Bridge to Higher Mathematics

1. Week 1 (week of 2025-09-01)

1.1. Logical propositions and quantifiers

When writing about mathematics, we will often use the language of predicate logic or first-order logic.

First of all, a proposition is a statement that can be classified as either true or false.

We can combine proposition to form new ones:

Definition 1.1.1: Let P and Q be propositions:

- the proposition $P \wedge Q$ (read: "P and Q") is true if both P and Q are true.
- the proposition $P \vee Q$ (read: "P or Q") is true if either P is true or Q is true (or both, of course).
- the proposition $\neg P$ (read: "not P") is true if P is false.
- the proposition $P \Rightarrow Q$ (read: "P implies Q") is equivalent to $Q \vee \neg P$.

For example:

- $2 > 0$ is a proposition (and it is true).
- $3 = 0$ is a proposition (and it is false).
- The proposition $(2 > 0) \wedge (3 = 0)$ is false, while $(2 > 0) \vee (3 = 0)$ is true.

Definition 1.1.2: A logical predicate is family of propositions depending on a variable.

More precisely, if a is a variable, we can consider a proposition Φa for each possible value of a; we say that Φa is a predicate.

For example:

- the statement $a^2 - 1 < 0$ is a predicate Φa depending on the variable a. For real numbers a, the corresponding proposition Φa is true for a in the interval $(-1, 1)$ and false otherwise.

Definition 1.1.3: If a is a *variable* and Φ is a logical *predicate* which depends on a, we write

- $\forall a, \Phi a$ for the proposition that Φa holds for all possible value of the variable a.
- $\exists a, \Phi a$ for the proposition that there exists *some* value of the variable a for which the proposition Φa is true.
- $\exists! a, \Phi a$ for the proposition that there exists a *unique* value of the variable a for which the proposition Φa is true.

Here are some examples:

- The proposition $\forall a \in \mathbb{R}, a^2 \geq 0$ means that for all real numbers a, the condition $a^2 \geq 0$ holds. This proposition is true!

- The proposition $\exists a \in \mathbb{R}, a^2 - 4 = 0$ means that there exists real numbers a for which the condition $a^2 - 4 = 0$. In fact, $a = 2$ and $a = -2$ both work, so the proposition is true.
- The proposition $\exists! a \in \mathbb{R}, a^3 = -8$ means that there exists a unique real number a satisfying the indicated equation. In fact $a = -2$ is the only solution, so the proposition is true.

1.2. Sets

We now introduce the language of set theory which is the basic notation used for reading and writing Mathematics.

We need to start somewhere, so although this is not a proper definition, we call a collection of objects a set.

For example:

- the collection of all students in our class is a set
- the collection of all negative real numbers is a set

  the collection of all pairs (n, m) of natural numbers is a set

1.2.1. Notations for standard mathematical sets

There are some sets of numbers that are used over and over in Math and we reserve some particular letters to design them.

- $\mathbb{N} = \{0, 1, 2, 3, ...\}$ is the set of natural numbers.
- $\mathbb{Z} = \{... - 2, -1, 0, 1, 2, ...\}$ is the set of integers ("*zahlen*" in German).
- $\mathbb{Q}$, the set of rational numbers is

  $$\mathbb{Q} = \{n/m \mid \text{for integers } n, m \text{ with } m \neq 0\},$$

  where fractions satisfy the condition $n/m = a/b$ if and only if $nb = ma$.

  ($\mathbb{Q}$ as in "q" for "quotient").
- $\mathbb{R}$, the set of real numbers that you know from calculus.
- $\mathbb{C}$, the set of complex numbers, where a complex number z has the form $z = a + bi$ for real numbers a and b.

1.2.2. Basic properties of sets.

We indicate that an object a is a member of a set A using the symbol $a \in A$. For example $2 \in \mathbb{N}$ and $-2 \in \mathbb{Z}$, while $1/2 \in \mathbb{Q}$ but $1/2 \notin \mathbb{Z}$.

By convention, we will normally denote sets with capital letters, and elements with lower-case letters. Thus $a, b \in A$.

For sets with a finite number of elements, we can specify the set by just listing the elements. For example, if A denotes the set consisting of the first three letters of the English alphabet, then we can simply write $A = \{a, b, c\}$.

Sometimes we specify a set using set builder notation. This means that we indicate some predicate required for membership in the set. Thus

$$B = \{a \in A \mid \Phi a\}$$

is the set of all elements a in A for which the predicate Φ is true.

This should be read: "B is the set of all a in A *such that* Φa holds."

