Proofs in Elementary Analysis

Summer 2007

June 26, 2007

CHAPTER 1

Introductory Material

1.1. Goals

- To provide a systematic foundation of some basic concepts encountered in calculus, particularly those associated with the structure of the real numbers and notions of limit and continuity for real-valued functions.
- To introduce students to the nature and role of proofs in mathematics. Specifically we assert that the only way to understand proofs is to construct proofs on your own.
- To develop ability to critically read and judge the correctness and the completeness of mathematical reasoning.
- To develop a skill in the clear and precise presentation of mathematical reasoning.

1.2. Strategies

How to get started towards a solution of a problem?

(1) Illustrate the problem with several examples.
(2) Make sure that you understand the terminology used in the problem. Review all relevant definitions.
(3) Can you restate the problem as an implication? (Clearly identify the assumptions and the conclusion of the implication.)
(4) Identify problems done in class that are in some sense related to the problem that you are working on. Review proofs of those problems.
(5) Try to identify tools that can be used in the solution of the problem.
(6) If you can not solve the given problem, try to formulate a related simpler problem that you can solve. For example, try to solve a special case.
(7) Be flexible. Have in mind that there are many ways to approach each problem.
(8) Keep a detailed written record of your work.

How to avoid mistakes?

(1) Write your solution out carefully. Include justifications for all arguments that you use.
(2) Read your solution critically after a day or two. Is everything that you use in your proof justified.
(3) Imagine that a skeptic is reading your proof. Can you answer all sceptic's question?

1.3. Mathematics and logic

Proofs in mathematics are logical arguments. The purpose of this section is to remind you briefly of some of the common strategies of proof, and of the facts of logical equivalence of certain kinds of statements on which these strategies depend.

1.3.1. Implications.

1.3.1. Implications. Most theorems in mathematics can be stated as *implications* (or *conditional statements*). An implication is a statement of the form "If P, then Q." Here P an Q are simple statements that can be either true or false. The statement "If P, then Q." is symbolically written as $P \Rightarrow Q$.

The implication $P \Rightarrow Q$ is false when P is true and Q is false, and true otherwise. This is summarized in the truth table on the right.

In the implication $P \Rightarrow Q$, P is called the *hypothesis* (or *premise*) and Q is called the *conclusion* (or *consequence*).

P	Q	$P \Rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

To make mathematical language more colorful we use a great variety of different ways of saying: "If P, then Q." Here are some of the most common:

Q when P.
Q if P.
Q by P.
When P, Q.
If P, Q.

Q follows from P.
Q whenever P.
P only if Q.
P implies Q.
By P, Q.

P is sufficient for Q.
Q is necessary for P.
A sufficient condition for Q is P.
A necessary condition for P is Q.
Q provided that P.

Try constructing different ways of saying "If P, then Q." using some everyday statements P and Q, and some mathematical statements P and Q suggested below.

P	Q
It rains.	WWU's Red Square is wet.
You get 100% on the final.	You will get an A.
It is sunny today.	We will go to the beach.
I get to the camp first.	I will raise the flag.
n is a positive integer.	$2\,n^2$ is not a square number.
An integer n is divisible by 9.	The sum of the digits in n is divisible by 9.
n is a positive integer.	$n(n+1)$ is even.
$x^2 < x$	$x > 0$ and $x < 1$.

Starting with an implication "If P, then Q." it is possible to produce three more implications by shuffling the order and possibly introducing some "nots". These are

(a) The *contrapositive* of the statement: If not Q, then not P.
(b) The *converse* of the statement: If Q, then P.
(c) The *inverse* of the statement: If not P, then not Q.

The contrapositive of a statement is logically equivalent to it, that is, the contrapositive is true if and only if the original implication is true. This is a useful fact in constructing proofs. (See an example below.)

The truth of the converse and inverse, on the other hand, is not related to that of the original statement, though they are equivalent to one another. (Why?)

Exercise 1.3.1. Write the contrapositive, converse, and inverse of each of the following true statements. Do you agree that the contrapositive is true in each case? What about the converse and inverse?

(a) If $2n$ is an odd integer, then n is not an integer.
(b) If $m > 0$, then $m^2 > 0$.

1.3.2. If and only if. In mathematics we often encounter situations that both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true. Then we write $P \Leftrightarrow Q$ and say that P and Q are equivalent. As before, there are several different ways of saying this in English. A popular one is to say: “P if and only if Q” or “P is necessary and sufficient condition for Q.”

