots$, where $a, r \in \mathbb{R}$. (Remember that $a = ar^0$, so the sequence can also be written as $ar^0, ar, ar^2, ar^3, \ldots$.) Geometric progressions (with common ratio r) have the property that the ratio of each term to the one immediately before it is (the same number) r. These sequences can be recursively defined by $g_0 = a$, and $g_{n+1} = rg_n$ for all $n \geq 0$.

We now generalize Example 4.1.3, part 2. An *arithmetic progression* (or arithmetic sequence) is a sequence $a, a+d, a+2d, a+3d, \ldots$, where $a, d \in \mathbb{R}$. Arithmetic progressions are sequences such that the difference between any term and the one after it is (*the common difference*) d. These sequences can be recursively defined by $b_0 = a$, and $b_{n+1} = b_n + d$ for all $n \geq 0$.

Other things besides sequences can also be recursively defined. As with the example of sequences, a *recursive definition* consists of two parts:

1. one or more *bases cases* that explicitly describe some of the basic items, and
2. a *recursion* that gives other items in terms of those already known.

Example 4.1.4 *Give a recursive definition of the quantity* $n! = 1 \times 2 \times \cdots \times n$, *where* n *is a non-negative integer. (An empty product equals 1. Why? Because you can multiply any number by a product with no terms and the value should not change.)*

Solution.
$0! = 1$ *and* $n! = n \times (n-1)!,\ n \geq 1$.

Example 4.1.5 *Suppose you are given numbers $x_1, x_2, \ldots, x_n$. Give a recursive definition of the sum $x_1 + x_2 + \cdots + x_n$.*

Solution.
For $1 \leq i \leq n$, let $S_i = x_1 + x_2 + \cdots + x_i$. Then $S_1 = x_1$, and $S_k = S_{k-1} + x_k$ for $2 \leq k \leq n$. The desired sum is S_n.

(Notice that this corresponds to the way you add n numbers on a calculator.)

Other (associative) operations like multiplication, set union, set intersection, conjunction of logical propositions, and disjunction of logical propositions can be recursively defined in a similar way.

Example 4.1.6 *Let X be the set of all positive integers that can be written as a sum of threes and fives. Give a recursive definition of the set X.*

Solution.
$3, 5 \in X$, *and if* $x \in X$, *then* $x + 3 \in X$ *and* $x + 5 \in X$.

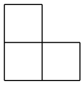
4.2 Induction: An introduction

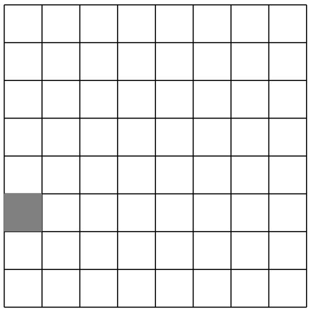
This section is intended as an introduction to *The Principle of Mathematical Induction* (PMI): a theorem that establishes the validity of the proof method which goes by the same name. There is a particular format for writing the proofs which makes it clear that PMI is being used. We will not explicitly use this format when introducing the method, but will do so thereafter.

Here is the first of the two introductory examples that will be discussed in this section: tiling punctured grids.

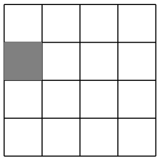
Suppose you are given a large supply of L-shaped tiles as shown on the left of the figure below. The question you are asked to answer is whether these tiles can be used to exactly cover the squares of an $2^n \times 2^n$ *punctured grid* – a $2^n \times 2^n$ grid that has had one square cut out – say the 8×8 example shown in the right of the figure.

In order for this to be possible at all, the number of squares in the punctured grid has to be a multiple of three. By direct calculation we can see that it is

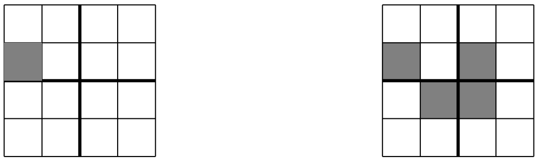




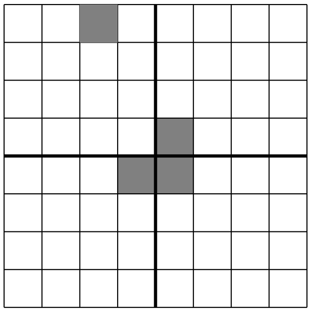
true when $n = 1, 2$ or 3, and these are the cases we're interested in here. It turns out to be true in general; this is easy to show using congruences, which we will study later, and also can be shown using methods in this chapter. But that does not mean we can tile the punctured grid. In order to get some traction on what to do, let's try some small examples. The tiling is easy to find if $n = 1$ because 2×2 punctured grid is exactly covered by one tile. Let's try $n = 2$, so that our punctured grid is 4×4. By rotating, we can assume the missing square is in the upper left quadrant, say as illustrated below.



Imagine the punctured grid partitioned into four 2×2 grids, one of which has a square missing, as shown on the left of the figure below. As shown on the right of the figure, we can astutely place one tile to transform our problem into four 2×2 problems, each of which we know how to solve.

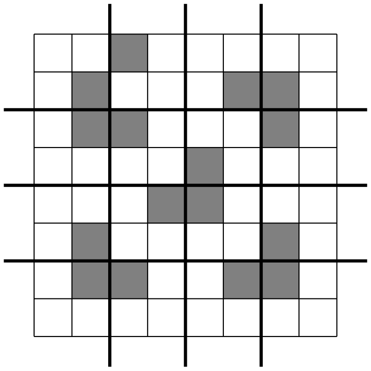


It is clear that this method works no matter which square in the upper left quadrant has been removed. Hence, if we can cover any 2×2 punctured grid, then we can cover and 4×4 punctured grid. Now we can see what to do to cover the 8×8 punctured grid: partition it into four 4×4 grids, one of which has a square removed, then astutely place a tile to transform the problem into four 4×4 problems we know how to solve because of our previous work.

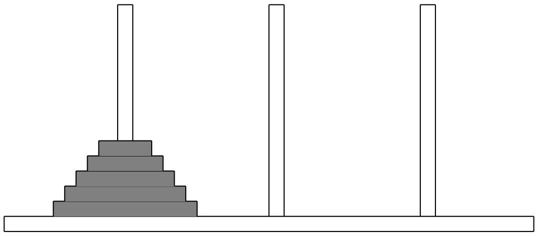


There is nothing special about the numbers 4 and 8 in the previous examples. Once we know how to cover all possible punctured grids of size 2×2, 4×4, and 8×8, we can use the same method on any 16×16 punctured grid. And we can keep going. Once we know how to cover all punctured grids of size $2 \times 2,\ 4 \times 4,\ \ldots, 2^k \times 2^k$, we can use the same method to reduce the problem of covering a $2^{k+1} \times 2^{k+1}$ grid to four smaller problems we know how to solve because of previous work. Therefore, for any $n \geq 1$, the squares of a $2^n \times 2^n$ punctured grid can be exactly covered by L-shaped tiles.

The previous example illustrates the strong form of the *Principle of Mathematical Induction* (PMI). One meaning of the word *induction* is "the act of bringing forward". Above, we brought forward our knowledge of how to solve smaller instances of the problem to solve all instances of the next possible size. Notice also that the solution can be obtained recursively. For example, to cover an 8×8 punctured grid, we cover four 4×4 punctured grids, and each of these is covered via covering four 2×2 punctured grids. This is illustrated in the figure below. Completing the tiling of each 2×2 punctured grid gives the tiling of the 8×8 punctured grid.



We now turn to our second informal introductory example. The *Towers of Hanoi* is a puzzle that begins with $n \geq 1$ rings, each with a different diameter, stacked in decreasing order of size on one of three towers. An example with five rings is shown below. The objective is to move the rings one at a time so that they are eventually stacked in the same order on one of the other towers. At no point in time may a larger ring rest on top of a smaller one.



It is easy to directly check that a solution exists when there are 1 or 2 rings. To obtain a solution when there are 3 rings, first use the 2-ring solution to move the top 2 rings to one of the unused towers. Then move the bottom (largest) ring to the remaining unused tower. Finally, use the 2-ring solution again to move the 2 smaller rings to the tower containing the largest ring. It does not matter if, at any point in this process, any of the other rings is placed on top of the largest one (since it is largest).

Suppose we can solve the puzzle when n is any of the integers $1, 2, \ldots, k$, where $k \geq 3$. Let's try to "bring forward" this knowledge to obtain a solution when there are $k + 1$ rings. We can proceed as in the 3-ring case. First, use the k-ring solution to legally move the k smallest rings to one of the other towers. Leaving the large ring in place will not cause the constraint that a larger ring may not rest atop a smaller one to be violated. Second, move the largest ring to the empty tower. Finally, use the k-ring solution to legally move the k smallest rings so that they are on top of the largest one.

Since we know how to solve the puzzle when there are 1, 2, and 3 rings, it follows that we can also solve it when there are 4 rings. Using this, we can also solve it when there are 5 rings. Repeating as often is needed, we can eventually obtain a solution for any integer $n \geq 1$. Therefore, for any $n \geq 1$ there is a solution to the Towers of Hanoi puzzle when there n rings.

It is possible go a bit farther and show that with n rings, the solution uses $2^n - 1$ moves. The argument proceeds similarly as above. Legend has it that the end of the world would come before a person could complete the solution to the puzzle with 64 rings. By the above, it would take $2^{64} - 1$ moves. There are $60 \times 60 \times 24 \times 365 = 31536000 \approx 2^{24.9}$ seconds in a year, ignoring leap years. Hence, if a person could move one ring per second, then solving the puzzle would take about 2^{39} years.

4.3 PMI – The Principle of Mathematical Induction

The Principle of Mathematical Induction (PMI) is a theorem that gives a method for establishing the truth of statements quantified over all integers greater than or equal to some given integer. An example of such a statement is "*For any $n \geq 1$, a $2^n \times 2^n$ punctured grid can be exactly covered by L-shaped tiles*". Another is "*The sum of the first n positive integers is $n(n+1)/2$*".

In computer science, statements like these regularly arise in the analysis of algorithms. But not only that, proofs by induction also tend to imply recursive algorithms for solving the problem at hand. Further, PMI is a main tool in proving the correctness of recursive algorithms. Witness the L-shaped tiles example in the previous paragraph.

Whenever you need to prove a statement that is quantified over all integers greater than of equal to some given integer, then one tool you should consider trying to use is PMI. (As usual, it may or not be successful to complete the task at hand.)

It turns out that there are two forms of PMI – a so-called strong form and a so-called weak form – but they are of identical expressive power. In other words, any statement that can be proved by one of them can be proved by the other. However, it is often true that a proof using one form (usually the strong form) involves a lot less writing than a proof using the other form. The choice of which to use is really a matter of mathematical aesthetics, and sheer laziness (wanting to write less, or wanting the writing to be easier). We will begin our discussion of PMI with the strong form of induction, and come to the weak form later. We'll discuss the qualifier "strong" at that time.

Theorem 4.3.1 (Strong Form of PMI) *Let $S(n)$ be a statement whose truth depends on the integer n. If the following two conditions hold:*

1. *the statement $S(n)$ is true when n is any of the integers $n_0, n_0+1, \ldots, t$, for some $t \geq n_0$;*

2. *for any integer $k \geq t$, the truth of the statement $S(n)$ for all of the integers $n_0, n_0+1, \ldots, k$ logically implies the truth of $S(n)$ when $n = k+1$;*

then, the statement $S(n)$ is true for all integers $n \geq n_0$.

The strong form of PMI is commonly referred to as *strong induction* or sometimes just *induction.* The theorem implies a proof method. It says we can prove $S(n)$ is true for all $n \geq n_0$ by doing two things:

1. Directly check that $S(n)$ is true for the first few possible values of n, say $n = n_0, n = n_0 + 1, \ldots, n = t$, where $t \geq n_0$. (It turns out that the size of t depends on what you're trying to prove.) This is called the *Basis* because it is the foundation that the rest of the argument rests on.

2. Prove that if $S(n)$ is true for all possible values of n from n_0 up to k, where $k \geq t$, then it is also true when $n = k + 1$. This is called the *Induction* because we use (bring forward) the truth of $S(n)$ for smaller values of n to prove that $S(n)$ is true for the next possible value of n. Usually the induction is separated into two parts.

   In the *Induction Hypothesis* one assumes there is an integer $k \geq t$ such that the statement $S(n)$ is true when $n = n_0, n = n_0 + 1, \ldots, n = k$.

> (Note: k must be at least as large as the last value checked in the Basis.)
>
> In the *Induction Step* one uses this information to show that $S(n)$ is also true when $n = k + 1$.

Having completed these steps, we can conclude that $S(n)$ is true for all $n \geq n_0$.

Why does an argument like this imply the conclusion we want? The Basis says the statement $S(n)$ is true for all values of n from n_0 up to t. Using this, the Induction Hypothesis (with $k = t$) and Induction Step show that the statement $S(n)$ is also true when $n = t+1$. So, now, we have that $S(n)$ is true or all values of n from n_0 up to $t+1$. But using the Induction Hypothesis (with $k = t + 1$), we get that $S(n)$ is true or all values of n from n_0 up to $t + 2$. This procedure can be repeated over and over. For any particular integer $\ell \geq n_0$, after enough applications of the procedure we have that the statement $S(n)$ is true when $n = \ell$. But ℓ is an arbitrary integer which is greater than or equal to n_0. Hence, we can conclude that $S(n)$ is true for any given integer $n \geq n_0$.

A proof using PMI has four components: (i) a Basis; (ii) an Induction Hypothesis; (iii) an Induction Step; and (iv) a Conclusion. It is customary to carry out these four steps in clearly labelled sections.

In carrying out a proof by PMI, it is important to carry out all four of the steps. The only two that require any real work are checking that the Basis holds (in enough cases so that the Induction Step works), and then proving that the logical implication needed for the Induction Step. The other two steps are important, however, especially for communication; *it is definitely worth making an effort to clearly state the Induction Hypothesis.*

We illustrate the steps described above with two examples.

Example 4.3.2 *Suppose you want to know which positive integers can be written as a sum of 3s and 5s. Clearly 1 and 2 can't, 3 can, 4 can't, 5 and 6 can, 7 can't, and* $8, 9, 10, 11, \ldots 15$ *all can. Based on this data it seems like every positive integer* $n \geq 8$ *can be written as a sum of 3s and 5s. Prove that this is true.*

The statement that we want to prove is "for all $n \geq 8$*, the integer* n *can be written as a sum of 3's and 5's".*

Proof.

Basis. Since 8 = 5+3, 9 = 3+3+3, and 10 = 5+5, each of 8, 9, and 10 can be written as a sum of 3s and 5s.

Induction Hypothesis. Suppose there is an integer $k \geq 10$ *such that each of* $8, 9, 10, \ldots, k$ *can be written as a sum of 3's and 5's.*

Induction Step. We want to show that $k + 1$ *can be written as a sum of 3's and 5's. Since* $k \geq 10$, $k+1-3 \geq 8$, *so by the Induction Hypothesis,* $k+1-3$ *can be written as a sum of 3's and 5's But then adding 3 to this sum gives* $k + 1$ *as a sum of 3's and 5's, which is what we wanted.*

Conclusion. Therefore, by the strong form of PMI, any integer $n \geq 8$ *can be written as a sum of 3's and 5's.* □

Problems like Example 4.3.2 are called *postage stamp problems* because they date back to the days when stamps came in denominations like 1 cent, 3 cents, 5 cents, and so on. People often kept a supply of stamps of various values, and then tried to combine them to make whatever postage was needed at the time. This is the same problem as writing a given positive integer as a sum of various other given positive integers, if possible.

The related problem of finding the largest integer that can not be written at the sum of two given positive integers m and n is known as the Frobenius Coin Problem. Its solution, that if m and n have no common factors then the number is $mn - m - n$ is known as the Chicken McNugget Theorem. Why? Originally, McDonald's sold its Chicken McNuggets in packs of 9 and 20. Math types were curious to figure out the largest number of nuggets that could not have been bought with these packs. It turns out to be $151 = 9 \cdot 20 - 9 - 20$.

Example 4.3.3 *Let* $a_0, a_1, \ldots$ *be the sequence recursively defined by* $a_0 = 0$, *and* $a_n = 2a_{n-1} + 1$ *for* $n \geq 1$. *Prove that* $a_n = 2^n - 1$ *for all* $n \geq 0$.

Proof.

Basis. By definition, $a_0 = 0 = 2^0 - 1$, $a_1 = 1 = 2^1 - 1$, *and* $a_2 = 3 = 2^2 - 1$. *Therefore, the statement that* $a_n = 2^n - 1$ *is true when* $n = 0, 1$ *or 2.*

Induction Hypothesis. Suppose there is an integer $k \geq 2$ *such that* $a_n = 2^n - 1$ *for* $n = 0, 1, \ldots, k$.

Induction Step. We want to show that the statement is true when $n = k+1$, that is, that $a_{k+1} = 2^{k+1} - 1$. Look at a_{k+1}. Since $k \geq 2$ we know $k+1 \geq 3$ and so

$$\begin{aligned} a_{k+1} &= 2a_k + 1 && \textit{(by the recursive definition)} \\ &= 2(2^k - 1) + 1 && \textit{(since } a_k = 2^k - 1 \textit{ by the induction hypothesis)} \\ &= 2^{k+1} - 2 + 1 && \textit{(since } 2^1 \cdot 2^k = 2^{k+1}\textit{)} \\ &= 2^{k+1} - 1, \textit{ as wanted.} \end{aligned}$$

Conclusion. Therefore, by induction, $a_n = 2^n - 1$ for all $n \geq 0$. □

4.4 PMI and the Well Ordering Principle

The Well-Ordering Principle (WOP) is the following self-evident theorem:

Theorem 4.4.1 (Well Ordering Principle) *Let X be a non-empty set of integers that is bounded below (ie. every integer in the set is at least as big as some constant $n_0 \in \mathbb{Z}$). Then X has a smallest element.*

Let n_0 be the constant in the statement of the WOP. If $n_0 \in X$, then it is the smallest element of X. Otherwise, since X is not empty and each integer has a successor (the *successor* of ℓ is $\ell + 1$), there is a first integer after n_0 which belongs to X (remember that infinity is not an integer!), and this integer is the smallest element of X.

We now explain how the WOP implies PMI. The proof is by contradiction. Suppose assertions (1) and (2) of PMI hold, but the conclusion that $S(n)$ is true for all $n \geq n_0$ is false. Then, the set X of integers greater than or equal to n_0 for which $S(n)$ is false is not empty. By assertion (1), none of the values $n_0, n_0 + 1, \ldots, t$ belong to X. Hence X is bounded below by n_0. By the WOP, the set X has a smallest element, call it $k+1$. Note that $k+1 \geq t+1$, so that $k \geq t$. Since $k+1$ is the smallest element in X, the statement $S(n)$ is true when n is any of the integers $n_0, n_0+1, \ldots, k$, where $k \geq t$. But then, by assertion (2) of PMI, the statement $S(n)$ is true when $n = k+1$, a contradiction to $k+1$ being the smallest integer n for which $S(n)$ is false. Hence $S(n)$ must be true for all $n \geq n_0$.

It transpires that if one assumes the truth of PMI, then one can use that assumption to prove the truth of the WOP. The WOP and PMI are regarded as equivalent in the sense that each logically implies the other.

4.5 Examples Involving Multi-term Recursively Defined Sequences

In this section we give examples of using PMI to prove statements about recursively defined sequences.

Example 4.5.1 *Let a_n be the sequence recursively defined by $a_0 = 1$, $a_1 = 2$, and for $n \geq 2$, $a_n = 3a_{n-1} - 2a_{n-2}$. Show that $a_n = 2^n$ for all $n \geq 0$.*

Proof.

Basis. When $n = 0$ we have $a_0 = 1 = 2^0$ and when $n = 1$ we have $a_1 = 2 = 2^1$. Hence the statement is true when $n = 0$ and $n = 1$.

Induction Hypothesis. Suppose there is an integer $k \geq 1$ such that $a_n = 2^n$ for $n = 0, 1, \ldots, k$.

Induction Step. We want to show that $a_{k+1} = 2^{k+1}$.

Consider a_{k+1}. Since $k + 1 \geq 2$ we have

$$a_{k+1} = 3a_k - 2a_{k-1} = 3 \times 2^k - 2 \times 2^{k-1}$$

by the Induction Hypothesis. The RHS of this expression equals $3 \times 2^k - 2^k = 2^k(3 - 1) = 2^{k+1}$, as needed.

Conclusion. Therefore, by PMI, $a_n = 2^n$ for all $n \geq 0$. □

Example 4.5.2 *Show that every third Fibonacci number is even.*

Proof.

Let's first translate the problem. We want to show that, for all $n \geq 1$, f_{3n} is even.

Basis. We have $f_{3 \cdot 1} = f_3 = 2$, which is clearly even. Thus, the statement is true when $n = 1$.

Induction Hypothesis. Suppose there is an integer $k \geq 1$ such that f_{3k} is even for $n = 1, 2, \ldots, k$.

Induction Step. We want to show that $f_{3(k+1)} = f_{3k+3}$ is even.

Consider f_{3k+3}. Since $k \geq 1$, $3k+3 \geq 6$ so we can use the recursion to write

$$f_{3k+3} = f_{3k+2} + f_{3k+1} = (f_{3k+1} + f_{3k}) + f_{3k+1} = f_{3k} + 2f_{3k+1}.$$

Now, the last term on the RHS is even because it is multiplied by 2, and the first term on the RHS is even by the Induction Hypothesis. Therefore, $f_{3k} + 2f_{3k+1} = f_{3k+3}$ is even, as desired.

Conclusion. Therefore, by PMI, for all $n \geq 1$, f_{3n} is even. □

Much more is true. Every fourth Fibonacci number is a multiple of 3, every fifth one is a multiple of 5, every sixth one is a multiple of 8, and in general every n-th Fibonacci number is a multiple of f_n. All of these statements can be proved similarly as above.

Example 4.5.3 *Prove that $f_n \leq 2^{n-1}$ for any natural number $n \geq 1$.*

Proof.

Basis. We have $f_1 = 1 \leq 2^0$ and $f_2 = 1 \leq 2^1$. Thus the statement is true when $n = 1$ and when $n = 2$.

Induction Hypothesis. Assume there is an integer $k \geq 2$ such that $f_n \leq 2^{n-1}$ for $n = 1, 2, \ldots, k$. That is, assume $f_1 \leq 2^0$, $f_2 \leq 2^1, \ldots, f_k \leq 2^{k-1}$.

Induction Step. We want to prove that $f_{k+1} \leq 2^{(k+1)-1} = 2^k$.

Consider f_{k+1}. Since $k+1 \geq 3$ we have

$$\begin{array}{rcll} f_{k+1} & = & f_k + f_{k-1} & \textit{(by definition of } f_{k+1}\textit{)} \\ & \leq & 2^{k-1} + 2^{(k-1)-1} & \textit{(by IH)} \\ & = & 2^{k-2}(2+1) & \textit{(algebra)} \\ & \leq & 2^{k-2}2^2 & \textit{(because } 3 \leq 4 = 2^2\textit{)} \\ & = & 2^k & \textit{as wanted.} \end{array}$$

Conclusion. Therefore, by PMI, $f_n \leq 2^{n-1}$ for all natural numbers $n \geq 1$. □

It is worth emphasizing the importance of having two cases in the Basis. In the Induction Step we want to take f_{k+1} and replace it by $f_k + f_{k-1}$. The recursive part of the definition can only be applied when $k+1$ is at least 3.

By using a bit more algebra, better upper bounds are possible. For example, for all integers $n \geq 1$, $f_n \leq (7/4)^{n-1}$.

4.6 The Weak Form of Induction

Among the induction examples we have done so far, in Examples 4.3.3 and 4.5.2, completing the Induction Step required only that we assume the statement $S(n)$ to be true when $n = k$ (and not all values from n_0 up to k). In the others, it required the truth of $S(n)$ for several values between n_0 and k.

Mathematicians care about aesthetics, and so we do not like to assume more than we need. If completing the Induction Step requires only that $S(n)$ be true when $n = k$, we don't want to assume any more than that. It is also true that some proofs become easier to write if we only need this (weaker) assumption because it is much easier to state the Induction Hypothesis. (The assumption is considered *weaker* because not as much is being assumed; in Strong Induction we're assuming more, in particular that $S(n)$ is true for all values of n from n_0 up to k.)

Theorem 4.6.1 (Weak Form of PMI) *Let $S(n)$ be a statement whose truth depends on the integer n. If the following two conditions hold:*

1. *the statement $S(n)$ is true when $n = n_0$;*

2. *for each $k \geq n_0$, the truth of the statement $S(n)$ for $n = k$, logically implies the truth of $S(n)$ when $n = k + 1$;*

then, the statement $S(n)$ is true for all integers $n \geq n_0$.

The reason the conclusion holds is the same as before. We know that the statement is true for n_0. The induction (assertion (2)) then allows us to conclude that the statement is true for $n_0 + 1$. Using this, the induction (assertion (2)) then allows us to conclude that the statement is true for n_0+2. And so on, until finally we can reach any integer $x \geq n_0$. Thus, as before, the only reasonable conclusion is that the statement is true for all integers $n \geq n_0$. Note, also, that by the time we have applied assertion (2) enough times to know the statement is true when $n = k$, we have actually proved that it is true for all integers between n_0 and k (identical to the assumption in the strong form of induction).

The proof of the weak form of PMI is virtually identical to the proof given for the strong form. It is a good exercise to write it out and see the underlying logic for yourself.

The weak form of induction can be imagined as the following logical argument where, for simplicity, we will use 1 in place of n_0. Suppose

- $S(1)$ is true,
- for each $k \geq 1$, the logical implication $S(k) \Rightarrow S(k+1)$ holds

and you want to verify that $S(5)$ holds. By the second bullet point, you know that

$$S(1) \Rightarrow S(2) \Rightarrow S(3) \Rightarrow S(4) \Rightarrow S(5)$$

so that $S(1) \Rightarrow S(5)$. By the first bullet point you know that $S(1)$ is true. Therefore, $S(5)$ is true. The same argument works with any integer n in place of 5, so $S(n)$ is true for all $n \geq 1$.

How do you know which form to use? Sometimes you don't until after completing the Induction Step and seeing the smaller values for which you need the truth of the statement. *It is always safe to use the strong form of PMI*, but your proofs might look a lot prettier (and you might look more aware of what's being assumed) with the weak form.

4.7 Examples Involving Summations

The key point in using PMI to prove summation identities occurs in the Induction Step: *remember the meaning of the ellipsis "…", and substitute the assumed value from the Induction Hypothesis for the first k terms in the sum (don't forget to keep the $(k+1)$-st term!) then do algebra to get what you want.*

Example 4.7.1 *Suppose that you are mathematically doodling and notice* *that:*

$$\begin{aligned} 1 &= 1 \\ 1+3 &= 4 \\ 1+3+5 &= 9 \\ 1+3+5+7 &= 16 \end{aligned}$$

and are led to guess that the sum of the first n odd positive integers equals n^2. Let's prove that is true.

Proof.

The statement to be proved is "for all integers $n \geq 1$, the sum $1+3+\cdots+2n-1 = n^2$."

