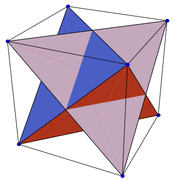
Chapter 1



Logic and Sets

1.1. Logical connectives

1.1.1. Unambiguous statements. Logic is concerned first of all with the logical structure of statements, and with the construction of complex statements from simple parts. A statement is a declarative sentence, which is supposed to be either true or false.

A statement must be made completely unambiguous in order to be judged as true or false. Often this requires that the writer of a sentence has established an adequate context which allows the reader to identify all those things referred to in the sentence. For example, if you read in a narrative: *"He is John's brother,"* you will not be able to understand this simple assertion unless the author has already identified John, and also allowed you to know who "*he*" is supposed to be. Likewise, if someone gives you directions, starting *"Turn left at the corner,"* you will be quite confused unless the speaker also tells you *what corner* and *from what direction* you are supposed to approach this corner.

The same thing happens in mathematical writing. If you run across the sentence $x^2 \geq 0$, you won't know what to make of it, unless the author has established what x is supposed to be. If the author has written, *"Let x be any real number. Then $x^2 \geq 0$,"* then you can understand the statement, and see that it is true.

A sentence containing variables, which is capable of becoming an an unambiguous statement when the variables have been adequately identified, is called a *predicate* or, perhaps less pretentiously, a *statement-with-variables*. Such a sentence is neither true nor false (nor comprehensible) until the variables have been identified.

It is the job of every writer of mathematics (you, for example!) to strive to abolish ambiguity. *The first rule of mathematical writing is this: any* *symbol you use, and any object of any sort to which you refer, must be adequately identified. Otherwise, what you write will be meaningless or incomprehensible.*

Our first task will be to examine how simple statements can be combined or modified by means of *logical connectives* to form new statements; the validity of such a composite statement depends only on the validity of its simple components.

The basic logical connectives are *and*, *or*, *not*, and *if...then*. We consider these in turn.

1.1.2. The conjunction *and*. For statements A and B, the statement "A and B" is true exactly when both A and B are true. This is conventionally illustrated by a *truth table*:

A	B	A and B
t	t	t
t	f	f
f	t	f
f	f	f

The table contains one row for each of the four possible combinations of truth values of A and B; the last entry of each row is the truth value of "A and B" corresponding to the given truth values of A and B.

For example:

- *"Julius Caesar was the first Roman emperor, and Wilhelm II was the last German emperor"* is true, because both parts are true.
- *"Julius Caesar was the first Roman emperor, and Peter the Great was the last German emperor"* is false because the second part is false.
- *"Julius Caesar was the first Roman emperor, and the Seventeenth of May is Norwegian independence day."* is true, because both parts are true, but it is a fairly ridiculous statement.
- "$2 < 3$, *and* π *is the area of a circle of radius 1"* is true because both parts are true.

1.1.3. The disjunction *or*. For statements A and B, the statement "A or B" is true when at least one of the component statements is true. Here is the truth table:

A	B	A or B
t	t	t
t	f	t
f	t	t
f	f	f

In everyday speech, "or" sometimes is taken to mean "one or the other, but not both," but in mathematics the universal convention is that "or" means "one or the other or both."

For example:

- *"Julius Caesar was the first Roman emperor, or Wilhelm II was the last German emperor"* is true, because both parts are true.
- *"Julius Caesar was the first Roman emperor, or Peter the Great was the last German emperor"* is true because the first part is true.
- *"Julius Caesar was the first Chinese emperor, or Peter the Great was the last German emperor."* is false, because both parts are false.
- "$2 < 3$, *or* π *is the area of a circle of radius 2*" is true because the first part is true.

1.1.4. The negation *not*. The negation "not(A)" of a statement A is true when A is false and false when A is true.

A	not(A)
t	f
f	t

Of course, given an actual statement A, we do not generally negate it by writing "not(A)." Instead, we employ one of various means afforded by our natural language.

Examples:

- The negation of " $2 < 3$" is " $2 \geq 3$".
- The negation of *"Julius Caesar was the first Roman emperor."* is *"Julius Caesar was not the first Roman emperor."*
- The negation of *"I am willing to compromise on this issue."* is *I am unwilling to compromise on this issue."*

1.1.5. Negation combined with conjunction and disjunction. At this point we might try to combine the negation "not" with the conjunction "and" or the disjunction "or." We compute the truth table of "not(A and B)," as follows:

A	B	A and B	not(A and B)
t	t	t	f
t	f	f	t
f	t	f	t
f	f	f	t

Next, we observe that "not(A) or not(B)" has the same truth table as "not(A and B)."