1.3.3. Quantifiers. Mathematical statements usually involve *quantifiers*, although they are not always made explicit. We write things like:

For every integer n, $n(n+1)$ is even.

There exists a real number x such that $x^3 - 2x + 1 = 0$

Some statements may involve several nested quantifiers:

For every cubic polynomial p with real coefficients there exists a real number x such that $p(x) = 0$.

Notice that the order of quantifiers is important.

Exercise 1.3.2. Explain the difference in meaning between the statement just given and this one:

There exists a real number x such that for every cubic polynomial f, $f(x) = 0$.

There are a number of different ways to express in English both the *universal quantifier* (for every, for each, for all...) and the *existential quantifier* (there exists, there is at least one...). We will regard each of these phrases as having exactly the same meaning as each of the others in its category. The logical symbol for the universal quantifier is $\forall$ and for the existential quantifier $\exists$.

1.3.4. Negations. It is often necessary to form the *negation* of a given statement. This is the statement that is true if and only if the original statement is false. (Thus the negation of the negation is the original statement.) Forming the negation is straightforward, but can demand careful attention if the original statement has many parts. Here are some examples.

Statement: If today is Tuesday, then the Western Front is published today.
Negation: Today is Tuesday, and the Western Front is not published today.

Recall that an implication is false only when the “if part” is true and the “then part” is false. Thus the negation must be true exactly under those conditions.

Statement: Bob and Bill are Western students.

Negation: Bob is not a Western student or Bill is not a Western student.

Notice that the original statement becomes false as soon as one man fails to be a Western student. Notice also that the second statement is still true if neither Bob nor Bill is a Western student. "Or" is always used in this way in mathematics.

Statement: Bob or Bill is a Western student.
Negation: Bob and Bill are not Western students.

In the same way, "for every" and "there exists" are interchanged when forming a negation.

Statement: For every x in A, $f(x) > 5$.
Negation: There exists an x in A such that $f(x) \leq 5$.

Statement: There is a rational number r such that $r^2 = 2$.
Negation: For every rational number r, $r^2 \neq 2$.

Here are some more complicated examples.

Statement: For every cubic polynomial f, there exists a real number x such that $f(x) = 0$.
Negation: There exists a cubic polynomial f such that for every real number x, $f(x) \neq 0$.

Statement: There exists a real number x such that for every cubic polynomial f, $f(x) = 0$.
Negation: For every real number x there exists a cubic polynomial f such that $f(x) \neq 0$.

Statement: For every $n \geq N$ and every x in E, $|f_n(x) - f(x)| < 1$.
Negation: There exists an $n \geq N$ and an x in E such that $|f_n(x) - f(x)| \geq 1$.

Think carefully about what each statement means before deciding that you agree that the negations are correct.

Exercise 1.3.3. Form the negation of each statement. Express the negation so that the word "not" or "no" does not occur.

(a) If n is divisible by 9, then the sum of the digits in n is divisible by 9.
(b) There exists an $x > 1$ such that $f(x) = 3$.
(c) For every integer n, 2n is even.
(d) For every $x > 1$, there exists a real number y such that $1 < y < x$.

1.4. Proofs

Most of the time in this class we will be constructing proofs. Here are some simple examples illustrating different styles of proof.

The first is a *direct* proof. Here one simply begins with the hypotheses and any other usable facts and reasons until one reaches the conclusion.

THEOREM 1.4.1. *The square of an odd integer has the form $8k + 1$ for some integer k.*

REMARK 1.4.2. Note that this is really an implication and could be rephrased: If n is an odd integer, then there is an integer k such that $n^2 = 8k + 1$.