Basis. *Since $1 = 1^2$, $1+3 = 2^2, 1+3+5 = 3^2$ and $1+3+5+7 = 4^2$, the statement is true for $n = 1, 2, 3, 4$.*

Induction Hypothesis. *Suppose there is an integer $k \geq 4$ such that $1+3+\cdots+2k-1 = k^2$.*

Induction Step. *We want to show that $1+3+\cdots+2(k+1)-1 = (k+1)^2$. Look at the LHS,*

$$\begin{aligned} 1+3+\cdots+2(k+1)-1 &= 1+3+\cdots+(2k-1)+2(k+1)-1 \\ &= k^2+2(k+1)-1 \quad \textit{(by IH)} \\ &= k^2+2k+1 \\ &= (k+1)^2, \quad \textit{as wanted.} \end{aligned}$$

Conclusion. *Therefore. by PMI, for any $n \geq 1$, $1+3+\cdots+2n-1 = n^2$.* □

Example 4.7.2 *Prove that, for any natural number $n \geq 1$, $1+2+\cdots+n = \frac{n(n+1)}{2}$.*

Proof.

Basis. *When $n = 1$, we have LHS$= 1$ and RHS$= 1(1+1)/2 = 1$. Thus the statement is true when $n = 1$.*

Induction Hypothesis. *Suppose there is an integer $k \geq 1$ such that $1+2+3+\cdots+k = k(k+1)/2$.*

Induction Step. We want to prove that $1+2+3+\cdots+(k+1) = (k+1)((k+1)+1)/2 = (k+1)(k+2)/2$.

Consider the LHS:
$1+2+\cdots+(k+1)$
$= 1+2+\cdots+k+(k+1)$ *(meaning of the elipsis)*
$= k(k+1)/2+2(k+1)/2$ *(by IH, and getting a common denominator)*
$= (k+1)(k+2)/2$ *as desired.*

Conclusion. Therefore, by induction, $1+2+3+\cdots+n = n(n+1)/2$ *for all* $n \geq 1$. □

There are a number of sums that arise frequently. You should both memorize them, and know how to prove each one. Induction always works, though there can be other proofs as well.

1. For any natural number $n \geq 1$,

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

2. For any natural number $n \geq 1$,

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

3. For any natural number $n \geq 1$,

$$1^3+2^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}.$$

   It is a fluke that the RHS is the square of the first identity above. The pattern does not continue.

4. (Sum of a geometric series.) For any natural number $n \geq 1$ and any real number $r \neq 1$,

$$1+r+r^2+\cdots+r^n = \frac{r^{n+1}-1}{r-1}.$$

4.8 Examples Involving Inequalities

The key to proving inequalities with induction is this: in the induction step, start on a side where you can see you to use the induction hypothesis somehow. After doing that, gradually change what you have until it is possible to see how to get what you need. If you are proving a less than inequality, then you can do anything you want that increases what you have, so long as the change does not make it exceed the upper bound you are trying to achieve. Similar considerations apply to other inequalities.

Example 4.8.1 *Prove that $n! > 3^n$ for all $n \geq 7$.*

Proof.

Basis. When $n = 7$ we have $n! = 7! = 5040$ and $3^n = 3^7 = 2187$. Hence the statement to be proved is true when $n = 7$.

Induction Hypothesis. Suppose there exists an integer $k \geq 7$ such that $k! > 3^k$.

Induction Step. We want to show that $(k+1)! > 3^{k+1}$.

Consider the RHS. We have $3^{k+1} = 3 \cdot 3^k < 3 \cdot k!$ by the Induction Hypothesis. Now, since $k \geq 7$ we have $3 < 8 \leq k+1$, so that $3 \cdot k! < (k+1)k! = (k+1)!$, as wanted.

Conclusion. Therefore, by PMI, $n! > 3^n$ for all $n \geq 7$. □

There is a fairly established hierarchy of the growth rates of functions, and it is used all the time when comparing the performance of algorithms on inputs of given size (for example, algorithms that operate on n items usually use a number of steps proportional to n^2, or to $n \log_2(n)$; when n is large, this difference matters in terms of how long it takes for the task to be completed). What that means is that for all large enough values of the input (and maybe not for small ones), functions at a higher level in the hierarchy have function values that are much larger that those at a lower level. Constants are at the bottom of the hierarchy, then logs. And then polynomials. The higher the degree, the faster the growth. Exponential functions always eventually become greater than any polynomial, and factorials always eventually become larger that exponentials. Finally, functions like n^n eventually become larger than factorials. Inequalities between functions at the various levels of this hierarchy can be proved with induction.

Before moving to an example involving polynomials, we illustrate a useful technique. The following sort of argument arises all the time in proving inequalities where one "side" is a polynomial. We will demonstrate how to argue that $n^3 + 4n^2 + 5n + 3 \leq 2n^3$ when $n \geq 6$. Suppose $n \geq 6$. Then we can change the right hand 3 to n, that is

$$n^3 + 4n^2 + 5n + 3 \leq n^3 + 4n^2 + 5n + n = n^3 + 4n^2 + 6n.$$

In the same way, replacing $6n$ by n^2 only makes the expression larger (because $n \geq 6$). Thus,

$$n^3 + 4n^2 + 6n \leq n^3 + 4n^2 + n^2 = n^3 + 5n^2.$$

And, doing the same again to replace $5n^2$ by n^3 (because $n \geq 6$) gives

$$n^3 + 5n^2 \leq n^3 + n^3.$$

Putting this all together, we have just shown that if $n \geq 6$, then $n^3 + 4n^2 + 5n + 3 \leq 2n^3$. We use this method in the example below.

Example 4.8.2 *Prove that for all $n \geq 5$, $2^n > n^2$.*

Proof.

Basis. When $n = 5$, $2^n = 2^5 = 32$ and $n^2 = 5^2 = 25$. As $32 > 25$ the statement is true for $n = 5$.

Induction Hypothesis. Suppose there is an integer $k \geq 5$ such that $2^k > k^2$.

Induction Step. We want to show $2^{k+1} > (k+1)^2$.

Consider $(k+1)^2 = k^2 + 2k + 1 < k^2 + 2k + k$ (as $k \geq 5 > 1$) $= k^2 + 3k < k^2 + k(k)$ (as $k \geq 5 > 3$) $= 2k^2 < 2(2^k)$ (by the induction hypothesis) $= 2^{k+1}$, as wanted.

Conclusion. Therefore, by the Principle of Mathematical Induction, for all $n \geq 5$, $2^n > n^2$. □

4.9 Finding Formulas for Sequences Generated by 1-Term Recurrences

For our work in this section it is important to know the value of the sum of the terms of a finite geometric progression , that is, of the sum $a + ar + ar^2 + \cdots +$

ar^n, for any integer n. Since $a+ar+ar^2+\cdots+ar^n = a(1+r+\cdots+r^n)$, it is enough to know the value of the bracketed sum. Suppose $S = 1+r+\cdots+r^n$. Then $rS = r+r^2+\cdots+r^{n+1}$, so that $rS - S = r^{n+1}-1$. All other terms cancel. Therefore, factoring the left hand side, $S(r-1) = r^{n+1}-1$ so that $S = \frac{r^{n+1}-1}{r-1}$ if $r \neq 1$; if $r = 1$, then $S = n+1$ as each of the $n+1$ terms in the sum is a 1.

Let $a_1, a_2, \ldots$ be the sequence recursively defined by $a_1 = 2$ and $a_n = 7a_{n-1}+2$ for $n \geq 2$. We now demonstrate a method that will make it possible to guess (conjecture) a formula for a_n that valid for all $n \geq 1$. We will then prove our conjecture is correct using PMI.

If we compute directly, we get

$$\begin{aligned}
a_1 &= 2\\
a_2 &= 7a_1+2 = 16\\
a_3 &= 7a_2+2 = 114\\
a_4 &= 7a_3+2 = 800
\end{aligned}$$

Computing the exact values in this way does not help find a formula for the n-term of the sequence unless you happen to have amazing powers of observation. The best way to obtain formula is to write out the computation for the first few cases, but don't perform any additions or multiplications (except for collecting exponents with the same base), and then try to recognize what you have as something you know. *If there is a pattern, it is typically fairly apparent after working out enough cases that the calculation is routine and boring – typically that means working out about 4 cases.*

$$\begin{aligned}
a_1 &= 2\\
a_2 &= 7a_1+2 = 7\cdot 2+2\\
a_3 &= 7a_2+2 = 7(7\cdot 2+2)+2 = 7^2\cdot 2+7\cdot 2+2\\
a_4 &= 7a_3+2 = 7(7^2\cdot 2+7\cdot 2+2)+2 = 7^3\cdot 2+7^2\cdot 2+7\cdot 2+2\\
a_5 &= 7a_4+2 = 7(7^3\cdot 2+7^2\cdot 2+7\cdot 2+2)+2\\
&= 7^4\cdot 2+7^3\cdot 2+7^2\cdot 2+7\cdot 2+2
\end{aligned}$$

At this point it seems reasonable to conjecture that

$$a_n = 2(7^{n-1} + 7^{n-2} + \cdots + 1) = 2\frac{7^n - 1}{7 - 1} = \frac{7^n - 1}{3}$$

for all $n \geq 1$. We can prove the conjectured formula is correct using PMI. The statement to prove is $a_n = \frac{7^n - 1}{3}$ for all $n \geq 1$.

Basis. When $n = 1$ we have $a_1 = 2 = \frac{7^1 - 1}{3}$, as desired. Thus the statement is true when $n = 1$.

Induction Hypothesis. Suppose there is an integer $k \geq 1$ such that $a_k = \frac{7^k - 1}{3}$.

Induction Step. We want to show that $a_{k+1} = \frac{7^{(k+1)} - 1}{3}$.

Since $k+1 \geq 2$ we can use the recursion to write $a_{k+1} = 7a_k + 2 = 7(\frac{7^k - 1}{3}) + 2$, by the Induction Hypothesis. Hence $a_{k+1} = \frac{7^{k+1} - 7}{3} + \frac{6}{3} = \frac{7^{k+1} - 1}{3}$, as wanted.

Conclusion. Therefore, by PMI, $a_n = \frac{7^n - 1}{3}$ for all $n \geq 1$. □

Example 4.9.1 *Let $a_0, a_1, \ldots$ be the sequence recursively defined by $a_0 = 0$ and $a_n = a_{n-1} + 3n^2$ for $n \geq 1$. Find, with proof, a formula for a_n for all $n \geq 0$.*

Solution.

We first use computation without simplification to look for a pattern so we can conjecture a formula.

$$\begin{aligned}
a_0 &= 0 \\
a_1 &= a_0 + 3 \cdot 1^2 = 0 + 3 \cdot 1^2 \\
a_2 &= a_1 + 3 \cdot 2^2 = 0 + 3 \cdot 1^2 + 3 \cdot 2^2 \\
a_3 &= a_2 + 3 \cdot 3^2 = 0 + 3 \cdot 1^2 + 3 \cdot 2^2 + 3 \cdot 3^2 \\
a_4 &= a_3 + 3 \cdot 4^2 = 0 + 3 \cdot 1^2 + 3 \cdot 2^2 + 3 \cdot 3^2 + 3 \cdot 4^2
\end{aligned}$$

At this point is seems reasonable to conjecture that $a_n = 3(1^2 + 2^2 + \cdots + n^2)$ for all $n \geq 0$. The bracketed expression is a known sum, so our conjecture really is that $a_n = 3n(n+1)(2n+1)/6 = n(n+1)(2n+1)/2$ for all $n \geq 0$.

We now prove the conjecture by induction. The statement to prove is $a_n = n(n+1)(2n+1)/2$ for all $n \geq 0$.

Basis When $n = 0$ we have $a_n = a_0 = 0$ and $n(n+1)(2n+1)/2 = 0(1)(1)/2 = 0$. Thus the statement is true when $n = 0$.

Induction Hypothesis. Suppose there is an integer $k \geq 0$ such that $a_k = k(k+1)(2k+1)/2$.

Induction Step. We want to show that $a_{k+1} = (k+1)((k+1)+1)(2(k+1)+1)/2 = (k+1)(k+2)(2k+3)/2$. Look at a_{k+1}. Since $k+1 \geq 1$, we can use the recursion to write

$$\begin{aligned} a_{k+1} &= a_k + 3(k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{2} + 3(k+1)^2 \\ &= \frac{k(k+1)(2k+1)}{2} + \frac{6(k+1)^2}{2} \end{aligned}$$

where, in the last two steps, we used the Induction Hypothesis, then got a common denominator. Now,

$$\begin{aligned} \frac{k(k+1)(2k+1)}{2} + \frac{6(k+1)^2}{2} &= \frac{(k+1)[k(2k+1)+6(k+1)]}{2} \\ &= \frac{(k+1)[2k^2+7k+6]}{2} \\ &= \frac{(k+1)(k+2)(2k+3)}{2}, \end{aligned}$$

as wanted.

Conclusion. Therefore, by PMI, $a_n = n(n+1)(2n+1)/2$ for all $n \geq 0$. □

4.10 A subtraction game

Subtraction games are two-player games in which there is a pile of objects, say coins. There are two players, Alice and Bob, who alternate turns subtracting from the pile some number of coins belonging to a set S (the *subtraction set*). Alice goes first. The first player who is unable to make a legal move loses.

For example, suppose the initial pile contains 5 coins, and each player can, on his turn, remove any number of coins belonging to the set $S = \{1, 2, 3\}$.

Who wins? Alice goes first. On her turn she removes 1, 2, or 3 coins from the pile. If she removes 3, then the game reduces to a 2-coin game with Bob going first. Bob wins on his next move. Similarly, if she removes 2, then the game reduces to a 3-coin game with Bob going first, and Bob wins on his next move. But, if she removes 1, then the game reduces to a 4-coin game with Bob going first, and no matter what move Bob makes, Alice wins on her next move.

In any subtraction game, the winner can be determined if we know how many coins are in the pile, and which player is next to play. Suppose there are n coins in the pile. If the player next to play can take some coins and leave a position from which the opponent (who becomes the player next to play) has no winning strategy, then he can win. If he can not do this, then every legal move leaves a position from which the opponent has a winning strategy, and so the player whose turn it is can not win.

In the table below, we enter N if the player next to play has a winning strategy, and O if the opponent has a winning strategy. The discussion above says that the n-th entry is N whenever there is a legal move so that the entry in the corresponding position is O, and otherwise (the entry corresponding to every legal move is N) it is O.

For the game at hand, we can summarize the winner for each value of n in a table.

n	1	2	3	4	5	6	7	8	9	10	11	12
Who	N	N	N	O	N	N	N	O	N	N	N	O

In making the table (do it!), a pattern of who wins for which values of n becomes apparent.

Proposition 4.10.1 *In the subtraction game with $n \geq 1$ coins and $S = \{1, 2, 3\}$, if n is not a multiple of 4 then the next player to play has a winning strategy, and if n is a multiple of 4 then the opponent has a winning strategy.*

Proof.
Basis. If $n = 1, 2$ or 3, then the next player to play can win on their move by taking all of the coins. Thus the statement to be proved is true when $n = 1, 2$, or 3.

Induction hypothesis. Suppose that the statement to be proved is true when n is any of $1, 2, \ldots, k$, where $k \geq 3$. That is, in each of these situations, if the number of coins in the pile is not a multiple of 4, then the next player to play has a winning strategy, and if the number of coins in the pile is a multiple of 4 , then the opponent has a winning strategy.

Induction step. Suppose the pile has $n = k + 1$ coins. There are 2 cases to consider.

If $k+1$ is a multiple of 4, then any legal move leaves a pile in which the number of coins is not a multiple of 4. By the induction hypothesis, from each of these positions the next player to play has a winning strategy. Hence, in this case, the position in which there are $k + 1$ coins is such that the opponent has a winning strategy.

If $k + 1$ is is not a multiple of 4, then the next player can remove $1, 2$ or 3 coins, as needed, so that the number of coins remaining in the pile will be a multiple of 4. By the induction hypothesis, the opponent has no winning strategy from resulting position. Hence, in this case, the position in which there are $k + 1$ coins is such that the next player to play wins.

Conclusion. By the Principle of Mathematical Induction, for any $n \geq 1$, if n is not a multiple of 4 then the next player to play has a winning strategy, and if N is a multiple of 4 then the opponent has a winning strategy. □

Games with other subtraction sets can be analyzed similarly. It is a fact that the pattern of Os and Ns is eventually periodic; repeating pattern may not start for a while, depending on the size of the numbers in the subtraction set and the gaps between them.

4.11 Induction Analogies and Fallacies

Some people draw an analogy between PMI and climbing as high as you want on a really tall ladder, starting from rung n_0. The induction says that if there is $k \geq t$ such that you have climbed up the steps $n_0, n_0 + 1, \ldots, k$ then you can climb up to step $k + 1$. By itself, this does not matter much. You have to be able to get on the ladder and complete the steps $n + 0, n_0 + 1, \ldots, t$, otherwise you can't climb the ladder. Thus the Basis is of crucial importance in the argument.

Other people draw an analogy between PMI and toppling dominoes. Suppose you have an infinite line of dominoes that are arranged close together, but that dominoes $n_0, n_0 + 1, \ldots, t$ are exceptionally hard to topple. The induction says that if there is a $k \geq t$ such that you can make dominoes $n_0, n_0+1, \ldots, k$ fall over, then domino $k+1$ is guaranteed to fall over. Pushing over domino n_0 alone won't help if domino n_0+1 is so heavy that it won't fall over when struck by domino n_0. And pushing over the first few dominoes won't help if the the next domino is also hard to topple. The only thing to do is make sure you push over each of the dominoes $n_0, n_0 + 1, \ldots, t$. After you do that, you can conclude from your argument that all of the dominos will fall over.

A classical example of needing both the Basis and Induction is the fallacious argument that *in any group of $n \geq 1$ people, all people in the group have the same hair colour*. Certainly it is true that in any group of 1 people, all people in the group have the same hair colour. Suppose there is an integer $k \geq 1$ such that in any group of 1 to k people, all people in the group have the same hair colour. Now consider a group of $k + 1$ people. We want to use this Induction Hypothesis to argue that all people in this group have the same hair colour. Consider any member of the group. Call her Anna. By the Induction Hypothesis, all k members of the group who are not Anna have the same hair colour. Now consider any other member of the group. Call him Bill. By the Induction Hypothesis, all k members of the group who are not Bill have the same hair colour. But now Anna and Bill each have the same hair colour as all the remaining members of the group, and so all $k+1$ members of the group have the same hair colour. Therefore, by PMI, in any group of $n \geq 1$ people, all people in the group have the same hair colour.

Now, the statement "proved" in the previous paragraph is certainly not true, and so there must something wrong with the argument. In the Basis we checked only up to $n = 1$. (Had we checked up to $n = 2$, and been the least bit alert, there would have been trouble.) So this means the first application of the Induction Step is supposed to take us from the truth of the statement for all values of n from 1 up to 1, to the truth of the statement for all values of n from 1 up to 2. But the argument does not work as there are no group members besides Anna and Bill. In saying that they each have the same hair colour as all members the rest of the group we are assuming that there is at least one more person in the group. There isn't. Thus the argument given to establish the Induction Step is wrong, as it does not work when $k = 1$. A different way to view the problem with the argument is that the Induction Step is a valid argument only when $k \geq 2$, but no Basis supports the truth of the Induction Hypothesis in that case.

4.12 Exercises

1. Prove that any integer greater than or equal to 35 can be written as a sum of 5's and 6's.

2. Prove by induction that the number of binary sequences (sequences of 0s and 1s) of length n is 2^n, for any $n \geq 1$.

3. Prove by induction that, for any $n \geq 1$, the number of binary sequences of length n with an even number of ones equals the number of binary sequences of length n with an odd number of ones.

4. The binary sequences of length 1 can be listed so that consecutive sequences in the list, including the first and last, differ in exactly one place. One such list is $L_1 = 0, 1$. The binary sequences of length 2 can also be listed so that consecutive sequences in the list, including the first and last, differ in exactly one place. One such list is $L_2 = 00, 01, 11, 10$. The list L_2 is constructed from L_1 in several steps. First, let $0 \cdot L_1$ be the list constructed from L_1 by adding a 0 to the left end of every sequence in L_1, so that $0 \cdot L_1 = 00, 01$. The list $1 \cdot L_1$ is constructed similarly. Then L_2 consists of the sequence $0 \cdot L_1$ followed by the sequence $1 \cdot L_1$ in reverse order (say $L_2 = 0 \cdot L_1, \mathit{reverse}(1 \cdot L_1))$.

   (a) Show, by producing the list, that the binary sequences of length 3 can be listed so that consecutive sequences in the list, including the first and last, differ in exactly one place.

   (b) Prove that, for any $n \geq 1$, the binary sequences of length n can be listed so that consecutive sequences in the list, including the first and last, differ in exactly one place.

5. Prove by induction that if $n \geq 1$ distinct dice are rolled, then the number of outcomes where the sum of the faces is an even integer equals the number of outcomes where the sum of the faces is an odd integer.

6. Consider the sequence $a_0, a_1, a_2, \dots$ of integers defined by $a_0 = 10$ and $a_n = 2a_{n-1}$, $n \geq 1$. Prove that $a_n = 2^n 10$ for all $n \geq 0$.

7. Prove that $4^n - 1$ is a multiple of 3 for any $n \geq 0$. Hint: $4^{k+1} - 1 = 3 \cdot 4^k + (4^k - 1)$. (Note that $4^n - 1$ is the numbers of squares in the punctured grid from the example at the start of the chapter.)

8. Let f_n denote the n-th Fibonacci number. Prove that for all $n \geq 6$, $f_n \geq (3/2)^{n-1}$.

9. Prove that every fifth Fibonnacci number is a multiple of 5.

10. Let f_n denote the n-th Fibonacci number. Prove that $f_1 + f_2 + \cdots f_n = f_{n+2} - 1$ for all $n \geq 1$.

11. Let $b_0, b_1, \dots$ be the sequence recursively defined by $b_0 = 1, b_1 = 4$ and $b_n = 8b_{n-1} - 16b_{n-2}$ for $n \geq 2$. Prove that $b_n = 4^n$ for all $n \geq 0$.

12. Let $t_0, t_1, \dots$ be the sequence recursively defined by $t_0 = 1, t_1 = -4$ and $t_n = -4t_{n-1} - 4t_{n-2}$ for $n \geq 2$. Prove that $t_n = (-2)^n + n(-2)^n$ for all $n \geq 0$.

13. Let $s_0, s_1, \dots$ be the sequence recursively defined by $s_0 = 1, s_1 = 6$ and $s_n = 5s_{n-1} - 6s_{n-2}$ for $n \geq 2$. Prove that $s_n = 4 \cdot 3^n - 3 \cdot 2^n$ for all $n \geq 0$.

14. Find, with proof, the least integer n_0 such that $n! > 3 \cdot 2^n$ for all $n \geq n_0$.

15. Find, with proof, the least integer n_0 such that $5^n > (n+1)^3$ for all $n \geq n_0$.

16. Guess and prove a formula for $1 - 2 + 3 - 4 + \cdots + (-1)^{n-1}n$ (i.e., one that works for any $n \geq 1$; there will be different expressions for the cases n even and n odd).

17. Prove that for all $n \geq 1$, $1(2) + 2(3) + 3(4) + \cdots + n(n+1) = n(n+1)(n+2)/3$.

18. Prove that for all $n \geq 1$, $1^3 + 2^3 + 3^3 + \cdots + n^3 = n^2(n+1)^2/4$.

19. Suppose $r \neq 1$. Use induction to prove that $1 + r + r^2 + \cdots + r^n = \frac{r^{n+1}-1}{r-1}$, for all $n \geq 0$.

20. Prove that for all $n \geq 1$, $\frac{1}{1(2)} + \frac{1}{2(3)} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.

21. Prove that for all $n \geq 1$, $1(1!) + 2(2!) + \cdots + n(n!) = (n+1)! - 1$.

22. Prove by induction that for any integer $n \geq 1$, $n^3 + (n+1)^3 + (n+2)^3$ is a multiple of 9.

23. Let $a_0, a_1, \ldots$ be the sequence recursively defined by $a_0 = 3$ and $a_n = 2a_{n-1} + 3$ for $n \geq 1$. Find a formula for a_n and prove it is correct by induction.

24. Let $a_0, a_1, \ldots$ be the sequence recursively defined by $a_0 = 2$ and $a_n = a_{n-1} + 2(n-1)$ for $n \geq 1$. Find a formula for a_n and prove it is correct by induction.

25. Consider the subtraction game with $S = \{1, 2\}$. A pile of coins is places on a table. There are two players, Alice and Bob, who alternate moves. Alice moves first. A legal move consists of removing one or two coins from the pile. The player who takes the last coin wins. Prove that Alice has a winning strategy if the number of coins in the pile is not a multiple of 3, and Bob has a winning strategy of the number of coins in the pile is a multiple of 3.

Chapter 5

Number Theory

The material in this chapter offers a small glimpse of why a lot of facts that you've probably known and used for a long time are true. It also offers some exposure to generalization, that is, of taking some specific examples that are true and finding a general statement that includes these as specific cases.

5.1 Floors and Ceilings

For $x \in \mathbb{R}$, the *floor* of x is the largest integer that is less than or equal to x, and is denoted by $\lfloor x \rfloor$. If x is an integer, then $\lfloor x \rfloor = x$, and otherwise it is the nearest integer to the left of x on the number line.

Correspondingly, for $x \in \mathbb{R}$, the *ceiling* of x is the smallest integer that is greater than or equal to x, and is denoted by $\lceil x \rceil$. If x is an integer, then $\lceil x \rceil = x$, and otherwise it is the nearest integer to the right of x on the number line.

Proposition 5.1.1 *Let x be a real number. Then*

- $x - 1 < \lfloor x \rfloor \leq x$*; and*
- $x \leq \lceil x \rceil < x + 1$.

Proof. We prove the first statement. The proof of the second statement is similar. By definition, $\lfloor x \rfloor \leq x$. If x is an integer, then $\lfloor x \rfloor = x$, so

$x - 1 < \lfloor x \rfloor \leq x$. If x is not an integer, then there is an integer n so that x belongs to the open interval $(n, n{+}1)$. In this case $x < n{+}1$. Rearranging this inequality and using the definition of the floor of x gives $x - 1 < n = \lfloor x \rfloor \leq x$. □

This section concludes with an example of proving a statement about the ceiling operation.

Proposition 5.1.2 *Let $x, y \in \mathbb{R}$. Then*

$$\lceil x \rceil + \lceil y \rceil \geq \lceil x + y \rceil.$$

Proof. Since $\lceil x \rceil \geq x$ and $\lceil y \rceil \geq y$, addition of inequalities gives $\lceil x \rceil + \lceil y \rceil \geq x + y$. Thus, $\lceil x \rceil + \lceil y \rceil$ is an integer that is greater than or equal to $x + y$. By definition $\lceil x + y \rceil$ is the *smallest* integer that is greater than or equal to $x + y$. Consequently, $\lceil x + y \rceil \leq \lceil x \rceil + \lceil y \rceil$. □

5.2 The Division Algorithm

Something everyone learns in elementary school is that when one integer is divided by another there is a unique quotient and a unique remainder. For example, when 65 is divided by 17 the quotient is 3 and the remainder is 14. That is, $65 = 3 \times 17 + 14$. What about when 65 is divided by -17? We have $65 = (-3) \times (-17) + 14$, and we also have $65 = (-4) \times (-17) - 3$. Should the remainder be 14 or -3? The convention is that *the remainder is always non-negative* when dividing by a negative number.

