# Chapter 2

# Topics in Logic and Proofs

Some mathematical statements carry a logical value of being true or false, while some do not. For example, the statement "$4 + 5 = 9$" is true, whereas the statement "2 is odd" is false. However, a statement like "$x^2 - 2x = 15$" is neither true nor false, until further information is given concerning $x$. We now make the following definition.

**Definition.** By a *truth value* we mean a logical value of true or false. A statement which possesses a truth value is called a *proposition*.

Technically, of course, a proposition can be stated in any language, not necessarily mathematical; the only requirement is that the statement must be quantifiable as being true or false.

This leads to the algebra of *boolean logic*, in which we are dealing with entities whose values can either be 0 (false) or 1 (true). In fact, this reminds us of the binary number system and the underlying structure (on/off switches) of computing machines.

## 2.1 Propositional Logic

As with numbers, we now treat propositions as mathematical quantities which can be operated one on another by a selection of proposition operators, or *logic operators*. The first and simplest operator is analogous to taking the negative of a number.

**Definition.** Let $p$ denote a proposition. The *negation* of $p$ is the proposition given by the statement "not $p$" and whose value is opposite that of $p$. The negation of $p$ can simply be called *not* $p$ and is denoted by $\neg p$.

**Example.** We give two propositions, one in mathematics and another in English, each with its negation.

$$\begin{array}{rlrl} p: & 4+5=9 & q: & \text{The earth is flat.} \\ \neg p: & 4+5\neq 9 & \neg q: & \text{The earth is not flat.} \end{array}$$

Note that each proposition has the opposite truth value from that of its negation; If $p$ is true then $\neg p$ is false, and vice versa.

*Question.* What would be the value of the proposition $\neg(\neg p)$?

### 2.1.1 Logic Operators and Truth Tables

A logic operator can be given by a table which displays the output value for every possible combination of the input values. The *truth table* for the negation operator, for instance, is given below.

Table 2.1: Truth table for $\neg p$.

| $p$ | $\neg p$ |
|---|---|
| T | F |
| F | T |

A number of logic operators will now be given by their truth tables. In general, the resulting proposition obtained by applying these operators will be called a *compound* proposition.

**Definition.** Let $p$ and $q$ be two propositions. The *conjunction* $p \wedge q$ and *disjunction* $p \vee q$ yield the compound statements $p$ *and* $q$, respectively, $p$ *or* $q$, and whose values are given according to the following table.

Table 2.2: Truth tables for $p \wedge q$ and $p \vee q$.

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | T |
| F | T | F | T |
| F | F | F | F |

**Example.** Suppose $p : 4+5=9$ and $q :$ 2 is odd. Write the statement and find the value of the compound proposition (a) $\neg p \wedge q$ (b) $p \vee \neg q$.

*Solution.* Note that $p$ has value true and $q$ false. The first statement is false $(F \wedge F)$ and the second true $(T \vee T)$, and they are given by

a) $\neg p \wedge q : 4 + 5 \neq 9$ and 2 is odd
b) $p \vee \neg q : 4 + 5 = 9$ or 2 is not odd

**Exercise 2.1.** Suppose $p$ is true and $q$ is false. Determine true or false for each compound proposition below.

a) $\neg p \vee \neg q$
b) $(p \wedge \neg q) \vee \neg p$
c) $(p \wedge q) \vee (\neg p \wedge \neg q)$
d) $(\neg p \vee (q \vee p)) \wedge (p \wedge q)$

**Example.** Construct a truth table to determine the possible output values of the compound proposition given by $(p \vee \neg q) \wedge (\neg p \vee q)$.

*Solution.* There are four possible rows. We show the intermediate steps according to the order in which the logic operations apply, as follows.

| $p$ | $q$ | $\neg p$ | $\neg q$ | $p \vee \neg q$ | $\neg p \vee q$ | $(p \vee \neg q) \wedge (\neg p \vee q)$ |
|---|---|---|---|---|---|---|
| T | T | F | F | T | T | T |
| T | F | F | T | T | F | F |
| F | T | T | F | F | T | F |
| F | F | T | T | T | T | T |

**Exercise 2.2.** Construct the truth table for each given compound proposition.

a) $\neg(\neg p \wedge \neg q)$
b) $\neg p \vee (p \wedge \neg q)$
c) $(p \wedge \neg q) \vee (\neg p \vee q)$
d) $(p \vee q) \wedge (\neg p \wedge \neg q)$

**Definition.** The *implication* $p \to q$ yields a compound proposition whose truth value is given in Table 2.3. The statement $p \to q$ is read *if $p$ then $q$*, or sometimes, *$p$ implies $q$*. Implication is also called the *if-then* operator.

Table 2.3: Truth table for $p \to q$.

| $p$ | $q$ | $p \to q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

*Question.* Do $p \to q$ and $q \to p$ always have the same truth value?

**Exercise 2.3.** Suppose $p : 4 + 5 = 9$ and $q : 2$ is odd. Write the statement and determine the value of each compound proposition below.

a) $p \to q$
b) $q \to p$
c) $\neg p \to q$
d) $\neg q \to \neg p$

**Example.** Construct the truth table for the proposition $(p \to q) \to r$.

*Solution.* This is the first time we see a compound proposition involving three propositional variables. The first three columns of the next table show the standard ordering for the eight possibilities of the values of $(p, q, r)$.

| $p$ | $q$ | $r$ | $p \to q$ | $(p \to q) \to r$ |
|---|---|---|---|---|
| T | T | T | T | T |
| T | T | F | T | F |
| T | F | T | F | T |
| T | F | F | F | T |
| F | T | T | T | T |
| F | T | F | T | F |
| F | F | T | T | T |
| F | F | F | T | F |

*Question.* How many rows are in the truth table, if there are four variables, $p, q, r, s$, in the compound proposition?

**Exercise 2.4.** Construct the truth table for each given compound proposition.

a) $\neg q \to \neg p$
b) $(p \wedge q) \to (p \vee q)$
c) $(p \vee q) \to r$
d) $(\neg p \to q) \wedge (\neg p \to r)$

**Definition.** The compound propositions $p \leftrightarrow q$ (read $p$ *if and only if* $q$, or $p$ *iff* $q$) and $p \oplus q$ (read $p$ *exclusive or* $q$, or $p$ *xor* $q$) are given by their truth tables, respectively, next.

Table 2.4: Truth tables for $p \leftrightarrow q$ and $p \oplus q$.

| $p$ | $q$ | $p \leftrightarrow q$ | $p \oplus q$ |
|---|---|---|---|
| T | T | T | F |
| T | F | F | T |
| F | T | F | T |
| F | F | T | F |

In the English language, the exclusive or is often translated *$p$ or $q$ but not both,* since the table shows that $p \oplus q$ is true when exactly one of them is true, not both. Moreover, a proposition of the form $p \leftrightarrow q$ is called a *biconditional* statement, and is used to connect two statements whose truth values are the same, i.e., $p$ is true if $q$ is true, and $p$ is false if $q$ is false.

Note that these two compound propositions have opposite values for each pair $(p, q)$. To help remember, $p \leftrightarrow q$ is true exclusively when $p$ and $q$ have identical values, whereas $p \oplus q$ is true exactly when $p$ and $q$ have unequal truth values.

**Exercise 2.5.** Suppose that we have the following propositions.

$p$ : It is hot today.
$q$ : It is windy today.
$r$ : It will rain tomorrow.

Translate the following sentences using the variables $p$, $q$, $r$, and the appropriate logic operators.

a) If today is hot and windy, then it will rain tomorrow.
b) Tomorrow will rain if and only if today is not windy.
c) Either today is hot or tomorrow will rain, but not both.
d) If today is neither hot nor windy, then it will not rain tomorrow.

**Exercise 2.6.** Construct the truth table for each given compound proposition.

a) $(p \leftrightarrow q) \wedge (p \oplus q)$
b) $(p \leftrightarrow \neg q) \rightarrow (\neg p \oplus \neg q)$
c) $(p \oplus q) \oplus r$
d) $[(\neg p \wedge q) \vee (\neg r \rightarrow p)] \leftrightarrow (r \oplus \neg q)$

### 2.1.2 Tautology and Contradiction

Consider the compound proposition $(p \wedge q) \rightarrow p$, whose truth table, displayed below, happens to show all true values. This is an example of a tautology.

| $p$ | $q$ | $p \wedge q$ | $(p \wedge q) \rightarrow p$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | T |
| F | T | F | T |
| F | F | F | T |

**Definition.** A *tautology* is a compound proposition whose truth table consists of all true values.

**Test 2.7.** Which one of the following propositions is a tautology?

a) $p \wedge \neg p$
b) $p \to \neg p$
c) $p \leftrightarrow \neg p$
d) $p \oplus \neg p$

**Definition.** The counterpart of a tautology is a *contradiction*, i.e., a compound proposition which shows all false values in the truth table. Incidently, a compound proposition whose table contains a mix of true and false, like most that we have seen thus far, is called a *contingency*.

A ready example of a contradiction is given by $\neg((p \wedge q) \to p)$. (Why?) Quite expectedly, both tautologies and contradictions are rather rare occurrences and, given a random compound proposition, chances are it is a contingency more likely than it is otherwise.