PROOF. First we need to rewrite the hypothesis in a more useful form. "n is odd" means that n is not divisible by 2, that is, if we try to do the division we'll get a quotient q and a remainder of 1. Equivalently, $n = 2q + 1$. Thus

$$n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1.$$

Now either q is even, $q = 2r$ for some integer r, or q is odd, $q = 2s + 1$ for some integer s. In the first case,

$$n^2 = 8r(q + 1) + 1.$$

In the second case $q + 1 = 2s + 2 = 2(s + 1)$ so that

$$n^2 = 8q(s + 1) + 1.$$

Thus, we do have $n^2 = 8k + 1$ in either case; $k = r(q + 1)$ or $k = q(s + 1)$ as appropriate. □

The second very useful strategy to prove the implication $P \Rightarrow Q$ (P implies Q) is to prove its contrapositive $\neg Q \Rightarrow \neg P$ (not Q implies not P). As we noted earlier:

THE CONTRAPOSITIVE OF A STATEMENT IS LOGICALLY EQUIVALENT TO IT, THAT IS, THE CONTRAPOSITIVE IS TRUE IF AND ONLY IF THE ORIGINAL IMPLICATION IS TRUE. (This can be shown using truth tables.)

REMARK 1.4.3. Whenever you work with an implication it is very useful to state its contrapositive as well. In fact, you should always write both direct implication and its contrapositive and then decide which one is easier to prove.

THEOREM 1.4.4. *If n^2 is even, then n is even.*

PROOF. The contrapositive of this statement is (using the fact that every integer is either even or odd): if n is odd, then n^2 is odd. This has just been proved, since an integer of the form $8k + 1$ is certainly odd. □

The third strategy to prove an implication is a proof by contradiction. In a proof of $P \Rightarrow Q$ by contradiction one assumes both P and $\neg Q$ (not Q) and derives a contradiction. This establishes that $P \Rightarrow Q$ is true because the only way for this implication to be false is for P to be true and Q to be false.

THEOREM 1.4.5. *$\sqrt{2}$ is irrational.*

Proof. We can rephrase the theorem as the following implication: If $x^2 = 2$, then x is irrational.

Suppose that x is rational. Then $x = a/b$ for some integers a and b. We may assume that this fraction is in lowest terms, that is, that a and b have no common factor. Then $2 = x^2 = (a/b)^2$ or $2b^2 = a^2$. Thus a^2 is even. By the previous theorem, a is even, i.e., $a = 2c$ for some integer c. But then

$$2b^2 = (2c)^2 = 4c^2 \quad \text{or} \quad b^2 = 2c^2.$$

Thus b is also even. But this contradicts our choice of a and b as having no common factor. Thus assuming that x is rational has led to a contradiction and we can conclude that x must be irrational. □

The proof above is an example of a proof by contradiction. Very often proofs by contradiction are in fact direct proofs of the contrapositive in disguise.

The direct proof of the contrapositive. We will prove the following implication: If x is rational, then $x^2 \neq 2$.

Let x be a rational number. Then there exist integers p and q which are not both even, such that $x = p/q$. Now we need to prove that $\bigl(p/q\bigr)^2 \neq 2$, or equivalently $p^2 \neq 2q^2$.

Consider two cases: Case 1: p is not even, and Case 2: q is not even.

Case 1. Assume that p is not even. Then p is odd. By Theorem 1.4.4, p^2 is odd. Therefore $p^2 \neq 2a$ for all integers a. Therefore $p^2 \neq 2q^2$.

Case 2. Assume that q is not even. Then q^2 is odd. Therefore there exists an integer k such that $q^2 = 2k + 1$. Consequently $2q^2 = 4k + 2$. This implies that $2q^2$ is not a square. (To see this prove: If an integer is an even square, then it is divisible by 4.) Therefore $2q^2 \neq p^2$. □

Very often proofs by contradiction are disguised proofs of the contrapositive. Before you do a proof by contradiction you should try to prove the contrapositive first.

1.5. Sets

By a *set* A we mean a well-defined collection of objects such that it can be determined whether or not any particular object is an element of A. If a is an object in the set A we say that a is an *element* of A and write $a \in A$. The negation of $x \in A$ is $x \notin A$.

The *empty set* is the unique set which contains no elements. The empty set is denoted by the symbol $\emptyset$.

Generally, capital letters will be used to denote sets of objects and lower case letters to denote objects themselves. However, watch for deviations of this rule. We will be concerned mainly with sets of real numbers. The specially designed letters $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ denote the following important sets of real numbers:

$\mathbb{N}$ denotes the set of all *natural numbers* (or *positive integers*),
$\mathbb{Z}$ denotes the set of all *integers*,
$\mathbb{Q}$ denotes the set of all *rational numbers*,
$\mathbb{R}$ denotes the set of all *real numbers*.