For example, the set E of even integers can be expressed in set builder notation using the predicate "is even"; thus we can write

$$E = \{x \in \mathbb{Z} \mid x \text{ is even}\}$$

read this as: "E is the set of all x in $\mathbb{Z}$ *such that* x is even".

Definition 1.2.2.1: If A and B are sets, then $A = B$ provided that $x \in A \Leftrightarrow x \in B$

Definition 1.2.2.2: When every element of a set A is also an element of another set B, we say that A is a subset of B and write $A \subseteq B$.

A more precise statement is as follows: if $\forall a \in A$ we have $a \in B$, then $A \subseteq B$.

Note that $A \subseteq B$ allows the possibility that A and B are equal. The condition $A \subset B$ – or more precisely $A \subsetneq B$ – is defined by $A \subseteq B$ and $\exists b \in B, b \notin A$.

.

Example 1.2.2.3:

(a). The number 2 is a natural number. We say that 2 is an element of – or is a member of - the set of natural numbers, and we indicate this by writing $2 \in \mathbb{N}$.

(b). The notation $\{2\}$ means a set whose only element is the number 2. It is not correct to write that $\{2\} \in \mathbb{N}$. Instead, we write $\{2\} \subseteq \mathbb{N}$.

(c). There are natural inclusions

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

In fact, all these sets are different, so we could also write

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

(d). The empty set is the set that has no elements. It is denoted with the symbol $\emptyset$. So, $\emptyset = \{\}$.

(e). Any set A has the empty set as a subset: $\emptyset \subseteq A$.

(f). And any set A has itself as a subset: $A \subseteq A$.

1.2.3. Equality of sets

Two sets A and B are equal provided they have precisely the same elements. Thus we have

$$A = B \Leftrightarrow (A \subseteq B) \text{ and } (B \subseteq A)$$

Example 1.2.3.1:

(a). Define

$$A = \{x \in \mathbb{R} \mid x^3 - 3x^2 + 2x = 0\}, \text{and } B = \{0, 1, 2\}.$$

We argue that $A = B$.

First we show that $B \subseteq A$. As B is given as a finite collection of real numbers, we can just check that all elements in B satisfy the condition that is required for a real number to be in A.

That is, we need to see that each $0, 1, 2$ satisfy the condition for membership in A. Thus we must confirm that

$$0^3 - 3 \times 0^2 + 2 \times 0 = 0, \qquad 1^3 - 3 \times 1^2 + 2 \times 1 = 0, \qquad 2^3 - 3 \times 2^2 + 2 \times 2 = 0.$$

These equalities are all satisfied, so indeed $B \subseteq A$.

We now need to prove the converse inclusion, i.e. that $A \subseteq B$. Essentially, this means finding the solutions to the equation $x^3 - 3x^2 + 2x = 0$ and proving that these solutions are among $0, 1, 2$.

Factoring the polynomial, we find

$$x^3 - 3x^2 + 2x = x(x^2 - 3x + 2) = x(x-1)(x-2)$$

For a product to be 0, one of the factors needs to be zero. This leads us to $x = 0, x = 1$, or $x = 2$ as required.

(b). Define

$$C = \{x \in \mathbb{R} \mid x^3 - 3x^2 + 2x > 0\}, \quad D = \{x \in \mathbb{R} \mid 0 < x < 1 \text{ or } 2 < x < \infty\}$$

Let us show that $C = D$.

We saw already seen the factorization $x^3 - 3x^2 + 2x = x(x-1)(x-2)$; thus

$$C = \{x \in \mathbb{R} \mid x(x-1)(x-2) > 0\}.$$

A product of three numbers is positive if all of them are positive or two of them are negative and one positive. Now,

- $x - 1 > 0$ is equivalent to $x > 1$,
- $x - 2 > 0$ is equivalent to $x > 2$, and of course
- $x > 0$ is equivalent to $x > 0$.

So a real number x is a member of the set C if all three of these three inqualities hold, or if exactly one of these inequalities hold. So, all three factors are positive for $x > 2$ while two of the factors are negative and the third positive for $0 < x < 1$. Using interval notation as in Calculus, the two sets are $(2, \infty)$ and $(0, 1)$ respectively. The set C is then composed of these two pieces (we will introduce notation for this soon) and this is precisely the way D was defined.

1.2.4. Operations on sets

In this section, we introduce some basic operations. Let A and B be sets.