**Test 2.8.** Which one of the following propositions is a contingency?

a) $p \wedge p$
b) $p \to p$
c) $p \leftrightarrow p$
d) $p \oplus p$

**Exercise 2.9.** Identify each compound proposition as a tautology, contradiction, or contingency.

a) $p \to (p \vee q)$
b) $(p \to q) \to q$
c) $(p \leftrightarrow q) \wedge (p \oplus q)$
d) $(p \leftrightarrow \neg q) \to (\neg p \oplus \neg q)$

### 2.1.3 Logical Arguments

In everyday's English we sometimes use the word *argument* to mean a reasoning, or a process of thought based on a set of assumptions from which we derive a conclusion. We consider an argument valid when the conclusion can be proved to be a logically sound consequence of the assumptions, disregarding the truth values of the assumptions themselves. For example, if we assume that all odd numbers are primes, then we may conclude that 15 is prime. Here, the argument is valid—because 15 is an odd number—even though the conclusion is actually false.

**Definition.** By a *premise* we mean a proposition whose value is assumed true. An *argument* is a set of premises $P_1, P_2, \ldots, P_k$, together with another proposition $Q$ which serves as the *conclusion*. The argument is said to be *valid* when the proposition $(P_1 \wedge P_2 \wedge \cdots \wedge P_k) \to Q$ is a tautology.

**Example.** Assume the following two premises.

$P_1$ : Tomorrow is not Friday.
$P_2$ : If today is not Sunday then tomorrow is Friday.

Therefore, we claim the following conclusion.

$Q$ : Today is Sunday.

Is the above argument valid?

*Solution.* Let us fix the following propositions.

$p$ : Today is Sunday.
$q$ : Tomorrow is Friday.

The two premises and the conclusion are then represented by, respectively,

$P_1$ : $\neg q$
$P_2$ : $\neg p \to q$
$Q$ : $p$

We need now study the truth table of the compound proposition

$$(P_1 \wedge P_2) \to Q : (\neg q \wedge (\neg p \to q)) \to p$$

given below.

| $p$ | $q$ | $\neg p$ | $\neg q$ | $\neg p \to q$ | $\neg q \wedge (\neg p \to q)$ | $(\neg q \wedge (\neg p \to q)) \to p$ |
|---|---|---|---|---|---|---|
| T | T | F | F | T | F | T |
| T | F | F | T | T | T | T |
| F | T | T | F | T | F | T |
| F | F | T | T | F | F | T |

The table shows that $(P_1 \wedge P_2) \to Q$ is indeed a tautology, establishing the validity of the argument.

**Example.** Assume that every even number is composite. Can we conclude that all odd numbers are prime?

*Solution.* Let $p$ denote the statement "$n$ is even" and $q$ the statement "$n$ is composite." Note that the premise is given by $p \to q$, and the conclusion $\neg p \to \neg q$. We look at the truth table, and find a contingency. Hence, the argument is not valid.

| $p$ | $q$ | $p \to q$ | $\neg p$ | $\neg q$ | $\neg p \to \neg q$ | $(p \to q) \to (\neg p \to \neg q)$ |
|---|---|---|---|---|---|---|
| T | T | T | F | F | T | T |
| T | F | F | F | T | T | T |
| F | T | T | T | F | F | F |
| F | F | T | T | T | T | T |

**Exercise 2.10.** Determine the validity of each given argument.

a) Premises: Today is not Sunday. Today is Sunday if and only if tomorrow is Tuesday. Conclusion: Tomorrow is not Tuesday.
b) Premises: If you like Discrete Mathematics, you will like Calculus. You like neither Discrete Mathematics nor Calculus. Conclusion: If you like Calculus, you will like Discrete Mathematics.
c) Premises: If $n$ is even then $n$ is composite. If $n$ is prime then $2n+1$ is also prime. Conclusion: If $2n+1$ is composite then either $n$ is prime or odd.
d) Premises: Either prime numbers are infinitely many or composites are, but not both. There are infinitely many primes. If composites are finitely many, so are even numbers. Conclusion: Both composites and even numbers are finitely many.

The following theorem lists a few conditional statements which are rather well-known tautologies. They can be used as models for a valid argument, and are sometimes refered to as *rules of inference.*

**Theorem 2.1.** Each of the following propositions is a tautology.

$$(p \wedge q) \to p \qquad p \to (p \vee q)$$
$$\neg p \to (p \to q) \qquad \neg(p \to q) \to p$$
$$(p \wedge (p \to q)) \to q \qquad (\neg q \wedge (p \to q)) \to \neg p$$
$$(\neg p \wedge (p \vee q)) \to q \qquad ((p \to q) \wedge (q \to r)) \to (p \to r)$$

*Proof.* We leave it to you to explore the truth tables for all the propositions stated above. ▽

**Test 2.11.** Let us agree on three premises: The earth is flat if and only if the moon is. If the earth is not flat, then neither is the sun. But if the sun is flat, so must the moon be. Which one of the following conclusions makes an invalid argument?

a) If the sun is flat, so are the moon and the earth.
b) If the moon is flat, so are the earth and the sun.
c) If the earth is not flat, neither are the sun and the moon.
d) All of the above conclusions are valid.

### 2.1.4 Logical Equivalence

Sometimes it may well be the case that two compound propositions have look-alike truth tables. Can you see, for instance, why the table for $p \oplus q$ is no different that that for $\neg(p \leftrightarrow q)$? Such a relation between two propositions is an important concept and shall be given a special name.

**Definition.** Two propositions are called *equivalent* to each other if their truth tables are identical. We employ the symbol $\equiv$ to denote this relation. Hence, for example, we have $\neg(p \leftrightarrow q) \equiv p \oplus q$.

**Example.** Prove the relation $p \rightarrow q \equiv \neg p \vee q$.

*Solution.* We have to create the two tables and arrive at the same results. To save some space, we will juxtapose the two tables into one as follows.

| $p$ | $q$ | $p \rightarrow q$ | $\neg p$ | $\neg p \vee q$ |
|---|---|---|---|---|
| T | T | T | F | T |
| T | F | F | F | F |
| F | T | T | T | T |
| F | F | T | T | T |

Note that both final columns show identical entries, justifying the equivalence between the two propositions.

**Exercise 2.12.** Verify the equivalence in each of the following statements.

a) $\neg p \wedge q \equiv \neg(p \vee \neg q)$
b) $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
c) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
d) $p \rightarrow (q \rightarrow r) \equiv q \rightarrow (p \rightarrow r)$

**Exercise 2.13.** Prove that all of the following compound propositions are equivalent one to another.

a) $p \rightarrow \neg q$
b) $q \rightarrow \neg p$
c) $\neg p \vee \neg q$
d) $\neg(p \wedge q)$

**Test 2.14.** Which one of the following is *not* equivalent to $p \oplus q$?

a) $p \leftrightarrow \neg q$
b) $\neg p \leftrightarrow q$
c) $\neg p \leftrightarrow \neg q$
d) $\neg p \oplus \neg q$

### 2.1.5 Implication and Its Contrapositive

**Definition.** Given an implication of the form $p \rightarrow q$, we define its *contrapositive* to be the proposition given by $\neg q \rightarrow \neg p$.

**Theorem 2.2.** An implication is always equivalent to its contrapositive.

*Proof.* We show the equivalence $p \to q \equiv \neg q \to \neg p$ by simply producing their respective tables below. $\triangledown$

| $p$ | $q$ | $p \to q$ | $\neg q$ | $\neg p$ | $\neg q \to \neg p$ |
|---|---|---|---|---|---|
| T | T | T | F | F | T |
| T | F | F | T | F | F |
| F | T | T | F | T | T |
| F | F | T | T | T | T |

**Example.** The English sentence "If today is Friday, then tomorrow is Saturday" is in the form of an implication. Convert the sentence using its contrapositive.

*Solution.* Let $p$ represent the statement "Today is Friday" and $q$ "Tomorrow is Saturday." The sentence we wish to convert is represented by $p \to q$. The contrapositive $\neg q \to \neg p$ says "If tomorrow is *not* Saturday, then today is *not* Friday." Can you see that the two sentences are equivalent in their meaning? They say the same thing in two different ways.

**Exercise 2.15.** Rewrite each statement using its contrapositive.

a) Today is Friday, if tomorrow is not Sunday.
b) When $x$ is not an integer, neither is $x^2$.
c) An even number is never a prime.
d) Every mathematician is wealthy.

*Question.* What is the contrapositive of René Descartes's famous philosophical quote "I think, therefore I am" (Cogito ergo sum)?

**Test 2.16.** Which one of the following is equivalent to $\neg q \to p$?

a) $p \to \neg q$
b) $\neg p \to q$
c) $\neg p \to \neg q$
d) $q \to \neg p$

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

For example, the converse of "If today is Friday, then tomorrow is Saturday" is given by "If tomorrow is Saturday, then today is Friday."

**Exercise 2.17.** Write the converse of each statement given in Exercise 2.15.

*Question.* For which truth values of $(p, q)$ can we have $p \to q \equiv q \to p$?

### 2.1.6 Common Equivalence Rules

Equivalence between two compound propositions, in a sense, allows the substitution of one by the other without altering its truth value. The following list contains some of the most common equivalence rules which may come in handy in problem solving.