A set can be described by:

- a statement such as "Let A be the set of real solutions of the equation $x^2 - x = 0$."
- a listing of all the elements; for example $A = \{0, 1\}$.
- notation such as $A = \bigl\{x \in \mathbb{R} : x^2 = x\bigr\}$.

Notice the usage of the braces (or curly brackets) $\{$ and $\}$ in the above examples. They are used to delimit the sets. The number 0 is an important real number. However, $\{0\}$ is the <u>set</u> whose only element is 0.

The expression $\bigl\{x \in \mathbb{R} : x^2 = x\bigr\}$ is read as "the set of all real numbers x such that $x^2 = x$". Here the colon (:) is used as an abbreviation for the phrase "such that".

Definition 1.5.1. A set A is a *subset* of a set B if every element of A is also an element of B. In this case we write $A \subset B$ or $B \supset A$. Formally, $A \subset B$ if and only if $x \in A$ implies $x \in B$.

Since the implication $x \in \emptyset \ \Rightarrow \ x \in A$ is always true, the empty set is a subset of each set. Below is the set of all subsets of the set $\{-1, 0, 1\}$.

$$\bigl\{\emptyset, \{-1\}, \{0\}, \{1\}, \{-1, 0\}, \{-1, 1\}, \{0, 1\}, \{-1, 0, 1\}\bigr\}$$

Definition 1.5.2. Two sets A and B are *equal*, denoted $A = B$, if they contain precisely the same elements, that is, if $A \subset B$ and $B \subset A$.

Notice that the elements are not repeated in a set; for example $\{0, 1, 0\} = \{0, 1\}$. Also, the order in which elements are listed is not important: $\{3, 2, 1\} = \{1, 2, 3\}$.

Remark 1.5.3. Equality is allowed in the definition of a subset, that is, a set is a subset of itself. If we wish to exclude this possibility we say A is a *proper subset* of B and we write $A \subsetneq B$. Formally, $A \subsetneq B$ if and only if $x \in A$ implies $x \in B$ and there exists $b \in B$ such that $b \notin A$.

The negation of $A \subset B$ is denoted by $A \not\subset B$. Formally, $A \not\subset B$ if and only if there exists $a \in A$ such that $a \notin B$.

Definition 1.5.4. The *union* of A and B is the set of all x such that x is an element of A or x is an element of B. It is denoted $A \cup B$. Thus

$$A \cup B = \bigl\{x : \ x \in A \ \text{ or } \ x \in B\bigr\}.$$

Remark 1.5.5. The conjunction "or" in mathematics is always in an inclusive sense, that is, it is allowed in the definition that x belong to both A and B. For example, $\{0, 1, 2, 3\} \cup \{2, 3, 4, 5\} = \{0, 1, 2, 3, 4, 5\}$.

Definition 1.5.6. The *intersection* of A and B is the set of all x such that x is an element of A and x is an element of B. It is denoted $A \cap B$. Thus

$$A \cap B = \bigl\{x : \ x \in A \quad \text{and} \quad x \in B\bigr\}.$$

Two sets A and B are said to be *disjoint* if their intersection is the empty set, i.e. if $A \cap B = \emptyset$.

Definition 1.5.7. The *difference* between the sets A and B is the set of all x such that x is an element of A and x is not an element of B. It is denoted $A \setminus B$. Thus

$$A\backslash B = \bigl\{x : \ x \in A \ \text{ and } \ x \notin B\bigr\}.$$

Definition 1.5.8. An *ordered pair* is a collection of two not necessarily distinct elements, one of which is distinguished as the first coordinate (or first entry) and the other as the second coordinate (second entry). The common notation for an ordered pair with first coordinate a and second coordinate b is (a, b).

Remark 1.5.9. The ordered pairs $(0, 1)$ and $(1, 0)$ are different since their first entries are different. The ordered pairs $(0, 0)$ and $(0, 1)$ are different since their second entries are different. In general, $(a, b) = (x, y)$ if and only if $a = x$ and $b = y$.

Notice the usage of the round brackets (and) in the definition of an ordered pair. Please distinguish between $\{0, 1\}$ and $(0, 1)$: $\{0, 1\}$ is a set with two elements, $(0, 1)$ is an ordered pair, an object defined by Definition 1.5.8.