The fact that there is a unique quotient and a unique remainder is a theorem. It bears the name “The Division Algorithm” because the proof tells you how to find the quotient and the remainder when an integer a is divided by an integer b – keep subtracting multiples of b from a until what's left is a number r between 0 and $|b| - 1$ (inclusive). The total number of times b was subtracted from a is the quotient, and the number r is the remainder. That is, $a = bq + r,\ 0 \leq r < |b|$.

Theorem 5.2.1 The Division Algorithm *Let $a, b \in \mathbb{Z}$, with $b \neq 0$. Then there exist unique integers q and r so that $a = bq + r$ and $0 \leq r < |b|$.*

The integers q and r in The Division Algorithm are the *quotient* and *remainder* when a is divided by b, respectively. The integer b is the *divisor*, and (for completeness we will note that) the integer a is the *dividend*.

Instead of proving the Division Algorithm, we illustrate the proof with the example below below where 2024 is divided by 75. First, ten 75s are subtracted, leaving 1274. Then, ten more 75s are subtracted, leaving 524. From this number five 75s are subtracted, leaving 149. And finally, one 75 is subtracted leaving 74 (the remainder). The quotient is the total number of 75s subtracted, which is 26. Thus $2024 = 26 \times 75 + 74$.

$$\begin{array}{rr|r}
75\;) & \overline{2024} & 10 \\
 & -750 & \\ \cline{2-2}
 & 1274 & 10 \\
 & -750 & \\ \cline{2-2}
 & 524 & 5 \\
 & -375 & \\ \cline{2-2}
 & 149 & 1 \\
 & -75 & \\ \cline{2-3}
 & 74 & 26
\end{array}$$

Suppose, for the moment, that a and b are both positive. The quotient when a is divided by b is the largest integer q such that $bq < a$. This is the floor of a/b: if $a = bq+r$ with $0 \le r < b$ then $\lfloor a/b \rfloor = \lfloor (bq+r)/b \rfloor = \lfloor q+(r/b) \rfloor = q$. The same thing happens when a is negative (notice that the quotient is a negative number).

Now suppose a is positive and b is negative. Again, the quotient when a is divided by b is the largest integer q such that $bq < a$. (Such a q is negative!) This is the ceiling of a/b: if $a = bq + r$ with $0 \le r < |b|$ then $\lceil a/b \rceil = \lceil (bq + r)/b \rceil = \lceil q + (r/b) \rceil = q$, where the last equality follows because b is negative and so r/b is in the interval $(-1, 0]$. The same thing happens when a is negative.

We state the observations just made formally, and also indicate a different proof.

Proposition 5.2.2 *Let $a, b \in \mathbb{Z}$, with $b \neq 0$. If q and r are integers such* *that* $a = bq + r,\ 0 \leq r < |b|$, *then*

$$q = \begin{cases} \lfloor a/b \rfloor & \text{if } b > 0, \text{ and} \\ \lceil a/b \rceil & \text{if } b < 0. \end{cases}$$

Proof. We give the proof when $b > 0$. The proof when $b < 0$ is similar. By Proposition 5.1.1, $(a/b) - 1 < \lfloor a/b \rfloor \leq a/b$. Multiplying through by the positive number b and simplifying gives $a - b < b\lfloor a/b \rfloor \leq a$. Let $r = a - b\lfloor a/b \rfloor$. Then $a = b\lfloor a/b \rfloor + r$. Rearranging the right hand inequality gives, $0 \leq a - b\lfloor a/b \rfloor = r$. Rearranging the left hand inequality gives $r = a - b\lfloor a/b \rfloor < b$. Therefore, by The Division Algorithm, r is the remainder when a is divided by b, and $\lfloor a/b \rfloor$ is the quotient. □

5.3 Representing Numbers in Base b

When we use the symbol 5374 to represent the integer five thousand, three hundred and seventy four, we understand the notation to mean $5 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 4 \times 10^0$. Every place in the notation has a value that is a power of ten, the *base* of the system. The number 5 is in the *thousands place*, 3 is in the *hundreds place*, 7 is in the *tens place* and 4 is in the *ones place.* (Aside: if there were a decimal point, then the places to the right of it would be the *tenths, hundredths*, and so on because $1/10 = 10^{-1}$, $1/100 = 10^{-2}$, etc.) If the *digits* $0, 1, \ldots 9$ are used in the various places, then every integer can be uniquely represented (in base 10). It turns out that there is nothing special about 10, any integer $b > 1$ can be used in its place, as can integers $b < -1$, though we will not consider this case.

Let $b > 1$ be an integer. A *base b digit* is one of the numbers $0, 1, \ldots, b - 1$. If $d_k, d_{k-1}, \ldots, d_0$ are all base b digits, then the notation $(d_k d_{k-1} \ldots d_1 d_0)_b$ is shorthand for $d_k \times b^k + d_{k-1} \times b^{k-1} + \cdots + d_1 \times b^1 + d_0 \times b^0$. Notice that every place in the notation has a value that is a power of the base: the value of the i-place from the right is b^{i-1} (the value of the rightmost place is $b^0 = 1$).

For an integer $n \geq 0$, if $n = d_k \times b^k + d_{k-1} \times b^{k-1} + \cdots + d_1 \times b^1 + d_0 \times b^0$ and $d_k \neq 0$, then $(d_k d_{k-1} \ldots d_1 d_0)_b$ is called the *base b representation of n.* By analogy with what happens in base 10, if $n \geq 0$ then the base b representation of $-n$ is $-(d_k d_{k-1} \ldots d_1 d_0)_b$.

For example, $(234)_5$ is the base 5 representation of the integer $2 \times 5^2 + 3 \times 5 + 4 = 69$ (in base 10).

Every integer has a unique base b representation. We illustrate the proof that a representation exists with an example.

Example 5.3.1 *Find the base 5 representation of 69.*

Solution. We need to find base 5 digits $d_0, d_1, \ldots$ so that

$$69 = d_k \times 5^k + d_{k-1} \times 5^{k-1} + \cdots + d_1 \times 5^1 + d_0 \times 5^0.$$

Rearranging the right hand expression gives

$$69 = (d_k \times 5^{k-1} + d_{k-1} \times 5^{k-2} + \cdots + d_1) \times 5 + d_0$$

so that the ones digit, d_0 is the remainder when 69 is divided by 5, that is, 4. Furthermore, the quotient is the number $(69 - 4)/5 = 13$, which equals

$$d_k \times 5^{k-1} + d_{k-1} \times 5^{k-2} + \cdots + d_1$$

and hence has base 5 representation $(d_k d_{k-1} \ldots d_1)_5$. (Notice the absence of d_0 in this representation.) Repeating what was just done, the ones digit of this number, that is d_1, is the remainder on dividing the 13 by 5. Hence $d_1 = 3$ and, continuing in this way (induction!), d_2 is the remainder on dividing the new quotient of $(13-3)/5 = 2$ by 5 (so $d_2 = 2$). Repeating again gives $d_j = 0$ for all $j > 2$. Hence $69 = (234)_5$, as above.

Why is the representation unique? Because of The Division Algorithm. It says that the quotient and remainder are unique. Since the base 5 digits are remainders on dividing a uniquely determined number by 5, there can be only one representation.

The argument given above generalizes to give the proof of the following theorem.

Theorem 5.3.2 *If $b > 1$, then every integer n has a unique base b representation.*

Proof. Since $0 = (0)_b$, and $-n$ has a representation if and only if n has a representation – it is the negative of the representation of n – it suffices to prove the statement when $n \geq 1$. Use The Division Algorithm to define the numbers $q_0, d_0, q_1, d_1, \ldots$ as follows:

$$\begin{array}{rcll} n & = & b \times q_0 + d_0 & 0 \leq d_0 < b \\ q_0 & = & b \times q_1 + d_1 & 0 \leq d_1 < b \\ q_1 & = & b \times q_2 + d_2 & 0 \leq d_2 < b \\ \vdots & \vdots & \vdots & \vdots \end{array}$$

We claim that this process terminates, that is, eventually some quotient $q_k = 0$, and then $q_j = d_j = 0$ for all $j > k$. To see this, notice that $b > 1$ and $n > 0$ implies $n/b < n$, so $0 \leq q_0 = \lfloor n/b \rfloor < n$. If $q_1 > 0$ then the same argument applies to give $n > q_0 > q_1 \geq 0$, and so on. The process must reach zero in at most n steps, which proves the claim.

Now, each number d_i is a base b digit, and

$$\begin{array}{rcllcl} n & = & q_0 \times b + d_0 & & & \\ & = & (q_1 \times b + d_1) \times b + d_0 & & = & q_1 \times b^2 + d_1 \times b + d_0 \\ & = & (q_2 \times b + d_2) \times b^2 + d_1 \times b + d_0 & & = & q_2 \times b^3 + d_2 \times b^2 + d_1 \times b + d_0 \\ & \vdots & & & & \\ & = & d_k \times b^k + d_{k-1} \times b^{k-1} + \cdots + d_0 & & & \end{array}$$

Hence $n = (d_k d_{k-1} \ldots d_1 d_0)_b$.

Uniqueness of the representation follows from The Division Algorithm. The digit d_0 is the remainder when n is divided by b, and is uniquely determined. The digit d_1 is the remainder when the integer $(n - d_0)/b$ is divided by b, and is uniquely determined. Continuing in this way, the entire base b representation is uniquely determined. □

The proof of Theorem 5.3.2 tells us how to find the base b representation of a natural number n.

- *The ones digit is the remainder when n is divided by b.*
- *When the quotient resulting from the previous division is divided by b, the remainder is the next digit to the left.*
- *The process stops when the quotient and remainders from a division by b are 0.*

If the base is bigger than 10, then we need to use other symbols to represent the digits. For example, in *hexadecimal* (base 16), the letters A, B, C, D, E, and F stand for 10 through 15, respectively. The hexadecimal number $(A3F)_{16} = 10 \times 16^2 + 3 \times 16 + 15$.

To convert between bases, say to convert $(A3F)_{16}$ to binary (base 2), one could first convert it to base 10 using the meaning of the notation, and then to base 2 as above. However, the fact that $2^4 = 16$ offers a shortcut. We know $(A3F)_{16} = 10 \times 16^2 + 3 \times 16 + 15 = 10 \times 2^8 + 3 \times 2^4 + 15$. Now replace each multiplier by its base 2 representation, inserting leading zeros if needed to get 4 binary digits, to get $(A3F)_{16} = (1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 0) \times 2^8 + (0 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 1) \times 2^4 + (1 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1)$. Multiplying everything out gives the binary representation: $(A3F)_{16} = (101000111111)_2$. The representation on the right is obtained by *replacing each hexadecimal digit by its representation as a 4-digit binary number (possibly having leading zeros).*

One can similarly use the fact that $2^4 = 16$ to convert from binary to hexadecimal. Consider the number:

$$\begin{aligned}
&(1010111101)_2\\
&= 1 \cdot 2^9 + 0 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1\\
&= (1 \cdot 2^1 + 0) \cdot 2^8 + (1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1) \cdot 2^4 + (1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1)\\
&= 2 \cdot 2^8 + 11 \cdot 2^4 + 13\\
&= 2 \cdot 16^2 + 11 \cdot 16 + 13\\
&= (2BD)_{16}.
\end{aligned}$$

This is the number obtained by adding leading zeros so the number of binary digits is a multiple of 4 and then *starting at the right and replacing each sequence of 4 binary digits by its hexadecimal equivalent.* (We use 4 digits at a time because $16 = 2^4$.)

The same sort of argument applies to convert between any two bases b and b^t, for example between binary and octal (base 8).

5.4 The number of digits

How many digits are there in the base 10 representation of $n \in \mathbb{N}$? Numbers from 1 to 9 have one digit, numbers from 10 to 99 have 2 digits, numbers from 100 to 999 have three digits, and so on.

The number of digits in the base 10 representation of n is one greater than in the base ten representation of $n-1$ whenever n is a power of 10. That is, the smallest base ten number with $k+1$ digits is 10^k, and the largest base 10 number with k digits is $10^k - 1$. Thus, *if* $10^{k-1} \leq n < 10^k$*, then the base 10 representation of* n *has* k *digits.*

For every n such that $10^{k-1} \leq n < 10^k$ we have $k-1 \leq \log_{10}(n) < k$. The number of digits in the base 10 representation of n equals k, and $\lfloor \log_{10}(n) \rfloor = k-1$. Thus $k = \lfloor \log_{10}(n) \rfloor + 1$.

There is nothing special about 10 in this discussion. *In any base* $b > 1$*, if* $b^{k-1} \leq n < b^k$*, then the base* b *representation of* n *has* k *digits.* It follows as above that k (the number of digits in the base b representation of n) equals $\lfloor \log_b(n) \rfloor + 1$ (recall that $\log_b(n) = x \Leftrightarrow b^x = n$).

As an aside, we note that logarithms to different bases differ only by multiplication by a constant. To see that, start with the fact that, for $a, b > 0$ and real number x we have $a^{\log_a(x)} = x = b^{\log_b(x)}$. Therefore, since the function a^y and $\log_a(z)$ are inverses, $\log_a(x) = \log_a(a^{\log_a(x)}) = \log_a(b^{\log_b(x)}) = \log_b(x)\log_a(b)$. Since $\log_a(b)$ is a constant that is does not depend on x, we have that, for any x, $\log_b(x)$ is a constant multiple of $\log_a(x)$. The same statement is true with a and b reversed: either repeat the calculation with a and b exchanged, or just divide through by the non-zero number $\log_a(b)$.

5.5 Divisibility

If a and b are integers, we say that a *divides* b, and write $a|b$, if there is an integer k such that $ak = b$.

When the statement $a|b$ is true, we also say:

- a *is a divisor of* b,
- b *is divisible by* a, or
- b *is a multiple of* a.

Equivalently, if $a \neq 0$, then a divides b when the remainder when b is divided by a equals 0. Thus b is a times some other integer. There is no discussion of fractions here (and there will not be one) even though it is true that if a and b are non-zero integers and a divides b then b/a is an integer. *It is important to recognize $a|b$ is not a number, it is a statement that's either true or false.*

According to the definition,

- $5|30$ because $5 \times 6 = 30$,
- $(-7)|28$ because $(-7) \times (-4) = 28$,
- $10|(-100)$ because $10 \times (-10) = -100$ and
- $(-4)|(-12)$ because $(-4) \times 3 = 12$.

Example 5.5.1 *Which numbers divide zero?*

Solution.
If a is any integer, then $a \times 0 = 0$ so $a|0$. In particular, $0|0$.

Question 5.5.2 *Explain why 0 is the only number that's divisible by 0.*

It is clear from the definition that, for any integer b, we have $1|b$ (because $1 \times b = b$), and also $b|b$ (because $b \times 1 = b$).

Divisibility is defined in terms of the existential quantifier "there exists" (the definition requires that *there exists k such that* ...), so proofs of divisibility involve demonstrating how such an integer k can be found. This is what was happening in the previous paragraph, and also what will happen in the proofs of the propositions below.

We know, for example, that $6|12$ (because $6 \times 2 = 12$). Hence any multiple of 12, say $12k$, is also a multiple of 6 because $12k = 6 \times (2k)$. There is nothing special about the numbers 6 and 12. The same factoring argument works when 6 and 12 are replaced by any two numbers a and b such that $a|b$.

Proposition 5.5.3 *Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$, then $a|c$.*

Proof. Suppose $a|b$ and $b|c$. We want to find an integer k so that $ak = c$. Since $a|b$, there is an integer m so that $am = b$. Since $b|c$, there is an integer n so that $bn = c$. Therefore, $c = bn = amn = a(mn)$. Since $mn \in \mathbb{Z}$, we have that $a|c$. □

In a manner similar to what's above, we know that since $6|12$ and $6|18$, then for any integers x and y we have $6|12x+18y = 6\times(2x)+6\times 3y = 6\times(2x+3y)$. As before, this factoring argument works whenever 6, 12 and 18 are replaced by numbers a, b and c such that $a|b$ and $a|c$.

Proposition 5.5.4 *Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|bx + cy$ for any integers x and y.*

Proof. Suppose $a|b$ and $a|c$. Let $x, y \in \mathbb{Z}$. We want to find an integer k so that $ak = bx+cy$. Since $a|b$, there is an integer m so that $am = b$. Since $a|c$, there is an integer n so that $an = c$. Therefore, $bx+cy = amx+any = a(mx+ny)$. Since $mx + ny \in \mathbb{Z}$, we have that $a|bx + cy$. □

By taking $y = 0$ in the proposition above, we obtain the result that if a divides b, then it divides any integer multiple of b.

The previous proposition can be generalized so that $bx + cy$ is replaced by a sum involving more than two terms, each of which has a factor divisible by a.

What could we say about the integers a and b if we have both $a|b$ and $b|a$? Let's look at an example. Take $b = 6$. If $a|6$, then a is one of the numbers $\pm1, \pm2, \pm3, \pm6$. The only numbers in this collection that are also divisible by 6 are -6 and 6. After checking out a couple more examples, one is led to the next proposition.

Proposition 5.5.5 *Let $a, b \in \mathbb{Z}$. If $a|b$ and $b|a$, then $a = \pm b$.*

Proof. Since $a|b$, there is an integer m so that $am = b$. Since $b|a$, there is an integer n so that $bn = a$. Therefore, $a = bn = amn$, so that $a = 0$ or $mn = 1$.

If $a = 0$, then since $a|b$ it follows that $b = 0$.

If $mn = 1$, then since m and n are integers, either $m = n = 1$ or $m = n = -1$. If $n = 1$ then $a = b$ and if $n = -1$ then $a = -b$. □

5.6 Prime numbers and unique factorization

An integer $p > 1$ is called *prime* if its only positive divisors are 1 and itself. An integer $n > 1$ which is not prime is called *composite*.

That is, an integer n is composite if there are integers a and b with $1 < a \leq b < n$ such that $n = ab$.

The integer 1 is neither prime nor composite. It is just a unit. The Greeks thought of numbers as lengths. Every length $n \geq 1$ is made up of n unit lengths. A length was regarded as prime if it was not a multiple of some length other than the unit, and composite if it was.

The following theorem asserts two things: *existence*, i.e., that every integer can be written as a product of primes, and *uniqueness*, i.e., that there is only one such product up to rearranging its factors.

Theorem 5.6.1 (Fundamental Theorem of Arithmetic). *Every integer $n > 1$ can be written as a product of primes in exactly one way, up to the order of the factors.*

Proof (of existence of the factorization). The proof is by induction on n. Both 2 and 3 can be written as a product of primes (the product has only one term). Hence the statement is true when $n = 2$ and when $n = 3$. Suppose there is an integer k such that each of $2, 3, \ldots, k$ can be written as a product of primes. We now want to argue that $k + 1$ can be written as a product of primes. There are two cases. If $k + 1$ is prime, then it can be written as a product of primes (containing one factor), as wanted. If $k + 1$ is composite, then there are integers a, b such that $1 < a < k + 1,\ 1 < b < k + 1$ and $k + 1 = ab$. By the induction hypothesis, a can be written as a product of primes, say $a = p_1p_2 \cdots p_r$, and b can be written as a product of primes, say $b = q_1q_2 \cdots q_s$. Then $ab = p_1p_2 \cdots p_rq_1q_2 \cdots q_s$, a product of primes, as wanted. Therefore, by induction, every integer $n > 1$ can be written as a product of primes. □

The proof of uniqueness of the factorization requires some results from later in the chapter.

The Fundamental Theorem of Arithmetic is also known as the Unique Factorization Theorem. It implies that every integer $n > 1$ has exactly one *prime factorization* (or *prime power decomposition*) as $n = p_1^{e_1}p_2^{e_2} \ldots p_k^{e_k}$, where $p_1 < p_2 < \cdots < p_k$ are different primes and $e_i \geq 1,\ 1 \leq i \leq k$.

The Fundamental Theorem of Arithmetic has some very basic consequences that one does not realize until thinking about them – that's why it is the "fundamental" theorem. Here are some examples.

Example 5.6.2 *Every integer $n > 1$ has a prime divisor (which could be itself).*

Proof.

By the Fundamental Theorem of Arithmetic, we can write $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$, where $p_1 < p_2 < \cdots < p_k$ are different primes and $e_i \geq 1,\ 1 \leq i \leq k$. Then $p_1 \times p_1^{e_1-1}p_2^{e_2}\dots p_k^{e_k}$ and the term on the right hand side is at least one, so the prime $p_1|n$. (If $p_1^{e_1-1}p_2^{e_2}\dots p_k^{e_k} = 1$, that is, if $k = 1$ and $e_1 = 1$, then $n = p_1$ is prime.) □

Example 5.6.3 *Show that if p is prime and $p|a^2$, then $p|a$.*

Proof.

The prime factorization of a^2 has the same primes as the prime factorization of a – the exponents are doubled. Hence, in fact, $p^2|a^2$. □

Example 5.6.4 *Suppose $ak = b$. Explain why the two numbers ak and b have exactly the same prime factorization.*

Solution. *By definition of equality, the expressions ak and b equal the same number. Thus, by the Fundamental Theorem of Arithmetic, ak and b have the same prime factorization. Therefore, if the prime p appears to the power e in the prime factorization of b, then p must appear a total of exactly e times in the prime factorizations of a and k.*

Example 5.6.5 *Suppose n has the prime factorization $p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$. Prove that the divisors of n are the numbers $p_1^{d_1}p_2^{d_2}\dots p_k^{d_k}$ where $0 \leq d_i \leq e_i$.*

Proof. *Suppose $d|n$. Then there is an integer ℓ such that $d\ell = n$. By Example 5.6.4 the numbers $d\ell$ and n have exactly the same prime factorization. Therefore the prime factorization of $d\ell$ is $p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$. It follows that $d = p_1^{d_1}p_2^{d_2}\dots p_k^{d_k}$ where $0 \leq d_i \leq e_i$ (some exponents may be 0 as perhaps some prime factors of n are not prime factors of d.).* □

5.7 Using the FTA in Proofs of Irrationality

The Fundamental Theorem of Arithmetic can be used in proofs of irrationality. For example, let's show that $\log_{10}(7)$ *is irrational.* The proof is by contradiction. Suppose there are integers a and b such that $\log_{10}(7) = a/b$. Then $10^{a/b} = 7$ or $10^a = 7^b$, contrary to the Fundamental Theorem of Arithmetic (a number can not be factored as $2^a 5^a$ and also as 7^b). As a second example, we generalize our previous result that $\sqrt{2}$ is irrational by characterizing the non-negative integers n such that $\sqrt{n}$ is irrational. We first prove the useful lemma that if two numbers have a common divisor greater than one, then they have a common prime divisor.

Lemma 5.7.1 *Let $a, b \in \mathbb{Z}$. If there is a positive integer $d > 1$ such that $d|a$ and $d|b$, then there is a prime number p such that $p|a$ and $p|b$.*

Proof. Suppose there is a positive integer $d > 1$ such that $d|a$ and $d|b$. If d is prime, then there is nothing to prove. Suppose, then, that d is not prime. Then, by the result of Example 5.6.2, there is a prime number p such that $p|d$. It follows from Proposition 5.5.3 that $p|a$ and $p|b$. □

In Section 2.4 we showed that $\sqrt{2}$ is irrational, and in the exercises for that chapter we showed that $\sqrt{5}$ is irrational. With enough patience and persistence, essentially the same argument can be used to prove that $\sqrt{p}$ is irrational for any prime p, and much more. The Fundamental Theorem of Arithmetic makes it possible to determine exactly when the square root of an integer is irational.

Theorem 5.7.2 *Let $n \geq 0$ be an integer. Then $\sqrt{n}$ is irrational unless n is the square of an integer.*

Proof. We show that if $\sqrt{n}$ is rational, then n is the square of an integer. Suppose there are integers a and b so that $\sqrt{n} = a/b$. Since $n \geq 0$ we may assume that $a \geq 0$ and $b \geq 1$. Further, we may take the fraction a/b to be in lowest terms, so that a and b have no common prime factor.

Squaring both sides gives $n = a^2/b^2$, so that $nb^2 = a^2$. If $b > 1$ then it has a prime divisor, say p. Then $p|b^2$, so p must be a divisor of a^2 and hence of a. But a and b have no common prime factors. Therefore $b = 1$ and $n = a^2$, the square of an integer. □

5.8 There are Infinitely Many Primes

The Greeks knew that there were infinitely many prime numbers. There is a remarkable proof in Euclid's *Elements*, published about 320BC. There is a temptation to think of this book only as a classic treatise on geometry (which it is). But, it also contains some very nice results in number theory. Euclid's argument uses proof by contradiction to show that there are more than n primes for any integer n; hence there are infinitely many primes.

Theorem 5.8.1 (Euclid, 320BC) *There are infinitely many prime numbers.*

Proof. Suppose not, and let $p_1, p_2, \ldots, p_n$ be the collection of all prime numbers. Consider the number $N = p_1 p_2 \ldots p_n + 1$. The number N has a prime divisor (possibly itself). But none of $p_1, p_2, \ldots, p_n$ divide N: each leaves a remainder of 1 when divided into N. Therefore there is a prime number not in the collection, a contradiction. □

While it is tempting to thing that the number N in Euclid's proof is prime, this is not always true. The number $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1$ is composite: it is divisible by 59.

5.9 The Sieve of Eratosthenes

The *Sieve of Eratosthenes* is a method for generating all of the prime numbers less than or equal to n.

1. Write the numbers $2, 3, 4, \ldots, n$ in a line. Circle the number 2.

2. Cross out all multiples of the number just circled. Circle the first number in the list which is neither circled nor crossed out. If the number just circled is less than $\sqrt{n}$, repeat this step using the newly circled number.

3. If the number just circled is greater than $\sqrt{n}$, then circle all remaining numbers that are neither already circled nor crossed out.

4. The set of circled numbers is the set of primes less than or equal to n.

So why does this work? The first number to be circled is prime, and each subsequent number circled in step 2 is not a multiple of a smaller prime, hence it must be prime. It remains to explain why the process can be "short circuited" after a number greater than $\sqrt{n}$ has been circled. That's because of the proposition below.

Proposition 5.9.1 *If $n > 1$ is composite, then it has a prime divisor p such that $2 \leq p \leq \sqrt{n}$.*

Proof. Suppose $n > 1$ is composite. Then there are integers a and b such that $1 < a \leq b < n$ and $n = ab$. If both a and b are greater than $\sqrt{n}$, then $n = ab > \sqrt{n}\sqrt{n} = n$, a contradiction. Thus $a \leq \sqrt{n}$. Any prime divisor of a is both less than or equal to a (and hence $\sqrt{n}$) and a divisor of n (because $p|a$ and $a|n$). Thus n has a prime divisor p such that $2 \leq p \leq \sqrt{n}$. □

5.10 The *gcd*

If a and b are integers which are not both zero, the *greatest common divisor* of a and b is the largest integer d such that $d|a$ and $d|b$. It is denoted by $gcd(a, b)$.

A number that divides both a and b is a *common divisor of a and b*. The number $gcd(a, b)$ is the greatest number in this collection. Since 1 is always a common divisor of a and b, the collection isn't empty and $gcd(a, b) \geq 1$.

Why is there a greatest number in the collection of common divisors of a and b? Since the numbers are not both zero, one of them is largest in absolute value, say b. No divisor of b can be greater that $|b|$, hence no common divisor of a and b can be larger than $|b|$. So $gcd(a, b)$ is the largest integer d with $1 \leq d \leq |b|$ that divides both a and b.

Why is there the restriction that a and b can not both be zero? Any number n is a divisor of zero (because $n \times 0 = 0$). Hence any integer n is a common divisor of 0 and 0, and there is no greatest such integer.