A	B	not(A)	not(B)	not(A) or not(B)
t	t	f	f	f
t	f	f	t	t
f	t	t	f	t
f	f	t	t	t

We say that two *statement formulas* such as "not(A and B)" and "not(A) or not(B)" are *logically equivalent* if they have the same truth table; when we substitute actual statements for A and B in the logically equivalent statement formulas, we end up with two composite statements with exactly the same truth value; that is one is true if, and only if, the other is true.

What we have verified with truth tables also makes perfect intuitive sense: "A and B" is false precisely if not both A and B are true, that is when one or the other, or both, of A and B is false.

Exercise 1.1.1. Check similarly that "not(A or B)" is logically equivalent to "not(A) and not(B)," by writing out truth tables. Also verify that "not(not(A))" is equivalent to "A," by using truth tables.

The logical equivalence of "not(A or B)" and 'not(A) and not(B)" also makes intuitive sense. "A or B" is true when at least one of A and B is true. "A or B" is false when neither A nor B is true, that is when both are false.

Examples:

- The negation of *"Julius Caesar was the first Roman emperor, and Wilhelm II was the last German emperor"* is *"Julius Caesar was not the first Roman emperor, or Wilhelm II was not the last German emperor."* This is false.
- The negation of *"Julius Caesar was the first Roman emperor, and Peter the Great was the last German emperor"* is *"Julius Caesar was not the first Roman emperor, or Peter the Great was not the last German emperor."* This is true.
- The negation of *"Julius Caesar was the first Chinese emperor, or Peter the Great was the last German emperor" "Julius Caesar was not the first Chinese emperor, and Peter the Great was not the last German emperor."* This is true.

- The negation of "$2 < 3$, *or* π *is the area of a circle of radius 2*" is "$2 \geq 3$, *and* π *is not the area of a circle of radius 2.*" This is false, because the first part is false.

1.1.6. The implication *if...then*. Next, we consider the implication *"if A, then B"* or *"A implies B."* We *define* "if A, then B" to mean "not(A and not(B))," or, equivalently, "not(A) or B"; this is fair enough, since we want "if A, then B" to mean that one cannot have A without also having B. The negation of "A implies B" is thus "A and not(B)".

Exercise 1.1.2. Write out the truth table for "A implies B" and for its negation.

Definition 1.1.1. The *contrapositive* of the implication *"A implies B"* is *"not(B) implies not(A)."* The *converse* of the implication *"A implies B"* is *"B implies A"*.

The converse of a true implication may be either true or false. For example:

- The implication "*If* $-3 > 2$, *then* $9 > 4$" is true. The converse implication "*If* $9 > 4$, *then* $(-3) > 2$" is false.

However, the contrapositive of a true implication is always true, and the contrapositive of a false implication is always false, as is verified in Exercise 1.1.3.

Exercise 1.1.3. "A implies B" is equivalent to its *contrapositive* "not(B) implies not(A)." Write out the truth tables to verify this.

Exercise 1.1.4. Sometimes students jump to the conclusion that "A implies B" is equivalent to one or another of the following: "A and B," "B implies A,", or "not(A) implies not(B)." Check that in fact "A implies B" is not equivalent to any of these by writing out the truth tables and noticing the differences.

Exercise 1.1.5. Verify that "A implies (B implies C)" is logically equivalent to "(A and B) implies C," by use of truth tables.

Exercise 1.1.6. Verify that "A or B" is equivalent to 'if 'not(A), then B," by writing out truth tables. (Often a statement of the form "A or B" is most conveniently proved by assuming A does not hold, and proving B.)

The use of the connectives "and," and "not" in logic and mathematics coincide with their use in everyday language, and their meaning is clear. The use of "or" in mathematics differs only slightly from everyday use, in that we insist on using the *inclusive* rather than the *exclusive* or in mathematics.

The use of "if ... then" in mathematics, however, is a little mysterious. In ordinary speech, we require some genuine connection, preferably a causal connection between the "if" and the "then" in order to accept an "if ... then" statement as sensible and true. For example:

- *If you run an engine too fast, you will damage it.*
- *If it rains tomorrow, we will have to cancel the picnic.*
- $2 < 3$ *implies* $3/2 > 1$.

These are sensible uses of 'if ... then" in ordinary language, and they involve causality: misuse of the engine will cause damage, rain will cause the cancellation of the picnic, and 2 being less than 3 is an explanation for 3/2 being greater than 1.

