Bridge to Higher Mathematics

Contents

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 <mark>subset</mark> 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 <mark>is an element of</mark> – or <mark>is a member of</mark> - 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 <mark>union</mark> $A \cup B$ 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.
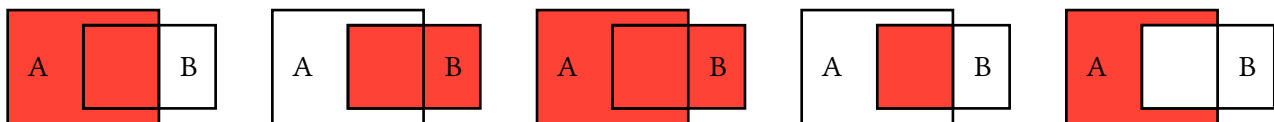

Figure 1: From left to right: A, B, $A \cup B$, $A \cap B$, $A - B$

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 $A \times B = \{(a_s, b_t) : 1 \le s \le n, 1 \le t \le m\}$.

(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 $\neg(b$ 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

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

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

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

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

(c). Consider the statement (♦) $\quad \forall a \in \mathbb{Q}, \exists b \in \mathbb{Q}$ 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

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

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

(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

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

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 $a \ne 0$ 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	$(p \land q) \lor r$	$(p \lor r) \to q$
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 $r \land s$ is: "$3 + 5 = 8$ and $3 \geq 8$.
- The proposition $p \lor q$ 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 $\neg p \lor q$.
(b). $\neg(p \Rightarrow q)$ is equivalent to $p \land \neg q$
(c). $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$ (contrapositive).

Proof:
(a). By definition, both of $p \Rightarrow q$ and $\neg p \lor q$ are always true when p is false. Moreover, $p \Rightarrow q$ and $\neg p \lor q$ 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 $\neg p \lor q$ 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	$p \Rightarrow q$	$\neg p \lor q$	$\neg q \Rightarrow \neg p$	$p \land \neg q$
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 $\neg p \Rightarrow \mathtt{false}$. This is often done by deriving two mutually contradictory assertions q and $\neg q$ and appealing to that fact that $q \wedge \neg q \Rightarrow \mathtt{false}$.
- Since $\neg p \Rightarrow \mathtt{false}$, we conclude that $\neg\neg p$ is $\mathtt{true}$. Since $\neg\neg p \Rightarrow p$, we finally conclude that p is $\mathtt{true}$.

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 which elements 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 $a^b = 3$.

3. **Week 3**

3.1. **Induction**

Consider a family $P(n)$ of propositions indexed by natural numbers $n \in \mathbb{N}$.

Mathematical Induction – when it can be applied - is a technique for proving all statements $P(n)$ at once, without having to give in finitely many proofs.

The basis of the proof is the following property of $\mathbb{N}$.

> **Fact 3.1.1**: **(The well-ordering principle)** Every non-empty subset of the set of natural numbers has a minimum element.

> **Proposition 3.1.2**: **(The principle of mathematical induction)** Given a family of propositions $P(n)$ for $n \in \mathbb{N}$, suppose the following:
>
> (a). $P(0)$ (i.e. suppose that $P(0)$ is true).
> (b). $\forall m \in \mathbb{N}, P(m) \Rightarrow P(m+1)$.

Then we can conclude that $P(n)$ holds for every $n \in \mathbb{N}$.

Proof: We need to prove: $\forall n, P(n)$. We use a proof by contradiction. Thus we suppose $\neg(\forall n, P(n))$, i.e. we suppose

$$\exists n, \neg P(n).$$

This shows that $S = \{n \in \mathbb{N} \mid \neg P(n)\}$ is a non-empty subset of $\mathbb{N}$. By [Fact 3.1.1](#), this set S has a *smallest* element n.

- Assumption (a) shows that $P(0)$ is true, so that $0 \notin S$. Thus $n > 0$ so that n has the form $k+1$ for $k \in \mathbb{N}$.

- Since $n = k+1$ is the smallest value of S, we know $k \notin S$ so that we know that $P(k)$ holds. But now (b) shows that $P(k+1)$ holds. On the other hand, since $k+1 \in S$, $\neg P(k+1)$ holds. Thus we have proved

$$P(k+1) \wedge \neg P(k+1).$$

This contradiction proves that $P(n)$ holds for every n. ∎

Remark 3.1.3:

(a). Note that the analogue of the well-ordering principle fails for $\mathbb{Z}$; for example, the set of even integers $\{..., -4, -2, 0, 2, 4, ...\}$ does not have a smallest element.