**Theorem 2.3.** The following equivalence rules hold.

1. $p \wedge q \equiv q \wedge p$
   $p \vee q \equiv q \vee p$
2. $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
   $p \vee (q \vee r) \equiv (p \vee q) \vee r$
3. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
   $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4. $\neg(\neg p) \equiv p$
   $\neg(p \wedge q) \equiv \neg p \vee \neg q$
   $\neg(p \vee q) \equiv \neg p \wedge \neg q$
5. $p \to q \equiv \neg p \vee q$
   $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
   $p \oplus q \equiv \neg(p \leftrightarrow q)$

*Proof.* These results can all be established with the help of truth tables. We omit the proof as an easy exercise. ▽

**Example.** Prove $p \to (q \to r) \equiv q \to (p \to r)$ by applying the above rules.

*Solution.* A series of substitutions takes place as follows.

$$\begin{aligned}
p \to (q \to r) &\equiv p \to (\neg q \vee r) && \text{(Rule 5a)}\\
&\equiv \neg p \vee (\neg q \vee r) && \text{(Rule 5a)}\\
&\equiv (\neg p \vee \neg q) \vee r && \text{(Rule 2b)}\\
&\equiv (\neg q \vee \neg p) \vee r && \text{(Rule 1b)}\\
&\equiv \neg q \vee (\neg p \vee r) && \text{(Rule 2b)}\\
&\equiv q \to (\neg p \vee r) && \text{(Rule 5a)}\\
&\equiv q \to (p \to r) && \text{(Rule 5a)}
\end{aligned}$$

**Exercise 2.18.** Prove by applying equivalence rules.
a) $\neg(p \to q) \equiv p \wedge \neg q$
b) $p \to q \equiv \neg q \to \neg p$
c) $p \to (q \wedge r) \equiv (p \to q) \wedge (p \to r)$
d) $p \oplus q \equiv (p \wedge \neg q) \vee (q \wedge \neg p)$

**Exercise 2.19.** Some of the following statements are false. Determine the validity of each one, using any method you prefer.
a) $p \to (q \to r) \equiv (p \to q) \to r$
b) $p \to (q \vee r) \equiv (p \to q) \vee (p \to r)$
c) $p \vee (q \oplus r) \equiv (p \vee q) \oplus (p \vee r)$
d) $\neg(p \oplus q) \equiv \neg p \leftrightarrow \neg q$

### 2.1.7 CNF and DNF

We have seen that a logic operator, such as $p \to q$, is defined by its truth table. In other words, a different table gives a different logic operator.

*Question.* How many different logic operators involving $p$ and $q$ are possible?

There is no doubt, however, that some of these operators are actually interchangeable via certain equivalence rules and hence not all of them are quite necessary to have. The next theorem, in fact, claims that every compound proposition can eventually be written using only conjunctions, disjunctions, and negations!

**Definition.** By a *conjunctive normal form*, or *CNF,* we mean a series of conjunctions operating on any number of compound propositions, each of which is the disjunctions of propositional variables or their negations. An example of a CNF involving three variables $p, q, r$, is

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

Similarly, we define a *disjunctive normal form*, or *DNF,* by reversing the roles of disjunction and conjunction in the CNF definition. Thus an example of a DNF with four variables could be

$$(p \wedge q \wedge \neg r \wedge s) \vee (p \wedge \neg q \wedge r \wedge \neg s) \vee (\neg p \wedge \neg q \wedge \neg r \wedge s)$$

Note that there is no limit to the number of variables nor to the number of brackets involved. A *normal form* refers to either a CNF or a DNF.

**Theorem 2.4.** Every compound proposition is equivalent to a CNF and to a DNF.

We will not formally prove this theorem. Instead, the next two examples will illustrate how and why the theorem works.

**Example.** Convert the given proposition below to a CNF and to a DNF.

$$(p \leftrightarrow q) \to (p \oplus q)$$

*Solution.* The first step is to construct the truth table, labeling the rows 1 to 4:

| | $p$ | $q$ | $p \leftrightarrow q$ | $p \oplus q$ | $(p \leftrightarrow q) \to (p \oplus q)$ |
|---|---|---|---|---|---|
| 1 | T | T | T | F | F |
| 2 | T | F | F | T | T |
| 3 | F | T | F | T | T |
| 4 | F | F | T | F | F |

The rows with *false* values, i.e., rows 1 and 4, will give us a CNF of two brackets, where the two variables $p$ and $q$ are negated if necessary, such that both values are *false* at each corresponding row:

$$\begin{aligned}(p \leftrightarrow q) \rightarrow (p \oplus q) &\equiv (\text{row } 1) \wedge (\text{row } 4) \\ &\equiv (\neg p \vee \neg q) \wedge (p \vee q) \qquad \text{(CNF)}\end{aligned}$$

But why is this algorithm correct? To justify the equivalence, simply verify that this CNF gives F T T F in its truth table. Without actually displaying the table, note that row 1 will be false because the first bracket is false (disjunction of two false propositions). In the same way, row 4 will be false since the second bracket is false. For the unselected rows 2 and 3, each bracket will be true since one of the two variables must be true (by design, both can be false simultaneously *only* in rows 1 or 4) so that the resulting conjunction is also true.

Similarly for DNF we select the *true* rows, and this time we want the variables to be *true* as well:

$$\begin{aligned}(p \leftrightarrow q) \rightarrow (p \oplus q) &\equiv (\text{row } 2) \vee (\text{row } 3) \\ &\equiv (p \wedge \neg q) \vee (\neg p \wedge q) \qquad \text{(DNF)}\end{aligned}$$

**Example.** For a second illustration, suppose that a compound proposition $X$ of three variables generates a truth table as given below. Convert the proposition $X$ to a CNF and to a DNF.

| | $p$ | $q$ | $r$ | $\cdots$ | $X$ |
|---|---|---|---|---|---|
| 1 | T | T | T | $\cdots$ | T |
| 2 | T | T | F | $\cdots$ | T |
| 3 | T | F | T | $\cdots$ | F |
| 4 | T | F | F | $\cdots$ | F |
| 5 | F | T | T | $\cdots$ | T |
| 6 | F | T | F | $\cdots$ | T |
| 7 | F | F | T | $\cdots$ | T |
| 8 | F | F | F | $\cdots$ | F |

*Solution.* For the CNF we take the false rows 3, 4, and 8. The variables $p, q, r$ will not be negated if already false:

$$\begin{aligned}X &\equiv (\text{row } 3) \wedge (\text{row } 4) \wedge (\text{row } 8) \\ &\equiv (\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee q \vee r) \qquad \text{(CNF)}\end{aligned}$$

We leave it to you to write down the DNF based on the remaining five rows.

**Exercise 2.20.** Convert to a CNF and to a DNF.

a) $\neg(p \wedge q) \to p$
b) $(p \oplus \neg q) \leftrightarrow (\neg p \vee q)$
c) $(p \to q) \to r$
d) $((p \wedge q) \to r) \oplus (\neg p \vee (q \leftrightarrow r))$

*Question.* Given a CNF, how can we quickly convert it to a DNF, or vice versa? Do we really need to construct the truth table?

**Test 2.21.** Convert the CNF $(p \vee \neg q) \wedge (\neg p \vee \neg q)$ to a DNF.

a) $(\neg p \wedge q) \vee (p \wedge q)$
b) $(\neg p \wedge q) \vee (\neg p \wedge \neg q)$
c) $(p \wedge \neg q) \vee (p \wedge q)$
d) $(p \wedge \neg q) \vee (\neg p \wedge \neg q)$

## 2.2 Introduction to Sets

The word set loosely means a collection or group of objects. In the present context, however, we shall define this term more restrictively as follows.

**Definition.** A *set* is a collection of any objects in which ordering and repetition of its members are ignored. The objects which make up the members of the set are called the *elements* of the set.

We assume the common notation of a set using a pair of braces and of membership using $\in$, e.g., $S = \{a, e, i\}$ represents the set $S$ whose elements are the first three vowels of the English alphabet: $a, e, i$. Of this example we may state that $a \in S$, whereas $u \notin S$. Note that the sets $\{a, e, i\}$ and $\{i, e, a\}$, as well as $\{a, i, a, e, a, e\}$ are to be treated as identical by our definition. More precisely,

**Definition.** Two sets $A$ and $B$ are identical, in which case we write $A = B$, when the following proposition holds for every element $x$.

$$x \in A \leftrightarrow x \in B$$

Having agreed on this, henceforth we shall use the following notation for some very common number sets.

$\mathbb{Z}$ the set of integers
$\mathbb{N}$ the set of positive integers
$\mathbb{Q}$ the set of rational numbers
$\mathbb{R}$ the set of real numbers

It is convenient, for instance, to simply write $\mathbb{N}$, which invariably refers to the set $\{1, 2, 3, \ldots\}$ throughout this text, rather than the phrase "the set of positive integers" or "the set of natural numbers."

If $A$ is a given set and $P(x)$ is a statement whose truth value shall be determined by the variable $x$, we may at times have a set $S$ whose elements are given implicitly in the following *set-builder notation.*

$$S = \{x \in A \mid P(x)\}$$

This is to mean that $a \in S$ if and only if $a \in A$ and for which $P(a)$ is true. If, however, the property that $x \in A$ is already implied in the statement $P(x)$, then we may just write $S = \{x \mid P(x)\}$. Hence, for example, the set of even numbers can be written as $\{x \in \mathbb{Z} \mid x \bmod 2 = 0\}$. Similarly, we have $\{x \in \mathbb{Z} \mid x > 0\} = \mathbb{N}$.

*Question.* What are the elements in the set $\{x \in \mathbb{R} \mid x^2 + 1 = 0\}$?