On the other hand, the implications:

- *If the Seventeenth of May is Norwegian independence day, then Julius Caesar was the first emperor of Rome.*
- $2 < 3$ *implies* $\pi > 3.14$.

would ordinarily be regarded as nonsense, as modern Norwegian history cannot have had any causal influence on ancient Roman history, and there is no apparent connection between the two inequalities in the second example. But according to our defined use of "if ... then," both of these statements must be accepted as a true. Even worse:

- *If the Eighteenth of May is Norwegian independence day, then Julius Caesar was the last emperor of Germany.*
- *If* $2 > 3$ *then* $\sqrt{2}$ *is rational.*

are also true statements, according to our convention. However unfortunate these examples may seem, we find it preferable in mathematics and logic not to require any causal connection between the "if" and the "then," but to judge the truth value of an implication "if A, then B" solely on the basis of the truth values of A and B.

1.1.7. Some logical expressions. Here are a few commonly used logical expressions:

- "A if B" means "B implies A."
- "A only if B" means "A implies B."
- "A if, and only if, B" means "A implies B, and B implies A."
- "Unless" means "if not," but "if not" is equivalent to "or." (Check this!)
- Sometimes "but" is used instead of "and" for emphasis.

1.2. Quantified statements

1.2.1. Quantifiers. One frequently makes statements in mathematics which assert that all the elements in some set have a certain property, or that there exists at least one element in the set with a certain property. For example:

- For every real number x, one has $x^2 \geq 0$.
- For all lines L and M, if $L \neq M$ and $L \cap M$ is non-empty, then $L \cap M$ consists of exactly one point.
- There exists a positive real number whose square is 2.
- Let L be a line. Then there exist at least two points on L.

Statements containing one of the phrases “for every”, “for all”, “for each”, etc. are said to have a *universal quantifier*. Such statements typically have the form:

- *For all x, $P(x)$,*

where $P(x)$ is some assertion about x. The first two examples above have universal quantifiers.

Statements containing one of the phrases “there exists,” “there is,” “one can find,” etc. are said to have an *existential quantifier*. Such statements typically have the form:

- *There exists an x such that $P(x)$,*

where $P(x)$ is some assertion about x. The third and fourth examples above contain existential quantifiers.

One thing to watch out for in mathematical writing is the use of implicit universal quantifiers, which are usually coupled with implications. For example,

- If x is a non-zero real number, then x^2 is positive

actually means,

- For all real numbers x, if $x \neq 0$, then x^2 is positive,

or

- For all non-zero real numbers x, the quantity x^2 is positive.

1.2.2. Negation of Quantified Statements. Let us consider how to form the negation of sentences containing quantifiers. The negation of the assertion that every x has a certain property is that *some* x does not have this property; thus the negation of

- *For every x, $P(x)$.*

is

- *There exists an x such that not $P(x)$.*

For example the negation of the (true) statement

- For all non-zero real numbers x, the quantity x^2 is positive

is the (false) statement

- There exists a non-zero real numbers x, such that $x^2 \leq 0$.

Similarly the negation of a statement

- *There exists an x such that* $P(x)$.

is

- *For every x, not* $P(x)$.

For example, the negation of the (true) statement

- *There exists a real number x such that* $x^2 = 2$.

is the (false) statement

- *For all real numbers x,* $x^2 \neq 2$.

In order to express complex ideas, it is quite common to string together several quantifiers. For example

- *For every positive real number x, there exists a positive real number y such that* $y^2 = x$.
- *For every natural number m, there exists a natural number n such that* $n > m$.
- *For every pair of distinct points* p *and* q*, there exists exactly one line* L *such that* L *contains* p *and* q.

All of these are true statements.

There is a rather nice rule for negating such statements with chains of quantifiers: one runs through chain changing every universal quantifier to an existential quantifier, and every existential quantifier to a universal quantifier, and then one negates the assertion at the end.

For example, the negation of the (true) sentence

- *For every positive real number x, there exists a positive real number y such that* $y^2 = x$.

is the (false) statement

- *There exists a positive real number x such that for every positive real number y, one has* $y^2 \neq x$.

1.2.3. Implicit universal quantifiers. Frequently "if ... then" sentences in mathematics also involve the *universal quantifier* "for every".

- *For every real number x, if* $x \neq 0$*, then* $x^2 > 0$.

Quite often the quantifier is only implicitly present; in place of the sentence above, it is common to write

- *If x is a non-zero real number, then* $x^2 > 0$.