Since a number and its negative have the same divisors, $gcd(a, b) = gcd(|a|, |b|)$. For this reason it is common to let a and b be non-negative numbers when computing $gcd(a, b)$.

Proposition 5.10.1

1. *If a is a positive integer, then* $\gcd(a, 0) = a$.
2. *If a is any integer, then* $\gcd(a, 1) = 1$.

Proof. The first statement is true because a divides 0. The second statement is true because 1 is the only positive divisor of 1. □

If $a > 1$ and $b > 1$, then $gcd(a, b)$ can be found using the prime factorizations of a and b. Before proving this is possible, we do an example that illustrates the proof.

Example 5.10.2 *Suppose $a = 2^3 5^4 11^1$ and $b = 2^2 7^8 11^4$. Find $gcd(a, b)$.*

Solution.

First, rewrite these in modified form so that the same primes appear in each decomposition. To do this, we need to allow exponents to be zero. Written in this modified form, $a = 2^3 5^4 7^0 11^1$ and $b = 2^2 5^0 7^8 11^4$.

The positive divisors of a are the numbers $2^a 5^b 7^c 11^d$ with $0 \le a \le 3$, $0 \le b \le 4$, $0 \le c \le 0$, $0 \le d \le 1$.

The positive divisors of b are the numbers $2^a 5^b 7^c 11^d$ with $0 \le a \le 2$, $0 \le b \le 0$, $0 \le c \le 8$, $0 \le d \le 4$.

Hence the positive common divisors of a and b are the numbers $2^a 5^b 7^c 11^d$ with $0 \le a \le \min\{3, 2\}$, $0 \le b \le \min\{4, 0\}$, $0 \le c \le \min\{0, 8\}$, $0 \le d \le \min\{1, 4\}$.

The largest number in this collection is $2^2 5^0 7^0 11^1$, so it must be the gcd.

Theorem 5.10.3 *If $a = p_1^{e_1} p_2^{e_2} \cdots\ p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots\ p_k^{f_k}$, where $e_i \ge 0$ and $f_i \ge 0$ for $i = 1, 2, \ldots, k$, then*

$$gcd(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots\ p_k^{\min\{e_k, f_k\}}.$$

Proof. The positive divisors of a are the numbers $p_1^{d_1} p_2^{d_2} \cdots\ p_k^{d_k}$ where $0 \le d_i \le e_i$ for $i = 1, 2, \ldots, k$. The positive divisors of b are the numbers $p_1^{d_1} p_2^{d_2} \cdots\ p_k^{d_k}$ where $0 \le d_i \le f_i$ for $i = 1, 2, \ldots, k$. Hence the positive

common divisors of a and b are the numbers $p_1^{d_1}p_2^{d_2}\cdots\ p_k^{d_k}$ where $0 \leq d_i \leq \min\{e_i, f_i\}$ for $i = 1, 2, \ldots, k$. The largest number in this collection is the greatest common divisor, hence $gcd(a, b) = p_1^{\min\{e_1,f_1\}}p_2^{\min\{e_2,f_2\}}\ \cdots\ p_k^{\min\{e_k,f_k\}}$.
□

5.11 The *lcm*

If a and b are integers, neither of which is 0, then the *least common multiple* of a and b is the smallest positive integer ℓ such that $a|\ell$ and $b|\ell$. It is denoted by $lcm(a, b)$.

That is, $lcm(a, b)$ is the smallest $\ell \geq 1$ number which is a common multiple of a and b.

Why can't a or b be zero? Because there are no positive multiples of zero.

Why do we require that the least common multiple be positive instead of just non-negative? (We could then allow a or b to be zero) Because zero is a common multiple of any two numbers, so the least common multiple would always be zero.

Since $|a| \cdot |b|$ is a positive common multiple of a and b, there is a smallest positive integer among the collection of common multiples of a and b.

Since $lcm(a, b) = lcm(|a|, |b|)$, it is customary to take a and b to be positive when computing the lcm.

The least common multiple of a and b can be computed using the modified prime factorizations of a and b in a similar way as the gcd. We first illustrate the method with an example.

Example 5.11.1 *Suppose* $a = 2^3 5^4 11^1$ *and* $b = 2^2 7^8 11^4$. *Find* $lcm(a, b)$.

<u>*Solution*</u>.

By the Unique Factorization Theorem, the prime factorization of any positive multiple of a contains $2^c 5^d 11^f$ *with* $c \geq 3,\ d \geq 4,\ f \geq 1$.

Similarly, the prime factorization of any positive multiple of b contains $2^c 7^e 11^f$ *with* $c \geq 2,\ e \geq 8,\ f \geq 4$.

Hence, the prime factorization of any positive common multiple of a and b contains $2^c 5^d 7^e 11^f$ *with* $c \geq \max\{3, 2\},\ d \geq \max\{4, 0\},\ e \geq \max\{0, 8\},$

$f \geq \max\{1, 4\}$. The 0s arise because the prime factorization does not contain 7, and the prime factorization of b does not contain 5.

The smallest number in this collection is $2^3 5^4 7^8 11^4$, so it must be the lcm.

The following theorem is proved similarly to the corresponding result for the *gcd*.

Theorem 5.11.2 *If $a = p_1^{e_1} p_2^{e_2} \cdots\ p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots\ p_k^{f_k}$, where $e_i \geq 0$ and $f_i \geq 0$ for $i = 1, 2, \ldots, k$, then*

$$lcm(a, b) = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots\ p_k^{\max\{e_k, f_k\}}.$$

Together, Theorems 5.10.3 and 5.11.2 give the following.

Corollary 5.11.3 *Let a and b be positive integers. Then $gcd(a, b) lcm(a, b) = ab$.*

The corollary says that if you know one of $gcd(a, b)$ and $lcm(a, b)$, then you can compute the other one by division.

5.12 The Euclidean Algorithm

In the previous section we saw that the *gcd* and *lcm* of two numbers can be computed using their prime factorizations. While the prime factorization is relatively easy to find for fairly small numbers, large numbers are notoriously difficult to factor, that is, a lot of computation is required. It is precisely this difficulty that lies at the heart of many cryptosystems.

By 300BC, the Greeks had an efficient algorithm for computing the *gcd*: *the Euclidean Algorithm.* Efficient? Finding the prime factorization of a by testing if each of $1, 2, \ldots, a/2$ is a divisor, dividing it out, and then repeating the same process with the quotient requires a number of arithmetic operations that is proportional to a. Similarly for b. Hence finding $gcd(a, b)$ by finding their prime factorization using this method takes a number of steps proportional to the larger of a and b. (Better algorithms for finding the prime factorization are known, however.) Lamé proved in 1844 that the Euclidean Algorithm requires a number of arithmetic operations proportional to the logarithm of the smaller of the two numbers.

To put Lamé's Theorem into perspective, imagine a and b each have 200 digits, that is, are approximately 10^{200}. Using the method based on the prime factorization requires roughly 10^{200} operations. If it were possible to do $1,000,000,000$ of these per second, then about 10^{191} seconds would be required for the computation (there are $31,536,000$ seconds in a year, so the computation would take about 24 years). Using the Euclidean Algorithm, about 200 operations are required.

The main idea behind the Euclidean Algorithm is to successively replace the two numbers a and b by two smaller numbers in such a way that both pairs of numbers have the same *gcd*. The following proposition is the key to the method.

Proposition 5.12.1 *If $a, b \in \mathbb{Z}$, not both zero, and $a = bq+r$, then $gcd(a, b) = gcd(b, r)$.*

Proof. We claim that d divides both a and b if and only if it divides b and r. If d divides a and b, it divides $a - bq = r$; hence it divides b and r. Similarly, if d divides both b and r, it divides $bq + r = a$; hence it divides a and b.

By the claim, the set of divisors of a and b is the same as the set of divisors of b and r. Therefore, $gcd(a, b) = gcd(b, r)$. □

Before describing the Euclidean Algorithm, we illustrate it with an example. We will compute $gcd(834, 384)$. The idea is to repeatedly apply Proposition 5.12.1 until arriving at a situation where one of the numbers involved is zero.

$$\begin{array}{rcll}
834 & = & 384 \times 2 + 66 & \therefore gcd(834, 384) = gcd(384, 66) \\
384 & = & 66 \times 5 + 54 & = gcd(66, 54) \\
66 & = & 54 \times 1 + 12 & \quad = gcd(54, 12) \\
54 & = & 12 \times 4 + 6 & \quad = gcd(12, 6) = 6 \\
12 & = & 6 \times 2 + 0 & \quad = gcd(6, 0) = 6 \\
 & & \quad \therefore gcd(\mathbf{834}, \mathbf{384}) = \mathbf{6} &
\end{array}$$

Suppose a and b are non-negative integers with $a \geq b$. The *Euclidean Algorithm* is the following process.

1. Let $a_0 = a$ and $b_0 = b$. Set $i = 0$.

2. Use the division algorithm to write $a_i = b_i q_i + r_i,\ 0 \leq r_i < b_i$.

3. If $r_i \neq 0$ then

    - Let $a_{i+1} = b_i$ and $b_{i+1} = r_i$.
    - Replace i by $i + 1$ and go back to step (2).

    Otherwise $gcd(a, b) = b_i$ (the last non-zero remainder).

Why does this work? By Proposition 5.12.1, $gcd(a_0, b_0) = gcd(a_1, b_1) = \cdots = gcd(a_i, b_i) = gcd(b_i, 0) = b_i$. Hence, if the process terminates, then the *gcd* is found. The process terminates because, for any i we have $b = b_0 > r_0 = b_1 > r_1 = b_2 > r_2 = b_3 > \cdots > r_i \geq 0$. That is, the sequence of remainders is a decreasing sequence of non-negative integers. Any such sequence must eventually reach zero.

5.13 Integer Linear Combinations

If x and y are integers, what integers arise as values of the sum $6x + 4y$? Certainly only even numbers can arise because $2|4x + 6x$ for all $x, y \in \mathbb{Z}$. Can we get them all?

- 0 by taking $x = y = 0$,
- 2 by taking $x = 1$ and $y = -1$; -2 by taking $x = -1$ and $y = 1$,
- 4 by taking $x = 0$ and $y = 1$; -4 by taking $x = 0$ and $y = -1$,
- 6 by taking $x = 1$ and $y = 0$; -6 by taking $x = -1$ and $y = 0$,
- and so on.

It seems reasonable to believe that all multiples of 2 arise. That this is true actually follows from the second bullet point. Since $2 = 6 \times 1 + 4 \times (-1)$, multiplying through by an integer k gives $2k = 6 \times k + 4 \times (-k)$. Thus all even integers can arise (remember that k can be negative).

We have just done an example of the next theorem, which says that for any integers a and b, not both zero, the numbers that can arise as an *integer linear combination* $ax + by$ are precisely the multiples of $gcd(a, b)$.

We now generalize the previous paragraph, replacing 4 and 6 by any integers a and b. The question is *which integers arise as values of the sum* $ax + by$*?.* It turns out that *for any integers* a *and* b*, not both zero, the numbers that can arise as an integer linear combination* $ax + by$ *are precisely the multiples of* $gcd(a, b)$*.*

Since $gcd(a, b)|a$ and $gcd(a, b)|b$, we have $gcd(a, b)|ax + by$ for any x and y. Hence only multiples of $gcd(a, b)$ can arise as integer linear combinations of a and b.

In order to show that every multiple of the *gcd* can arise, it is enough to show that there are integers x_0 and y_0 such that $ax_0 + by_0 = gcd(a, b)$; then, the multiple $k \times gcd(a, b) = a(kx_0) + b(ky_0)$.

To find x_0 and y_0, use the computation arising from the Euclidean Algorithm from bottom to top: the second to last line tells you you to write the *gcd*, r_{i-1}, as a difference $a_{i-1} - q_{i-1}b_{i-1}$. That is, as a difference involving the smallest pair of numbers in the *gcd* computation. Each line above gives a substitution that allows the *gcd* to be expresses in terms of the next largest pair, until finally it is expressed in terms of a and b. We illustrate by writing $6 = gcd(834, 384)$ as an integer linear combination of 834 and 384.

$$\begin{aligned}
6 &= 54 - 12 \times 4 && \text{because } 54 - 12 \times 4 = 6 \\
&= 54 - (66 - 54 \times 1) \times 4 && \text{because } 66 - 54 \times 1 = 12 \\
&= 54 \times 5 - 66 \times 4 && \\
&= (384 - 66 \times 5) \times 5 - 66 \times 4 && \text{because } 384 - 66 \times 5 = 54 \\
&= 384 \times 5 - 66 \times 29 && \\
&= 384 \times 5 - (834 - 384 \times 2) \times 29 && \text{because } 834 - 384 \times 2 = 66 \\
&= 384 \times 63 - 834 \times 29 && \\
&= 834 \times (-29) + 384 \times (63) && \therefore \quad x_0 = -29 \text{ and } y_0 = 63
\end{aligned}$$

We summarize our work in this section in the following theorem.

Theorem 5.13.1 *Let* a *and* b *be integers which are not both 0, and let* $d \in \mathbb{Z}$*. There exist integers* x *and* y *such that* $ax + by = d$ *if and only if* $gcd(a, b)|d$*.*

5.14 Relatively prime integers

Integers a and b are called *relatively prime* if $gcd(a, b) = 1$. The name can be thought of originating from "prime relative to each other" – if the gcd equals 1 then a and b have no common prime factors.

When there are integers x and y such that $ax + by = d$, then (from the discussion at the end of the last section) we know that d is a multiple of $gcd(a, b)$, so that $gcd(a, b)$ is one of the positive divisors of d. The case $d = 1$ is exceptional because there is only one possible positive divisor, namely 1, so it must be the gcd.

Corollary 5.14.1 *Let $a, b \in \mathbb{Z}$, not both zero. There are integers x and y so that $ax + by = 1$ if and only if $gcd(a, b) = 1$.*

Proof. ($\Leftarrow$)By Theorem 5.13.1 if $gcd(a, b) = 1$ then there are integers x and y so that $ax + by = 1$.

($\Rightarrow$) Suppose here are integers x and y so that $ax + by = 1$. We know $gcd(a, b)|ax + by = 1$. Thus $gcd(a, b) \leq 1$. Since $gcd(a, b)$ is always at least 1, it follows that $gcd(a, b) = 1$. □

It is sometimes said that anything that can be proved about relatively prime integers follows from the above proposition. Here are three examples, the last of which is designated as a Proposition.

Example 5.14.2 *Prove that, for any integer a, $gcd(a, a + 1) = 1$.*

Proof.

Since $(a + 1) - a = 1$, the result follows from Corollary 5.14.1. □

Example 5.14.3 *Suppose $gcd(a, b) = d$. Prove that $gcd(a/d, b/d) = 1$.*

Proof.

By Theorem 5.13.1 there are integers x and y so that $ax + by = d$. Divide both sides by d to obtain $(a/d)x + (b/d)y = 1$. The result now follows from Corollary 5.14.1. □

Proposition 5.14.4 *Let $a, b,$ and c be integers such that $a|bc$. If $gcd(a, b) = 1$, then $a|c$.*

Proof. Since $gcd(a, b) = 1$, there are integers x and y so that $ax + by = 1$. Multiply both sides by c to get $acx + bcy = c$. Since $a|ac$ and $a|bc$, the integer $a|acx + bcy = c$. □

Notice that the statement in the above proposition is not true without the hypothesis that $gcd(a, b) = 1$. That is, *it is not true that if $a|bc$ then $a|b$ or $a|c$*. For example $6|4 \times 15$ but $6 \not| 4$ and $6 \not| 15$.

By the Fundamental Theorem of Arithmetic, if p is a prime number, then the possibilities for $gcd(p, a)$ are 1 and p: either p appears in the prime factorization of a or it doesn't. Both the Fundamental Theorem of Arithmetic, and the proposition above, can be used to show the following (compare the comment in the previous paragraph – it is important that p is prime).

Proposition 5.14.5 *If p is prime and $p|ab$, then $p|a$ or $p|b$.*

Proof. Suppose $p|ab$. If $p|a$ there is nothing to prove. Otherwise $gcd(p, a) = 1$, and hence $p|b$. □

5.15 Modular Arithmetic (Congruences)

Most of us can tell time on a 24 hour clock. The time 15:00 is 3PM, 22:00 is 10PM and so on. Forgetting about AM and PM for a moment, the time on a 12 hour clock is obtained by subtracting 12 from 24 hour times that are greater than 12. That is, *it is the remainder on division by 12*. We can extend this idea. When it is 38:00 the 12 hour clock time should be 2 (the remainder when 38 is divided by 12), and when it is −45:00 the time should be 3. (Notice how the remainder being positive is important here.)

Our work in this section arises from deeming two integers to be "the same" with respect to division by m (we will say that they are the same "modulo m") when they have the same remainder on division by m. We first show that two integers leave the same remainder on division by m if and only if their difference is a divisible by m.

Proposition 5.15.1 *Let $m \in \mathbb{N}$. Two integers a and b leave the same remainder on division by m if and only if $m \mid a - b$.*

Proof. ($\Rightarrow$) Suppose a and b leave the same remainder on division by m. Then there exist integers k_1, k_2 and r such that $a = k_1m+r$ and $b = k_2m+r$. Therefore $a - b = m(k_1 - k_2)$. Since $k_1 - k_2$ is an integer, $m \mid a - b$.

($\Leftarrow$) Suppose $m \mid a - b$. Then $a - b = km$ for some integer k, or equivalently $a = b + km$. By the Division Algorithm, we can write $b = qm + r$, $0 \leq r \leq m - 1$. Then $a = b + km = qm + r + km = (q + k)m + r$. Since the quotient and remainder guaranteed by the division algorithm are unique, a and b leave the same remainder on division my m. □

If $a, b \in \mathbb{Z}$, and $m \in \mathbb{N}$, we say that *a is congruent to b modulo m*, and write $a \equiv b \bmod m$ if a and b leave the same remainder on division by m.

Example 5.15.2

- $10 \equiv 24 \bmod 7$ *(and* $7 \mid 10 - 24$*).*
- $-15 \equiv 12 \bmod 9$ *(and* $9 \mid -15 - 12$*).*
- $442 \equiv 2 \bmod 10$ *(and* $10 \mid 442 - 2$*).*
- *Any multiple of m is congruent to zero* $\text{mod} m$*.*

The proposition above can be restated in the language of congruence modulo m.

Proposition 5.15.3 *Let $m \in \mathbb{N}$. For any integers a and b, $a \equiv b \bmod m \Leftrightarrow m \mid a - b$.*

Although the definition of congruence is in terms of remainders, it is sometimes easier to use Proposition 5.15.3 when proving statements about congruences.

In many programming languages there is a function *mod*. If $m \in \mathbb{N}$, then $a \bmod m$ is the unique number among $0, 1, 2, \ldots, m - 1$ to which a is congruent modulo m. That is, it is the remainder (as in the division algorithm - that's why its unique) when a is divided by m.

You can think of the integers $\text{mod} m$ as the hours on a circular clock with m hours, where "noon" is 0. The number of times you go around the circle and return to your starting point makes no difference to where you end up. What matters is the number of places you move when it is no longer possible to make it around the circle any more, and this number is one of $0, 1, 2, \ldots, m-1$. These are the possible remainders on division by m.

Another perspective is to take the number line and wrap it around the circular clock just mentioned so that 0 coincides with 0, and the positive direction is wrapped clockwise around the circle. Every integer then coincides with the member of $\{0, 1, 2, \ldots, m-1\}$ to which it is congruent.

The universe of integers $\bmod m$ *really only consists of the numbers* $0, 1, 2, \ldots, m-1$. As in the previous paragraph, modulo m any other integer is just one of these with another name (in the same way that 3/6 is another name for 1/2). The expression $a \equiv b \bmod m$ says that a and b are two names for the same position on the "number circle" with m positions.

A point that is worth special attention is *any multiple of m leaves remainder 0 when divided by m, so* $m|n$ *if and only if* $n \equiv 0 \bmod m$.

We will show that congruence $\bmod m$ has a lot in common with our usual notion of equality of integers. In particular (leaving out the $\bmod m$ in an attempt to make the similarity more obvious):

- Every number is congruent to itself.
- If a is congruent to b then b is congruent to a.
- If a is congruent to b and b is congruent to c, then a is congruent to c (numbers congruent to the same thing are congruent to each other).

Proposition 5.15.4 *Let* $m \in \mathbb{N}$. *Then,*

(1) For all integers a we have $a \equiv a \bmod m$.

(2) For all integers a and b we have $a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$.

(3) For all integers a, b, *and c, if* $a \equiv b \bmod m$ *and* $b \equiv c \bmod m$, *then* $a \equiv c \bmod m$.

Proof. We prove (3). The proofs of (1) and (2) are similar. Suppose $a \equiv b \bmod m$ and $b \equiv c \bmod m$. Then a and b leave the same remainder on division by m, and so do b and c. Thus, a and c leave the same remainder on division by m. That is, $a \equiv c \bmod m$. This completes the proof of (3). □

The following theorem is important because it tells you how to calculate mod$m$. It says that at any point in any calculation you can replace any number by one it is congruent to and not change the answer.

Theorem 5.15.5 *Let $m \in \mathbb{N}$. For any integers a, b, c and d, if $a \equiv b \bmod m$ and $c \equiv d \bmod m$, then,*

(1) $a + c \equiv b + d \bmod m$*,*

(2) $a - c \equiv b - d \bmod m$*,*

(3) $ac \equiv bd \bmod m$*.*

Proof. We will use Proposition 5.15.3. Suppose $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then $m|(a-b)$ and $m|(c-d)$, so that $a = b + km$ and $c = d + \ell m$ for some integers k and ℓ.

Thus, $a + c = b + km + d + \ell m = b + d + (k + \ell)m$, so $m|[(a + c) - (b + d)]$ and we have $a + c \equiv b + d \bmod m$. Similarly, $a - c \equiv b - d \bmod m$. Finally, $ac = (b + km)(d + \ell m) = bd + b\ell m + dkm + k\ell m^2 = bd + m(b\ell + dk + k\ell m)$. Therefore, $m|ac - bd$, so that $ac \equiv bd \bmod m$. □

We illustrate the use of Theorem 5.15.5 with two examples.

Example 5.15.6 *Find the integer n such that $7 \leq n < 14$ and $n \equiv 15 \cdot 17 - 19 \mod 7$.*

Solution.

By Theorem 5.15.5, $15 \cdot 17 - 19 \equiv 1 \cdot 3 - 5 \equiv -2 \equiv 5 \bmod 7$*. The integer n such that $7 \leq n < 14$ and $n \equiv 5 \bmod 7$ is 12.*

Let $n = (d_k d_{k-1} \cdots d_0)_{10}$. We saw before that d_0 is the remainder on division by 10. The same sort of argument shows that $(d_1 d_0)_{10}$ is the remainder on division by 100, that $(d_2 d_1 d_0)_{10}$ is the remainder on division by 1000, and so on. That is, $n \equiv d_0 \bmod 10$, $n \equiv (d_1 d_0)_{10} \bmod 100$ and so on. In general *the last t digits of the base 10 representation of n are the remainder when n is divided by 10^t, so for $t \geq 1$, every integer $n = (d_k d_{k-1} \cdots d_0)_{10} \equiv (d_{t-1} d_{t-2} \cdots d_0)_{10} \bmod 10^t$.*

Example 5.15.7 *Find the last digit of* 7^{99}.

<u>*Solution.*</u>

We need to evaluate $7^{99} \bmod 10$. *Since* $7^2 = 49 \equiv -1 \bmod 10$ *we have* $7^{99} \equiv (7^2)^{49}7^1 \equiv (-1)^{49}7 \equiv -7 \equiv 3 \bmod 10$. *Thus the last digit is* 3.

In the previous example we could have used the fact that $49 \equiv 9 \bmod 10$ and worked from there. Using -1 rather than 9 made the calculation easier. The lesson is that, among the many possible replacements for a number, you should choose one that's convenient to work with.

Notice that if $ac \equiv bc \bmod m$, then it may not be true that $a \equiv b \bmod m$. (That is, you can't necessarily cancel the c.) For example $2 \times 3 \equiv 6 \times 3 \bmod 12$, but $2 \not\equiv 6 \bmod 12$. The statement is true when c and m are relatively prime. The following is a translation of Proposition 5.14.4.

Proposition 5.15.8 *Let* a, b, c *and* m *be integers such that* $ac \equiv bc \bmod m$. *If* $gcd(c, m) = 1$, *then* $a \equiv b \bmod m$.

5.16 Testing for divisibility by 3 and by 9

We can use properties of congruence to prove the (familiar) rule that an integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3. The key is to observe that $10 \equiv 1 \bmod 3$ and so by Theorem 5.15.5 you can change 10 to 1 wherever it occurs. Remember that $3|n$ if and only if $n \equiv 0 \bmod 3$.

Proposition 5.16.1 *Suppose* $n = (d_k d_{k-1} \dots d_1 d_0)_{10}$. *Then 3 divides* n *if and only if 3 divides the sum of the digits in the base-10 representation of* n.

Proof. We have

$$\begin{aligned} 3|n &\Leftrightarrow n \equiv 0 \bmod 3 \\ &\Leftrightarrow d_k \times 10^k + d_{k-1} \times 10^{k-1} + \cdots + d_1 \times 10^1 + d_0 \times 10^0 \equiv 0 \bmod 3 \\ &\Leftrightarrow d_k \times 1^k + d_{k-1} \times 1^{k-1} + \cdots + d_1 \times 1^1 + d_0 \times 1^0 \equiv 0 \bmod 3 \end{aligned}$$

which is what we wanted. □

One interesting thing about this criterion is that it can be applied recursively. For example, $3|123456789$ if and only if $3|(1+2+\cdots+9)=45$ if and only if $3|(4+5)=9$. If the criterion is applied enough times, then it always ends with testing whether some one digit number is divisible by 3. So, in some sense it is not necessary to know the multiplication table for 3 beyond 3×3.

Question 5.16.2 *Suppose $n=(d_kd_{k-1}\dots d_1d_0)_{10}$. Prove that $n\equiv d_k+d_{k-1}+\cdots+d_1+d_0 \bmod 3$. (Hint: eliminate part of the proof of Proposition 5.16.1.)*

Since $10\equiv 1 \bmod 9$, almost exactly the same argument shows that an integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.

Question 5.16.3 *Suppose $n=(d_kd_{k-1}\dots d_1d_0)_{10}$. Prove that $n\equiv d_k+d_{k-1}+\cdots+d_1+d_0 \bmod 9$.*

Question 5.16.4 *Suppose $n=(d_kd_{k-1}\dots d_1d_0)_{10}$. Then 9 divides n if and only if 9 divides the sum of the digits in the base-10 representation of n. (Hint: it is easy if you use the result of Question 5.16.3).*

Only a small change to the argument needed to show that $(d_kd_{k-1}\dots d_1d_0)_{10}$ is divisible by 11 if and only if $d_k-d_{k-1}+d_{k-2}-\cdots\pm d_0$ is divisible by 11. That is, $11|n$ if and only if 11 divides the alternating sum of the decimal digits of n. The alternating sum arises because $10\equiv -1 \bmod 11$.

More complicated, but similar, tests for divisibility can be similarly devised for any divisor that is relatively prime to 10.

5.17 Exercises

1. Let $x,y\in\mathbb{R}$. Prove that

$$\lfloor x\rfloor+\lfloor y\rfloor\le\lfloor x+y\rfloor.$$

2. Indicate whether each statement is true or false, and briefly justify your answer.

(a) The integer n is odd if and only if $2 \times \left\lceil \frac{n}{2} \right\rceil - 1 = n$.