Definition 1.5.10. The *Cartesian product* (or *direct product*) of two sets A and B, denoted $A \times B$, is the set of all possible ordered pairs whose first entry is a member of A and whose second entry is a member of B:

$$A \times B = \bigl\{(a, b) \ : \ a \in A \ \text{ and } \ b \in B\bigr\}.$$

The main example of a Cartesian product is $\mathbb{R} \times \mathbb{R}$ which provides a coordinate system for the plane.

Example 1.5.11. Let $A = \{1, 2, 3, 4\}$ and let $C = \{\mathtt{R}, \mathtt{G}, \mathtt{B}\}$ be the set of primary colors where R stands for red, G for green, and B for blue. Then

$$A \times C = \bigl\{(1, \mathtt{R}), (1, \mathtt{G}), (1, \mathtt{B}), (2, \mathtt{R}), (2, \mathtt{G}), (2, \mathtt{B}),$$
$$(3, \mathtt{R}), (3, \mathtt{G}), (3, \mathtt{B}), (4, \mathtt{R}), (4, \mathtt{G}), (4, \mathtt{B})\bigr\}.$$

Ideally, mathematical terminology and notation should be completely free of ambiguities. We strive for the absolute certainty. However, very soon we will introduce the concept of an open interval and for this concept we will use the same notation as for an ordered pair. It should be clear from the context what is meant. Whenever you are uncertain look for the resolution of the uncertainty.

We conclude this section with a remark about families of sets. In this class we mostly talk about sets of real numbers. Sometimes we will talk about sets whose elements are also sets. It is customary to use the word "*family*" instead of "set" when we talk about sets of sets; see examples in Section 2.3.

For any nonempty family of sets we can define the concepts of union and intersection. Let $\mathcal{A}$ be a nonempty family of sets. We define the intersection of the family $\mathcal{A}$ to be

$$\bigcap \bigl\{A \, : \, A \in \mathcal{A}\bigr\} := \bigl\{x \, : \, x \in A \ (\forall\, A \in \mathcal{A})\bigr\}.$$

We define the union of the family $\mathcal{A}$ to be

$$\bigcup \bigl\{A \, : \, A \in \mathcal{A}\bigr\} := \bigl\{x \, : \, \exists\, A \in \mathcal{A} \ \text{ such that } \ x \in A\bigr\}$$

1.6. Functions

Let A and B be nonempty sets. A *function* from A to B is a rule f which assigns a unique element of B to each element of A.

The set A is called the *domain* of the function. We denote by $f(x)$ the element of B which is assigned to a particular $x \in A$. This element is called a value of f at x, or image of x under f.

As a simple example we can define the identity function on a set A, $\mathrm{id}_A : A \to A$, by $\mathrm{id}_A(x) = x$ for all $x \in A$.

A weakness of the above definition of a function is that it relies on the undefined concept of a "rule". It is not clear what constitutes a valid rule defining a function. To overcome this weakness we identify a function f with its graph G_f which is a subset of the cartesian product $A \times B$:

$$G_f = \bigl\{ \bigl(x, f(x)\bigr) \; : \; x \in A \bigr\}.$$

and we require that for each x in A there is at most one pair (x, y) in this subset. The formal definition of a function from A to B is given in terms of subsets of $A \times B$.

Definition 1.6.1. A *function* from A into B is a subset G_f of the Cartesian product $A \times B$ such that

(i) for every $x \in A$ there exists $y \in B$ such that $(x, y) \in G_f$;
(ii) if $(x, y), (x, z) \in G_f$, then $y = z$.

Consider the sets A and C given in Example 1.5.11. The subset

$$\bigl\{(1, \mathtt{G}), (2, \mathtt{R}), (3, \mathtt{G}), (4, \mathtt{B})\bigr\}.$$

of $A \times C$ is a function in the sense of Definition 1.6.1. In the traditional notation this function is given by $f(1) = \mathtt{G}, f(2) = \mathtt{R}, f(3) = \mathtt{G}, f(4) = \mathtt{B}$. In contrast, the subset

$$\bigl\{(1, \mathtt{B}), (2, \mathtt{G}), (2, \mathtt{R}), (3, \mathtt{R}), (4, \mathtt{G})\bigr\}$$

is not a function since $(2, \mathtt{G}), (2, \mathtt{R})$ are in the set and $\mathtt{G} \neq \mathtt{R}$. Hence (ii) in Definition 1.6.1 does not hold for this set.

For small sets A and B we can list all the functions from A to B.