**Exercise 2.22.** Describe each set given below; they are all familiar number sets.

a) $\{x \in \mathbb{Z} \mid x \bmod 2 = 1\}$
b) $\{x \in \mathbb{Q} \mid x/2 \in \mathbb{Z}\}$
c) $\{a/b \mid a \in \mathbb{Z} \wedge b \in \mathbb{N}\}$
d) $\{x \in \mathbb{R} \mid nx \notin \mathbb{Z} \text{ for all } n \in \mathbb{Z}\}$

A set is allowed to be empty, that is, to have no elements whatsoever in it. We reserve the notation $\emptyset$ (read *phi*) to always denote the empty set, as far as set theory is concerned. Thus, $\emptyset = \{\ \}$.

*Question.* Is it true that $\{\emptyset\} = \emptyset$?

**Test 2.23.** Which one of the following sets is *not* empty?

a) $\{x \in \mathbb{Z} \mid x \bmod 2 = 2\}$
b) $\{x \in \mathbb{Q} \mid x^2 = 2\}$
c) $\{x \in \mathbb{R} \mid x^2 = -1\}$
d) $\{x \in \mathbb{R} \mid x^2 < x\}$

### 2.2.1 Set Operators

Two sets can be operated on and yield a new set, in ways which resemble the logical operations on two propositions that we have learned in the previous section. We introduce the first four of such operators in the next definition.

**Definition.** Let $A$ and $B$ be any two sets. The operations *union* $A \cup B$, *intersection* $A \cap B$, *difference* $A - B$, and *symmetric difference* $A \oplus B$ are given by their set-builder notation, respectively, as follows.

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$
$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$
$$A - B = \{x \mid x \in A \wedge x \notin B\}$$
$$A \oplus B = \{x \mid x \in A \oplus x \in B\}$$

Note that the set operator symmetric difference in $A \oplus B$ is given by the logical operator exclusive or, appearing in the statement $x \in A \oplus x \in B$—the same notation, and essentially the same operation, with two different names, one applying for sets and the other for propositions.

**Example.** Let $A = \{1, 3, 5, 7\}, B = \{0, 1, 2, 3\}$, and $C = \{0, 2\}$. Determine the output of each set operation given below.

a) $A \cup B, A \cup C, B \cup C$
b) $A \cap B, A \cap C, B \cap C$
c) $A - B, A - C, B - C$
d) $A \oplus B, A \oplus C, B \oplus C$

*Solution.* We refer to the four definitions given above.

a) By definition, $x \in A \cup B$ if and only if $x \in \{1, 3, 5, 7\}$ or $x \in \{0, 1, 2, 3\}$. For this to hold, $x$ can be any one of the elements in either set. Hence, $A \cup B = \{0, 1, 2, 3, 5, 7\}$. Similarly, $A \cup C = \{0, 1, 2, 3, 5, 7\}$ and $B \cup C = \{0, 1, 2, 3\} = B$.
b) Since $x \in A \wedge x \in B$ is true if only if $x$ is a common element of $A$ and $B$, then we have $A \cap B = \{1, 3\}$. Similarly, $A \cap C = \emptyset$ and $B \cap C = C$.
c) Of the elements in $A = \{1, 3, 5, 7\}$, only 5 and 7 do not belong to $B$. Hence, $A - B = \{5, 7\}$. Similarly, $A - C = A$ and $B - C = \{1, 3\}$.
d) Note that $x \in \{1, 3, 5, 7\} \oplus x \in \{0, 1, 2, 3\}$ is true exactly when $x$ belongs to one, but not both, of the two sets. So we have $A \oplus B = \{0, 2, 5, 7\}$. Similarly, $A \oplus C = \{0, 1, 2, 3, 5, 7\}$ and $B \oplus C = \{1, 3\}$.

*Question.* Is it true that $A \cup B = B \cup A$? What about $\cap$, or $-$, or $\oplus$?

**Exercise 2.24.** Let $A = \{x \in \mathbb{Z} \mid 3 < x < 9\}$, $B = \{0, 2, 4, 6, 8\}$, and $C = \{x \in A \mid x \bmod 2 = 1\}$. In the following set operations, write out the elements of each resulting set.

a) $(A - B) \cup (A \cap C)$
b) $(A \cap B) \oplus (B \cup C)$
c) $(C \oplus B) - B$
d) $C - (A \oplus C)$

**Exercise 2.25.** Let $A$ be any given set. Describe the sets given below.
a) $A \cup A$
b) $A \cap A$
c) $A - A$
d) $A \oplus A$

**Definition.** When $A \cap B = \emptyset$, we say that the two sets $A$ and $B$ are *disjoint*.

**Example.** Explain why $A \oplus B = A \cup B$ if $A$ and $B$ are disjoint sets.

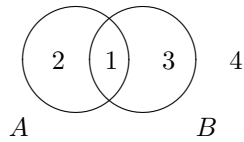
*Solution.* We have $x \in A \oplus B$ exactly when $x$ belongs to $A$ or $B$ but not both. The "both" part may be ignored, since $A \cap B$ is empty in this case. Therefore, $A \oplus B = A \cup B$.

*Question.* Is it possible to have $A \oplus B = A \cup B$ if $A$ and $B$ are *not* disjoint?

**Test 2.26.** Suppose that $A$ and $B$ are disjoint sets. Which one of the following set identities is true?
a) $A - B = A$
b) $A - B = B$
c) $A \cup B = A$
d) $A \cup B = B$

### 2.2.2 Venn Diagrams and Set Identities

Venn diagrams are a great tool for describing set operations, in much the same way truth tables are for logical operations. Here the set $A$ is represented by a circle, the region inside of which is where the elements of $A$ reside. If $A$ and $B$ are two sets, then, there are four partitioned regions which we label 1, 2, 3, 4 in the drawing below.




*Question.* How would you draw the Venn diagram in the special case where $A$ and $B$ are disjoint?

Now if we associate two propositions with these two sets,

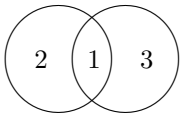
$$p: \quad x \in A$$
$$q: \quad x \in B$$

then we see that the four labels respectively correspond to the four rows of $(p, q)$ values in the following truth table.

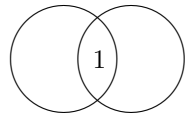
| | | | $A \cup B$ | $A \cap B$ | $A - B$ | $A \oplus B$ |
|---|---|---|---|---|---|---|
| | $p$ | $q$ | $p \vee q$ | $p \wedge q$ | $p \wedge \neg q$ | $p \oplus q$ |
| 1 | T | T | T | T | F | F |
| 2 | T | F | T | F | T | T |
| 3 | F | T | T | F | F | T |
| 4 | F | F | F | F | F | F |

*Question.* How would you draw the Venn diagram for three sets $A, B, C$, associated with the three propositions $p, q, r$, in the truth table?

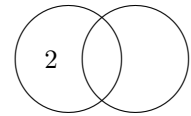
Note that the table includes the truth values of the four set operations $\cup, \cap, -$, and $\oplus$. These give their Venn diagrams below, showing the regions where each resulting set contains its elements, i.e., where the truth value is true.



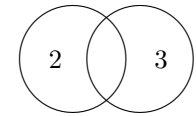

$A \cup B$




$A \cap B$




$A - B$




$A \oplus B$

With Venn diagrams, we are able to give intuitive proofs to certain set identities. It is convincing enough, for instance, to deduce that $(A - B) \cup (A \cap B) = A$ since both consist of regions 1 and 2 in the diagrams. The next theorem is another example.

**Theorem 2.5.** Let $A$ and $B$ be any two sets. Then

$$A \oplus B = (A - B) \cup (B - A)$$

*Proof.* The proof is an easy visualization with Venn diagrams. Or, if you prefer truth tables to Venn diagrams, we may let $p : x \in A$ and $q : x \in B$ as before, and note that $(A - B) \cup (B - A)$ is given by the proposition $(p \wedge \neg q) \vee (q \wedge \neg p)$. The truth table below show that $(p \wedge \neg q) \vee (q \wedge \neg p) \equiv p \oplus q$, which defines the set $A \oplus B$. $\bigtriangledown$

| $p$ | $q$ | $\neg p$ | $\neg q$ | $p \wedge \neg q$ | $q \wedge \neg p$ | $(p \wedge \neg q) \vee (q \wedge \neg p)$ |
|---|---|---|---|---|---|---|
| T | T | F | F | F | F | F |
| T | F | F | T | T | F | T |
| F | T | T | F | F | T | T |
| F | F | T | T | F | F | F |

**Exercise 2.27.** Use truth table to establish the set identity

$$A \oplus B = (A \cup B) - (A \cap B)$$

**Exercise 2.28.** Use Venn diagrams to find the resulting set identical to each one given below.

a) $(A \cap B) \oplus (A - B)$
b) $(A - (A - B)) \oplus B$
c) $(A \cup B) \oplus (A \cap B)$
d) $(A \cup B) \oplus (A \oplus B)$

We have seen that set operations closely resemble logical operations. To make the analogy more complete, we define the negation of a set as follows.

**Definition.** Let the set $A$ be understood to be part of a larger universal set $U$. Then by the *complement* of $A$ we mean the set $\neg A = U - A$. For example, if $A$ is the set of even numbers, an appropriate choice of $U$ could be $U = \mathbb{Z}$. In that case, the negation of $A$ is given by $\neg A = \mathbb{Z} - A$, that is, the set of odd numbers.

With that, we are ready to state the following analog of logical equivalence rules for sets.