(b) If $x \in \mathbb{R} \setminus \mathbb{Z}$, then $\lfloor x \rfloor = \lceil x \rceil - 1$.

3. Let n be an integer. Prove that n is even if and only if $2\lfloor n/2 \rfloor = n$. Now, recall that n is even if and only if $2 \mid n$. Complete the following statement, and then prove that your assertion is true: *"n is a multiple of k if and only if ..."*

4. Find the base 16 representation of 262 139.

5. Is it true that $(121)_b$ is a square in any base b? Why or why not?

6. Find a base b such that $(122)_b = 101$.

7. Find x if $(123)_4 = x_5$.

8. Show that a number in base 3 is even if and only of the sum of its digits is even. In which other bases is this true?

9. Let $a, b, c, d \in \mathbb{Z}$. Prove that if $a|b$ and $c|d$, then $ac|bd$.

10. Let $a, b, d \in \mathbb{Z}$. Prove that if $d|a$ and $d|b$, then $d^2|ab$.

11. Let $a, b, c, d \in \mathbb{Z}$, and suppose that $a + b = c$. Prove that if d divides and two of a, b, c, then it also divides the third of these.

12. Prove that if $a|b$, then $\frac{b}{a}|b$. Make sure you are using the definition of the statement "a divides b".

13. Explain why the Fundamental Theorem of Arithmetic implies that there are no positive integers a and b such that $2^a = 3^b$.

14. Let n be a positive integer. Prove that $\log_2(n)$ is irrational unless n is a power of 2.

15. For a positive integer n, recall that n *factorial* is the integer $n(n-1)(n-2)\cdots 1$.

    (a) Suppose $1 \leq k \leq n$. What are the quotient and remainder when $N = n! + 1$ is divided by k?

    (b) Explain why part (a) implies that N has a prime divisor greater than n.

(c) Explain why part (b) implies that there are infinitely many prime numbers. (Note that of there are only finitely many prime numbers, then there is a largest prime.)

16. Find the prime factorization of 16!. (Note that it is not necessary to compute 16! first.

17. Let q_1, q_2 and q_3 be different primes. Prove that if p is prime and $p|q_1q_2q_3$, then $p \in \{q_1, q_2, q_3\}$.

18. Prove that the integer n is a perfect square if and only if every exponent in its prime factorization is even. State the corresponding result for perfect k-th powers, $k \geq 2$.

19. Find the smallest natural number that is divisible by 2 and by 3, and which is simultaneously the fourth power of an integer, and the sixth power of an integer. Answer the same question when 2 is replaced by 4.

20. Let n be a positive integer. Is it possible for a prime p to divide both n and $n + 1$?

21. Suppose $gcd(a, b) = 4$. Explain why the possible values of $gcd(9a, b)$ are 4, 12, and 36. For each of these values, d, give an example of integers a, b such that $gcd(a, b) = 4$ and $gcd(9a, b) = d$

22. Use the prime factorizations of $25 \cdot (24)^3$ and 10! to find the prime factorizations of $gcd(25 \cdot (24)^3, 10!)$ and $lcm(25 \cdot (24)^3, 10!)$.

23. How many positive divisors does $2^5 3^4 5^3$ have?

24. Suppose that a and b are integers such that $ab = -2^7 3^8 5^2 7^6$ and $gcd(a, b) = 2^3 3^4 5$. Is it possible that $a = 2^5 3^4 5$? Why or why not? What is $lcm(a, b)$?

25. Let a and b be positive integers such that $gcd(a, b) = 1$. Prove that $lcm(a, b) = ab$.

26. Use the Euclidean Algorithm to find $gcd(8288, 15392)$. Use your work to find

    (a) $lcm(8288, 15392)$;

   (b) Integers x and y such that $8288x + 15392y = gcd(8288, 15392)$;

   (c) For $k \in \mathbb{Z}$, integers x_k and y_k such that $8288x_k + 15392y_k = k \cdot gcd(8288, 15392)$.

27. Suppose c is a common divisor of a and b, that is $c \,|\, a$ and $c \,|\, b$. Prove that $c \,|\, gcd(a, b)$.

28. Suppose that there are integers x and y so that $ax + by = 2$. Suppose d is an odd divisor of a such that $d|bc$. Prove that $d|c$.

29. Suppose there are integers x and x such that $ax + by = 12$. What are the possibilities for $gcd(a, b)$? Why?

30. Prove that $gcd(n, n + 1) = 1$ for all $n \in \mathbb{Z}$. What are the possibilities for $gcd(n, n + 2)$, $gcd(n, n + 3)$ and $gcd(n, n + 4)$?

31. Let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Prove that one of the numbers $a, a + 1, \ldots, a + (k - 1)$ is divisible by k.

32. (a) Let $n \in \mathbb{Z}$ and $m \in \mathbb{N}$. The *least residue of n modulo m* is the unique integer among $0, 1, \ldots, m - 1$ to which n is congruent modulo m. For $k \in \mathbb{Z}$, which numbers can be the least residue of k^2 modulo 4?

   (b) Prove that no integer which is congruent to 3 modulo 4 can be written as a sum of two squares. That is, if $n \equiv 3 \ (mod\ 4)$, then there are no integers x and y such that $n = x^2 + y^2$. (Hint: the contrapositive.)

33. (a) Given that $k \equiv 2 \ (mod\ 4)$, determine the remainder when $5k + 13$ is divided by 4.

   (b) Given that $k \equiv 1 \ (mod\ 4)$, determine the remainder when $7k^{333} + 11$ is divided by 4.

34. Use congruences to prove that $13 \mid 19^n - 6^n$ for any $n \geq 0$. More generally, prove that if a and b are integers, then $d = a - b$ divides $a^n - b^n$ for any $n \geq 0$.

35. Show that every odd prime is congruent to 1 or 3 modulo 4. If $p > 3$ is prime, to what can p be congruent to modulo 6?

36. Use congruences to find the last digit of 43^{43}, and the last two digits of 7^{47}.

37. (a) Let $b > 1$ be an integer, and $n = (d_k d_{k-1} \dots d_1 d_0)_b$. Show that $(b-1) \mid n \quad \Leftrightarrow \quad (b-1) \mid d_0 + d_1 + d_2 + \cdots + d_k$.

    (b) Let $n = (d_k d_{k-1} \dots d_1 d_0)_{10}$. Show that $11 \mid n \quad \Leftrightarrow \quad 11 \mid d_0 - d_1 + d_2 - \cdots + (-1)^k d_k$. (Hint: $10 \equiv (-1) \pmod{11}$).

    (c) Part (a) is a generalization of the familiar statement that $9|n$ if and only if it divides the sum of the digits of n. State a similar generalization of the result in part (b).

Chapter 6

Cartesian Products and Relations

6.1 Cartesian Products

If A and B are sets, the *Cartesian product* of A and B is the set

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

The following points are worth special attention:

- The Cartesian product of two sets is a set.
- The elements of that set (the Cartesian product) are ordered pairs.
- In each ordered pair, the first component is an element of A, and the second component is an element of B.

In plane analytic geometry, we associate the set of points in the (Cartesian) plane with the set of all ordered points (x, y), where x and y are both real numbers, that is, by the elements of the set $\mathbb{R} \times \mathbb{R}$. This explains why the plane, together with this coordinate system, is referred to as $\mathbb{R}^2$, and also the similar terms used to describe its higher dimensional analogues.

Example 6.1.1 *Let* $A = \{1, 2, 3\}$ *and* $B = \{a, b\}$*. Then,*

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

and

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

Note, in particular, that $A \times B \neq B \times A$: these two sets have different elements. (Two ordered pairs (x_1, y_1) and (x_2, y_2) are equal when $x_1 = x_2$ and $y_1 = y_2$, that is, when the first components are equal, and the second components are equal.)

Suppose A has m elements and B has n elements. Then, each element of A is the first component of n ordered pairs in $A \times B$: one for each element of B. Thus the number of elements in $A \times B$ equals $m \times n$, the number of elements in A times the number of elements in B. This is one way in which the "×" symbol is suggestive notation for the Cartesian product.

Example 6.1.2 *Let A be a set. What set is $A \times \emptyset$?*

Solution.
By definition, $A \times \emptyset$ is the set of all ordered pairs (a, b) where $a \in A$ and $b \in \emptyset$. There are no such pairs, as there are no elements $b \in \emptyset$. Hence $A \times \emptyset = \emptyset$.

Question 6.1.3 *Let B be a set. Explain why $\emptyset \times B = \emptyset$.*

When is it true that $A \times B = B \times A$? We have seen in Example 6.1.2 that the equality does not hold for all sets A and B. It is certainly true that if $A = B$, then $A \times B = A \times A = B \times A$. By Example 6.1.2 and Question 6.1.3, if $A = \emptyset$ or $B = \emptyset$, then $A \times B = \emptyset = B \times A$. It turns out that these are the only circumstances under which $A \times B = B \times A$.

Proposition 6.1.4 *Let A and B be sets. Then $A \times B = B \times A$ if and only if $A = B$, or $A = \emptyset$, or $B = \emptyset$.*

Proof. ($\Rightarrow$) We prove the contrapositive. Suppose A and B are non-empty sets such that $A \neq B$. Then one of them has an element which does not belong to the other. Suppose first that there exists $x \in A$ such that $x \notin B$. Since $B \neq \emptyset$, the set $A \times B$ has an ordered pair with first component x, whereas $B \times A$ has no such ordered pair. Thus $A \times B \neq B \times A$. The argument is similar in the other case, when there exists $y \in B$ such that $y \notin A$.

($\Leftarrow$). If $A = B$ then $A \times B = A \times A = B \times A$. If $A = \emptyset$, then $A \times B = \emptyset = B \times A$. The case where $B = \emptyset$ is similar. □

The set $A \times (B \cup C)$ is the set of all ordered pairs where the first component is an element of A, and the second component is an element of $B \cup C$. That is, the second component is an element of B or an element of C. This is the same collection that would be obtained from the union $(A \times B) \cup (A \times C)$, which is made from the union of the set of all ordered pairs where the first component is an element of A and the second component is an element of B, and the set of all ordered pairs where the first component is an element of A, and the second component is an element of C. This is the outline of the proof of the following proposition.

Proposition 6.1.5 *Let A, B and C be sets. Then, $A \times (B \cup C) = (A \times B) \cup (A \times C)$.*

Proof. ($LHS \subseteq RHS$) Let $(x, y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in (B \cup C)$. That is, $y \in B$ or $y \in C$. This leads to two cases. If $y \in B$, then $(x, y) \in A \times B$, and so $(x, y) \in (A \times B) \cup (A \times C)$. If $y \in C$, then $(x, y) \in A \times C$, and so $(x, y) \in (A \times B) \cup (A \times C)$. Therefore, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

($RHS \subseteq LHS$) Let $(x, y) \in (A \times B) \cup (A \times C)$. Then $(x, y) \in A \times B$ or $(x, y) \in A \times C$. This leads to two cases. If $(x, y) \in A \times B$, then $x \in A$ and $y \in B$. Since $y \in B$, we have $y \in B \cup C$, so $(x, y) \in A \times (B \cup C)$. If $(x, y) \in A \times C$, then $x \in A$ and $y \in C$. Since $y \in C$, we have $y \in B \cup C$, so $(x, y) \in A \times (B \cup C)$. Therefore, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. □

The proposition above can also be proved using set builder notation and showing that the two sets are described by logically equivalent expressions. One hint that this is so is in the informal proof outline that precedes the proposition. Another one is in the proof of the proposition: the second part of the proof above is essentially the first part written from bottom to top. Each step is an equivalence rather than just an implication.

The same methods can be used to prove the following similar statements:

- $A \times (B \cap C) = (A \times B) \cap (A \times C)$;

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

It is a good exercise to investigate, then prove or disprove as appropriate, similar statements involving the Cartesian product and operations like set difference, $A \setminus B$, and symmetric difference, $A \oplus B$.

6.2 The Definition of a Relation

A *binary relation from a set A to a set B* is a subset $\mathcal{R} \subseteq A \times B$. A *binary relation on a set A* is a subset of $\mathcal{R} \subseteq A \times A$.

The word "binary" arises because the relation contains *pairs* of objects. Ternary relations (on A, say) would contain triples of elements, quaternary relations would contain quadruples of elements, and in general n-ary relations would contain ordered n-tuples of elements. *We will only consider binary relations, so we will drop the adjective "binary". When we talk about relations, we mean binary relations.* We will focus almost exclusively on relations on a set A.

Example 6.2.1 *Suppose A is the set of all students registered at UVic this term, and B is the set of all courses offered at UVic this term.*

Then $A \times B$ is the set of all ordered pairs (s, c), where s is a student registered at UVic this term, and c is a course offered at UVic this term. It represents all possible registrations by a current student in a current course.

Let $\mathcal{R} \subseteq A \times B$ be the subset consisting of the ordered pairs (s, c) where the course c is in Science and the student s is actually registered in the course. Then $\mathcal{R}$ is a relation from A to B.

Similarly, if $\mathcal{D} \subseteq A \times B$ is the subset consisting of the ordered pairs (s, c) where completion of course c would make student s eligible to receive a degree from the Faculty of Fine Arts (i.e. c is the last course needed to complete the requirements for the degree).

Other relationships between the elements of A and the elements of B can be represented by other subsets of $A \times B$.

Example 6.2.2 *Let* $A = \{1, 2, 3, 4\}$. *Let* $\mathcal{R} \subseteq A \times A$ *be*

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

Then $\mathcal{R}$ *is a relation on* A.

It can be observed that $(a, b) \in \mathcal{R}$ *if and only if* $a \mid b$, *that is,* $\mathcal{R}$ *is the divisibility relation on* A.

A relation may or may not express a particular type of relationship between its elements. The definition says that a relation is simply a subset. *Any* subset. If an ordered pair (x, y) belongs to a relation, it could be that the only relationship between x and y is that (x, y) is in the subset. Subsets like $\mathcal{R}_1 = \emptyset$ and $\mathcal{R}_2 = A \times A$ are perfectly good relations on A.

On the other hand, familiar things can be seen as relations. As a sample:

1. *Equality* between integers is represented by the relation $\mathcal{R}$ on $\mathbb{Z}$ where $(x, y) \in \mathcal{R}$ if and only if $x = y$.

2. *Equivalence* of fractions is represented by the relation $\mathcal{E}$ on $\mathbb{Q}$ where $(\frac{a}{b}, \frac{c}{d}) \in \mathcal{E}$ if and only if $\frac{a}{b} = \frac{c}{d}$, that is, the fractions represent the same number.

3. *Strictly greater than* between real numbers is represented by the relation $\mathcal{S}$ on $\mathbb{R}$ where $(x, y) \in \mathcal{S}$ if and only if $x > y$.

4. The property of being a *subset* is represented by the relation $\mathcal{C}$ on $\mathcal{P}(\mathcal{U})$ where $(X, Y) \in \mathcal{C}$ if and only if $X \subseteq Y$.

5. *Logical implication* between statements p and q is represented by the relation $\mathcal{I}$ on the set of all statements (say involving a certain set of Boolean variables) where $(p, q) \in \mathcal{I}$ if and only if $p \Rightarrow q$.

Because of these examples, and many others like them involving common mathematical symbols (that express particular relationships), infix notation is used: *sometimes we write* $x\mathcal{R}y$ *instead of* $(x, y) \in \mathcal{R}$, *and say that* x *is related to* y *(under* $\mathcal{R}$*).*

Frequently a symbol like "$\sim$" is used to denote a relation instead of a letter like $\mathcal{R}$. The letter $\mathcal{R}$ has the advantage that it emphasizes that relation is a set. A symbol like "$\sim$" looks familiar when infix notation is used: $x \sim y$ seems to look less awkward than $x \mathcal{R} y$. It also had the advantage of emphasizing that many familiar mathematical properties (as above, for example) can be seen as relations.

6.3 Properties of Relations: An Introduction

The relation "$=$" on the set of real numbers has the following properties:

1. Every number is equal to itself.

2. If x is equal to y, then y is equal to x.

3. Numbers that are equal to the same number are equal to each other. That is, if $x = y$ and $y = z$, then $x = z$.

The relation "$\Leftrightarrow$" on the set of all propositions (in a finite number of variables) has properties that look strongly similar to these.

1. Every proposition is logically equivalent to itself.

2. If p is logically to q, then q is logically equivalent to p.

3. Propositions that are logically equivalent to the same proposition are logically equivalent to each other to each other. That is, if $p \Leftrightarrow q$ and $q \Leftrightarrow r$, then $p \Leftrightarrow r$.

The relation "$\leq$" on the set of real numbers has the following properties:

1. $x \leq x$ for every $x \in \mathbb{R}$.

2. If $x \leq y$ and $y \leq x$, then $x = y$.

3. If $x \leq y$ and $y \leq z$, then $x \leq z$.

The relation "$\subseteq$" on the the power set of a set S has similar properties:

1. $X \subseteq X$ for every $X \in \mathcal{P}(S)$.

2. If $X \subseteq Y$ and $Y \subseteq X$, then $X = Y$.

3. If $X \subseteq Y$ and $Y \subseteq Z$, then $X \subseteq Z$.

The relation "$\Rightarrow$" on the set of all propositions (in a finite number of variables) looks to have the same properties as the previous two, so long as we accept "$\Leftrightarrow$" playing the role of "=". There is, however, something subtle and beyond the scope of this discussion, going on in the second bullet point because we use "$\Leftrightarrow$" instead of "=".

1. $p \Rightarrow p$ for every proposition x.

2. If $p \Rightarrow q$ and $q \Rightarrow p$, then $p \Leftrightarrow q$.

3. If $p \Rightarrow q$ and $q \Rightarrow r$, then $p \Rightarrow r$.

It may or may not be clear that point 1. in each of the above five collections of three points describes the same abstract property. And the same for the third point. The middle point describes the same abstract property in the first two collections and in the first two of the last three, but these two properties are fundamentally different.

1. The first property in the five collections above is "reflexivity". The dictionary defines "reflexive" as meaning "directed back on itself". In a relation, we interpret that as meaning every element is related to itself. Thus, each of the relations described above is reflexive.

2. The second property in the first two collections, but not the last three, is "symmetry": if x is related to y, then y is related to x.

3. The third property in all five collections is "transitivity": if x is related to y, and y is related to z, then x is related to z.

4. The second property in collection three and four is "anti-symmetry": if x is related to y and y is related to x, then x is the same as y. Later, we will see that being anti-symmetric is very different from being not symmetric. We will also get a hint of the origin of the (unfortunate) term "anti-symmetric".

Relations that are reflexive, symmetric, and transitive behave a lot like "equals": they partition the set A into disjoint collections of elements that are "the same" (equivalent) with respect to whatever property is used to define the relation. These are called *equivalence relations*, and will be considered in more detail later in this chapter.

Relations that are that reflexive, anti-symmetric, and transitive behave a lot like "less than or equal to" in the sense that they imply an ordering of some of the elements of A. To interpret this for the subset relation, think of $X \subseteq Y$ as reading "X precedes or equals Y" (there are some pairs of sets for which neither "precedes or equals" the other). These are called *partial orders*. They will not be considered further in this course.

6.4 Reflexive Relations

A relation $\mathcal{R}$ on a set A is *reflexive* if $(x, x) \in \mathcal{R}$ for every $x \in A$. (Written in infix notation, the condition is $x\mathcal{R}x$ for every $x \in A$.)

The property of being reflexive is informally described as "*every element of A is related to itself*".

Example 6.4.1 *Let $\mathcal{R}_1$ be the relation on $A = \{1, 2, 3\}$ given by*

$$\mathcal{R}_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3)\}.$$

Is $\mathcal{R}_1$ reflexive?

Solution.
Yes. Since $A = \{1, 2, 3\}$, by definition $\mathcal{R}_1$ is reflexive when $(1, 1), (2, 2)$ and $(3, 3)$ all belong to $\mathcal{R}_1$. They do.

Question 6.4.2 *Explain why $R_2 = \emptyset$ and $R_3 = \{(1, 1), (1, 2), (2, 1), (3, 3)\}$ are not reflexive relations on $A = \{1, 2, 3\}$.*

Question 6.4.3 *Let A be a set. Is $A \times A$ a reflexive relation on A?*

Example 6.4.4 *Let $\mathcal{R}_4$ be the subset relation on $\mathcal{P}(S)$, the set of all subsets of $S = \{1, 2, 3, 4\}$. That is, let $\mathcal{R}_4$ be defined by $(X, Y) \in \mathcal{R}_4$ if and only $X \subseteq Y$. Prove that $\mathcal{R}_4$ is reflexive.*

Solution.
We need to explain why $(X, X) \in \mathcal{R}_4$ for every $X \in \mathcal{P}(S)$. Consider any $X \in \mathcal{P}(S)$. Then, X is a set (which is a subset of S). Since $X \subseteq X$ (every set is a subset of itself) we have $(X, X) \in \mathcal{R}_4$. Therefore $\mathcal{R}_4$ is reflexive.

Question 6.4.5 *Let $\mathcal{R}_5$ be the relation on $\mathbb{Z}$ where $(a, b) \in \mathcal{R}_5$ if and only of $a \mid b$. Prove that $\mathcal{R}_5$ is reflexive.*

Question 6.4.6 *Let $\mathcal{R}_6$ be the relation on $\mathbb{R}$ defined by $(x, y) \in \mathcal{R}_6$ if and only if $xy > 0$. Is $\mathcal{R}_6$ reflexive?*

6.5 Symmetric Relations

A relation $\mathcal{R}$ on a set A is *symmetric* if $(y, x) \in \mathcal{R}$ whenever $(x, y) \in \mathcal{R}$, for all $x, y \in A$. (Written in infix notation, the condition is if $x\mathcal{R}y$ then $y\mathcal{R}x$, for all $x, y \in A$.)

The property of being symmetric is informally described as "*whenever x is related to y, it is also true that y is related to x*".

Example 6.5.1 *Let $\mathcal{R}_1$ be the relation on $A = \{1, 2, 3\}$ given by*

$$\mathcal{R}_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3)\}.$$

Is $\mathcal{R}_1$ symmetric?

Solution.
No, $(2, 3) \in \mathcal{R}_1$ but $(3, 2) \notin \mathcal{R}_1$. Therefore, $\mathcal{R}_1$ is not symmetric.

Question 6.5.2 *Explain why $R_2 = \emptyset$ and $R_3 = \{(1, 1), (1, 2), (2, 1), (3, 3)\}$ are symmetric relations on $A = \{1, 2, 3\}$.*

Question 6.5.3 *Let A be a set. Is $A \times A$ a symmetric relation on A?*

Example 6.5.4 *Let $\mathcal{R}_4$ be the subset relation on $\mathcal{P}(S)$, the set of all subsets of $S = \{1, 2, 3, 4\}$. That is, let $\mathcal{R}_4$ be defined by $(X, Y) \in \mathcal{R}_4$ if and only $X \subseteq Y$. Explain why $\mathcal{R}_4$ is not symmetric.*

Solution.
Let $X = \{1\}$ and Y $\{1, 2\}$. Then $X, Y \in \mathcal{P}(S)$, and $(X, Y) \in \mathcal{R}_4$ (because $X \subseteq Y$). Since $Y \not\subseteq X$, $(Y, X) \notin \mathcal{R}_4$. Therefore, $\mathcal{R}_4$ is not symmetric.

Question 6.5.5 *Let $\mathcal{R}_5$ be the relation on $\mathbb{Z}$ where $(a, b) \in \mathcal{R}_5$ if and only of $a \mid b$. Explain why $\mathcal{R}_5$ is not symmetric.*

Example 6.5.6 *Let $\sim$ be the relation on $\mathbb{N}$ defined by $m \sim n$ if and only if $m + 3n$ is even. Is $\sim$ symmetric?*

Solution.
Let's first try a few examples:
$1 \sim 3$ *because* $1 + 3 \cdot 3$ *is even, and also* $3 \sim 1$ *because* $3 + 3 \cdot 1$ *is even.*
$2 \sim 4$ *because* $2 + 3 \cdot 4$ *is even, and also* $4 \sim 2$ *because* $4 + 3 \cdot 2$ *is even.*
$3 \sim 5$ *because* $3 + 3 \cdot 5$ *is even, and also* $5 \sim 3$ *because* $5 + 3 \cdot 3$ *is even.*
Based on this information it seems likely that $\sim$ is symmetric. Let's prove that it is.

Let $a, b \in \mathbb{N}$. Suppose $m \sim n$. Then $m+3n$ is even. If m is even then $m+3n$ is even only if n is even, and in this case $n + 3m$ is also even. If m is odd then $m + 3n$ is even only if n is odd, and in this case $n + 3m$ is also odd. In either case $n \sim m$. Therefore $\sim$ is symmetric.

Question 6.5.7 *Let $\mathcal{R}_6$ be the relation on $\mathbb{R}$ defined by $(x, y) \in \mathcal{R}_6$ if and only if $xy > 0$. Is $\mathcal{R}_6$ symmetric?*

6.6 Transitive Relations

A relation $\mathcal{R}$ on a set A is *transitive* if $(x, z) \in \mathcal{R}$ whenever $(x, y), (y, z) \in \mathcal{R}$, for all $x, y, z \in A$. (Written in infix notation, the condition is if $x\mathcal{R}y$ and $y\mathcal{R}z$, then $x\mathcal{R}z$, for all $x, y, z \in A$.)

The property of being transitive is informally described as "*whenever x is related to y, and y is related to z, it is true that x is related to z*".

Example 6.6.1 *Let $\mathcal{R}_1$ be the relation on $A = \{1, 2, 3\}$ given by*

$$\mathcal{R}_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3)\}.$$

Is $\mathcal{R}_1$ transitive?

Solution.
No, $(1, 2), (2, 3) \in \mathcal{R}_1$ but $(1, 3) \notin \mathcal{R}_1$. Therefore, $\mathcal{R}_1$ is not transitive.

Question 6.6.2 *Explain why* $R_2 = \emptyset$ *is a transitive relation on* $A = \{1, 2, 3\}$*, but* $R_3 = \{(1, 2), (2, 1), (3, 3)\}$ *is not.*

Question 6.6.3 *Let* A *be a set. Is* $A \times A$ *a transitive relation on* A*?*

Example 6.6.4 *Let* $\mathcal{R}_4$ *be the subset relation on* $\mathcal{P}(S)$*, the set of all subsets of* $S = \{1, 2, 3, 4\}$*. That is, let* $\mathcal{R}_4$ *be defined by* $(X, Y) \in \mathcal{R}_4$ *if and only* $X \subseteq Y$*. Explain why* $\mathcal{R}_4$ *is transitive.*

Solution.
Let $X, Y, Z \in \mathcal{P}(S)$*. Then* X, Y *and* Z *are all subsets of* S *Suppose* (X, Y)*,* $(Y, Z) \in \mathcal{R}_4$*. Then* $X \subseteq Y$ *and* $Y \subseteq Z$*. Therefore,* $X \subseteq Z$*. Hence* $(X, Z) \in \mathcal{R}_4$*, and* R_4 *is transitive.*

Example 6.6.5 *Let* $\sim$ *be the relation on* $\mathbb{N}$ *defined by* $m \sim n$ *if and only if the sum of the digits of* m *equals the sum of the digits of* n *(for example* $123 \sim 51$ *because* $1 + 2 + 3 = 5 + 1$*). Is* $\sim$ *transitive?*

Solution.
Yes. Let $x, y, z \in \mathbb{N}$*. Suppose* $x \sim y$ *and* $y \sim z$*. Then the sum of the digits of* x *equals the sum of the digits of* y*, and the sum of the digits of* y *equals the sum of the digits of* z*. Therefore, the sum of the digits of* x *equals the sum of the digits of* z*, so that* $x \sim z$*. Therefore,* $\sim$ *is transitive.*

Question 6.6.6 *Let* $\mathcal{R}_5$ *be the relation on* $\mathbb{Z}$ *where* $(a, b) \in \mathcal{R}_5$ *if and only if* $a \mid b$*. Explain why* $\mathcal{R}_5$ *is transitive.*

Question 6.6.7 *Let* $\mathcal{R}_6$ *be the relation on* $\mathbb{R}$ *defined by* $(x, y) \in \mathcal{R}_6$ *if and only if* $xy > 0$*. Is* $\mathcal{R}_6$ *transitive?*

6.7 Anti-symmetric Relations

A relation $\mathcal{R}$ on a set A is *anti-symmetric* if $(x, y) \in \mathcal{R}$ and $(y, x) \in \mathcal{R}$ implies $x = y$, for all $x, y \in A$. (Written in infix notation, the condition is if $x\mathcal{R}y$ and $y\mathcal{R}x$, then $x = y$, for all $x, y \in A$.)