The negation of this is *not*

- x is a non-zero real number and $x^2 \leq 0$,

as one would expect if one ignored the (implicit) quantifier. Because of the universal quantifier, the negation is actually

- *There exists a real number x such that $x \neq 0$ and $x^2 \leq 0$.*

It might be preferable if mathematical writers made all quantifiers explicit, but they don't, so one must look out for and recognize implicit universal quantifiers in mathematical writing. Here are some more examples of statements with implicit universal quantifiers:

- *If two distinct lines intersect, their intersection contains exactly one point.*
- *If $p(x)$ is a polynomial of odd degree with real coefficients, then p has a real root.*

Something very much like the use of implicit universal quantifiers also occurs in everyday use of implications. In everyday speech, "if ... then" sentences frequently concern the uncertain future, for example:

($*$) *If it rains tomorrow, our picnic will be ruined.*

One notices something strange if one forms the negation of this statement. (When one is trying to understand an assertion, it is often illuminating to consider the negation.) According to our prescription for negating implications, the negation ought to be:

- *It will rain tomorrow, and our picnic will not be ruined.*

But this is surely not correct! The actual negation of the sentence ($*$) ought to comment on the consequences of the weather without predicting the weather:

($**$) *It is possible that it will rain tomorrow, and our picnic will not be ruined.*

What is going on here? Any sentence about the future must at least implicitly take account of uncertainty; the purpose of the original sentence ($*$) is to deny uncertainty, by issuing an absolute prediction:

- *Under all circumstances, if it rains tomorrow, our picnic will be ruined.*

The negation ($**$) denies the certainty expressed by ($*$).

1.2.4. Order of quantifiers. It is important to realize that the order of universal and existential quantifiers cannot be changed without utterly changing the meaning of the sentence. For example, if you start with the true statement:

- *For every positive real number x, there exists a positive real number y such that $y^2 = x$*

and reverse the two quantifiers, you get the totally absurd statement:

- *There exists a positive real number y such that for every positive real number x, one has* $y^2 = x$.

1.2.5. Negation of complex sentences. Here is a summary of rules for negating statements:

1. The negation of "A or B" is "not(A) and not(B)."
2. The negation of "A and B" is "not(A) or not(B)."
3. The negation of "For every x, P(x)" is "There exists x such that not(P(x))."
4. The negation of "There exists an x such that P(x)" is "For every x, not(P(x))."
5. The negation of "A implies B" is "A and not(B)."
6. Many statements with implications have implicit universal quantifiers, and one must use the rule (3) for negating such sentences.

The negation of a complex statement (one containing quantifiers or logical connectives) can be "simplified" step by step using the rules above, until it contains only negations of simple statements. For example, a statement of the form "For all x, if $P(x)$, then $Q(x)$ and $R(x)$" has a negation which simplifies as follows:

not(For all x, if $P(x)$, then $Q(x)$ and $R(x)$) $\equiv$
There exists x such that not(if $P(x)$, then $Q(x)$ and $R(x)$) $\equiv$
There exists x such that $P(x)$ and not($Q(x)$ and $R(x)$) $\equiv$
There exists x such that $P(x)$ and not($Q(x)$) or not($R(x)$) .

Let's consider a special case of a statement of this form:

- *For all real numbers x, if* $x < 0$, *then* $x^3 < 0$ *and* $|x| = -x$.

Here we have $P(x) : x < 0$, $Q(x) : x^3 < 0$ and $R(x) : |x| = -x$. Therefore the negation of the statement is:

- *There exists a real number x such that* $x < 0$, *and* $x^3 \geq 0$ *or* $|x| \neq -x$.

Here is another example

- *If L and M are distinct lines with non-empty intersection, then the intersection of L and M consists of one point.*

This sentence has an implicit universal quantifier and actually means:

- *For every pair of lines L and M, if L and M are distinct and have non-empty intersection, then the intersection of L and M consists of one point.*

Therefore the negation uses both the rule for negation of sentences with universal quantifiers, and the rule for negation of implications:

- *There exists a pair of lines L and M such that L and M are distinct and have non-empty intersection, and the intersection does not consist of one point.*

Finally, this can be rephrased as:

- *There exists a pair of lines L and M such that L and M are distinct and have at least two points in their intersection.*

Exercise 1.2.1. Form the negation of each of the following sentences. Simplify until the result contains negations only of simple sentences.