Example 1.6.2. Let $A = \{0, 1\}$ and let $C = \{\mathtt{R}, \mathtt{G}, \mathtt{B}\}$. The following is the list of all functions from A to C.

$$\bigl\{(0, \mathtt{R}), (1, \mathtt{R})\bigr\}, \quad \bigl\{(0, \mathtt{R}), (1, \mathtt{G})\bigr\}, \quad \bigl\{(0, \mathtt{R}), (1, \mathtt{B})\bigr\}, \quad \bigl\{(0, \mathtt{G}), (1, \mathtt{R})\bigr\}, \quad \bigl\{(0, \mathtt{G}), (1, \mathtt{G})\bigr\}$$
$$\bigl\{(0, \mathtt{G}), (1, \mathtt{B})\bigr\}, \quad \bigl\{(0, \mathtt{B}), (1, \mathtt{R})\bigr\}, \quad \bigl\{(0, \mathtt{B}), (1, \mathtt{G})\bigr\}, \quad \bigl\{(0, \mathtt{B}), (1, \mathtt{B})\bigr\}.$$

In the rest of these notes we will use the informal definition of a function. The symbol $f : A \to B$ stands for a function from A to B. If we want to emphasize the rule that defines f we write $f : x \mapsto f(x), \; x \in A$. For example, $x \mapsto x^2, \; x \in \mathbb{R}$, denotes the square function defined on $\mathbb{R}$ without giving this function a specific name.

The set $\bigl\{f(x) \; : \; x \in A\bigr\}$ is the *range* of f. Formally, y is in the range of f if and only if there exists $x \in A$ such that $y = f(x)$.

A function $f : A \to B$ is *one-to-one* (or *injection*) if distinct elements of A have distinct images in B, i.e., if for all $x, \; y \in A, \; x \neq y$ implies $f(x) \neq f(y)$. Notice that the contrapositive of the last implication is: for all $x, \; y \in A, \; f(x) = f(y)$ implies $x = y$. To prove that a function $f : A \to B$ is not one-to-one we have to find $x_1, x_2 \in A$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

There are only three functions listed in Example 1.6.2 which are not one-to-one. Find them!

The function $x \mapsto x^2,\ x \in \mathbb{R}$, is not one-to-one since -1 and 1 are in the domain of this function and $-1 \neq 1$ and $1 = (-1)^2 = 1^2$. However, with $A = \{x \in \mathbb{R} : x \geq 0\}$, the function $x \mapsto x^2,\ x \in A$, is one-to-one. This will be proved in the next chapter.

A function $f : A \to B$ is *onto* (or *surjection*) if for every point $y \in B$ there is at least one point $x \in A$ such that $f(x) = y$. Another way of saying that $f : A \to B$ is onto B is to say that the range of f is whole B. To prove that $f : A \to B$ is not onto we have to prove that there exists $b \in B$ such that for all $x \in A$ we have $f(x) \neq b$.

Let $A = \{x \in \mathbb{R} : x \geq 0\}$ and $s(x) = x^2, x \in \mathbb{R}$. Then $s : \mathbb{R} \to A$ is a surjection. To prove this we have to prove that for every $a \geq 0$ there exists $x \in \mathbb{R}$ such that $x^2 = a$. The case $a = 0$ is easy; we can take $x = 0$. The case $a > 0$ will be discussed at the end of the next section.

It is interesting to note that with $B = \{x \in \mathbb{Q} : x \geq 0\}$ the function $s : \mathbb{Q} \to B$ is not a surjection. This was essentially proved in Theorem 1.4.5. In the direct proof of the contrapositive of this theorem we proved that $x^2 \neq 2$ for every $x \in \mathbb{Q}$. Since $2 \in B$, this proves that $s : \mathbb{Q} \to B$ is not a surjection.

A function $f : A \to B$ which is both one-to-one and onto is called *bijection*.

Let $f : A \to B$ and $g : C \to D$ be given functions. Assume that the range of f is contained in the domain of g. Then we can define the function $h : A \to D$ by

$$h(x) = g\bigl(f(x)\bigr), \qquad x \in A.$$

The function h is called a composition of f and g and it is denoted by $g \circ f$.

Exercise 1.6.3. Let A and B be nonempty sets. Let $f : A \to B$ be a given function. Prove f is a bijection if and only if there exists a function $h : B \to A$ such that $h \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$.