The property of being anti-symmetric is informally described as "*the only time we can have both* x *related to* y *and* y *related to* x *is when* $x = y$". This informal description is better for understanding than the definition, which is better for proofs.

Example 6.7.1 *Let $\mathcal{R}_1$ be the relation on $A = \{1, 2, 3\}$ given by*

$$\mathcal{R}_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3)\}.$$

Is $\mathcal{R}_1$ anti-symmetric?

Solution.
$\mathcal{R}_1$ is not anti-symmetric because $(1, 2), (2, 1) \in \mathcal{R}_1$ but $1 \neq 2$.

Example 6.7.2 *Let A be a set. Is $\mathcal{R}_2 = \emptyset$ an anti-symmetric relation on A?*

Solution.
Yes, $\mathcal{R}_2 = \emptyset$ is anti-symmetric because the condition $(x, y), (y, x) \in \mathcal{R}_2$ is never true, so the implication in the definition always holds.

Question 6.7.3 *Explain why $R_3 = \{(1, 2), (2, 3), (3, 3)\}$ is an anti-symmetric relation on $A = \{1, 2, 3\}$.*

Question 6.7.4 *Let A be a set. Is $A \times A$ an anti-symmetric relation on A?*

Example 6.7.5 *Let $\mathcal{R}_4$ be the subset relation on $\mathcal{P}(S)$, the set of all subsets of $S = \{1, 2, 3, 4\}$. That is, let $\mathcal{R}_4$ be defined by $(X, Y) \in \mathcal{R}_4$ if and only $X \subseteq Y$. Prove that $\mathcal{R}_4$ is anti-symmetric.*

Solution.
Let $X, Y \in \mathcal{P}(S)$. Then X and Y are all subsets of S Suppose $(X, Y), (Y, X) \in \mathcal{R}_4$. Then $X \subseteq Y$ and $Y \subseteq X$. Therefore, $X = Y$ Hence $\mathcal{R}_4$ is anti-symmetric.

Question 6.7.6 *Let $\mathcal{R}_5$ be the relation on $\mathbb{Z}$ where $(a, b) \in \mathcal{R}_5$ if and only of $a \mid b$. Explain why $\mathcal{R}_5$ is not anti-symmetric. Is it an anti-symmetric relation on $\mathbb{N}$?*

Question 6.7.7 *Let $\mathcal{R}_6$ be the relation on $\mathbb{R}$ defined by $(x, y) \in \mathcal{R}_6$ if and only if $xy > 0$. Is $\mathcal{R}_6$ anti-symmetric?*

Notice that "anti-symmetric" is different from "not symmetric". It is possible for a relation to be both anti-symmetric and symmetric, for example the relation $\{(1,1),(2,2),(3,3)\}$ on the set $A=\{1,2,3\}$.

On the one hand, the name "anti-symmetric" is a bit unfortunate because it suggests something that isn't always true. On the other hand, it does mean what the name suggests when the elements x and y in the respective definitions are different. Let $\mathcal{R}$ be a relation on a set A. Suppose $(x,y)\in\mathcal{R}$. If $\mathcal{R}$ is symmetric, then $(y,x)\in\mathcal{R}$ (no matter whether or not $x=y$). If $\mathcal{R}$ is anti-symmetric and $x\neq y$, then $(y,x)\notin\mathcal{R}$.

6.8 Relations and Matrices

Let $\mathcal{R}$ be a relation on the set $A=\{a_1,a_2,\ldots,a_n\}$. We can use an $n\times n$ array $M(\mathcal{R})$ to record which ordered pairs belong to $\mathcal{R}$. The entry in row i and column j of $M(\mathcal{R})$ is the truth value of the statement $(a_i,a_j)\in\mathcal{R}$, that is, it is 1 if the ordered pair $(a_i,a_j)\in\mathcal{R}$ and 0 otherwise.

If $\mathcal{R}$ is the relation $\{(1,3),(2,1),(3,2),(3,3)\}$ on the set $A=\{1,2,3\}$, then

$$M(\mathcal{R})=\begin{bmatrix}0&0&1\\1&0&0\\0&1&1\end{bmatrix}.$$

From the definitions we see that the matrix of a relation describes a

1. reflexive relation when every entry on the main diagonal equals 1,

2. symmetric relation when it is symmetric about the main diagonal: the (i,j)-entry equals the (j,i)-entry, and an

3. anti-symmetric relation when there is no $i\neq j$ such that the (i,j)-entry and the (j,i)-entry are both equal to 1. (Entries on the main diagonal don't matter, and it acceptable for the (i,j)-entry and the (j,i)-entry to both equal 0.)

It is not easily possible to look at the matrix and see if the relation is transitive.

Example 6.8.1 *Suppose $\mathcal{R}$ is a relation on $\{1,2,3,4\}$ which is reflexive, anti-symmetric, and transitive. Suppose also that $(1,2),(2,3),(3,4),(1,4) \in \mathcal{R}$. What else must be in $\mathcal{R}$?*

Solution.
We will use a 4×4 array to record information, and write $*$ for any entries not (yet) determined. Since $\mathcal{R}$ is reflexive, $(1,1),(2,2),(3,3),(4,4) \in \mathcal{R}$. At this point our array is:

$$\begin{bmatrix} 1 & * & * & * \\ * & 1 & * & * \\ * & * & 1 & * \\ * & * & * & 1 \end{bmatrix}$$

We are given that $(1,2),(2,3),(3,4),(1,4) \in \mathcal{R}$. Since $\mathcal{R}$ is anti- symmetric, we must have $(2,1),(3,2),(4,3),(4,1) \notin \mathcal{R}$. The updated array is:

$$\begin{bmatrix} 1 & 1 & * & 1 \\ 0 & 1 & 1 & * \\ * & 0 & 1 & 1 \\ 0 & * & 0 & 1 \end{bmatrix}$$

Since $(1,2),(2,3) \in \mathcal{R}$, transitivity implies $(1,3) \in \mathcal{R}$. Anti-symmetry gives $(3,1) \notin \mathcal{R}$. Similarly, since $(2,3),(3,4) \in \mathcal{R}$ we have $(2,4) \in \mathcal{R}$ by transitivity, and then $(4,2) \notin \mathcal{R}$ by anti-symmetry. The updated array is:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Thus, $\mathcal{R}$ must also contain $(1,1),(2,2),(3,3),(4,4),(1,3)$ and $(2,4)$. In this case we can also infer that no other ordered pairs can be in $\mathcal{R}$, so that the relation $\mathcal{R}$ is completely determined by the given conditions.

Question 6.8.2 *Let $\mathcal{R}$ be a relation on $A = \{1,2,3\}$ which is symmetric and transitive. Show that if $(1,2),(3,2) \in \mathcal{R}$, then $\mathcal{R} = A \times A$.*

6.9 Equivalence Relations

An *equivalence relation* on a set A is a relation on A that is

1. reflexive;

2. symmetric; and

3. transitive

Relations with these three properties are similar to "=". Suppose $\mathcal{R}$ is an equivalence relation on A. Instead of saying "$(x, y) \in \mathcal{R}$" or "x is related to y under $\mathcal{R}$", for the sake of this discussion let's say "x is equivalent to y". The reflexive property then says *everything in A is equivalent to itself.* The symmetric property says *if x is equivalent to y, then y is equivalent to x.* And the transitive property says *things that equivalent to the same thing are equivalent to each other.*

Example 6.9.1 *The following are examples of equivalence relations:*

1. *logical equivalence on the set of all propositions;*

2. *the relation $\mathcal{R}$ on $\mathbb{Z}$ defined by $x\mathcal{R}y$ if and only if $x - y$ is even;*

3. *the relation $\mathcal{T}$ on $\{0, 1, \ldots, 24\}$ defined by $h_1\mathcal{T}h_2$ if any only if h_1 hours is the same time as h_2 hours on a 12-hour clock;*

4. *the relation $\mathcal{S}$ on the set of all computer programs defined by $p_1\mathcal{S}p_2$ if and only if p_1 computes the same function as p_2;*

5. *the relation $\mathcal{E}$ on the set of all mathematical expressions in x defined by $p(x)\ \mathcal{E}\ q(x)$ if and only if $p(x) = q(x)$ for every real number x. For example, if $p(x) = x^2 - 1$ and $q(x) = (x + 1)(x - 1)$, then $p(x)\ \mathcal{E}\ q(x)$.*

It is a useful exercise to convince yourself that each of the relations in Example 6.9.1 is an equivalence relation.

Every equivalence relation "carves up" (mathematicians would say "partitions") the underlying set into collections (sets) of "equivalent" things (things that are "the same"), where the meaning of "equivalent" depends on the definition of the relation. In Example 6.9.1:

1. logical equivalence partitions the universe of all statements into collections of statements with the same logical meaning, and that can be freely substituted for each other;

2. $\mathcal{R}$ partitions the integers into the even integers and the odd integers;
3. $\mathcal{T}$ partitions $\{0, 1, \ldots, 24\}$ into collections of hours that represent the same time on a 12-hour clock;
4. $\mathcal{S}$ partitions the set of all computer programs into collections that do the same thing;
5. $\mathcal{E}$ partitions the set of all algebraic expressions into collections that give the same numerical value for every real number x, and hence can be freely substituted for each other when manipulating equations.

Each of these collections of "equivalent" things is an example of what is called an "equivalence class".

Let $\mathcal{R}$ be an equivalence relation on A, and $x \in A$. The *equivalence class of* x is the set $[x] = \{y : y\mathcal{R}x\}$.

Example 6.9.2 *Let $\mathcal{R}$ be the relation on $\{1, 2, \ldots, 20\}$ where $a\mathcal{R}b$ if and only if $a \equiv b \pmod 4$. Given that $\mathcal{R}$ is an equivalence relation, find $[1], [2]$ and $[6]$.*

<u>Solution</u> *By definition, $[x]$ is the set of elements that are related to x. Thus*

$$[1] = \{1, 5, 9, 13, 17\}, \quad \textit{and } [2] = \{2, 6, 10, 14, 18\} = [6].$$

Question 6.9.3 *For the same relation as in Example 6.9.2, find $[3], [5]$ and $[8]$.*

6.10 Equivalence Relations and Partitions

Let A be a set. A *partition of A* is a collection of disjoint, non-empty subsets whose union is A. That is, it is a set of subsets of A such that

1. the empty set is not in the collection; and
2. every element of A belongs to exactly one set in the collection.

Each set in the collection is called a *cell*, or *block*, or *element* of the partition. Note that a partition may contain infinitely many subsets.

Example 6.10.1 *Let $A = \{a, b, c, d, e\}$. The following are all partitions of A:*

1. $\{\{a\}, \{b, e\}, \{c, d\}\}$;
2. $\{A\}$;
3. $\{\{a, c, e\}, \{b, d\}\}$;
4. $\{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\}$.

Question 6.10.2 *Let $A = \{a, b, c, d, e\}$. Explain why each of the following is not a partition of A.*

1. $\{\{a\}, \{b, e\}, \{c, d\}, \emptyset\}$;
2. $\{\{a, c, e\}, \{d\}\}$;
3. $\{\{a\}, \{b\}, \{c\}, \{a, d\}, \{e\}\}$;

Technically, $\{a\}, \{b\}, \{c\}, \{d\}, \{e\}$ isn't a partition of $A = \{a, b, c, d, e\}$. It isn't a set, hence it can't be a partition. But this is just a technicality – mathematicians frequently write partitions in this way. This point is raised to make sure you're aware of what happens sometimes, and what is intended when it does.

Equivalence relations and partitions are actually two sides of the same coin. This is the main consequence of the two theorems below. The first theorem says that the collection of equivalence classes is a partition of A (which is consistent with what we observed above). The second theorem says that for any possible partition of A there is an equivalence relation for which the subsets in the collection are exactly the equivalence classes.

Theorem 6.10.3 *Let $\mathcal{R}$ be an equivalence relation on A. Then*

1. $x \in [x]$;

2. if $x\mathcal{R}y$ then $[x]=[y]$; and

3. if x is not related to y under $\mathcal{R}$, then $[x]\cap[y]=\emptyset$.

Proof. The first statement follows because $\mathcal{R}$ is reflexive.

To see the second statement, suppose $x\mathcal{R}y$. If $z\in[x]$ then (by definition of equivalence classes) $z\mathcal{R}x$. By transitivity, $z\mathcal{R}y$. That is $z\in[y]$. Therefore $[x]\subseteq[y]$. A similar argument proves that $[y]\subseteq[x]$, so that $[x]=[y]$.

To see the third statement, we proceed by contradiction. Suppose x is not related to y under $\mathcal{R}$, but $[x]\cap[y]\neq\emptyset$. Let $z\in[x]\cap[y]$. Then $z\mathcal{R}x$ and $z\mathcal{R}y$. By symmetry, $x\mathcal{R}z$. And then by transitivity, $x\mathcal{R}y$, a contradiction. Therefore, $[x]\cap[y]=\emptyset$. □

Part 1 of the above theorem says that the equivalence classes are all non-empty, and parts 2 and 3 together say that every element of X belongs to exactly one equivalence class. Parts 2 and 3 also tell you how to determine if two equivalence classes are the same: $[x]=[y]$ if and only if x is related to y (equivalently, since $\mathcal{R}$ is symmetric, y is related to x).

Part 2 of Theorem 6.10.3 is worth special attention. By definition, $[x]$ is the set of all elements which are related to x, and $[y]$ is the set of all elements which are related to y. If $[x]=[y]$, then every element which is related to x is related to y, and every element related to y is related to x.

Similarly, part 3 of Theorem 6.10.3 says that if x is not related to y, then no element related to x is related to y, and no element related to y is related to x.

Example 6.10.4 *Suppose $\mathcal{R}$ is the relation on $\mathbb{R}$ defined by $x\mathcal{R}y$ if and only if x rounds to the same integer as y. Prove that $\mathcal{R}$ is an equivalence relation and describe the partition of $\mathbb{R}$ it determines. How many of the equivalence classes $[1],[\sqrt{2}],[\sqrt{3}],[2],[e],[\pi]$ are different?*

Solution.
We must show that $\mathcal{R}$ is reflexive, symmetric, and transitive.

(reflexive) Let $x\in\mathbb{R}$. Then x rounds to the same integer as itself, so $x\mathcal{R}x$, and $\mathcal{R}$ is reflexive.

(symmetric) Let $x, y \in \mathbb{R}$. Suppose $x\mathcal{R}y$. Then x rounds to the same integer y. Therefore y rounds to the same integer as x. Thus $y\mathcal{R}x$, and $\mathcal{R}$ is symmetric.

(transitive) Let $x, y, z \in \mathbb{R}$. Suppose $x\mathcal{R}y$ and $y\mathcal{R}z$. Then x rounds to the same integer y, and y rounds to the same integer z. Therefore x rounds to the same integer as z. Thus $x\mathcal{R}z$, and $\mathcal{R}$ is transitive.

Therefore, $\mathcal{R}$ is an equivalence relation.

The partition of $\mathbb{R}$ determined by $\mathcal{R}$ is $\{[n-0.5, n+0.5) : n \in \mathbb{Z}\}$, where each half-open interval $[n-0.5, n+0.5) = \{x : n+0.5 \le x < n+0.5\}$.

We know two equivalence classes $[x]$ and $[y]$ are identical if and only if x is related to y. Among $[1], [\sqrt{2}], [\sqrt{3}], [2], [e], [\pi]$ there are exactly three different equivalence classes because

- *1 is related to $\sqrt{2}$ and not to any of $2, \sqrt{3}, e, \pi$;*
- *2 is related to $\sqrt{3}$ and not to any of $1, \sqrt{2}, e, \pi$;*
- *e is related to π and not to any of $1, \sqrt{2}, 2\sqrt{3}$.*

Therefore the different equivalence classes among those given are $[1] = [\sqrt{2}]$; $[\sqrt{3}] = [2]$, and $[e] = [\pi]$.

Question 6.10.5 *Let $\mathcal{R}$ be the relation on $\mathbb{R}$ defined by $x\mathcal{R}y$ if and only if $\lceil x \rceil = \lceil y \rceil$. Prove that $\mathcal{R}$ is an equivalence relation and describe the partition of $\mathbb{R}$ it determines.*

Question 6.10.6 *Let $m \ge 2$ be an integer, and let $\sim$ be the relation on $\mathbb{Z}$ defined by $a \sim b$ if and only if $a \equiv b \pmod{m}$. Which Theorem in Section 5.15 implies that $\sim$ is an equivalence relation? How many different equivalence classes are there in all?*

Theorem 6.10.7 *Let $\Pi = \{X_1, X_2, \ldots\}$ be a partition of a set A. Then*

1. *the relation $\mathcal{R}$ on A defined by $x\mathcal{R}y$ if and only if x belongs to the same cell of Π as y is an equivalence relation; and*
2. *Π is the partition of A determined by the set of equivalence classes of $\mathcal{R}$.*

Proof. The argument that shows $\mathcal{R}$ is an equivalence relation is left as an exercise.

We argue that Π is the partition of A determined by the set of equivalence classes of $\mathcal{R}$. That is, it must be shown that, for any $x \in A$, the equivalence class of x equals the cell of the partition that contains x.

Take any $x \in A$, and suppose $x \in X_i$. We need to show that $[x] = X_i$. On the one hand, if $y \in X_i$ then $y\mathcal{R}x$ by definition of $\mathcal{R}$. Hence, $y \in [x]$. Therefore, $X_i \subseteq [x]$. On the other hand, if $y \in [x]$ then $y\mathcal{R}x$. By definition of $\mathcal{R}$, the element y belongs to the same cell of Π as x. That is, $y \in X_i$. Therefore $[x] \subseteq X_i$. It now follows that $[x] = X_i$. □

Example 6.10.8 *Find an equivalence relation $\mathcal{F}$ on $[0, \infty)$ for which the partition of $\mathbb{R}$ determined by $\mathcal{F}$ is $\{[n, n+1) : n \in \mathbb{N} \cup \{0\}\}$.*

Solution.
By Theorem 6.10.7, we define $x\mathcal{F}y$ if and only if there exists $n \in \mathbb{N} \cup \{0\}$ such that $x, y \in [n, n+1)$.

Now, looking at the definition of $\mathcal{F}$ we see that $x\mathcal{F}y$ if and only if the integer part *of x (the part before the decimal point) is the same as the integer part of y. Equivalently, $x\mathcal{F}y$ if and only if $\lfloor x \rfloor = \lfloor y \rfloor$.*

Question 6.10.9 *Let $\mathcal{R}$ be an equivalence relation on $A = \{1, 2, 3, 4\}$ that determines the partition $\{\{1, 3\}, \{2, 4\}\}$. Write $\mathcal{R}$ as a set of ordered pairs.*

6.11 Exercises

1. Answer each question true or false, and briefly explain your reasoning.
   (a) Cartesian product is commutative on sets: $A \times B = B \times A$ for all A, B.
   (b) $\emptyset$ is a binary relation on any set A.
   (c) If $A \times B = B \times A$ then either $A = \emptyset$ or $B = \emptyset$.
2. Let A, B and C be sets. Prove that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
3. Let A, B and C be sets. Prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

4. Prove that for all sets A, B, C and D, if $A \cap C = \varnothing$, then $(A \times B) \cap (C \times D) = \varnothing$.

5. Let $A = \{1, 2, 3\}$. Give an example of a relation on A (that is, list the ordered pairs in your example) that is:

   (a) reflexive, but neither symmetric nor transitive;

   (b) symmetric, but neither reflexive nor transitive;

   (c) reflexive and transitive, but not symmetric;

   (d) antisymmetric and transitive;

   (e) neither symmetric nor antisymmetric.

6. Answer each question true or false, and briefly explain your reasoning.

   (a) If $|A| = 4$, then there are exactly 2^{16} relations on A.

   (b) If $\mathcal{R}$ is an anti-symmetric relation on $\mathbb{Z}$ and $(1, 2) \notin \mathcal{R}$, then $(2, 1) \in \mathcal{R}$.

   (c) For any set A, there is exactly one relation on A which is reflexive, symmetric, transitive and anti-symmetric.

   (d) The relation $\sim$ on $\{2, 3\}$, defined by $x \sim y$ if and only if xy is odd, is reflexive.

   (e) The set of all relations from A to B is $\mathcal{P}(A \times B)$.

   (f) For the set $A = \{1, 2, 3\}$, if the relation $\mathcal{R}$ on A is anti-symmetric and $(1, 3) \in \mathcal{R}$, then $\mathcal{R}$ is not symmetric.

   (g) For any set A, there is a relation $\mathcal{R}$ on A that is both symmetric and anti-symmetric.

7. Let $\sim$ be a reflexive, symmetric and transitive relation on $A = \{1, 2, 3\}$ such that $2 \sim 3$ and $1 \not\sim 2$. Write $\sim$ as a set of ordered pairs.

8. Suppose $\mathcal{R}$ is a symmetric and transitive relation on $A = \{1, 2, 3, 4\}$ such that $(3, 1), (3, 2), (2, 4) \in \mathcal{R}$. Must $\mathcal{R} = A \times A$?

9. (a) Suppose A is a non-empty set and $\mathcal{R}$ is a symmetric and transitive relation on A. Suppose further that each element $x \in A$ appears in some ordered pair in $\mathcal{R}$ (as either the first coordinate or the second coordinate). Prove that $\mathcal{R}$ is reflexive.

(b) Why is the statement in part (a) true if $A = \emptyset$?

10. Let $\mathcal{R}$ be the relation on $\mathbb{Z}$ defined by $(a, b) \in \mathcal{R}$ if and only if $a-b \leq 1$. Determine, with a proof or counterexample as appropriate, whether $\mathcal{R}$ is (i) reflexive, (ii) symmetric, (iii) anti-symmetric, (iv) transitive.

11. Let $A = \{1, 2, 3, 4\}$. Determine, with proof, whether each statement below is True or False.

    (a) If a relation $\mathcal{R}$ on A is anti-symmetric, then $\mathcal{R}$ can not be symmetric.

    (b) If a relation $\mathcal{R}$ on A is symmetric and transitive, and $(1, 2), (1, 3), (1, 4) \in \mathcal{R}$, then $\mathcal{R}$ is reflexive.

12. Suppose that $\mathcal{R}$ and $\mathcal{S}$ are relations on a non-empty set A. Determine if each of the following statements is true or false. Prove each true statement. For each false statement, give a counterexample using $A = \{1, 2, 3\}$.

    (a) If $\mathcal{R}$ and $\mathcal{S}$ are both anti-symmetric, then $\mathcal{R} \setminus \mathcal{S}$ is anti-symmetric.

    (b) If neither $\mathcal{R}$ nor $\mathcal{S}$ is symmetric, then $\mathcal{R} \cup \mathcal{S}$ is not symmetric.

    (c) If $\mathcal{R}$ and $\mathcal{S}$ are both equivalence relations, then so is $\mathcal{R} \cap \mathcal{S}$.

13. Let C be the set of all circles drawn in the plane with centre at $(0, 0)$. Let $\mathcal{R}$ be the relation on C defined by $c_1 \mathcal{R} c_2$ if and only if the radius of c_1 is at least as large as the radius of c_2. Prove that $\mathcal{R}$ is anti-symmetric.

14. Let $\sim$ be the relation on $\mathbb{N} = \{1, 2, \ldots\}$ defined by $x \sim y$ if and only if x/y is an integer. Prove that $\sim$ is anti-symmetric.

15. Let $\mathcal{R}$ be the relation on $\mathbb{N}$ defined by $(a, b) \in \mathcal{R}$ if and only if b is a multiple of a, that is, $b = ak$ for some integer k. Prove that $\mathcal{R}$ is reflexive, anti-symmetric and transitive. Which of these three properties would no longer hold if the relation $\mathcal{R}$ were on $\mathbb{Z}$ instead?

16. Let $\mathcal{E}$ be the relation on $\mathbb{Q}$ defined by $(a/b, c/d) \in \mathcal{E}$ if and only if $ad = bc$.

    (a) Show that $\mathcal{E}$ is reflexive, symmetric and transitive, but not anti-symmetric.

(b) What can you say about the fractions a/b and c/d if $(a/b, c/d) \in \mathcal{E}$? And why?

17. Let S be a set that contains at least two different elements. Let $\mathcal{R}$ be the relation on $\mathcal{P}(S)$, the set of all subsets of S, defined by $(X, Y) \in \mathcal{R}$ if and only if $X \cap Y = \emptyset$. Determine whether $\mathcal{R}$ is reflexive, symmetric, antisymmetric, or transitive. Why is it important that S has at least 2 different elements? Would any of the answers change if S was empty or had only one element?

18. Repeat the previous question using the relation $\mathcal{R}$ defined by $(X, Y) \in \mathcal{R}$ if and only if $X \subsetneqq Y$.

19. Let $\sim$ be an equivalence relation on $A = \{v, w, x, y, z\}$ with three equivalence classes. Suppose $v \sim y$ and $z \in [x]$, where $[x]$ denotes the equivalence class of x. Write $\sim$ as a subset of $A \times A$ and find the partition of A determined by the equivalence classes.

20. Let $\sim$ be an equivalence relation on the set $A = \{1, 2, \ldots, 8\}$, and denote the equivalence class of $x \in A$ by $[x]$.

    (a) Suppose that $1 \in [3], 4 \in [2]$, and $2 \in [1]$. Prove that $[4] = [3]$.

    (b) Ignore part (a) and suppose now that $\sim$ has 3 equivalence classes. If $[1]$ has 2 elements, $[2]$ has 3 elements, $1 \sim 6$, $2 \sim 5$, and $7 \sim 5$, then

       i. Write $\sim$ as a set of ordered pairs.

       ii. Find the partition of A determined by $\sim$.

21. Let T be a equilateral triangle with each side having length 1. Imagine T in a fixed position in the plane, say with the bottom side on the x-axis and the opposite angle above it. Let S be the set of coloured triangles obtainable from T by painting each side with one of the colours red and blue. Any combination of colours is allowed, for example all sides could have the same colour. Note that S has 8 elements: for example the bottom side being red and all other sides being blue is a different painting than the leftmost side being red and all other sides being blue.