**Theorem 2.6.** The following set identities hold.

1. $A \cap B \equiv B \cap A$
   $A \cup B \equiv B \cup A$
2. $A \cap (B \cap C) \equiv (A \cap B) \cap C$
   $A \cup (B \cup C) \equiv (A \cup B) \cup C$
3. $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$
   $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$
4. $\neg(\neg A) \equiv A$
   $\neg(A \cap B) \equiv \neg A \cup \neg B$
   $\neg(A \cup B) \equiv \neg A \cap \neg B$
5. $A \cap A = \emptyset$
   $A \cup A = A$
   $A - A = \emptyset$
   $A \oplus A = \emptyset$

*Proof.* We may translate the identities using the language of logical operators, and the proof is a simple checking of truth tables. ▽

### 2.2.3 Power Sets and Direct Product

The concept of a set being part of another, bigger set is a useful set relation. We shall call the smaller set a subset of the bigger. More precisely,

**Definition.** A set $A$ is a *subset* of a set $B$, denoted by $A \subseteq B$, when the following proposition holds for every element $x$.

$$x \in A \to x \in B$$

This definition simply says that $A \subseteq B$ exactly when the set $A$ is contained in the set $B$, in the sense that every element of $A$ also belongs to $B$. For example, $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.

*Question.* How would you draw the Venn diagram in order to show the relation $A \subseteq B$?

**Test 2.29.** For arbitrary sets $A$ and $B$, which proposition is false?

a) $A - B \subseteq A \cup B$
b) $A - B \subseteq A \oplus B$
c) $A \cap B \subseteq A \oplus B$
d) $A \oplus B \subseteq A \cup B$

**Test 2.30.** Suppose that $A \subseteq B$. Which one of the following sets is necessarily empty?

a) $A \cup B$
b) $A \cap B$
c) $A - B$
d) $A \oplus B$

**Exercise 2.31.** Suppose that $A \subseteq B$ and $B \subseteq C$. Explain logically why we then have $A \subseteq C$.

Note that by the definition of the operator if-then, both the relations $A \subseteq A$ and $\emptyset \subseteq A$ are always true, for any set $A$.

*Question.* Is it true that $\emptyset \subseteq \emptyset$?

**Theorem 2.7.** Let $A$ and $B$ be any two sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

*Proof.* Assume first that $A = B$. Then the only-if statement reduces to $A \subseteq A$, which is true. Conversely, assume that $A \subseteq B$ and $B \subseteq A$ both hold. By the definition of subset, if $x \in A$ then $x \in B$, and vice versa. It follows that $x \in A \leftrightarrow x \in B$, hence $A = B$. $\bigtriangledown$

**Example.** Suppose that $A \cap B = \emptyset$. Use Theorem 2.7 to prove that $A \oplus B = A \cup B$.

*Solution.* It is clear that, in general, $A \oplus B \subseteq A \cup B$. Hence, it suffices to show that $A \cup B \subseteq A \oplus B$. Let $x \in A \cup B$. Then either $x \in A$ or $x \in B$, but not both since $A$ and $B$ are disjoint. Hence, $x \in A \oplus B$. This shows that $A \cup B \subseteq A \oplus B$, and consequently $A \oplus B = A \cup B$.

**Exercise* 2.32.** Suppose that $A \subseteq B$. Use Theorem 2.7 to prove that $A \oplus B = B - A$.

**Definition.** If $A$ is a set, the *power set* of $A$, denoted by $P(A)$, is the set consisting of all the subsets of $A$, i.e., $P(A) = \{S \mid S \subseteq A\}$.

Note that this is the first time we introduce a set whose elements are again sets.

**Example.** Find $P(A)$ for the set $A = \{1, 2\}$.

*Solution.* We first identify all the subsets of $A$—there are four of them, i.e., $\{1\}$, $\{2\}$, and $A = \{1, 2\}$ and $\emptyset$. Hence, $P(\{1, 2\}) = \{\{1\}, \{2\}, \{1, 2\}, \emptyset\}$.

**Exercise 2.33.** Find $P(A)$.

a) $A = \{a, b, c\}$
b) $A = \{2, 3, 4, 5\}$
c) $A = \emptyset$
d) $A = \{x, \{7\}\}$

*Question.* Is it true that $P(\emptyset) = \emptyset$?

Having done the last exercise, you may have deduced the result of the next theorem, which explains why the name *power* set.

**Theorem 2.8.** If a set $A$ consists of $n$ elements, then $A$ has exactly $2^n$ subsets, i.e., $P(A)$ is a set of $2^n$ elements.

*Proof.* Let $A = \{a_1, a_2, \ldots, a_n\}$. A subset $S \subseteq A$ can be represented by $\{s_1, s_2 \ldots, s_n\}$, where $s_i = 0$ if $a_i \notin S$ and $s_i = 1$ if $a_i \in S$. It is then clear that there are $2^n$ possible representations, hence that many subsets of $A$. $\bigtriangledown$

**Definition.** The *cardinality* of a set $A$, denoted by $|A|$, is the number of elements in $A$, if finite.

Hence for example, $|\{a, b, c\}| = 3$ and $|\emptyset| = 0$. With this new notation we may rewrite Theorem 2.8 using the following proposition.

$$|A| = n \rightarrow |P(A)| = 2^n$$

**Exercise 2.34.** Evaluate $|P(A)|$.

a) $A = \{1, 2, 3, 4\} \cup \{3, 4, 5, 6\}$
b) $A = \{1, 2, 3, 4\} \oplus \{3, 4, 5, 6\}$
c) $A = P(\emptyset)$
d) $A = P(P(\emptyset))$

*Question.* What are the elements of the set $P(P(P(\emptyset)))$?

**Definition.** If $A$ and $B$ are two given sets, the *direct product* $A \times B$, read *$A$ cross $B$*, is defined by $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.

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

$$A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$$
$$B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2)\}$$

**Test 2.35.** With $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5\}$, what is $|P(A \times B)|$?

a) 32
b) 64
c) 128
d) 4096

*Question.* Is it true that $\emptyset \times \emptyset = \emptyset$?

Note that an element of the form $(a, b)$ is treated as an ordered pair, e.g., $(1, 4) \neq (4, 1)$—just like what we have in the Cartesian coordinate system. Hence, in general, we have $A \times B \neq B \times A$.

**Exercise* 2.36.** Is it possible to have $A \times B = B \times A$ sometimes? Think of an example, other than $A = B$, or explain why it is not possible.

**Exercise 2.37.** For each claim below, investigate true or false.

a) $|A \times B| = |B \times A|$
b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
c) $P(A \times B) = P(A) \times P(B)$
d) $|P(A \times B)| = |P(A) \times P(B)|$

**Theorem 2.9.** If $|A| = m$ and $|B| = n$, then $|A \times B| = mn$.

*Proof.* An element $(a, b) \in A \times B$ can be selected from any one of the $m$ elements in $A$, for $a$, and from $n$ choices for $b$. Hence there are exactly $mn$ such ordered pairs. ▽

## 2.3 Techniques of Proof

Proving a mathematical statement is an art of writing. There is no strict convention as to how a proof should look like. However, there are commonly accepted methods of proof which follow certain laws of logic. We look into a few of these methods, trying wherever possible to communicate in the language of propositions as we have learned it in this chapter.

### 2.3.1 Direct Proof and Contrapositive

Recall the definitions of even and odd numbers given at the beginning of Chapter 1. We will use these numbers to illustrate our first proof technique, called *direct proof*. The technique of direct proof applies to statements in the form of an implication $p \to q$. It begins by assuming $p$ and shows, through a succession of implications, that $q$ inevitably follows.

**Example.** Prove that if $x$ is even then $x^2$ is also even.

*Solution.* If we let $p$ denote the statement "$x$ is even" and $q$ the statement "$x^2$ is even," then we are to prove the proposition $p \to q$.

$$
\begin{aligned}
&p : x \text{ is even} \\
&\quad \to x = 2n \text{ for some } n \in \mathbb{Z} && \text{(definition of even numbers)} \\
&\quad \to x^2 = 4n^2 && \text{(by squaring both sides)} \\
&\quad \to x^2 = 2(2n^2) \\
&\quad \to x^2 = 2m \text{ where } m = 2n^2 \in \mathbb{Z} && \text{(since } n \text{ is integer)} \\
&\quad \to x^2 \text{ is even} : q && \text{(by definition)}
\end{aligned}
$$

**Example.** Prove that the product of two odd numbers is again odd.

*Solution.* This statement does not look like an implication, but it really is. Simply let $p : x$ and $y$ are odd and $q : xy$ is odd. The proposition to be proved is essentially $p \to q$.

$$
\begin{aligned}
&p : x \text{ and } y \text{ are odd} \\
&\quad \to x = 2n + 1 \text{ and } y = 2m + 1 \text{ with both } m, n \in \mathbb{Z} \\
&\quad \to xy = (2n + 1)(2m + 1) \\
&\quad \to xy = 4nm + 2n + 2m + 1 \\
&\quad \to xy = 2(2nm + n + m) + 1 \\
&\quad \to xy = 2k + 1 \text{ where } k = 2nm + n + m \in \mathbb{Z} \\
&\quad \to xy \text{ is odd} : q
\end{aligned}
$$

*Question.* Is it wrong if we let $x = 2n + 1$ and $y = 2n + 1$ in the above?

**Exercise 2.38.** Prove the following statements using direct proof.

a) If $x$ is odd, then $x^3$ is also odd.
b) If $x$ is even, then so is $x^2 - 4x + 2$.
c) The sum of two odd numbers is even.
d) The sum of two rational numbers is again rational.