Solution. Assume that $f : A \to B$ is a bijection. Then for every $b \in B$ there exists unique $a \in A$ such that $f(a) = b$. Define the function $h : B \to A$ by $h(y) = x$. Let $x \in A$ be arbitrary and let $y = f(x)$. Then, by the definition of h, $h(y) = x$ and $h(f(x)) = x$. Since $x \in A$ was arbitrary we proved that $h \circ f = \mathrm{id}_A$. Let $v \in B$ be arbitrary and let $v = f(u)$. Then, by the definition of h, $h(v) = u$ and $f(h(v)) = v$. Since $v \in B$ was arbitrary we proved that $f \circ h = \mathrm{id}_B$.

To prove the converse, assume that there exists a function $h : B \to A$ such that $h \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$. To prove that f is a surjection, let $b \in B$ be arbitrary. Set $a = h(b)$. Than $f(a) = f(h(b)) = \mathrm{id}_B(b) = b$. Hence f is a surjection. To prove that f is an injection let $a_1, a_2 \in A$ and $f(a_1) = f(a_2)$. Since $f(a_1) = f(a_2) \in B$ and since $h : B \to A$ is a function, we have $h(f(a_1)) = h(f(a_2))$. Since $h \circ f = \mathrm{id}_A$ we have $h(f(a_1)) = \mathrm{id}_A(a_1) = a_1$ and $h(f(a_2)) = \mathrm{id}_A(a_2) = a_2$. Thus $a_1 = a_2$. This proves that f is an injection. □

The function f^{-1} is called the inverse function of f. Clearly $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$.

Exercise 1.6.4. Let A, B and C be nonempty sets. Let $f : A \to B$ and $g : B \to C$ be injections. Prove that $g \circ f : A \to C$ is an injection.

Exercise 1.6.5. Let A, B and C be nonempty sets. Let $f : A \to B$ and $g : B \to C$ be surjections. Prove that $g \circ f : A \to C$ is a surjection.

Solution. To prove that $g \circ f : A \to C$ is a surjection we have to prove that for each $c \in C$ there exists $a \in A$ such that $g(f(a)) = c$. Let $c \in C$ be arbitrary. Then, since $g : B \to C$ is a surjection, there exists $b \in B$ such that $g(b) = c$. Since $b \in B$ and since $f : A \to B$ is a surjection, there exists $a \in A$ such that $f(a) = b$. Now it is easy to show that $g(f(a)) = g(b) = c$. □

Exercise 1.6.6. Let A, B and C be nonempty sets. Let $f : A \to B$ and $g : B \to C$ be bijections. Prove that $g \circ f : A \to C$ is a bijection. Prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

We conclude this section with a negation exercise.

Exercise 1.6.7. Formulate the negation of the following claim.

Claim. *Let A and B be nonempty sets. There exists a surjection $f : A \to B$.*

Solution. The negation is: For an arbitrary function $g : A \to B$, g is not a surjection. But the statement “g is not a surjection” is itself a negation which means: There exists $b \in B$ such that for all $x \in A$ we have $g(x) \neq b$. Hence the negation of the given claim is:

For an arbitrary function $g : A \to B$ there exists $b \in B$ such that for all $x \in A$ we have $g(x) \neq b$. Symbolically this can be written as

$$\forall\ g : A \to B \quad \exists\ b \in B \quad \text{such that} \quad \forall\ x \in A \quad g(x) \neq b.$$

Sometimes the set of all functions defined on A with the values in B is denoted by B^A. With this notation the last statement can be written nicer as

$$\forall\ g \in B^A \quad \exists\ b \in B \quad \text{such that} \quad \forall\ x \in A \quad g(x) \neq b.$$

It is important to note that b in this statement depends on g. In a proof the last statement one would start from an arbitrary g and then try to construct $b \in B$ with the desired property. □

1.7. Four basic ingredients of a Proof

Since in this course you will be writing your own proofs and studying proofs of others, we conclude this chapter with four basic ingredients of a Proof.

A proof should contain ingredients which answer the following four questions:

- What is being assumed?
- What is being proved?
- What are the tools that are being used?
- Why is it legitimate to use those tools?

Sometimes the presence of these ingredients in a proof is implicit. But, it should always be easy to identify them.

These four questions are a good starting point when you critically evaluate your own proofs or when you comment on the proofs of others.