    Define a relation $\mathcal{R}$ on S by $s_1 \, \mathcal{R} \, s_2$ if and only if s_1 can be rotated so that the rotated coloured triangle is identical to s_2. Prove that $\mathcal{R}$ is an equivalence relation and find the equivalence classes. (The elements of your sets can be pictures of the coloured triangles.)

22. Let $\sim$ be the relation on $T = \{10, 11, \ldots, 99\}$ defined by $a \sim b \Leftrightarrow a$ has the same first digit as b (that is, the same leftmost digit as b). Prove that $\sim$ is an equivalence relation.

23. Take it as given that the relation $\mathcal{R}$ on $A = \{1, 2, \ldots, 46\}$ defined by $x\mathcal{R}y$ if and only if $x - y$ is a multiple of 10 is an equivalence relation.

    (a) How many of the equivalence classes $[6], [13], [16], [28], [38], [46]$ are different? Why? Explain in at most two sentences.

    (b) How many subsets belong to the partition of A determined by $\mathcal{R}$? Why?

Chapter 7

Functions

The goal of this chapter is to talk about functions from a set A to a set B by generalizing the corresponding concepts from real valued functions of a real variable to this slightly different setting.

One description of a real-valued function of a real variable is that it is a rule that associates exactly one (output) real number $y = f(x)$ with every (input) real number x for which the function is defined. Sometimes "way of associating" is used in place of "rule that associates". But this isn't great. What, exactly, is a rule? And what is the "way"? We will get there by regarding a function as a collection of ordered pairs.

A function $y = f(x)$ corresponds to curve in the x-y plane that passes the *vertical line test*: for any real number x, the vertical line passing through x meets the curve in at most one point. If it does, then the *domain of f* is the set of all points x where the vertical line passing through x meets the graph (exactly once). This is the set of all numbers x at which the function is defined. The *range of f* is the set of all points y where the horizontal line passing through y meets the graph at least once. This is the set of all numbers y that occur as a value of the function, that is, are such that $y = f(x)$ for some x.

The graph of the function f is the set of all points $(x, f(x))$, where x is in the domain of f. Passing the vertical line test is equivalent to the graph of f containing exactly one ordered pair with first component x, for every x in the domain. This collection of points completely describes the function: the domain is the set of all numbers x that occur as the first component of an ordered pair in the collection, and the range is the set of all values that occur as the second component of an ordered pair in this collection. Further, this set of points explicitly gives the association between each x in the domain and the corresponding value $f(x)$ in the range.

7.1 The Definition of a Function and Some Related Terminology

Let A and B be sets. A *function f from A to B*, denoted $f : A \to B$, is a subset $f \subseteq A \times B$ in which, for every $a \in A$, there exists exactly one $b \in B$ such that $(a, b) \in f$.

Here are some points worth remembering.

- A function from A to B is a special kind of subset of $A \times B$.
- Each element $a \in A$ is the first component of exactly one ordered pair in the function. Thus (for finite sets) the number of ordered pairs in the function equals the number of elements of A.
- There are no restrictions on how elements of B occur as the second components of ordered pairs in a function. In particular, there is no guarantee that any given element of B appears as the second component of any ordered pair.

The main focus in the definition of a function from A to B is on what happens with the elements of A. There must be exactly one ordered pair in the function for each element of A; the second component of each of these ordered pairs is an element of B.

Example 7.1.1 *Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Why does the relation $f_1 = \{(1, a), (2, a), (3, b), (4, b), (1, b)\}$ fail to be a function?*

Solution.
It contains two ordered pairs with first component 1, contrary to the definition.

Question 7.1.2 *Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Why does the relation $f_2 = \{(2, a), (4, b), (1, b)\}$ fail to be a function?*

If $|A| = 4$ and $|B| = 3$, a function from A to B is a set consisting of exactly four ordered pairs; $\{(1,\_),(2,\_),(3,\_),(4,\_)\}$, where each blank is filled in with some element of B. Let's count the number of functions from A to B for these sets A and B. There are 3 options for the element of B to put in the first blank. For each of there, there are three options for the element of B to put in the second blank. For each of these nine options, are three options for the element of B to put in the third blank. And for each of these 27 options, reasoning in the same way gives that there are $81 = 3^4$ functions from A to B.

If A has m elements and B has n elements, then similar reasoning gives that there are n^m functions from A to B.

Let $f : A \to B$ be a function. Here is some notation and terminology that is commonly used so that it is possible to communicate ideas about functions.

- The set A is called the *domain* of f. To the extent that the elements of A are regarded as inputs and the elements of B are regarded as outputs, the domain is where the inputs live.

- The set B is called the *target* (or, more commonly, the *co-domain*). The term target is suggestive if you remember that it is where the arrow is pointed.

- If $(a, b) \in f$, then the element b is called the *image of a under f*, or the *value of f at a*, and is denoted by $f(a)$. The element a is called a *preimage* of b. Notice that it is "a" preimage, not "the" preimage; b could be $f(a)$ for several elements of a.

- The range of f is the set $\mathit{range}(f)$ of elements of B that are values of f. That is, $\mathit{range}(f) = \{b \in B : b = f(a) \text{ for some } a \in A\}$. It is easy to remember the term "range" if you think of it as suggesting the values of f range over the elements in this set. The notation $f(A)$ is sometimes used to denote the range of f.

Example 7.1.3 *Let A be the set of all faculty and students at UVic, and let B be the set of all amounts of money in dollars and cents. Let f be the relation from A to B where $(a, b) \in f \Leftrightarrow$ person $a \in A$ owes amount b to the library.*

Since for every person $a \in A$ there is a unique amount of money that they owe to the library (possibly \$0), f is a function. The domain of f is A, its target is B, and its range is the set of all amounts of money that are owed (each by at least one person).

If $(\textit{Gary}, \$1.59) \in f$*, then* $f(\textit{Gary}) = \$1.59$*, the image of Gary is* \$1.59*, a pre-image of* \$1.59 *is Gary, and the amount* \$1.59 *belongs to the range of* f*. (Note: any person who owes* \$1.59 *to the library is also a pre-image of* \$1.59*.)*

7.2 Equality of functions

Recalling the definition of a function as a set of ordered pairs, it makes sense that two functions should be equal if they are described by the same set of ordered pairs. This means that they have the same domain, A (because there is one ordered pair corresponding to each element of the same domain) and, for each $a \in A$, they have the same value at a. However, we can only have a relation from a set A to a set B if the set B is also known. This leads to the following definition.

Two functions f and g are *equal* if

1. they have the same domain,
2. they have the same target, and
3. $f(x) = g(x)$ for every x in the domain.

Thus, according to the definition, the following pairs of functions are not equal:

- $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x \rfloor$, and $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(x) = \lfloor x \rfloor$.
- $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \lfloor x \rfloor$, and $g : \mathbb{R} \to \mathbb{Z}$ defined by $g(x) = \lfloor x \rfloor$.
- $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \lfloor x \rfloor$, and $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \lceil x \rceil$.

7.3 1-1 Functions

Let $f : A \to B$ be a function. Then f is called *one to one*, or 1-1, or *injective*, if every element of B is the second component of at most one element of an ordered pair in f.

Informally, a function f is called *one to one*, or 1-1, if different inputs produce different outputs, or if each *output* value arises from a unique input value. Notice that the property of being 1-1 is determined by what happens in the target B: if there exists $b \in B$ which is the image of two different elements of A, then the function is not 1-1, and otherwise it is.

The definition is equivalent to the statement that if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$. It is also equivalent to the contrapositive of this statement: if $f(x_1) = f(x_2)$ then $x_1 = x_2$. The latter statement is useful in determining whether a function is 1-1. Throughout mathematics, a common method used to show something is unique is to *assume there are two and argue that they must actually be the same.* Here we would be assuming that the same output arises from two different inputs and arguing that those inputs are actually the same (so there is only one).

Example 7.3.1 *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 5$. Show that f is 1-1.*

Solution.
Suppose $f(x_1) = f(x_2)$. Then $2x_1 + 5 = 2x_2 + 5$. Therefore $2x_1 = 2x_2$, and consequently $x_1 = x_2$. Therefore f is 1-1.

Question 7.3.2 *Let $f : (0, \infty) \to (1, \infty)$ be defined by $f(x) = \frac{1}{x} + 1$. Prove that f is 1-1.*

If it is not possible to show a function f is not 1-1 by easily identifying elements x_1 and x_2 in the domain so that $f(x_1) = f(x_2)$, then a good way to proceed is to start trying to prove that f is 1-1. If f isn't 1-1, then the proof will break down at some point, and this will lead to the required elements.

Example 7.3.3 *Let $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = (x + 4)^2$. It turns out that f is not 1-1 because, for example, $f(0) = f(-8)$, but suppose we did not see that and, instead, tried to prove that f is 1-1.*

Suppose $f(x_1) = f(x_2)$. Then $(x_1 + 4)^2 = (x_2 + 4)^2$, so that $|x_1 + 4| = \sqrt{(x_1 + 4)^2} = \sqrt{(x_2 + 4)^2} = |x_2 + 4|$.

The presence of the absolute value is a clue that there may be more than one value in the domain corresponding to a particular value in the range. Here, if we let $x_1 = 0$ (note that x_1 is in the domain) then we get $4 = |x_2 + 4|$. Checking the two cases in the definition of absolute value gives the two solutions $x_2 = 0$ (in the case $x_2 \geq 0$) or $x_2 = -8$ (in the case $x_2 < 0$). Both of these values are in the domain, and substituting them into the formula for f shows $f(0) = f(-8)$. Therefore, f is not 1-1.

There is nothing special about the choice of 0 *except that it is possible to see up front that choosing it will serve our purposes.*

Question 7.3.4 *Let $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$ be defined by $f(x) = \frac{1}{x^2} + 3$. Prove that f is not 1-1.*

Suppose A and B are sets such that $|A| = m$ and $|B| = n$. Let's count the number of 1-1 functions from A to B. Notice that if $m > n$ then this number is zero because there are more ordered pairs in f than there are elements of B, so some element of B must appear in two of them. Suppose, then, that $m \leq n$. There are n choices for the image of the first element of A, then $n-1$ choices for the image of the second element of A, and so on until, finally, there are $n - (m - 1)$ choices for the image of the last element of A. This the number of 1-1 functions from A to B is

$$n(n-1)(n-2)\cdots(n-(m-1)) \cdot \frac{(n-m)(n-m-1)\cdots 1}{(n-m)(n-m-1)\cdots 1} = \frac{n!}{(n-m)!}.$$

To close this section, we note that if a function is not 1-1, then it is always possible to restrict its domain to get a new function that is 1-1. Further, it is possible to do so in such a way that the new function has the same range as the old one. In Example 7.3.3, if the domain is replaced by $[-4, \infty) = \{x : x \geq -4\}$, then the new function $f : [-4, \infty) \to \mathbb{R}$, defined by $f(x) = (x+4)^2$, is 1-1. To see this, suppose $f(x_1) = f(x_2)$. Then $(x_1 + 4)^2 = (x_2 + 4)^2$, so that $|x_1 + 4| = |x_2 + 4|$. But $x_1, x_2 \in [-4, \infty)$, so $x_1 + 4 \geq 0$ and $x_2 + 4 \geq 0$. Hence $x_1 + 4 = x_2 + 4$. It now follows that $x_1 = x_2$ and this function f is 1-1.

7.4 Onto Functions

Let $f : A \to B$ be a function. Then f is called *onto*, or *surjective*, if for every $b \in B$ there is an $a \in A$ such that $(a, b) \in f$.

The property of a function f being onto is determined by what happens with elements of the target B. If each of them is the image of at least one element of A, then f is onto. If there is an element of B which is not the image of an element of A, then f is not onto.

The best way to prove a function f is onto is constructive. Given $b \in B$, somehow use the information given to find $a \in A$ such that $f(a) = b$. When f is given by a formula giving b as the value of an expression involving a, this usually amounts to solving the equation $b = f(a)$ for a.

Example 7.4.1 *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 5$. Prove that f is onto.*

Solution.
Take any $y \in \mathbb{R}$. If $y = f(x)$ then $y = 2x + 5$ and, after some algebra, $x = (y - 5)/2$.

Therefore, if y is $f(x)$, then x must equal $(y - 5)/2$. For any $y \in \mathbb{R}$ we have $x = (y - 5)/2 \in \mathbb{R}$ and, further $f((y - 5)/2) = 2(y - 5)/2 + 5 = y$. Hence f is onto.

Example 7.4.2 *Let $f : (0, \infty) \to (0, \infty)$ be defined by $f(x) = -27 + (x + 3)^3$. Prove that f is onto.*

Solution.
Take any $y \in (0, \infty)$. Then $f(x) = y \Leftrightarrow -27 + (x + 3)^3 = y \Leftrightarrow (x + 3)^3 = y + 27 \Leftrightarrow x + 3 = \sqrt[3]{y + 27}$. (Every number has a unique cube root.) We must verify that this x belongs to the domain. Since $y \in (0, \infty)$ we have $y + 27 > 27$ and $\sqrt[3]{y + 27} > 3$. Therefore $-3 + \sqrt[3]{y + 27} \in (0, \infty)$. Hence, if $x = -3 + \sqrt[3]{y + 27}$, then $f(x) = -9 + ((-3 + \sqrt[3]{y + 27}) + 3)^3 = -27 + (\sqrt[3]{y + 27})^2 = y$, and so f is onto.

Question 7.4.3 *Let $f : \mathbb{R} \to [1, \infty)$ be defined by $f(x) = (x - 1)^2 + 1$. Prove that f is onto.*

The function f in Example 7.4.1 is not onto when the domain and target are replaced by $\mathbb{Z}$. To see this, argue as before to get that $y = f(x)$ implies

$x = (y-5)/2$. But it is possible to choose y in the target so that $(y-5)/2$ is not in the domain. For example, if $y = 6$ then $(y-5)/2 = 1/2 \notin \mathbb{Z}$. Hence there is no $x \in \mathbb{Z}$ to that $f(x) = 6$, and this function f is not onto.

To prove that a function is not onto you must find an element $b \in B$ which is not $f(a)$ for any $a \in A$. How you do this depends on f. In general, it is useful to try to prove that f is onto. If it isn't onto, then you will reach a point where either you can't solve for a in terms of b, or you will succeed in doing this but the only possibilities you find are not elements of A. In either case you are done as it will have been shown that the assumption f is onto leads to (logically implies) a contradiction. Thus by the inference rule Proof by Contradiction it must be that the assumption that f is onto is false, that is, f is not onto.

Example 7.4.4 *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = (x+4)^2$. It turns out that f is not onto. We can observe that $f(x) \geq 0$ for all x, thus there can't be an x for which $f(x) = -1$. Suppose we did not notice that and, instead, tried to prove that f is onto*

Take any $y \in \mathbb{R}$. If $y = f(x)$, then $y = (x+4)^2$, so that $\sqrt{y} = |x+4|$. The left hand side of this expression is not defined for all $y \in \mathbb{R}$: no real number is the square root of a negative number. Hence, if $y < 0$, then there is no real number x for which $f(x) = y$, and this function f is not onto.

Question 7.4.5 *Let $f : [0, \infty) \to \mathbb{R}$ be defined by $f(x) = -2 + \sqrt{x}$. Prove that f is not onto.*

In contrast to 1-1 functions, we note that there is no way to count the number of functions from a set A onto a set B using the methods we have available. However, if A has fewer elements than B, then no function f from A to B can be onto. There are fewer ordered pairs in f than there are elements of B, some element of B must not appear in any of them.

To close this section, we note that if a function is not onto, the new function obtained by replacing the target by the range is onto. In Example 7.4.4 the function $f : \mathbb{R} \to [0, \infty)$ defined by $f(x) = (x+4)^2$ is onto. To see this, argue as before. Take any $y \in [0, \infty)$. If $y = f(x)$, then $y = (x+4)^2$, so that $\sqrt{y} = |x+4|$. Since $y \geq 0$, the square root of y exists. If $x + 4 \geq 0$ we have $x = -4 + \sqrt{y}$, and if $x + 4 < 0$ we have $x = -4 - \sqrt{y}$. Since both $-4 + \sqrt{y}$

and $-4-\sqrt{y}$ are in the domain (though we only need one of them to be in the domain) and $f(-4+\sqrt{y}) = f(4-\sqrt{y}) = y$, this function f is onto.

7.5 Bijections

A function that is both injective (1-1) and surjective (onto) is sometimes called *bijective*, or *a bijection*. Another term for a bijection is a *1-1 correspondence*.

How can you remember injective, surjective, and bijective? Functions that are 1-1 go "in" to the target in separate places, the French word for on is "sur", and a *bi*-jection enjoys both properties.

The following two propositions establish important properties of bijections and make it possible to count the number of bijections from a finite set A to a finite set B.

Proposition 7.5.1 *Let A and B be finite sets. There exists a bijection $f : A \to B$ if and only if $|A| = |B|$.*

Proof. ($\Rightarrow$) Suppose there exists a bijection $f : A \to B$. Since f is 1-1 we have $|A| \leq |B|$. Since f is onto we have $|A| \geq |B|$. Therefore, $|A| = |B|$.

($\Leftarrow$) Suppose $|A| = |B|$. Let $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$. Let $f : A \to B$ be defined by $f(a_i) = b_i$ for $i = 1, 2, \ldots, n$. Then f is 1-1 because if $a_i \neq a_j$ then $f(a_i) = b_i \neq b_j = f(b_j)$. And f is onto because, for $i = 1, 2, \ldots, n$, the element b_i is the image of a_i. Therefore f is a bijection. □

Proposition 7.5.1 is the starting point for taking about "sizes" of infinite sets. Infinite sets A and B are defined to have the same cardinality ("size") if there is a 1-1 correspondence (bijection) $f : A \to B$. We will consider the cardinality of infinite sets in Chapter 8

Proposition 7.5.2 *Let A and B be finite sets such that $|A| = |B|$. A function $f : A \to B$ is 1-1 if and only if it is onto.*

Proof. Let A and B be finite sets such that $|A| = |B| = n$, and let $f : A \to B$ be a function. Then f is a set of n ordered pairs such that for each $a \in A$ there is exactly one ordered pair in f with first component a.

Suppose that f is 1-1. Then no two of the n ordered pairs in f have the same second component. Since $|B| = n$, it follows that every element of B appears as the second component of an ordered pair in f. Therefore f is onto.

Suppose that f is onto. Then every element of B appears as the second component of an ordered pair in f. Since $|B| = n$, it follows that no two of the n ordered pairs in f have the same second component. Therefore f is 1-1.

The proof is now complete. □

Let A and B be finite sets. Let's count the number of bijections $f : A \to B$. By Proposition 7.5.1, there are none unless $|A| = |B|$. If $|A| = |B|$, then by Proposition 7.5.2, the number of bijections equals the number of 1-1 functions, which is $n!$.

7.6 Function composition

Let A, B, and C be sets, and $f : A \to B$ and $g : B \to C$ be functions. The *composition of f and g* is the function $g \circ f : A \to C$ defined by $g \circ f(a) = g(f(a))$, for every element a in A.

Example 7.6.1 *Suppose $A = \{1, 2, 3\}$, $B = \{a, b, d, e\}$ and $C = \{w, z\}$. Let $f : A \to B$ be $f = \{(1, b), (2, e), (3, a)\}$, and $g : B \to C$ be $g = \{(a, w), (b, z), (d, z), (e, z)\}$. Then $g \circ f : A \to C$ is defined.*

The value $g \circ f(1) = g(f(1)) = f(b) = z$. Similar reasoning for 2 and 3 gives that $g \circ f = \{(1, z), (2, z), (3, w)\}$. Notice that $f \circ g$ is not defined because $g(x)$ is an element of C and f applies to elements of A.

Order matters in function composition. This is clear in Example 7.6.1 because $g \circ f$ is defined and $f \circ g$ is not defined. Even in cases where both are defined, they are usually different functions.

Example 7.6.2 *Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^2$ and $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(x) = x + 3$.*

Both $g \circ f$ and $f \circ g$ have domain $\mathbb{Z}$ and target $\mathbb{Z}$. But they don't have the same values: since $g \circ f(x) = g(f(x)) = g(x^2) = x^2 + 3$ and $f \circ g(x) =$

$f(g(x)) = f(x+3) = (x+3)^2 = x^2+6x+9$, we have $g \circ f(0) = 3$ and $f \circ g(0) = 9$. Thus, $g \circ f \neq f \circ g$.

We conclude this section by describing what happens when a function is a composition of 1-1 and onto functions.

Proposition 7.6.3 *If $f : A \to B$ and $g : B \to C$ are both 1-1 and onto, then $g \circ f$ is 1-1 and onto.*

Proof. We first show that $g \circ f$ is 1-1. Suppose $g \circ f(a_1) = g \circ f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$. Since $f(a_1)$ and $f(a_2)$ are elements of B and g is 1-1, $f(a_1) = f(a_2)$. Now, since f 1-1, $a_1 = a_2$. Therefore, $g \circ f$ is 1-1.

We now show that $g \circ f$ is onto. Take any $c \in C$. Since g is onto, there exists $b \in B$ such that $g(b) = c$. Since f is onto, there exists $a \in A$ such that $f(a) = b$. For this a we have $g \circ f(a) = g(f(a)) = g(b) = c$. Therefore, $g \circ f$ is onto. □

The proof shows the following two facts, which together give the proposition.

- If $f : A \to B$ and $g : B \to C$ are both 1-1, then $g \circ f$ is 1-1.
- If $f : A \to B$ and $g : B \to C$ are both onto, then $g \circ f$ is onto.

It is natural to wonder if the converse of Proposition 7.6.3 holds. That is, if $g \circ f$ is 1-1 and onto, must both f and g be 1-1 and onto. It doesn't, as we now demonstrate.

Example 7.6.4 *Suppose $f : A \to B$ and $g : B \to C$ are functions such that $g \circ f$ is 1-1 and onto. Prove that g is onto and f is 1-1.*

Proof.

The function g must be onto because an element which is not in the range of g can not be in the range of $g \circ f$.

The function f must be 1-1 because if there exist different elements $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, then $g \circ f(a_1) = g \circ f(a_2)$.

Question 7.6.5 *Let $A = \{1\}$, $B = \{1, 2\}$, and $C = \{2\}$. Find functions $f : A \to B$ and $g : B \to C$ such that $g \circ f$ is 1-1 and onto but f is not onto and g is not 1-1.*

7.7 The identity function

In the arithmetic of real numbers, 0 is an identity for addition: $x + 0 = x$ for all real numbers x (adding zero does not change anything). Further, the additive inverse of x (i.e. its negative) is the number $-x$ such that $x + (-x) = 0$ (the sum is the additive identity). Similarly, 1 is an identity for multiplication: $1x = x$ for all real numbers x. The multiplicative inverse of a non-zero number x (i.e. its reciprocal) is the number $1/x$ such that $x(1/x) = 1$ (the product is the multiplicative identity).

In this section we describe an identity for function composition. If there is such a function, it should have the property that it changes nothing when *its* operation (function composition) is applied, just like identities for addition and multiplication in real numbers. That is, we want an "identity function" to have the property that the result of composing it with a function f is the function f. In the next section we will relate this identity to inverses of functions.

Let A be a set. The *identity function on* A is the function $\iota_A : A \to A$ defined by $\iota_A(a) = a$ for every $a \in A$. (Note: the symbol ι is the Greek letter iota.)

The identity function does absolutely nothing in the sense that it sends every element of A to itself. It is an easy exercise to check that ι_A is 1-1 and onto.

Proposition 7.7.1 *Let A and B be sets, and $f : A \to B$ a function. Then $f \circ \iota_A = f$ and $\iota_B \circ f = f$.*

Proof. We prove only the first statement. The proof of the second statement is similar. Since $\iota_A : A \to A$, we have $f \circ \iota_A : A \to B$, so this function has the same domain and target as f. It remains to show it has exactly the same values. Take any $a \in A$. Then $f \circ \iota_A(a) = f(\iota_A(a)) = f(a)$. This completes the proof. □

Two different identity functions appeared in the previous proposition because otherwise the function composition is not defined.

7.8 Inverse functions

By analogy with additive inverses and multiplicative inverses for real numbers (see the discussion at the start of the last section), an inverse for a function $f : A \to B$ should be a function $g : B \to A$ such that $g \circ f = \iota_A$. That is, the function g should have the property that $f(a) = b \Leftrightarrow g(b) = a$. If this happens, then f should also be an inverse for g, and so we should have $f \circ g = \iota_B$.

Formally, we define functions $f : A \to B$ and $g : B \to A$ to be *inverses* if $f(a) = b \Leftrightarrow g(b) = a$. Equivalently, $f : A \to B$ and $g : B \to A$ are inverses if $g \circ f = \iota_A$ and $f \circ g = \iota_B$. A function is called *invertible* if it has an inverse.

Hidden in the definition is the condition that if f and g are inverses, then that the target of f is the domain of g, and the domain of f is the target of g.

The equivalent statement of the definition gives *a method for checking if functions f and g are inverses: show that $g \circ f = \iota_A$ and $f \circ g = \iota_B$.* It is important that both $g \circ f = \iota_A$ and $f \circ g = \iota_B$ hold. To see that, take $A = \{1, 2\}$ and $B = \{w, y, z\}$, and let $f = \{(1, w), (2, z)\}$ and $g = \{(w, 1), (y, 1), (z, 2)\}$. Then $g \circ f = \iota_A$. But f and g are not inverses: g maps y to 1 but f maps 1 to w. That is, $f \circ g \neq \iota_B$.

When does a function $f : A \to B$ have an inverse, g? If g exists, then (remembering the definition of f as a set of ordered pairs) by the definition of inverses it must be that $g = \{(b, a) : (a, b) \in f\}$. For this to be a function, there must be exactly one ordered pair with first component b for each $b \in B$. Therefore, f must map exactly one element of A to each element of B. Since "exactly one" implies "at most one", f must be 1-1. And since "exactly one" implies "at least one", f must be onto. We have just proved half of the theorem that characterizes (completely describes) the functions that have an inverse.

Theorem 7.8.1 *A function $f : A \to B$ has an inverse $g : B \to A$ if and only if it is 1-1 and onto.*

Proof. We have already seen (above) that if f has an inverse, then f is 1-1 and onto. It remains to prove the converse implication. Suppose f is 1-1 and onto. Then every element of B is the image of exactly one element of

A (at most one because f is 1-1, and at least one because f is onto). Hence $g = \{(b, a) : (a, b) \in f\}$ is a function. By the definition of inverses, it is the inverse of f. □

It follows from the definition that if g is the inverse of f, then f is the inverse of g. Hence *g is also 1-1 and onto.*

The inverse of a function $f : A \to B$ is commonly denoted by f^{-1}. It is a function with domain B and target A. (Remember that the inverse here is with respect to function composition, so this is neither the negative of f nor the reciprocal of f.) Since the inverse of the inverse is the original function (that is, if the inverse of f is g, then the inverse of g is f), we have $(f^{-1})^{-1} = f$. Further, $f^{-1} \circ f = \iota_A$ and $f \circ f^{-1} = \iota_B$.

7.9 Exercises

1. For each of the following, if the statement is true then prove it, and if it is false then give an example or explanation demonstrating it is false.

   (a) The function $f : \mathbb{Q} \to \mathbb{R}$ defined by $f(x) = x$ is invertible.

   (b) The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 3x - 2$ is onto.

   (c) The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 7x + 9$ is 1-1.

2. List all of the functions from $\{a, b, c\}$ to $\{a, b\}$ and identify the ones that are (i) one-to-one, (ii) onto, (iii) both one-to-one and onto, (iv) neither one-to-one nor onto.