Definition 1.2.4.1: The union $A \cup B$ is the set whose elements are in either A or B (or both). In symbols,

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

Definition 1.2.4.2: The intersection $A \cap B$ is the set whose elements are in both A and B. In symbols,

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}.$$

Definition 1.2.4.3: A and B are said to be disjoint if their intersection is the empty set – i.e if $A \cap B = \emptyset$.

If A and B are disjoint, the union $A \cup B$ is sometimes called a disjoint union, since an element $x \in A \cup B$ satisfies either $x \in A$ or $x \in B$ but not both.

Definition 1.2.4.4: The difference $A - B$ of the sets A and B is the set of elements that are in the first set and not in the second set:

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

Definition 1.2.4.5: If the set A is a subset of a set U, the complement of A (in U) is defined to be the set

$$\bar{A} = \{x \in U \mid x \notin A\} = U - A.$$

Remark 1.2.4.6: Unions and intersections can be taken for several (more than two) sets, even for infinite collections.

Set operations are sometimes represented and visualized using *Venn Diagrams*; each set is represented as a shape, and the results of the set operations are represented by certain regions, as in Figure 1.

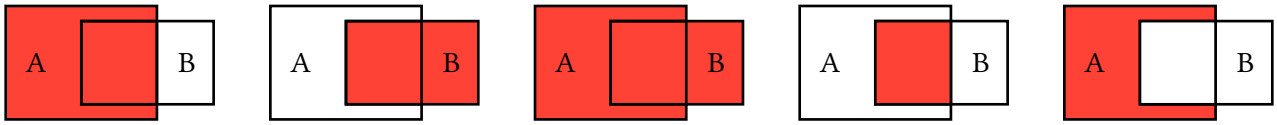

Figure 1: From left to right: A, B, $A \cup B$, $A \cap B$, $A - B$

Example 1.2.4.7:

(a). In Example 1.2.3.1, we showed that $C = D$. By its definition, the set D is equal to the union $(0, 1) \cup (2, \infty)$. Thus, this set is the union of two intervals in the real line.

(b). The intersection of $(0, 1)$ and $(2, \infty)$ is empty; i.e. $(0, 1) \cap (2, \infty) = \emptyset$. So , the expression $C = (0, 1) \cup (2, \infty)$ shows that C is the disjoint union of two open intervals in the real line.

(c). For every $n \in \mathbb{N} - \{0\}$ define the semiopen interval of the real line A_n by $A_n = \left(-\frac{1}{n}, n\right]$. The parentheses (on the left indicates that $-\frac{1}{n}$ is not in the set while the bracket] means that n is. Then

$$\bigcap_{n \in \mathbb{N} - \{0\}} A_n = [0, 1]$$

First of all $[0, 1]$ is contained in each A_n and therefore in its intersection. Also any real number greater than 1 is not contained in A_1 and therefore not contained in the intersection of all A_n.

Now, the sequence $\left\{-\frac{1}{k}\right\}$ has limit zero. Thus for any strictly negative number x, we can find some k such that x is smaller than $-\frac{1}{k}$ and therefore $x \notin A_k$ and *a fortiori* x is not in the intersection of all of the A_n.

Similarly, we can compute the union:

$$\bigcup_{n \in \mathbb{N} - \{0\}} A_n = (-1, \infty).$$

No number smaller than or equal to –1 is in any A_k, therefore, it cannot be in its union. The numbers between -1 and 0 are in A_1 and therefore in the union.

Any positive number is smaller than some natural number m and therefore it is in A_m.

Definition 1.2.4.8: The cartesian product $A \times B$ of the sets A and B is the set whose elements are ordered pairs of elements with the first one in A the second one in B:

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$$

Example 1.2.4.9:

(a). You are already familiar with at least one cartesian product. The set of real numbers is represented geometrically as a real line. The cartesian product of two real lines is the set of pairs of real numbers. This is a representation of the points in the plane with each point determined by its two coordinates. That is, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the set of points in the plane.

(b). If $A = \{a_1, a_2, ..., a_n\}$ and $B = \{b_1, b_2, ..., b_m\}$ for natural numbers $n, m \in \mathbb{N}$, then $A \times B = \{(a_s, b_t) : 1 \leq s \leq n, 1 \leq t \leq m\}$.