(a) Tonight I will go to a restaurant for dinner or to a movie.
(b) Tonight I will go to a restaurant for dinner and to a movie.
(c) If today is Tuesday, I have missed a deadline.
(d) For all lines L, L has at least two points.
(e) For every line L and every plane P, if L is not a subset of P, then $L \cap P$ has at most one point.

Exercise 1.2.2. Same instructions as for the previous problem Watch out for implicit universal quantifiers.

(a) If x is a real number, then $\sqrt{x^2} = |x|$.
(b) If x is a natural number and x is not a perfect square, then $\sqrt{x}$ is irrational.
(c) If n is a natural number, then there exists a natural number N such $N > n$.
(d) If L and M are distinct lines, then either L and M do not intersect, or their intersection contains exactly one point.

1.2.6. Deductions. Logic concerns not only statements but also deductions. Basically there is only one rule of deduction:

- *If A, then B. A. Therefore B.*

For quantified statements this takes the form:

- *For all x, if $A(x)$, then $B(x)$. $A(\alpha)$. Therefore $B(\alpha)$.*

Example:

- *Every subgroup of an abelian group is normal. $\mathbb{Z}$ is an abelian group, and $3\mathbb{Z}$ is a subgroup. Therefore $3\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.*

It doesn't matter if you don't know what this means! You don't *have* to know what it means in order to appreciate its form. Here is another example of exactly the same form:

- *Every car will eventually end up as a pile of rust. My brand new blue-green Miata is a car. Therefore it will eventually end up as a pile of rust.*

Most statements requiring proof are "if ... then" statements. To prove "if A, then B," one has to assume A, and prove B under this assumption. To prove "For all x, $A(x)$ implies $B(x)$," one assumes that $A(\alpha)$ holds for a particular (but arbitrary) α, and proves $B(\alpha)$ for this particular α.

1.3. Sets

1.3.1. Sets and set operations. A *set* is a collection of (mathematical) objects. The objects contained in a set are called its *elements*. We write $x \in A$ if x is an element of the set A. Two sets are equal if they contain exactly the same elements. Very small sets can be specified by simply listing their elements, for example $A = \{1, 5, 7\}$. For sets A and B, we say that A is *contained* in B, and we write $A \subseteq B$ if each element of A is also an element of B. That is, if $x \in A$ then $x \in B$. (Because of the implicit universal quantifier, the negation of this is that there exists an element of A which is not an element of B.)

Two sets are *equal* if they contain exactly the same elements. This might seem like a quite stupid thing to mention, but in practice one often has two quite different descriptions of the same set, and one has to do a lot of work to show that the two sets contain the same elements. To do this, it is often convenient to show that each is contained in the other. That is, $A = B$ if, and only if, $A \subseteq B$ and $B \subseteq A$.

Subsets of a given set are frequently specified by a property or predicate; for example, $\{x \in \mathbb{R} : 1 \leq x \leq 4\}$ denotes the set of all real numbers between 1 and 4. Note that set containment is related to logical implication in the following fashion: If a property $P(x)$ implies a property $Q(x)$, then the set corresponding to $P(x)$ is contained in the set corresponding to $Q(x)$. For example, $x < -2$ implies that $x^2 > 4$, so $\{x \in \mathbb{R} : x < -2\} \subseteq \{x \in \mathbb{R} : x^2 > 4\}$.

The *intersection* of two sets A and B, written $A \cap B$, is the set of elements contained in both sets. $A \cap B = \{x : x \in A \quad \text{and} \quad x \in B\}$. Note the relation between intersection and the logical conjunction. If $A = \{x \in C : P(x)\}$ and $B = \{x \in C : Q(x)\}$, then $A \cap B = \{x \in C : P(x) \quad \text{and} \quad Q(x)\}$.

The *union* of two sets A and B, written $A \cup B$, is the set of elements contained in at least one of the two sets. $A \cup B = \{x : x \in A \quad \text{or} \quad x \in B\}$. Set union and the logical disjunction are related as are set intersection and logical conjunction. If $A = \{x \in C : P(x)\}$ and $B = \{x \in C : Q(x)\}$, then $A \cup B = \{x \in C : P(x) \quad \text{or} \quad Q(x)\}$.

Given finitely many sets, for example, five sets A, B, C, D, E, one similarly defines their intersection $A \cap B \cap C \cap D \cap E$ to consist of those elements which are in all of the sets, and the union $A \cup B \cup C \cup D \cup E$ to consist of those elements which are in at least one of the sets.