There are times when direct proof may not be the easiest way to establish $p \to q$. In such cases, the contrapositive of this implication is often a useful substitute for the statement before we attempt to prove it. If you recall, Theorem 2.2 states that

$$p \to q \equiv \neg q \to \neg p$$

**Example.** Let $x$ be an integer. Prove that if $x^2$ is even then so is $x$.

*Solution.* As before, we let $p : x^2$ is even and $q : x$ is even. We wish to prove the validity of $p \to q$. Direct proof would start with $x^2 = 2n$ and have us show that $x = \sqrt{2n}$ is twice an integer. That would be hard. To circumvent this difficulty, we shall instead prove the equivalent statement $\neg q \to \neg p$.

$$\begin{aligned}
&\neg q : x \text{ is odd} \qquad (\text{the integer } x \text{ is } \textit{not} \text{ even}) \\
&\quad \to x = 2n + 1 \text{ for some } n \in \mathbb{Z} \\
&\quad \to x^2 = 4n^2 + 4n + 1 \\
&\quad \to x^2 = 2(2n^2 + 2n) + 1 \\
&\quad \to x^2 = 2m + 1 \text{ where } m = 2n^2 + 2n \in \mathbb{Z} \\
&\quad \to x^2 \text{ is odd} : \neg p
\end{aligned}$$

At this point it is appropriate to remark that writing a mathematical proof need not be so formal as to represent every statement using $p$ and $q$. The next example is simply meant to show how our writing style can be more casual for the sake of better readability.

**Example.** Prove that if $2n$ is an irrational number, then $n$ is too.

*Solution.* We use contrapositive. Suppose that $n$ is rational. We may write $n = a/b$ for some integers $a, b$. Then $2n = 2a/b$, which shows that $2n$ is also a rational number. This completes the proof.

**Exercise 2.39.** Prove the following statements using contrapositive.

a) If $x^3$ is odd, then $x$ is also odd.
b) If $x^2 - 3$ is irrational, so is $x - 3$.
c) If the sum of two integers is odd, then one of them is odd.
d) If the product of two integers is even, then one of them is even.

*Question.* How can one solve Exercise 2.39(d) using direct proof, instead of contrapositive, plus the fact that 2 is prime?

**Exercise 2.40.** If $x$ is odd, then $x^2 - 1$ is divisible by 8. Elias proved this statement as follows. If $x$ is even, then $x = 2n$. And therefore $x^2 - 1 = 4n^2 - 1$ is an odd number, not divisible by 8. Please explain to Elias why his proof is fundamentally wrong, then write the correct proof.

**Exercise* 2.41.** Explain why, if $p > 2$ is a prime number, then $p$ is odd. Then use this knowledge to prove that if $p \bmod 3 = 1$, then $p \bmod 6 = 1$.

### 2.3.2 Proof by Cases

Consider the following proof problem and its solution.

**Example.** Prove that the quantity $x^2 - 3x + 2$ is even for any $x \in \mathbb{Z}$.

*Solution.* Let $p : x \in \mathbb{Z}$ and $q : x^2 - 3x + 2$ is even. We consider two cases: $x$ is even and $x$ is odd.

1. Let $p_1 : x$ is even. We shall establish $p_1 \to q$ using direct proof. Let $x = 2n$ with $n\mathbb{Z}$. Then $x^2 - 3x + 2 = 4n^2 - 6n + 2 = 2m$, where $m = 2n^2 - 3n + 1 \in \mathbb{Z}$. Hence, $x^2 - 3x + 2$ is even.

2. Let $p_2 : x$ is odd. We will also prove $p_2 \to q$. Let $x = 2n + 1$ for some $n \in \mathbb{Z}$. Then $x^2 - 3x + 2 = 4n^2 - 2n = 2m$, where $m = 2n^2 - n \in \mathbb{Z}$. It follows that $x^2 - 3x + 2$ is even.

Since every integer is either even or odd, we have actually proved that $p \to q$.

This example illustrates the method of *proof by cases*. In this instance we have $p \equiv p_1 \vee p_2$, which enables us to substitute $p \to q$ by the proposition $(p_1 \to q) \wedge (p_2 \to q)$. Logically speaking, this is justified by the equivalence

$$(p_1 \vee p_2) \to q \equiv (p_1 \to q) \wedge (p_2 \to q)$$

Of course, there are times when $p$ more conveniently breaks down to three or more cases, instead of just two, like in the next example.

**Example.** Prove that every odd number $x$ can be written either in the form $x = 4n + 1$ or $x = 4n + 3$.

*Solution.* By Theorem 1.1, we have $0 \leq x \bmod 4 \leq 3$. This gives four possible cases, i.e., $x = 4n$, $x = 4n+1$, $x = 4n+2$, and $x = 4n+3$, for some $n \in \mathbb{Z}$. The first case and the third case apply to an even number $x$. Hence if $x$ is odd, then either $x = 4n + 1$ or $x = 4n + 3$.

**Exercise 2.42.** Use proof by cases to establish each claim below.

a) The number $x^2 + x$ is even for all integers $x$.
b) For any $x \in \mathbb{Z}$, the number $x^2 + 2$ is not a multiple of 4.
c) If $x \in \mathbb{Z}$ then $x^3 - x$ is a multiple of 3. (Hint: consider $x \bmod 3 = 0, 1, 2$.)
d) For any two real numbers, we have $|xy| = |x|\ |y|$. (Hint: consider the four cases where $x < 0$ or $x \geq 0$, and for $y$ similarly.)

**Exercise* 2.43.** Prove that every prime number $p > 3$ can be written in the form $p = 6n \pm 1$.

### 2.3.3 Proving Equivalence

Proving an equivalence means proving a biconditional statement $p \leftrightarrow q$. Since we have the established fact that

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

then in order to assert $p \leftrightarrow q$, it suffices to prove both $p \to q$ and $q \to p$.

**Example.** Prove that an integer $x$ is even if and only if $x^2$ is even.

*Solution.* We are to prove $p \leftrightarrow q$, where $p : x$ is even and $q : x^2$ is even. Both parts, proving $p \to q$ and $q \to p$, have been demonstrated as the examples of Section 2.3.1. In particular, establishing $q \to p$ in this case is best done via contrapositive.

As a second example, this time without explicitly stating the propositions in terms of $p$ and $q$, we state a useful theorem concerning the congruence $a \equiv b \pmod{n}$, which means that $a \bmod n = b \bmod n$. (See Section 1.2.1.)

**Theorem 2.10.** Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $a \equiv b \pmod{n}$ if and only if $n$ divides $a - b$.

*Proof.* We note that, by definition, $a \bmod n = a - \lfloor \frac{a}{n} \rfloor n$ and quite similarly, $b \bmod n = b - \lfloor \frac{b}{n} \rfloor n$. It follows that

$$a \bmod n - b \bmod n = a - b - \left( \lfloor \tfrac{a}{n} \rfloor - \lfloor \tfrac{b}{n} \rfloor \right) n \tag{2.1}$$

Hence, if $a \bmod n = b \bmod n$ then $a - b = \left( \lfloor \frac{a}{n} \rfloor - \lfloor \frac{b}{n} \rfloor \right) n$, which is a multiple of $n$ since the floor function is integer valued.

Conversely, assume that $n$ divides $a - b$. By Theorem 1.2, (2.1) implies that $n$ also divides $a \bmod n - b \bmod n$. But from Theorem 1.1, we know that the value of a remainder mod $n$ is between 0 and $n - 1$, inclusive. Hence, $-n < a \bmod n - b \bmod n < n$, and so to be divisible by $n$, we must have $a \bmod n - b \bmod n = 0$. That gives $a \bmod n = b \bmod n$. ▽

*Question.* What exactly is meant by the word *conversely*?

**Exercise 2.44.** Prove the following biconditional statements.

a) The number $x^2 - 4x + 2$ is odd if and only if $x$ is.
b) The product of two numbers is odd if and only if both of them are.
c) The product of two integers is divisible by 5 if and only if one of them is.
d) The sum of two integers is odd if and only if one of them is odd and the other even.

Another example, involving sets, is even more subtle in the only-if part of the proof. Note that by contrapositive, in order to establish $p \leftrightarrow q$, we may simply prove "if $p$ is true then $q$ is true" and "if $p$ is false then $q$ is false." Moreover, $p \leftrightarrow q$ may well be replaced by $q \leftrightarrow p$.

**Example.** Suppose that $A$ and $B$ are two arbitrary non-empty sets. Prove that $A \times B = B \times A$ if and only if $A = B$.

*Solution.* The case $A = B$ is trivial. Suppose now $A \neq B$. We may assume, *without loss of generality,* that there exists $x \in A - B$. (If this assumption turns false, then there is $x \in B - A$, and we simply exchange the roles of $A$ and $B$.) This will give an element $(x, y) \in A \times B$ such that $(x, y) \notin B \times A$, implying that $A \times B \neq B \times A$.

**Exercise 2.45.** With sets, prove that $A \oplus B = B - A$ if and only if $A \subseteq B$.

**Exercise* 2.46.** Let both $m, n \in \mathbb{N}$. Show that $\gcd(m, n) = \text{lcm}(m, n)$ if and only if $m = n$.

### 2.3.4 Proof by Contradiction

There are times when proving the validity of a proposition $p$ is difficult, whereas verifying the absurdity of $\neg p$ is not as hard. This is an acceptable alternative proof technique, called *proof by contradiction.* As a first example, we demonstrate that the number $\sqrt{2}$ is irrational, thus keeping our promise made at the beginning of Chapter 1.