(c). Let $A = \{x \in \mathbb{R} \mid x^3 - 3x^2 + 2x = 0\}, B = \{x \in \mathbb{R} \mid x^2 - 4 = 0\}$. We have seen in Example 1.2.3.1 that A may written $A = \{0, 1, 2\}$. Similarly, $B = \{2, -2\}$. Therefore,

$$A \times B = \{(0, 2), (1, 2), (2, 2), (0, -2), (1, -2), (2, -2)\}.$$

Definition 1.2.4.10: The power set $\mathcal{P}(A)$ of a set A is the set consisting of all subsets of A:

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Example 1.2.4.11:

(a). Take $A = \emptyset$. Then, $\mathcal{P}(\emptyset) = \{\emptyset\}$. This is a set whose only element is the empty set. In particular,

$$\mathcal{P}(\emptyset) \neq \emptyset$$

, as it contains one element.

(b). If $A = \{a\}$ is a singleton set – i.e. a set with exactly one element – then $\mathcal{P}(A) = \{\emptyset, \{a\}\}$ contains exactly 2 elements.

(c). If $A = \{a, b\}$ is a set with exactly two elements, then $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ contains exactly $4 = 2^2$ elements.

(d). We see from the previous examples that every time that we add a new element to a set, we double the number of elements in $\mathcal{A}$. We should expect that if A has exactly n elements, then $\mathcal{P}(A)$ has exactly 2^n elements.

We can see this as follows: to construct a subset of A, we must decide for each element of A whether or not the element belongs to the subset. This gives two options for each element. These options can be combined in any arbitrary way, so there are in total 2^n possibilities.

2. Week 2 (week of 2025-09-08)

2.1. About proofs

In Mathematics, a Theorem is a statement that it is known to be true. A proof is the formal evidence for the validity of the Theorem.

Proofs begin from some definitions and some results known to be true or that you accepts as a "axioms"; from there, the proof gives logical steps demonstrating the stated result.

There is a hierarchy among Theorems, less important ones are usually called Propositions and Lemmas.

The word Lemma is normally used for a result that will later be used to prove another result. And the word Corollary is usually used for a result which is (relatively straightforward) consequence of some other Theorem.

But what is a Proposition, a Lemma, a Corollary, or a Theorem varies depending on your point of view or your needs.

This course is meant to make you acquainted with proof techniques that work in a number of settings. But this course will teach you to prove everything you might want! Nobody knows how to prove everything.

Every problem requires specific ideas and methods. The more time you spend working out similar problems, the more likely you are to have seen something similar and come up with an idea that will help you in a proof.

2.2. Some building-block results for proof

Fact 2.2.1: In this course, we will freely use basic properties of addition and product of numbers in the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ including the following. To state them, we use the symbol R to mean one of the sets of numbers $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(a). Associative law: $\forall a, b, c \in R$

$$(a+b)+c = a+(b+c), a(bc) = (ab)c.$$

(b). Commutative laws: $\forall a, b \in R$

$$a+b = b+a \text{ and } ab = ba.$$

(c). Additive and multiplicative identity elements exist: $\exists 0 \in R$ and $\exists 1 \in R$ such that $\forall a \in R$ one has

$$a+0 = a \text{ and } a \times 1 = a.$$

(d). Distributive property: for all $a, b, c \in R$

$$a(b+c) = ab + ac$$

(e). Existence of additive inverses: Suppose that R is not $\mathbb{N}$. $\forall a \in R$, there is another element in R that we call $-a$ such that $a + (-a) = 0$.

(f). Existence of multiplicative inverses: Suppose that R is not $\mathbb{N}$ or $\mathbb{Z}$. $\forall a \in R$ such that $a \neq 0$, there is another element in R that we call $a^{-1} = 1/a$ such that

$$a \cdot a^{-1} = a \cdot 1/a = 1$$

.

(g). Existence of an order: for R one of the sets of numbers $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (but not $\mathbb{C}$):

- for any two distinct elements $a, b \in R$, either $a < b$ or $b < a$.
- Conversely, $a, b \in R$ and $a < b$, then $a \neq b$.
- Moreover, if $a, b, c \in R$, $a < b$ and $b < c$, then $a < c$.
- If $a, b, c \in R$ and $a < b$, then $a + c < b + c$.
- If $a, b, c \in R$, $a < b$ and $c > 0$, then $ac < bc$.

2.3. Some examples of proofs

Definition 2.3.1: Let $a, b \in \mathbb{Z}$.

(a). The integer a is said to divide b if there exists a third integer $c \in \mathbb{Z}$ such that $b = ac$. In this situation, we also say that b is divisible by a.

We write $a \mid b$ to indicate that a divides b.

(b). b is said to be even if $2 \mid b$. Equivalently, b is even if there $\exists c \in \mathbb{Z}$ such that $b = 2c$.

(c). b is said to be odd if $\neg(b \text{ is even})$ i.e. if b is not even.