There is a unique set with no elements at all which is called the *empty set*, or the *null set* and usually denoted $\emptyset$.

Proposition 1.3.1. *The empty set is a subset of every set.*

Proof. Given an arbitrary set A, we have to show that $\emptyset \subseteq A$; that is, for every element $x \in \emptyset$, one has $x \in A$. The negation of this statement is that there exists an element $x \in \emptyset$ such that $x \notin A$. But this negation is false, because there are no elements at all in $\emptyset$! So the original statement is true. □

If the intersection of two sets is the empty set, we say that the sets are *disjoint*, or *non-intersecting*.

Here is a small theorem concerning the properties of set operations.

Proposition 1.3.2. *For all sets A, B, C,*

(a) $A \cup A = A$, *and* $A \cap A = A$.

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

(c) $(A \cup B) \cup C = A \cup B \cup C = A \cup (B \cup C)$, *and* $(A \cap B) \cap C = A \cap B \cap C = A \cap (B \cap C)$.

(d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, *and* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

The proofs are just a matter of checking definitions.

Given two sets A and B, we define the *relative complement* of B in A, denoted $A \setminus B$, to be the elements of A which are not contained in B. That is, $A \setminus B = \{x \in A : x \notin B\}$.

In general, all the sets appearing in some particular mathematical discussion are subsets of some "universal" set U; for example, we might be discussing only subsets of the real numbers $\mathbb{R}$. (However, there is no universal set once and for all, for all mathematical discussions; the assumption of a "set of all sets" leads to contradictions.) It is customary and convenient to use some special notation such as $\mathcal{C}(B)$ for the complement of B relative to U, and to refer to $\mathcal{C}(B) = U \setminus B$ simply as *the complement of B*. (The notation $\mathcal{C}(B)$ is not standard.)

Exercise 1.3.1. The sets $A \cap B$ and $A \setminus B$ are disjoint and have union equal to A.

Exercise 1.3.2 (de Morgan's laws)**.** For any sets A and B, one has:

$$\mathcal{C}(A \cup B) = \mathcal{C}(A) \cap \mathcal{C}(B),$$

and

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

Exercise 1.3.3. For any sets A and B, $A \setminus B = A \cap C(B)$.

Exercise 1.3.4. For any sets A and B,

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

1.3.2. Functions. We recall the notion of a *function from A to B* and some terminology regarding functions which is standard throughout mathematics. A function f from A to B is a rule which gives for each element of $a \in A$ an "outcome" in $f(a) \in B$. A is called the *domain* of the function, B the *co-domain*, $f(a)$ is called the *value* of the function at a, and the set of all values, $\{f(a) : a \in A\}$, is called the *range* of the function.

In general, the range is only a subset of B; a function is said to be *surjective*, or *onto*, if its range is all of B; that is, for each $b \in B$, there exists an $a \in A$, such that $f(a) = b$. Figure 1.3.1 exhibits a surjective function. Note that the statement that a function is surjective has to be expressed by a statement with a string of quantifiers.

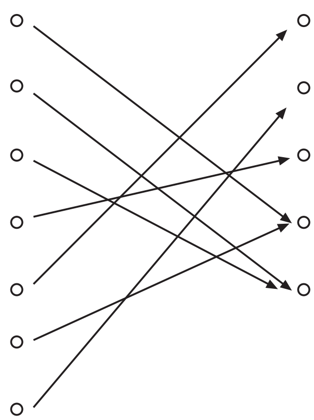


Figure 1.3.1. A Surjection

A function f is said to be *injective*, or *one-to-one*, if for each two distinct elements a and a' in A, one has $f(a) \neq f(a')$. Equivalently, for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$. Figure 1.3.2 displays an injective and a non- injective function.

Finally f is said to be *bijective* if it is both injective and surjective. A bijective function (or *bijection*) is also said to be a *one-to-one correspondence* between A and B, since it matches up the elements of the two sets one-to-one. When f is bijective, there is an *inverse function* f^{-1} defined

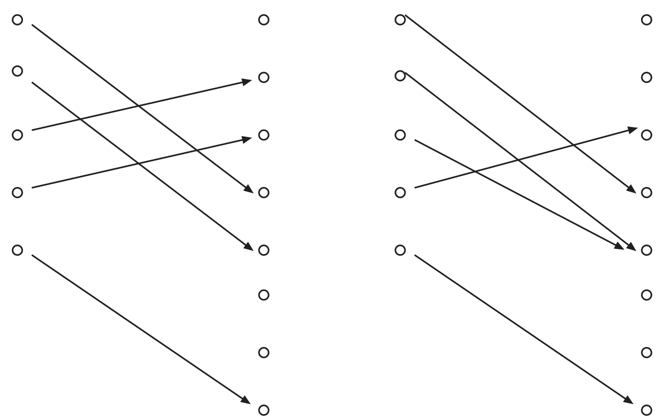


Figure 1.3.2. Injective and Non-injective functions

by $f^{-1}(b) = a$ if, and only if, $f(a) = b$. Figure 1.3.3 displays a bijective function.