**Example.** Prove that the number $\sqrt{2}$ is irrational.

*Solution.* We will show that the negated statement "The number $\sqrt{2}$ is rational" is absurd, so we may conclude that the statement "The number $\sqrt{2}$ is irrational" is true.

Suppose that $\sqrt{2} \in \mathbb{Q}$. Then we may write $\sqrt{2} = a/b$, where $a, b \in \mathbb{Z}$ with no common factor except 1. Then $2 = a^2/b^2$, that is, $2b^2 = a^2$. It follows that the number $a^2$ is even, hence $a$ is even. (Remember?) We now write $a = 2c$ for some $c \in \mathbb{Z}$. Substituting, we get $2b^2 = 4c^2$, which simplifies to $b^2 = 2c^2$. By similar reasoning, we see that $b$ is as well even. This is absurd (a contradiction) since now $a$ and $b$ have 2 as a common factor, contradicting our assertion earlier that they have no common factor.

**Exercise 2.47.** Prove the following claims by way of contradiction.

a) The number $\sqrt[3]{3}$ is irrational.
b) The number $\sqrt[n]{p}$ is irrational when $p$ is prime and $n \geq 2$.
c) The number $\log_{10} 2$ is irrational.

d) The sum of an irrational number and a rational is irrational.

*Question.* Is the sum of two irrational numbers again irrational?

Proof by contrapositive is really a form of contradiction. Suppose that we are to prove the compound statement $p \to q$. We assume, as in direct proof, that $p$ holds and try to show that $q$ must follow. Instead, we demonstrate why $\neg q$ is absurd (proof by contradiction) by showing that $\neg q \to \neg p$ (proof by contrapositive). And since $\neg p$ and $p$ cannot both be true, we arrive at the desired contradiction.

**Exercise 2.48.** Show that if $a$ and $b$ are odd, then $x^2 = a^2 + b^2$ has no integer solution.

As a second example, we present again the proof that there exist infinitely many prime numbers. Differing from the proof of Theorem 1.10, however, this time we closely follow Euclid's original proof.

**Example.** Prove that the are infinitely many prime numbers.

*Solution.* We assume, by contradiction, that only $p_1, p_2, \ldots, p_n$ are prime numbers. Obviously the number $N = p_1 p_2 \cdots p_n + 1$ is larger than any of these primes, so by assumption $N$ is composite. By the fundamental theorem of arithmetic (Theorem 1.8), one of these primes divides $N$. That same prime will divide $N - p_1 p_2 \cdots p_n = 1$, according to Theorem 1.2. This is absurd because the number 1 does not have any prime divisor.

**Exercise* 2.49.** Prove the following claims, in the given order.

a) If $a \bmod 4 = 1$ and $b \bmod 4 = 1$ then $ab \bmod 4 = 1$.
b) If $p > 2$ is a prime number, then $p \bmod 4 = 1$ or 3.
c) If $n \bmod 4 = 3$, then $n$ has a prime factor $p$ such that $p \bmod 4 = 3$.
d) There are infinitely many primes $p$ such that $p \bmod 4 = 3$.

**Exercise* 2.50.** Use contradiction to prove that a Carmichael number must have at least three prime factors. See Section 1.4.5 for definition.

## 2.4 Predicates and Quantifiers

In Mathematics we come across a statement like $x^2 = 4$, whose truth value shall be determined by the variable $x$. If we let $P(x)$ stand for the statement $x^2 = 4$, then $P(2)$ becomes a proposition whose value in this case is true. Similarly, $P(3.14)$ will be false. This proposition function $P(x)$ is an example of what we call a *predicate*.

*Question.* Where have we seen a predicate $P(x)$ earlier in this chapter?

### 2.4.1 There Is and For All

A predicate can also become a proposition when prefixed by a *quantifier*. There are two quantifiers, i.e.,

$\exists$ read: *there is* or *there exists*
$\forall$ read: *for all* or *for every*

**Example.** Let $P(x) : x^2 = 4$ and $Q(x) : x^2 > 0$. Determine true or false.

a) $\exists x \in \mathbb{R} : P(x)$
b) $\forall x \in \mathbb{Z} : P(x)$
c) $\exists x \in \mathbb{Z} : Q(x)$
d) $\forall x \in \mathbb{R} : Q(x)$

*Solution.* Note as follows how each statement is supposed to read.

a) $\exists x \in \mathbb{R} : P(x)$ represents the statement "There is a real number $x$ such that $x^2 = 4$." This statement is *true* because there does exist such a number $x \in \mathbb{R}$, e.g., $x = 2$. (In fact there is another example, $x = -2$, but producing one example is enough.)
b) $\forall x \in \mathbb{Z} : P(x)$ stands for "For all integers $x$, we have $x^2 = 4$. This is *false*, for example consider $x = 1$, which gives "$1^2 = 4$." (*Sometimes* this predicate can be true, e.g., for $x = 2$, but not *always* true.)
c) $\exists x \in \mathbb{Z} : Q(x)$ is true; just let $x = 3$, for instance. (In fact, there are abundantly many examples, for as long as $x \neq 0$.)
d) $\forall x \in \mathbb{R} : Q(x)$ is false, for when $x = 0$ we get "$0^2 > 0$" (even though $x = 0$ is the *only* instance for which $Q(x)$ becomes false).

**Exercise 2.51.** For each predicate $P(x)$ given below, determine the truth values of $\exists x \in \mathbb{R} : P(x)$ and $\forall x \in \mathbb{R} : P(x)$.

a) $P(x) : x > 2x$
b) $P(x) : x^4 < -1$
c) $P(x) : 3x^2 - 15x + 7c = 0$
d) $P(x) : 2x^2 - 9x + 11 > 0$

**Exercise* 2.52.** Let $S$ be any set whose elements are again sets. Define the *generalized union* and *generalized intersection* of sets over $S$, respectively,

$$\bigcup_{A \in S} A = \{x \mid \exists A \in S : x \in A\} \quad \text{and} \quad \bigcap_{A \in S} A = \{x \mid \forall A \in S : x \in A\}$$

In particular, if $A_n = \{x \in \mathbb{R} \mid 0 \leq x \leq \frac{1}{n}\}$ then prove that

$$\bigcup_{n \in \mathbb{N}} A_n = A_1 \quad \text{and} \quad \bigcap_{n \in \mathbb{N}} A_n = \{0\}$$

## Appendix: Reading Double Quantifiers

A predicate, like any other function, may well involve two or more variables. The predicate $P(x,y) : (x+y)^2 = x^2 + y^2$ is an example.

*Question.* For which values of $(x,y) \in \mathbb{R} \times \mathbb{R}$ is $P(x,y) : (x+y)^2 = x^2 + y^2$ true?

**Example.** Let $P(x,y) : x^2 \geq y^2$. Determine true or false, where $x, y \in \mathbb{R}$.

a) $\exists x \exists y : P(x,y)$
b) $\forall x \forall y : P(x,y)$
c) $\exists x \forall y : P(x,y)$
d) $\forall x \exists y : P(x,y)$
e) $\exists y \forall x : P(x,y)$

*Solution.* It is important to note how each statement reads.

a) $\exists x \exists y : P(x,y)$ represents the statement "There is a real number $x$ and another number $y$ such that $x^2 \geq y^2$. This is *true*, e.g., $x = 5$ and $y = 3$.
b) $\forall x \forall y : P(x,y)$ stands for "For all numbers $x$ and all numbers $y$, we have $x^2 \geq y^2$. This is *false*, for example if $x = 3$ and $y = 5$.
c) $\exists x \forall y : P(x,y)$ reads "There is a number $x$ such that $x^2 \geq y^2$ for all numbers $y$. The fact is there is *no* number $x$ satisfying the condition, for say if $x = A$ then the statement $A^2 \geq y^2$ is not true when $y = |A| + 1$ and definitely not for all $y$. Hence this proposition is *false.*
d) $\forall x \exists y : P(x,y)$ reads "For every number $x$, there is a number $y$ such that $x^2 \geq y^2$. This is actually *true* because given a number $x = A$, we can simply let $y = A$ to satisfy the inequality $A^2 \geq y^2$.
e) $\exists y \forall x : P(x,y)$ is a *true* statement, e.g., let $y = 0$ so that for all numbers $x$ the inequality $x^2 \geq 0$ holds. (There are no other examples really, for if $y \neq 0$ then the proposition $\forall x : P(x,y)$ is false. But, we have agreed that one example suffices.)