Remark 2.3.2: Of course, one knows for $b \in \mathbb{Z}$, that b is odd if and only if $\exists c \in \mathbb{Z}, b = 2c + 1$.

This is a consequence of "division with remainder": $\forall b \in \mathbb{Z}, \exists c \in \mathbb{Z}$ and $r \in \{0,1\}$ such that $b = 2c + r$.

We are going to prove:

Proposition 2.3.3:
(a). The sum of two even integers is even.
(b). The sum of two odd integers is even.
(c). The sum of an even and an odd integer is odd.

Proof: Let $a, b \in \mathbb{Z}$.

For (a), suppose that a, b are even. Thus by Definition 2.3.1, $\exists c, d \in \mathbb{Z}$ such that $a = 2c$ and $b = 2d$. Using the distributive law Fact 2.2.1(d) we find that

$$a + b = 2c + 2d = 2(c + d).$$

Thus $a + b$ is indeed even.

For (b), suppose a, b are odd. Using Remark 2.3.2, $\exists c, d \in \mathbb{Z}$ such that $a = 2c + 1$ and $b = 2d + 1$. Using the distributive law We find that

$$a + b = (2c + 1) + (2d + 1) = 2c + 2d + 2 = 2(c + d + 1)$$

where the equality in the second line holds since addition is associative and commutative Fact 2.2.1(a,b), and the equality in the third line holds by the distributive law Fact 2.2.1(d).

For (c), without loss of generality we can assume a is even and b is odd. As before, we can use Definition 2.3.1 and Remark 2.3.2 to find $c, d \in \mathbb{Z}$ such that $a = 2c$ and $b = 2d + 1$. Again using the distributive law Fact 2.2.1(d), we find that

$$a + b = 2c + 2d + 1 = 2(c + d) + 1$$

so that $a + b$ is indeed odd.

■

Definition 2.3.4: Let $n \in \mathbb{N}$.

The number n is prime if $n \neq 1$ and if $\forall m \in \mathbb{N}, m \mid n$ implies that $m = 1$ or $m = n$.

The number n is composite if $n \neq 1$ and if n is not prime.

Proposition 2.3.5: Let $n \in \mathbb{N}$ and suppose that $n \geq 2$.
(a). If n is a natural number greater than or equal than 3, then $n^2 - 1$ is composite.
(b). If n is a natural number greater than or equal than 2, then $n^3 + 1$ is composite.

Proof: (a) Using the equation for the difference of squares we find for $n \in \mathbb{N}$ that

$$n^2 - 1 = (n - 1)(n + 1).$$

Note that while this seems to suggest that $n^2 - 1$ is always composite, that is only true if neither factor is equal to 1. So the required condition is that $n - 1 > 1$ or - since n is a natural number - equivalently $n \Rightarrow 3$.

We remark that the condition that $n \Rightarrow 3$ can't be omitted; when $n = 2$, $n^2 - 1 = 4 - 1 = 3$ is prime and thus not composite

(b) We can write $n^3 + 1 = (n+1)(n^2 - n + 1)$ as you can confirm using the distributive law for the expression on the right-hand-side. This shows that $n^3 + 1$ is composite provided that $n + 1 > 1$ – i.e. $n \geq 2$ – and that $n^2 - n + 1 > 1$.

The condition $n^2 - n + 1 > 1$ is equivalent to $n(n-1) = n^2 - n > 0$ by Fact 2.2.1(g), and this inequality is true for any real number outside the interval $[0, 1]$. In particular, both inequalities hold when $n \geq 2$, as required. ■

2.4. The importance of quantifiers

Sometimes we use several quantifiers in a sentence. The order in which we use them is important

Example 2.4.1:

(a). Consider the two statements:

- $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}$ such that $a + b = 0$
- $\exists b \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}, a + b = 0$

The first statement is true, it is the existence of inverse for addition; this follows from Fact 2.2.1(e) taking $b = -a$. You notice that this b depends on a.

Now this is fine because once we fix our attention on a particular a, we choose the b that works.

The second statement is false, however. This statement claims that there is can find a single interger that is inverse of *every element* in $\mathbb{Z}$.

While we can individually find additive inverses, no number will do the job for all integers at once.

(b). When the two quantifiers are of the same type, then the order does not matter. For example the two statements below are equivalent (and are true by the commutative property Fact 2.2.1(b).