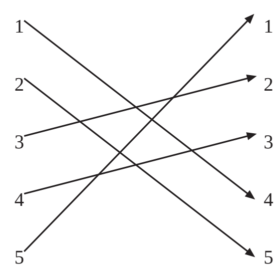


Figure 1.3.3. A Bijection

If $f : X \to Y$ is a function and A is a subset of X, we write $f(A)$ for $\{f(a) : a \in A\} = \{y \in Y :$ there exists $a \in A$ such that $y = f(a)\}$. We refer to $f(A)$ as the *image of A under f*. If B is a subset of Y, we write $f^{-1}(B)$ for $\{x \in X : f(x) \in B\}$. We refer to $f^{-1}(B)$ as the *preimage of B under f*.

1.4. Induction

1.4.1. Proof by Induction. Suppose you need to climb a ladder. If you are able to reach the first rung of the ladder and you are also able to get from any one rung to the next, then there is nothing to stop you from climbing the whole ladder. This is called *the principle of mathematical induction*.

Mathematical induction is often used to prove statements about the natural numbers, or about families of objects indexed by the natural numbers. Suppose that you need to prove a statement of the form:

- *For all* $n \in \mathbb{N}$, $P(n)$,

where $P(n)$ is a predicate. Examples of such statements are:

- *For all* $n \in \mathbb{N}$, $1 + 2 + \cdots + n = (n)(n+1)/2$.
- *For all* $n \in \mathbb{N}$, *the number of permutations of n objects is* $n!$.

To prove that $P(n)$ holds for all $n \in \mathbb{N}$, it suffices to show that $P(1)$ holds (you can reach the first rung), and that whenever $P(k)$ holds, then also $P(k+1)$ holds (you can get from any one rung to the next). Then, $P(n)$ holds for all n (you can climb the whole ladder).

Principle of Mathematical Induction *For the statement "For all* $n \in \mathbb{N}$, $P(n)$*" to be valid, it suffices that:*

1. $P(1)$, *and*
2. *For all* $k \in \mathbb{N}$, $P(k)$ *implies* $P(k+1)$.

To prove that "*For all* $k \in \mathbb{N}$, $P(k)$ *implies* $P(k+1)$," you have to assume $P(k)$ for a fixed but arbitrary value of k and prove $P(k+1)$ under this assumption. This sometimes seems like a big cheat to beginners, for we seem to be assuming what we want to prove, namely, that $P(n)$ holds. But it is not a cheat at all; we are just showing that it is possible to get from one rung to the next.

As an example we prove the identity

$$P(n) : 1 + 2 + \cdots + n = (n)(n+1)/2$$

by induction on n. The statement $P(1)$ reads

$$1 = (1)(2)/2,$$

which is evidently true. Now, we assume $P(k)$ holds for some k, that is,

$$1 + 2 + \cdots + k = (k)(k+1)/2,$$

and prove that $P(k+1)$ also holds. The assumption of $P(k)$ is called the *induction hypothesis*. Using the induction hypothesis, we have

$$1 + 2 + \cdots + k + (k+1) = (k)(k+1)/2 + (k+1) = \frac{(k+1)}{2}(k+2),$$

which is $P(k+1)$. This completes the proof of the identity.

The principle of mathematical induction is equivalent to the

Well ordering principle *Every non-empty subset of the natural numbers has a least element.*

Another form of the principle of mathematical induction is the following:

Principle of Mathematical Induction, 2nd form *For the statement "For all $n \in N$, $P(n)$" to be valid, it suffices that:*

1. $P(1)$, *and*
2. *For all $k \in \mathbb{N}$, if $P(r)$ for all $r \leq k$, then also $P(k+1)$.*

The two forms of the principle of mathematical induction and the well ordering principle are all equivalent statements about the natural numbers. That is, assuming any one of these principles, one can prove the other two. The proof of the equivalence is somewhat more abstract than the actual subject matter of this course, so I prefer to omit it. When you have more experience with doing proofs, you may wish to provide your own proof of the equivalence.