**Exercise 2.53.** Let $P(x,y) : x^2 + y^2 > 5$. Determine true or false, assuming that all numbers are real numbers.

a) $\exists x \forall y : P(x,y)$
b) $\forall x \exists y : P(x,y)$
c) $\exists y \forall x : P(x,y)$
d) $\forall y \exists x : P(x,y)$

**Exercise 2.54.** Repeat the previous exercise using each predicate below.

a) $P(x,y) : x^2 - y^2 > 5$
b) $P(x,y) : x^2 - y > 5$
c) $P(x,y) : x^2 + y^2 = (x+y)^2$
d) $P(x,y) : x^2 < x + y^2$

**Test 2.55.** Which predicate makes the proposition $\exists y \forall x : P(x, y)$ true?

a) $P(x, y) : x^2 - y^2 > 0$
b) $P(x, y) : x^2 - y > 0$
c) $P(x, y) : x - y^2 > 0$
d) $P(x, y) : x - y > 0$

### 2.4.2 Proving Existential Statements

We see that, in order to verify a proposition of the form $\exists x : P(x)$, it suffices to find a particular value of $x$ which will make the predicate true. To prove that $\exists x : P(x)$ is false, on the other hand, we have to demonstrate that the proposition $\forall x : \neg P(x)$ holds. Conversely, to show that $\forall x : P(x)$ is false, we essentially seek to establish $\exists x : \neg P(x)$. Intuitively, we have the following pair of logical equivalence.

$$\neg \exists x : P(x) \equiv \forall x : \neg P(x)$$
$$\neg \forall x : P(x) \equiv \exists x : \neg P(x)$$

*Question.* How do we rewrite the statement "Not all prime numbers are odd" using the quantifier *for all*?

**Example.** Prove that there is a prime number with unit digit 1, but never with 0. Moreover, prove that not all prime numbers are odd.

*Solution.* There is a prime with unit digit 1, e.g., $p = 11$. But if $p$ has unit digit 0, then $p$ is a multiple of 10, hence composite. Therefore, no prime has unit digit 0. To show that not all primes are odd, it suffices to find an even prime number, i.e., $p = 2$.

**Exercise 2.56.** Prove the following propositions.

a) There is a prime number $p$ such that $p \bmod 4 = 1$ and $p \bmod 5 = 4$.
b) Not all quadratic equations $ax^2 + bx + c = 0$ have a root $x \in \mathbb{R}$.
c) There is no prime number $p$ for which $\sqrt{p} \in \mathbb{N}$.
d) For all $x \in \mathbb{R}$, we have $x^2 - 6x + 11 > 0$.

**Exercise* 2.57.** Prove that the number $\log_2 3$ is irrational, and use this fact to show that there exist irrational numbers $a$ and $b$ such that $a^b$ is rational, with the particular choice of $a = \sqrt{2}$.

At times we need to prove the *uniqueness* of the existence $\exists x : P(x)$, i.e., that $P(x)$ holds for one and only one element $x$. For this, the proposition $\exists\, !x : P(x)$ reads "There exists a unique element $x$ for which $P(x)$ holds. To prove $\exists\, !x : P(x)$, we establish $\exists x : P(x)$ as well as $P(a) \wedge P(b) \rightarrow a = b$.

**Example.** Prove that there exists a unique set of cardinality zero. (This justifies the definition of *the* empty set $\emptyset$.)

*Solution.* Since $\forall x \in \mathbb{R} : x^2 \geq 0$, we see that the set $\{x \in \mathbb{R} \mid x^2 = -1\}$ has cardinality zero. This shows existence. To prove uniqueness, assume that $A$ and $B$ are two sets such that $|A| = |B| = 0$. Since the proposition $\exists x : x \in A$ has value false, then $A \subseteq B$ by the definition of a subset. Similarly, $B \subseteq A$. Hence, $A = B$ by Theorem 2.7.

**Exercise 2.58.** Prove that there is a unique $x \in \mathbb{R}$ such that $x^3 = -1$.

**Exercise* 2.59.** Prove that every positive rational number can be written as $m/n$, using a unique pair of natural numbers with $\gcd(m, n) = 1$.

### 2.4.3 Mathematical Induction

The technique of *mathematical induction* applies to a statement involving a predicate and the quantifier $\forall$ with the domain of positive integers. For example, consider the statement

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for all } n \in \mathbb{N}$$

Here, the predicate $P(n) : 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ claims to hold for all integer values of $n \geq 1$. How do we prove such a statement? We need only establish the following two propositions.

1) $P(1)$
2) $P(n) \to P(n+1)$

Intuitively, the second statement, with $n = 1$ says that if $P(1)$ holds, so does $P(2)$. Since $P(1)$ holds, i.e., by (1), then $P(2)$ is true. But by (2) again, since $P(2)$ is true, so is $P(3)$. And again, $P(3)$ implies $P(4)$, then $P(5)$, and on for all $P(n)$, where $n \in \mathbb{N}$. Proving (2) is what we call the *induction step.*

**Example.** Prove that the identity $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ holds for all integers $n \geq 1$.

*Solution.* We let $P(n)$ denote this predicate,

$$P(n) : 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

The statement we are to prove can be represented by $\forall n \geq 1 : P(n)$. Note that $P(5)$, for instance, stands for the proposition $1 + 2 + 3 + 4 + 5 = \frac{5(5+1)}{2}$, whose value is true. This is just an example. We proceed with the two parts of the proof.

1) $P(1)$ is the proposition $1 = \frac{1(1+1)}{2}$. Obviously then, $P(1)$ is true.

2) Using direct proof, we will show $P(n) \to P(n+1)$. Note first the statement $P(n+1) : 1+2+3+\cdots+(n+1) = \frac{(n+1)(n+2)}{2}$, as we proceed.

$$\begin{aligned}
P(n) : 1+2+3+\cdots+n &= \frac{n(n+1)}{2} \\
&\to 1+2+3+\cdots+n+(n+1) = \frac{n(n+1)}{2} + (n+1) \\
&\to 1+2+3+\cdots+n+(n+1) = \frac{n(n+1)+2(n+1)}{2} \\
&\to 1+2+3+\cdots+n+(n+1) = \frac{n^2+3n+2}{2} \\
&\to 1+2+3+\cdots+n+(n+1) = \frac{(n+1)(n+2)}{2} \\
&\to P(n+1)
\end{aligned}$$

**Exercise 2.60.** Use induction to prove each identity below for all $n \in \mathbb{N}$.

a) $1+2+4+\cdots+2^{n-1} = 2^n - 1$
b) $1+3+9+\cdots+3^{n-1} = (3^n-1)/2$
c) $1+4+9+\cdots+n^2 = n(n+1)(2n+1)/6$
d) $1+9+25+\cdots+(2n-1)^2 = n(2n-1)(2n+1)/3$

*Question.* How do we prove a proposition $\forall n \geq 2 : P(n)$ using induction?

**Example.** Prove that $2^n < n!$ whenever $n \geq 4$.

*Solution.* For $n = 4$, we have $2^4 < 4! = 24$, which is true. Now let $n \geq 4$. Assuming that $2^n < n!$, then $2^{n+1} = 2(2^n) < 2n! < (n+1)n! = (n+1)!$, which proves the inductive step.

**Exercise 2.61.** Use mathematical induction, where $n$ is understood integer.

a) Prove that $3^n < n!$ whenever $n \geq 7$.
b) Prove that $3^n > 1 + 2^n$ provided that $n \geq 2$.
c) Prove that $n^2 < 2^n$ for every $n \geq 5$.
d) Prove that $n^n > n!$ for all $n \geq 2$.

**Test 2.62.** We wish to prove using induction that $2^n > n^3$ for all integers $n \geq k$. What value of $k$ is most suitable?

a) 0
b) 1
c) 10
d) The statement is false.

**Exercise 2.63.** Prove for all $n \in \mathbb{N}$, using induction.
a) The number $2^{2n} - 1$ is a multiple of 3.
b) The number $n^3 + 2n$ is divisible by 3.
c) The number 5 divides $n^5 - n$.
d) The number $\frac{1}{7}(2^{n+2} + 3^{2n+1})$ is an integer.

For our final example on the proof by mathematical induction, we shall reestablish Theorem 2.8.

**Example.** Prove the proposition $\forall n \geq 0 : |A| = n \to |P(A)| = 2^n$.

*Solution.* For $n = 0$ of course, $A = \emptyset$, and $A$ has exactly $2^0 = 1$ subset, namely $A$ itself. We proceed by induction.

Assume that the theorem holds and consider a set $A$ with $n+1$ elements, one of which we call $x \in A$. Divide the subsets of $A$ in two groups: those which contain $x$ and those which do not. Those which do not, are exactly the subsets of $B = A - \{x\}$. Since $B$ consists of $n$ elements, $B$ has $2^n$ subsets according to our hypothesis. Moreover, the other group has $2^n$ subsets too because they are given by $S \cup \{x\}$ for every subset $S \subseteq B$. Hence $A$ has a total of $2^n + 2^n = 2^{n+1}$ subsets, proving the induction step.

**Exercise* 2.64.** Use induction to prove the following set identities involving generalized union and intersection, defined in Exercise 2.52.

$$\neg \bigcup_{n\in\mathbb{N}} A_n = \bigcap_{n\in\mathbb{N}} \neg A_n \quad \text{and} \quad \neg \bigcap_{n\in\mathbb{N}} A_n = \bigcup_{n\in\mathbb{N}} \neg A_n$$

**Exercise* 2.65.** Using mathematical induction, prove again the fact that every integer $n \geq 2$ can be written as a product of prime numbers. This statement is part of the fundamental theorem of arithmetic (Theorem 1.8). Although logically equivalent, note and explain a significant modification on the inductive step of the proof.

# Books to Read

1. M. Aigner and G. M. Ziegler, *Proofs from THE BOOK,* Fourth Edition, Springer 2010.

2. J.M. De Koninck and A. Mercier, *1001 Problems in Classical Number Theory,* American Mathematical Society 2007.

3. G. Pólya, *How to Solve It: A New Aspect of Mathematical Method,* Second Edition, Princeton University Press 1988.

4. D. Solow, *How to Read and Do Proofs: An Introduction to Mathematical Thought Processes,* Fifth Edition, Wiley 2009.