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, 3a + 5b = 5b + 3a$$

$$\forall b \in \mathbb{Z}, \forall a \in \mathbb{Z}, 3a + 5b = 5b + 3a$$

Similarly, the two statements below

$$\exists a \in \mathbb{Z} \text{ such that } \exists b \in \mathbb{Z} \text{ with } 3a + 2b = 1$$

$$\exists b \in \mathbb{Z} \text{ such that } \exists a \in \mathbb{Z} \text{ with } 3a + 2b = 1$$

are equivalent and true taking for instance $a = 1, b = -1$.

Example 2.4.2: Note that when you want to negate a sentence that contains a quantifier, you will need to change the quantifier. Here are some examples:

(a). Consider the statement

$$(\clubsuit) \quad \forall a \in \mathbb{Z}, 2a > a.$$

The statement (♣) is false because there is at least one a that does not satisfy the condition. The statement that is correct is the negation of (♣). Saying that (♣) is not true is the same as saying that at least one integer does not satisfy the condition. Therefore, the negation of the above statement is

$$\exists a \in \mathbb{Z}, 2a \leq a.$$

We could take $a = -1$ to verify the statement.

(b). Consider the statement

$$(\heartsuit) \quad \exists a \in \mathbb{N}, 2a < a.$$

(♥) is false because no natural number a satisfies the condition. The statement that is correct is the negation of (♥) which may be re-stated

$$\forall a \in \mathbb{N}, 2a \geq a.$$

This statement is equivalent to $a \geq 0$ and every natural number satisfies the condition.

(c). Consider the statement (♦) $\forall a \in \mathbb{Q}, \exists b \in \mathbb{Q}$ such that $ab = 1$. This statement is false because there is one $a \in \mathbb{Q}$ that does not satisfy the condition (namely, $a = 0$).

The statement that is correct is the negation of (♦), which may be stated

$$\exists a \in \mathbb{Q} \text{ such that } \forall b \in \mathbb{Q}, ab \neq 1.$$

If we take $a = 0$, then for all b rational, $ab = 0 \neq 1$.

(d). Consider the statement

$$(\spadesuit) \quad \exists a \in \mathbb{Q} - \{0\} \text{ such that } \forall b \in \mathbb{Q} - \{0\}, ab > 0.$$

This statement is false because no matter which $a \in \mathbb{Q} - \{0\}$ we can always find some b with the opposite sign that will not satisfy the condition. The statement that is correct is the negation of (♠) which may be stated

$$\forall a \in \mathbb{Q} - \{0\} \exists b \in \mathbb{Q} - \{0\} \quad \text{such that} \quad ab \leq 0.$$

Given $a \in \mathbb{Q} - \{0\}$, we can choose $b = -a$ and $ab = -a^2$. A square of a non-zero number is always greater than 0 (see below) and therefore the negative of a square is greater than 0.

Let us check that the square of a non-zero number is always greater than 0: using Fact 2.2.1(g), if $a \neq 0$ either $a > 0$ or $a < 0$. If $a > 0$, using (g) again find that $a \times a > a \times 0 = 0$. If $a < 0$, adding $-a$ to both sides of the inequality and using (g) again, we obtain $0 = a - a < 0 - a = -a$. Multiplying both sides of the inequality $0 \leftarrow a$ by $-a$, we obtain $0 < a^2$ as we claimed

2.5. Propositional logic, again

Recall that we said a (logical) proposition is a statement that is either true or false (and not both).

And we described various ways of combining propositions, using

- and, i.e. $\wedge$
- or, i.e. $\vee$
- not, i.e. $\neg$
- implies, i.e. $\rightarrow$

In this section, we point out that one can "calculate" the truth value of an expression involving propositions combined with these symbols.

p	q	not p	p and q	p or q	$p \to q$
true	true	false	true	true	true
true	false	false	false	true	false
false	true	true	false	true	true
false	false	true	false	false	true

Notice that we can for example also handle cases with 3 propositional variables:

p	q	r	$(p \wedge q) \vee r$	$(p \vee r) \to q$
true	true	true	true	true
true	true	false	true	true
true	false	true	true	false
true	false	false	false	false
false	true	true	true	true
false	true	false	false	true
false	false	true	true	false
false	false	false	false	true

Example 2.5.1: Consider the propositions

- p: "I like hiking"
- q: "tomato plants need at least 6 hours of sun each day"
- r: "$3 + 5 = 8$"
- s: "$3 \geq 8$""

Let's write English sentences describing some of our propositional operations:

- The proposition $\neg p$ is: "I don't like hiking".
- The proposition $r \wedge s$ is: "$3 + 5 = 8$ and $3 \geq 8$.
- The proposition $p \vee q$ is: "I like hiking, or tomato plants need at least 6 hours of sun each day."
- The proposition $r \to s$ is: "If $3 + 5 = 8$ then $3 \geq 8$"

The most interesting logical equivalences for us will be the ones that allow us to prove things in different ways.