Recall that a natural number is *prime* if it is greater than 1 and not divisible by any natural number other than 1 and itself.

Proposition 1.1. *Any natural number other than* 1 *can be written as a product of prime numbers.*

Proof. We prove this statement by using the second form of mathematical induction. Let $P(n)$ be the statement: "*n is a product of prime numbers.*" We have to show that $P(n)$ holds for all natural numbers $n \geq 2$. $P(2)$ is valid because 2 is prime. We make the inductive assumption that $P(r)$ holds for all $r \leq k$, and prove $P(k+1)$. $P(k+1)$ is the statement that $k+1$ is a product of primes. If $k+1$ is prime, there is nothing to show. Otherwise $k+1 = (a)(b)$, where $2 \leq a \leq k$ and $2 \leq b \leq k$. By the induction hypothesis, both a and b are products of prime numbers so $k+1 = ab$ is also a product of prime numbers. □

Remark 1.2. It is a usual convention in mathematics to consider 0 to be the sum of an *empty* collection of numbers and 1 to be the product of an *empty* collection of numbers. This convention saves a lot of circumlocution and argument by cases. So we will consider 1 to have a prime factorization as well; it is the product of an empty collection of primes.

The following result is attributed to Euclid:

Theorem 1.3. *There are infinitely many prime numbers.*

Proof. We prove for all natural numbers n the statement $P(n)$: *there are at least n prime numbers.* $P(1)$ is valid because 2 is prime. Assume $P(k)$

holds and let $2, 3, \ldots, p_k$ be the first k prime numbers. Consider the natural number $M = (2)(3) \ldots (p_k) + 1$. M is not divisible by any of the primes $2, 3, \ldots, p_k$, so either M is prime, or M is a product of prime numbers each of which is greater than p_k. In either case, there must exist prime numbers which are greater than p_k, so there are at least $k + 1$ prime numbers. □

1.4.2. Definitions by Induction. It is frequently necessary or convenient to define some sequence of objects (numbers, sets, functions, ...) *inductively* or *recursively*. That means the nth object is defined in terms of the first, second,..., $n - 1$-st object, instead of there being a formula or procedure which tells you once and for all how to define the nth object. For example, the sequence of Fibonacci numbers is defined by the recursive rule:

$$f_1 = f_2 = 1 \quad f_n = f_{n-1} + f_{n-2} \quad \text{for } n \geq 3.$$

The well ordering principle, or the principle of mathematical induction, implies that such a rule suffices to define f_n for all natural numbers n. For f_1 and f_2 are defined by an explicit formula (we can get to the first rung), and if $f_1, \ldots, f_k$ have been defined for some k, then the recursive rule $f_{k+1} = f_k + f_{k-1}$ also defines f_{k+1} (we can get from one rung to the next).

Principle of Inductive Definition: To define a sequence of objects $A_1, A_2, \ldots$ it suffices to have:

1. A definition of A_1.
2. For each $k \in \mathbb{N}$, a definition of A_{k+1} in terms of $\{A_1, \ldots, A_k\}$.

Here is an example relevant to this course: Suppose a patient is given a drug which has the property that about 70body at a given moment is retained after one day. The patient recieves 300 mg of the drug each day at the same time. We model this situation by the sequence x_n of positive numbers defined by

1. $x_1 = 300$.
2. For each $n \in \mathbb{N}$, $x_{n+1} = 300 + .7x_n$.

Here is another example where the objects being defined are intervals in the real numbers. The goal is to compute an accurate approximation to $\sqrt{7}$. We define a sequence of intervals $A_n = [a_n, b_n]$ with the properties:

1. $b_n - a_n = 6/2^n$,
2. $A_{n+1} \subseteq A_n$ for all $n \in \mathbb{N}$, and
3. $a_n^2 < 7$ and $b_n^2 > 7$ for all $n \in \mathbb{N}$.

Define $A_1 = [1, 7]$. If $A_1, \ldots, A_k$ have been defined, let $c_k = (a_k + b_k)/2$. If $c_k^2 < 7$, then define $A_{k+1} = [c_k, b_k]$. Otherwise, define $A_k = [a_k, c_k]$.

(Remark that all the numbers a_k, b_k, c_k are rational, so it is never true that $c_k^2 = 7$.) You ought to do a proof (by induction) that the sets A_n defined by this procedure do satisfy the properties listed above. This example can easily be transformed into a computer program for calculating the square root of 7.