3. (a) Give an example of a function from $\mathbb{N}$ to $\mathbb{Z}$ that is onto. Is your function also 1-1?

   (b) Give an example of a 1-1 function from $\mathbb{Z}$ to $\mathbb{N}$. Is your function also onto?

4. Let a and b be integers, with $a \neq 0$.

   (a) Is the function $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = ax + b$, 1-1 and onto?

   (b) When is the function $f : \mathbb{Q} \to \mathbb{Q}$, where $f(x) = ax + b$, 1-1 and onto?

   (c) Repeat part (b) with $\mathbb{Q}$ replaced by $\mathbb{Z}$.

5. Suppose that f is a function from A to B. Let $g = \{(y, x) : (x, y) \in f\}$. Explain why g being a function from B to A implies that f is 1-1 and onto (hint: the definition of function).

6. Let f and g be the functions from $\{a, b, c, d, e, f\}$ to $\{a, b, c, d, e, f\}$ given in the following table:

$x =$	a	b	c	d	e	f
$f(x) =$	c	d	a	e	f	b
$g(x) =$	b	c	a	e	f	d

   (a) Find $f \circ g$ and $g \circ f$.

   (b) Show that $g^{-1} = g^2$. The notation g^2 means $g \circ g$. In general, g^n means $g \circ g \circ g \cdots \circ g$, where g appears n times ($n-1$ compositions).

   (c) Find f^2 and $f^4 = (f^2)^2$. What does this tell you about f^{-1}?

7. Let $f : A \to B$ and $g : B \to C$ be functions with $A = \{a, b, c, d\}$, $B = \{1, 2, 3\}$, $C = \{w, x, y, z\}$ such that $g \circ f = \{(a, y), (b, x), (c, w), (d, w)\}$ and $g = \{(1, y), (2, w), (3, x)\}$. Find f.

8. Let $f : A \to B$ and $g : B \to C$ be functions. Prove:

   (a) If $g \circ f$ is one-to-one and f is onto, then g is one-to-one.

   (b) If $g \circ f$ is onto and g is one-to-one, then f is onto.

   (c) Give an example to show that, in (a) and (b) above, f need not be onto and g need not be one-to-one.

   (d) Let $A = \{1, 2\}$ and $B = \{a, b, c\}$. Let the functions f and g be

$$f = \{(1, a), (2, b)\} \quad \text{and} \quad g = \{(a, 1), (b, 2), (c, 1)\}.$$

   Verify that $g \circ f = \iota_A$, and then explain why g is not the inverse of f.

9. Indicate whether each statement is true or false, and briefly justify your answer.

   (a) The relation $\{(x, y) : y^2 = (x - 2)^2 + 4\}$ is a function from $\mathbb{R}$ to $\mathbb{R}$.

   (b) Suppose $|A| \geq 6$. Every function $f : A \to \{1, 2, 3, 4, 5, 6\}$ that is onto contains exactly six ordered pairs.

(c) If $f : \{a, b, c, d\} \to \{1, 2, 3\}$ and $g : \{1, 2, 3\} \to \{a, b, c, d\}$ are such that $f \circ g(x) = x$ for every $x \in \{1, 2, 3\}$, then g is the inverse of f.

(d) Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is a 1-1 correspondence, then $g \circ f$ has an inverse and $|A| = |C|$.

10. Let a and b be integers, with $a \neq 0$.

    (a) Is the function $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = ax + b$, 1-1 and onto?

    (b) When is the function $f : \mathbb{Q} \to \mathbb{Q}$, where $f(x) = ax + b$, 1-1 and onto?

    (c) Repeat part (b) with $\mathbb{Q}$ replaced by $\mathbb{Z}$.

Chapter 8

Cardinality of sets

8.1 1-1 Correspondences and Cardinality

A *1-1 correspondence from a set A to a set B* is a bijection $f : A \to B$, that is, a function from A to B which is 1-1 and onto.

If f is a 1-1 correspondence between A and B, then f associates every element of B with a unique element of A (at most one element of A because it is 1-1, and at least one element of A because it is onto). That is, for each element $b \in B$ there is exactly one $a \in A$ so that the ordered pair $(a, b) \in f$. Since f is a function, for every $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in f$. Thus, f "pairs up" the elements of A and the elements of B.

Proposition 8.1.1 *Let $\sim$ be the relation on the collection of all subsets of the universe $\mathcal{U}$ defined by $A \sim B$ if and only if there is a 1-1 correspondence from A to B. Then $\sim$ is an equivalence relation.*

Proof. Let A be a set. The identify function ι_A is a 1-1 correspondence from A to A. Therefore $A \sim A$ and $\sim$ is reflexive.

Suppose A and B are sets such that $A \sim B$. Therefore, there is a 1-1 correspondence f from A to B. Since the function f is invertible and f^{-1} is a 1-1 correspondence from B to A, we have $B \sim A$, and $\sim$ is symmetric.

Suppose A, B and C are sets such that $A \sim B$ and $B \sim C$. Then there are 1-1 correspondences $f : A \to B$ and $g : B \to C$. By Proposition 7.6.3 the function $g \circ f$ is a 1-1 correspondence from A to C we have $A \sim C$, and $\sim$ is transitive.

Therefore, $\sim$ is an equivalence relation. $\square$

As in the proof of Proposition 8.1.1, if there is a 1-1 correspondence from A to B, then there is also a 1-1 correspondence from B to A. Thus, where there is a 1-1 correspondence from A to B (and hence also from B to A), then we say that *A and B can be put into 1-1 correspondence.*

Let's think a bit about the the equivalence classes of the equivalence relation in Proposition 8.1.1. If $|A| = n$, then we know from Proposition 7.5.1 that A can be put into 1-1 correspondence with a set B if and only if $|B| = n$. Therefore, if A is a finite set, then the equivalence class $[A]$ consists of the sets with the same number of elements as A. If we extend this thinking to infinite sets, then we arrive at a way to talk about the "size" of infinite sets.

We say that sets A and B *have the same cardinality*, and write $|A| = |B|$, if A and B can be put into 1-1 correspondence. If A can be put into 1-1 correspondence with a subset of B (that is, there is a 1-1 function from A to B), we write $|A| \leq |B|$.

8.2 Cardinality of finite sets

A set is called *finite* if it can be put into 1-1 correspondence with $\{1, 2, \ldots, n\}$ for some integer $n \geq 0$. (Note that $\{1, 2, \ldots, n\} = \emptyset$ when $n = 0$.)

The *cardinality* (size) of a finite set X is the number $|X|$ defined by $|X| = n$ if X can be put into 1-1 correspondence with $\{1, 2, \ldots, n\}$.

When we count the number of objects in a collection (that is, set), say $1, 2, 3, \ldots,\ n$, we are forming a 1-1 correspondence between the objects in the collection and the numbers in $\{1, 2, \ldots, n\}$. The same is true when we arrange the objects in a collection in a line or sequence. The first object in the sequence corresponds to 1, the second to 2, and so on. Thus an equivalent definition of the cardinality of a finite set X is that $|X| = n$ if and only if there is a sequence of n terms in which each element of the set appears exactly once.

8.3 Cardinality of infinite sets

A set is *infinite* if it is not finite.

The definition of "infinite" is worth a closer look. It says that a set is infinite if it is not empty and can not be put into 1-1 correspondence with $\{1, 2, \ldots, n\}$ for any $n \in \mathbb{N}$. That means it has more than n elements for any natural number n.

Strange and wonderful things happen when the definition of two sets having the same cardinality is applied to infinite sets.

Example 8.3.1 *The function $f : \mathbb{N} \to \{1^2, 2^2, 3^2, \ldots\}$ defined by $f(n) = n^2$ is a 1-1 correspondence between $\mathbb{N}$ and the set of squares of natural numbers. Hence these sets have the same cardinality.*

Example 8.3.2 *The function $f : \mathbb{Z} \to \{\ldots, -2, 0, , 2, 4\}$ defined by $f(n) = 2n$ is a 1-1 correspondence between the set of integers and the set $2\mathbb{Z}$ of even integers. Hence these sets have the same cardinality.*

The notation $2\mathbb{Z}$ is used in the previous example because its elements are obtained by multiplying each element of $\mathbb{Z}$ by 2. For an integer $k \geq 1$, the set $k\mathbb{Z}$ is the set whose elements are obtained by multiplying each element of $\mathbb{Z}$ by k.

Question 8.3.3 *Prove that $|\mathbb{Z}| = |k\mathbb{Z}|$.*

Question 8.3.4 *Prove that $|\mathbb{N}| = |\mathbb{Z}|$ by proving that $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(n) = (-1)^n \lfloor n/2 \rfloor$ is a 1-1 correspondence.*

Theorem 8.3.5 *Any non-empty open interval of real numbers has the same cardinality as $\mathbb{R}$.*

Proof. Every non-empty open interval of real numbers is of the form (a, b), or (a, ∞), or (∞, b), where $a, b \in \mathbb{R}$.

We first show any two non-empty open intervals of finite length have the same cardinality as $(0, 1)$. Let $a, b \in \mathbb{R}$ such that $a < b$. Since the function

$f : (0,1) \to (a,b)$ defined by $f(x) = a + (b-a)x$ is a 1-1 correspondence between $(0,1)$ and (a,b) (exercise: verify this), we have $|(0,1)| = |(a,b)|$.

Now let $a \in \mathbb{R}$ and consider the open interval (a,∞). Since the function $g : (0,1) \to (a,\infty)$ defined by $g(x) = \frac{1}{x} + (a-1)$ is a 1-1 correspondence between $(0,1)$ and (a,∞) (exercise: verify this), we have $|(a,\infty)| = |(0,1)|$.

Similarly, $|(-\infty,b)| = |(0,1)|$.

We complete the proof by showing that $|(0,1)| = |\mathbb{R}|$. Since $|(0,1)| = |(-1,1)|$, it is enough to describe a 1-1 correspondence between $(-1,1)$ and $\mathbb{R}$. The function $h : (-1,1) \to \mathbb{R}$ defined by

$$h(x) = \begin{cases} 0 & \text{if } x = 0 \\ -1 + 1/x & \text{if } x > 0 \\ 1 + 1/x & \text{if } x < 0 \end{cases}$$

is a 1-1 correspondence between the open interval $(-1,1)$ and $\mathbb{R}$ (exercise: verify this). Therefore, $|\mathbb{R}| = |(-1,1)| = |(0,1)|$.

The proof is now complete. □

Notice, for example, that

$$(0,1) \subsetneqq (0,2) \subsetneqq \cdots \subsetneqq (0,\infty) \subsetneqq \mathbb{R}$$

but

$$|(0,1)| = |(0,2)| = \cdots |(0,\infty)| = |\mathbb{R}|.$$

It will turn out that $\mathbb{N}$ and $\mathbb{R}$ do not have the same cardinality ($\mathbb{R}$ is “bigger”, in fact so is $(0,1)$). Some theory must be developed before this statement can be made meaningful.

8.4 Countable Sets and Sequences

A set X is *countably infinite* if there is a 1-1 correspondence between $\mathbb{N}$ and X. A set X is *countable* if it is finite, or countably infinite.

According to the examples in the previous section, the set of squares of natural numbers is a countably infinite set, and so are $\mathbb{Z}$ and $2\mathbb{Z}$. It will turn out that any infinite subset of the integers is countably infinite, and there are lots of other countably infinite sets. Surprisingly, perhaps, the set of rational numbers is also countably infinite. The argument used to prove that rests on the principles that follow.

We mentioned before that if a set is finite then its elements can be arranged in a sequence. When this happens we're actually forming a 1-1 correspondence with $\{1, 2, \ldots, n\}$. Something similar happens with countably infinite sets.

If there is a 1-1 correspondence $f : \mathbb{N} \to X$, then there is a sequence of elements of X that contains every element of X exactly once: $f(1), f(2), f(3), \ldots$. The converse is also true. A sequence $x_1, x_2, \ldots$ that contains every element of X exactly once is the same as a 1-1 correspondence $f : \mathbb{N} \to X$: define $f(n) = x_n$, the n-th element of the sequence.

We can drop the condition that every element of X be contained in the sequence exactly once and, instead, require only that every element of X be guaranteed to appear somewhere in the sequence. Why? If such a sequence exists, then we can get a sequence that contains every element of X exactly once by deleting elements that have appeared earlier in the sequence (that is, there is a subsequence in which every element of X appears exactly once). This gives our main tool for proving that sets are countable.

Theorem 8.4.1 *A set X is countable if and only if there is a sequence in which every element of X appears (at least once).*

Proof.

($\Rightarrow$) The implication is easy to see if X is a finite set. If X is countably infinite, then there is a 1-1 correspondence $f : \mathbb{N} \to X$, and the sequence $f(1), f(2), f(3), \ldots$ contains every element of X.

($\Leftarrow$) Suppose there is a sequence $x_1, x_2, \ldots$ that contains every element of X (at least once). Define $f(1)$ to be the first element of the sequence that belongs to X (such an element exists because $X \neq \emptyset$). For $n \geq 2$ let $f(n)$ be the first element of X in the sequence that is not an element of $\{f(1), f(2), \ldots, f(n-1)\}$ (such an element exists because X is countably infinite). Then f is 1-1 by its construction. To see that f is onto, take any $y \in X$. Then y appears somewhere in the sequence. Suppose x_i is the first element of the sequence that equals y. Then, by the description of f, $y = f(n)$ for $n = 1 + |\{x_1, x_2, \ldots, x_{i-1}\}|$. Hence f is onto. Since f is also 1-1, it is a 1-1 correspondence. □

Theorem 8.4.1 suggests a really good way to think about countable sets. *A countable set is a set whose elements can be systematically listed so that every element eventually appears.* Since every element of the set appears in the list, if we go far enough along the list we will eventually find any element we're looking for.

8.5 Examples of Countably Infinite Sets

We will now explore some amazing consequences of Theorem 8.4.1. Notice that the sequence in the statement can contain elements that are not in X.

Corollary 8.5.1 *Any subset of $\mathbb{Z}$ is countable.*

Proof. Let X be a subset of $\mathbb{Z}$. The sequence $0, -1, 1, 2, -2, \ldots$ contains every integer exactly once. The result follows from Theorem 8.4.1. □

Almost exactly the same argument that proves Corollary 8.5.1 can be used to prove a stronger result.

Question 8.5.2 *Prove that any subset of a countable set is countable.*

It can come as quite a shock that the set of rational numbers is countable. We have all of the tools to prove it, but first will illustrate the argument by showing that $\mathbb{N} \times \mathbb{N}$ is countable. For reasons that will become evident, the method of proof is called "diagonal sweeping".

Theorem 8.5.3 *The set $\mathbb{N} \times \mathbb{N}$ is countable.*

Proof. It suffices to describe a sequence in which every element of $\mathbb{N} \times \mathbb{N}$ is guaranteed to appear. The elements of $\mathbb{N} \times \mathbb{N}$ are the coordinates of the lattice points (points with integer coordinates) in the first quadrant of the Cartesian plane. The sequence is illustrated by the arrows in Figure 8.1. It is clear that every element of $\mathbb{N} \times \mathbb{N}$ eventually appears: the components in the ordered pairs on subsequent diagonals sum to $2, 3, \ldots$. Therefore the ordered pair (a, b) appears on diagonal $a + b$, and the elements on this diagonal all appear in the list when it is "swept out". □

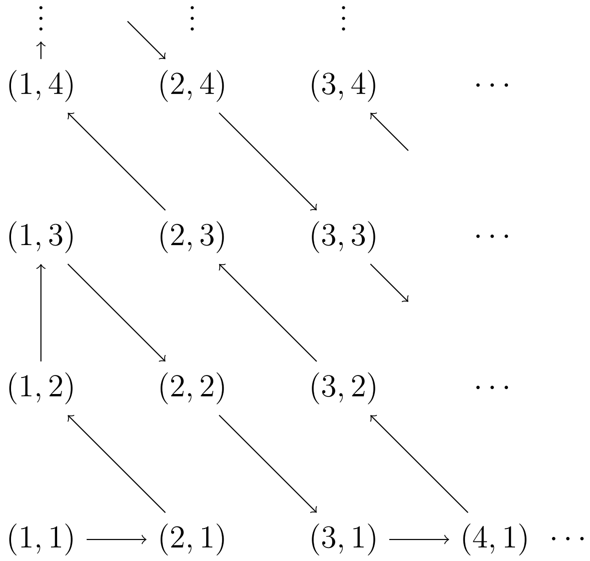


Figure 8.1: Using diagonal sweeping to list the elements of $\mathbb{N} \times \mathbb{N}$

Theorem 8.5.4 *The set, $\mathbb{Q}$, of rational numbers is countable.*

Proof. List the rationals as shown in Figure 8.2. The first row consists of the rational numbers with denominator 1, the second row consists of those with denominator 2, and so on. In each row, the numerators appear in the order $0, -1, 1, -2, 2, \ldots$. Every rational number appears because its sign (+ or −) can be associated with its numerator. □

Notice that, on the diagonals in the figure, the sum of the absolute value of the numerator and the absolute value of the denominator is constant. The sum of these numbers on the i-th diagonal is i. Hence, a rational number a/b appears in the list when the elements on diagonal $|a| + |b|$ are listed.

Almost exactly the same argument – make an array and systematically sweep it out – proves a more general theorem.

Question 8.5.5 *The union of any countable number of countable sets is countable.*

The cardinality of $\mathbb{N}$ is often denoted by $\aleph_0$ (pronounced aleph-naught or

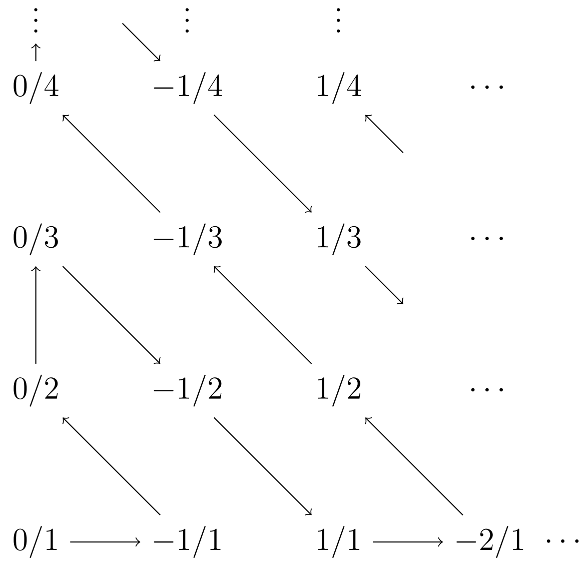


Figure 8.2: Using diagonal sweeping to list the rational numbers

aleph-zero; aleph is a letter in the Hebrew alphabet). Thus the cardinality of any countably infinite set is $\aleph_0$.

8.6 Proving Sets are Countable

From the preceding section we have the following methods of demonstrating that a set is countable. Show that:

- it is finite; or
- it is a subset of a countable set; or
- there is a sequence in which each of its elements is guaranteed to appear at least once (the list may be made by "diagonal sweeping"); or
- it can be put into 1-1 correspondence with a set that's known to be countable; or
- it is the union of countably many countable sets.

8.7 Uncountable Sets

A set is *uncountable* if it is not countable.

What does it mean for a set to be uncountable? According to the definitions, it means the set is infinite, and can not be put into 1-1 correspondence with $\mathbb{N}$. That means that there is no sequence that contains all of its elements.

To show that a set like $(0,1)$ is uncountable (which it is), proceed by contradiction. Assume that it is countable. That means there is a list (sequence) that contains each of its elements. Then, use the description of the list to show that there is something that should be in the list, but isn't. This is a contradiction, so the negation of the hypothesis that the set is countable must be true.

In the proof below, we use the fact that the real numbers are exactly the numbers that have an infinite decimal expansion. The real numbers that have a terminating decimal expansion have two of these: one ends in an infinite sequence of zeros, and the other ends in an infinite sequence of nines. Every other real number has a unique decimal expansion.

Theorem 8.7.1 *The set* $(0,1)$ *is uncountable.*

Proof. Suppose $(0,1)$ is countable. Then there is a sequence that contains at least one infinite decimal expansion of each of its elements.

$$\begin{array}{ll} 1. & 0.\underline{d_{11}}d_{12}d_{13}\ldots \\ 2. & 0.d_{21}\underline{d_{22}}d_{23}\ldots \\ 3. & 0.d_{31}d_{32}\underline{d_{33}}\ldots \\ \vdots & \vdots \end{array}$$

Each d_{ij} is a decimal digit, that is, a number between 0 and 9 inclusive.

We now describe a real number $x \in (0,1)$ which is not in the sequence above. The infinite decimal expansion of x is $x = 0.x_1x_2x_3\ldots$ where, for $i = 1,2,\ldots$

$$x_i = \begin{cases} 5 & \text{if } d_{ii} = 6 \\ 6 & \text{otherwise} \end{cases}$$

Then $x \in (0,1)$. Notice that the number x has a unique decimal expansion.

We claim that x can not appear anywhere in the sequence. Suppose to the contrary that it appears in position i, that is, $x = 0.d_{i1}d_{i2}\ldots$. Since x has a unique decimal expansion, we must have $x_j = d_{ij}$ for $j = 1, 2, \ldots$. But, by definition, $x_i \neq d_{ii}$ (that is, these numbers differ in the i-th digit after the decimal point), a contradiction. This proves the claim.

We now have that x appears in the sequence above, and that x does not appear in the sequence above, a contradiction. Therefore, $(0, 1)$ is uncountable. □

The proof method is called "Cantor diagonalization" after Georg Cantor, and because the number x is constructed by changing the value of the "diagonal" digits d_{ii}. The numbers 5 and 6 were used because they are not 0 and 9, that is, by using 5 and 6 we could not inadvertently construct a decimal expansion of a number that is in the list because it has a second, different, decimal expansion.

The same proof shows, for example, that the set of infinite sequences of 0s and 1s is uncountable.

Question 8.7.2 *Show that the set of infinite sequences of 0s and 1s is uncountable.*

Question 8.7.3 *Show that the set of finite sequences of 0s and 1s is countable. (Hint: systematically list the sequences of length 0, then those of length 1, and so on.)*

8.8 Proving Sets are Uncountable

So far, we have two methods to prove that a set is uncountable. We add a third to the list, and provide a justification for the second and third methods.

- Cantor diagonalization.
- Show there is a 1-1 correspondence with a set known to be uncountable.
- Show it contains an uncountable subset.

To justify the second bullet point, suppose X is uncountable. By definition of uncountability, X can not be put into 1-1 correspondence with a countable set. Therefore, any set that can be put into 1-1 correspondence with X is uncountable. This leads to the following corollary of Theorem 8.7.1.

Corollary 8.8.1 *The set $\mathbb{R}$ of real numbers is uncountable.*

Proof. We know $|\mathbb{R}| = |(0, 1)|$. Since $|(0, 1)|$ is uncountable, so is $\mathbb{R}$. □

Question 8.8.2 *Prove that any non-empty open interval of real numbers is uncountable.*

To justify the third bullet point, notice that the contrapositive of the statement "if X is countable then every subset of X is countable" is "If X has an uncountable subset then X is not countable".

We illustrate the method in the proof from the third bullet point by giving another argument that shows $\mathbb{R}$ is uncountable: *If R were countable, then* $(0, 1)$ *would be a subset of a countable set and would be countable. Since* $(0, 1)$ *is not countable, the result follows.*

Sometimes the cardinality of the real numbers is denoted by $\mathfrak{c}$, where the choice of letter is intended to convey that it is the cardinality of "the continuum". Since $\mathbb{N} \subseteq \mathbb{R}$, we have $\aleph_0 < \mathfrak{c}$.

Cantor's Continuum Hypothesis (1878) asserts that there is no set X such that $\aleph_0 < |X| < \mathfrak{c}$. The truth or falsity of this hypothesis is unknown, but results of Godel and Cohen imply that its truth can not be settled using the standard axioms of set theory. (That is, we can't prove it in our logic, but we can prove that we can't prove it.)

8.9 Other cardinalities

The only result in this section says that, for any set X, there is a set with cardinality larger than $|X|$, namely its power set. The function $f : X \to \mathcal{P}(X)$ defined by $f(x) = \{x\}$ for each $x \in X$ is 1-1, so (since replacing the target of this function by its range gives a 1-1 correspondence between X and a subset of $\mathcal{P}(X)$) the cardinality of $\mathcal{P}(X)$ is "at least as big" as the cardinality of X.

Theorem 8.9.1 *No set can be put into 1-1 correspondence with its power set.*

Proof. Let X be a set, and $f : X \to \mathcal{P}(X)$ a function. We claim that f is not onto. Consider the set Y defined by $Y = \{x \in X : x \notin f(x)\}$. Then $Y \in \mathcal{P}(X)$. Suppose there exists $x \in X$ such that $Y = f(x)$. If $x \in Y$, then by definition of Y, $x \notin Y$, and if $x \notin Y$, then by definition of Y, $x \in Y$. Both possibilities lead to a contradiction. Therefore there is no $x \in X$ such that $Y = f(x)$, and hence f is not onto. □

As a matter of interest, it turns out that $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = \mathfrak{c}$.

8.10 Exercises

1. Give a reason to explain why each set is countable.

   (a) $\{x \in \mathbb{R} : x^2 = 1\}$

   (b) The set P of prime numbers.

   (c) $\{2n + 1 : n \in \mathbb{Z}\} \cup \{3^k : k \in \mathbb{N}\}$.

   (d) The set of rational numbers with numerator between -3 and 5.

   (e) The set of years since 1970 that the Vancouver Canucks have won the Stanley Cup.

2. Let $A = \{a_1, a_2, \ldots\}$ and $B = \{b_1, b_2, \ldots\}$ be countably infinite sets. Prove that $A \times B$ is a countable set. (Hint: use the same idea as was used to prove $\mathbb{N} \times \mathbb{N}$ is countable. Explain why this implies that $\mathbb{Z} \times \mathbb{Z}$ is countable.

3. Prove that $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable. Does your argument generalize to the Cartesian product of k copies of $\mathbb{N}$, where k is a positive integer?

4. Show that if $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set, then the set of all infinite length sequences of elements of A is uncountable.

5. Prove that any non-empty half-open interval of real numbers, $[a, b)$ is uncountable. (Note: $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$.) Do the same for any non-empty half-closed interval $(a, b]$.

6. Prove that any closed interval of real numbers with positive length is uncountable. What happens if the length is not positive?

7. Let $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ be the set of irrational numbers. Explain why the fact that $\mathbb{R}$ is uncountable, and the fact that $\mathbb{Q}$ is countable, together imply that $\mathbb{I} \neq \emptyset$. More generally, explain why $\mathbb{I}$ must be uncountable. (Note: $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$.)

8. Classify the given set as countable or uncountable, and supply a brief justification for your answer.

   (a) $\mathbb{Q} \cap (0, 1)$.

   (b) The closed interval of real numbers, $[0, 2]$.

   (c) The set $\mathbb{C}$ of complex numbers.

   (d) The set of all prime factors of $1000!$.

   (e) The set of all integers with at most 2^{100} digits in their base 16 representation.

   (f) The power set of the set of natural numbers.

   (g) $\emptyset$.

   (h) $\mathbb{N} \times \mathbb{R}$.

9. Let $\mathcal{F} = \{f : \mathbb{N} \to \{0, 1\}\}$. Prove that $\mathcal{F}$ is uncountable. Explain why this implies that the set of all functions from $\mathbb{Z}$ to $\mathbb{Z}$ is uncountable.