In particular, we have the following:

Proposition 2.5.2:
(a). $p \Rightarrow q$ is equivalent to $\neg p \vee q$.
(b). $\neg(p \Rightarrow q)$ is equivalent to $p \wedge \neg q$
(c). $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$ (contrapositive).

Proof:
(a). By definition, both of $p \Rightarrow q$ and $\neg p \vee q$ are always true when p is false. Moreover, $p \Rightarrow q$ and $\neg p \vee q$ are both always true when q is true. The only remaining situation is: "p true and q false"; in this case, both $p \Rightarrow q$ and $\neg p \vee q$ are false. Since the two propositions take the same truth values, they are equivalent.
(b). For (b) and (c) we simply confirm these identities by checking that it holds for all possible values of p and q:

p	q	$p \Rightarrow q$	$\neg p \vee q$	$\neg q \Rightarrow \neg p$	$p \wedge \neg q$
`true`	`true`	`true`	`true`	`true`	`false`
`true`	`false`	`false`	`false`	`false`	`true`
`false`	`true`	`true`	`true`	`true`	`false`
`false`	`false`	`true`	`true`	`true`	`false`

■

Finally, we consider the logic underlying "proof by contradiction".

Proposition 2.5.3: Let p be a proposition.
(a). $p \Rightarrow$ `false` is equivalent to $\neg p$.
(b). $\neg\neg p \Rightarrow p$.

Proof: For (a), we just check that the statement $p \Rightarrow$ `false` is equivent to $\neg p$

For (b), we just check that the statement $\neg\neg p \Rightarrow p$ is always true.

We carry out these checks in the following table:

p	$\neg p$	$\neg\neg p$	$\neg\neg p \Rightarrow p$	$p \Rightarrow$ `false`
`true`	`false`	`true`	`true`	`false`
`false`	`true`	`false`	`true`	`true`

■

Remark 2.5.4: Here is the logic behind a proof by contradiction.
- the goal is to prove that p holds

- proceed by assuming that p is false, i.e. that $\neg p$ holds.
- prove that $\neg p$ leads to a falsehood; in other words, prove that $\neg p \Rightarrow$ `false`. This is often done by deriving two mutually contradictory assertions q and $\neg q$ and appealing to that fact that $q \wedge \neg q \Rightarrow$ `false`.
- Since $\neg p \Rightarrow$ `false`, we conclude that $\neg\neg p$ is `true`. Since $\neg\neg p \Rightarrow p$, we finally conclude that p is `true`.

Example 2.5.5:

(a). Let us show that in the set of real numbers, the function $f(x) = 3x + 5$ has no repeated images; that is, no two real numbers map to the same real number.

We can write this symbolically as follows

$$\forall x_1, x_2 \in \mathbb{R}, \text{if } x_1 \neq x_2, \text{then } f(x_1) \neq f(x_2)$$

If p is the proposition $x_1 \neq x_2$ and q is the proposition $f(x_1) \neq f(x_2)$, then the statement takes the form $p \Rightarrow q$.

We carry out a proof by contraposition.

We know that $p \Rightarrow q$ is logically equivalent to $\neg q \Rightarrow \neg p$. The proposition $\neg q \Rightarrow \neg p$ takes the form

$$\forall x_1, x_2 \in \mathbb{R}, \text{if } \ f(x_1) = f(x_2), \text{then } \ x_1 = x_2$$

Let us prove this statement: we assume we have two real numbers $x_1, x_2 \in \mathbb{R}$ such that

$$f(x_1) = f(x_2).$$

From the definition of f, this means that

$$3x_1 + 5 = 3x_2 + 5$$

As we are working with numbers in $\mathbb{R}$, each number has an additive inverse and we can subtract 5 from both sides and get

$$3x_1 = 3x_2$$

We can multiply this equality by $1/3$ and obtain

$$x_1 = x_2$$

which is precisely what we were after.

(b). We are going to show that if an integer is a square then two more than this integer is not a square. We can write this symbolically as follows

$$\forall x \in \mathbb{Z}, \text{if } \exists a \in \mathbb{Z}, \text{such that } x = a^2, \text{then } \nexists b \in \mathbb{Z} \text{ such that } x + 2 = b^2$$

Fix an $x \in \mathbb{Z}$. Let p be the proposition

$$\exists a \in \mathbb{Z}, \text{such that } x = a^2.$$

Let q be the proposition

$$\nexists b \in \mathbb{Z}, \text{such that } x + 2 = b^2.$$

We want to prove the statement $p \Rightarrow q$. We will use a proof by contradiction.

Namely, we will assume that $\neg(p \Rightarrow q)$ and prove `false`.

Now, According to Proposition 2.5.2, $\neg(p \Rightarrow q)$ is equivalent to $p \wedge \neg q$; thus we assume that x is a square and that $x+2$ is a square.

We know that $p \Rightarrow q$ is logically equivalent to $(p \wedge \neg q) \Leftrightarrow F$. The statement

$$p \wedge \neg q$$

takes the form

$$\exists a \in \mathbb{Z}, \text{such that } x = a^2 \wedge \exists b \in \mathbb{Z} \text{ such that } x+2 = b^2$$

Our assumption leads to the existence of $a, b \in \mathbb{Z}$ with $a^2 = x$ and $b^2 = x+2$. Since $(-z)^2 = z^2$, we may as well suppose that a and b are non-negative.

Now

$$2 = x + 2 - x = b^2 - a^2 = (b-a)(b+a).$$

Since a and b are non-negative, we have $b - a \leq b + a$. Since 2 is prime, we conclude that $b - a = 1$ and $b + a = 2$; adding these equations, we find that $2b = 3$ or $b = 3/2$.

Now we have arrived at a contradiction; namely, by assumption $b \in \mathbb{Z}$, but we just argued that $b = 3/2 \in \mathbb{Q} - \mathbb{Z}$ so that $b \notin \mathbb{Z}$.

This contradiction proves that $\neg(p \Rightarrow q)$ implies `false`; thus we have proved $\neg\neg(p \Rightarrow q)$ – see Proposition 2.5.3(a) – by Proposition 2.5.3(b) we deduce that $p \Rightarrow q$ as required.

(c). The square root of 2 is not rational.

Let p be the proposition $x = \sqrt{2}$. Let q be the proposition $x \notin \mathbb{Q}$. We want to prove the statement $p \Rightarrow q$. We will do a proof by contradiction.

Thus we are going to suppose $\neg(p \Rightarrow q)$. Now, Proposition 2.5.2 shows that $\neg(p \Rightarrow q)$ is logically equivalent to $p \wedge \neg q$. Thus we suppose that $x = \sqrt{2}$ and that $x \in \mathbb{Q}$, and we must deduce a contradiction.

Since $x \in \mathbb{Q}$, $\exists a, b \in \mathbb{Z}$ with $b \neq 0$ and

$$(\clubsuit) \quad \sqrt{2} = x = a/b$$

.

We may suppose that the integers a, b have no common factor.

Now, squaring each side of $(\clubsuit)$, we find

$$2 = a^2/b^2 \Rightarrow 2b^2 = a^2.$$

The prime factors of a^2 are the same as the prime factors of a, just with twice the exponent. It follows that, 2 must divide a. Then,

$$a = 2c, \text{so } 2b^2 = a^2 = 4c^2$$

. Dividing both sides by 2, find that

$$b^2 = 2c^2$$

which now shows that 2 must divide b. We have arrived at a contradiction; on the one hand, we assume that a and b have no common factors, but on the other hand we just proved that $2 \mid a$ and $2 \mid b$. This contradiction proves $p \Rightarrow q$, thus $\sqrt{2} \notin \mathbb{Q}$.

Example 2.5.6: Here is an example of a *non-constructive* proof.

Claim: $\exists a, b \in \mathbb{R}$ such that $a, b \notin \mathbb{Q}$ and $a^b \in \mathbb{Q}$.

Proof: We say above that $\sqrt{2} \notin \mathbb{R}$. Consider the number $\sqrt{2}^{\sqrt{2}}$.

If this number is rational, the proof is complete.

Otherwise, if $\sqrt{2}^{\sqrt{2}}$ is irrational, set $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.

Then

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2 \in \mathbb{Q}.$$

Thus, whether or not $\sqrt{2}^{\sqrt{2}}$ is irrational, we have in all cases found $a, b \in \mathbb{R}$ with the desired properties. ■

This proof is *non-constructive* since it does not explicitly tell its reader what a, b work!

In fact, there are constructive proofs of the given statement. For example $a = \sqrt{2}$ and $b = \log_2(9)$ are both easily shown to be irrational, and $a^b = 3$.