(b). The situation is even worse for rational or real numbers: even if a subset of $\mathbb{Q}$ or of $\mathbb{R}$ is bounded below, it does not in general have a minimal element. For example, the open interval of the real line $(0, 1)$ does not have a minimal element because 0 is not in the set $(0, 1)$ contains elements arbitrarily close to 0

(c). For an integer k, we can carry out induction on sets of the form $X_k = \{n \in \mathbb{N} \mid k \leq n\}$. Namely, given a family of propositions $P(n)$ for $n \in X_k$, if we prove that $P(k)$ is true, and if we prove that $\forall m \in X_k, P(m) \Rightarrow P(m+1)$ then we can conclude that $P(n)$ is true for every $n \in X_k$.

(d). When proving in (b) that $P(m) \Rightarrow P(m+1)$, the validity of $P(m)$ is often referred to as the *induction hypothesis*.

3.2. **The size of the power set, using mathematical induction**

Definition 3.2.1: For a set A, the power set of A is the set

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

in words, $\mathcal{P}(A)$ consists of all subsets of A.

Example 3.2.2:

(a). If $A = \emptyset$ then $\mathcal{P}(A) = \{\emptyset\}$. In particular, $\mathcal{P}(\emptyset)$ contains one element.

(b). If $A = \{a, b, c\}$ then

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

In particular, $\mathcal{P}(\{a, b, c\})$ contains $8 = 2^3$ elements.

Proposition 3.2.3: If A is a finite set with n elements, then $\mathcal{P}(A)$ has 2^n elements.

Proof: Let us write $n(A) \in \mathbb{N}$ for the number of elements in A. We write $P(n)$ for the proposition

$$P(n): \qquad \forall A, (n(A) = n) \Rightarrow (n(\mathcal{P}(A)) = 2^n).$$

We are going to prove that $P(n)$ holds using Proposition 3.1.2.

For this we must do two things:

- First, we must show that $P(0)$ holds. For this, we suppose that $n(A) = 0$ and we must show that $n(\mathcal{P}(A)) = 2^0 = 1$. Now, $n(A) = 0 \Rightarrow A = \emptyset$ and we already computed that $\mathcal{P}(\emptyset)$ has precisely one element, as required.

- Second, we must show that $\forall m \in \mathbb{N}, P(m) \Rightarrow P(m+1)$. Thus, let $m \in \mathbb{N}$ and assume $P(m)$. In other words, we assume that

$$\forall A, (n(A) = m) \Rightarrow (n(\mathcal{P}(A)) = 2^m).$$

We must prove that $P(m+1)$ holds; i.e. that

$$\forall A, (n(A) = m+1) \Rightarrow (n(\mathcal{P}(A)) = 2^{m+1}).$$

So, let A be a finite set with $n(A) = m+1$, and let $x \in A$. Then $A = \{x\} \cup A'$ where A' is a subset of A with $n(A') = m$.

We apply the induction hypothesis $P(m)$ to A' to learn that $n(\mathcal{P}(A')) = 2^m$.

For any subset B of A, either $x \in B$ or $x \notin B$.

If $x \notin B$, then $B \subseteq A' \Rightarrow B \in \mathcal{P}(A')$, and it follows that there are 2^m such subsets B.

If $x \in B$, then B has the form $B = \{x\} \cup B'$ where B' is a subset of A'; thus $B' \in \mathcal{P}(A')$. It again follows that there are 2^m such subsets B.

Thus there are $2^m + 2^m = 2 \cdot 2^m = 2^{m+1}$ subsets of A, so that indeed $n(\mathcal{P}(A)) = 2^{m+1}$. We have now proved that $P(m+1)$ is true.

Now Proposition 3.1.2 shows that $P(n)$ holds for every $n \in \mathbb{N}$, as required.

∎

3.3. More examples of induction

Proposition 3.3.1: Let $n \in \mathbb{N}$ and put $S_n = \sum_{i=0}^{n} i$. Then $S_n = \dfrac{n(n+1)}{2}$.

Proof:

We give a proof by mathematical induction. Let $P(n)$ be the proposition $S_n = \dfrac{n(n+1)}{2}$. To prove that $P(n)$ holds for every n, we are going to apply Proposition 3.1.2.

We must first confirm that $P(0)$ holds. On the one hand, $S_0 = \sum_{\{i=0\}}^{0}$ is the sum of no terms, and is thus 0. On the other hand, $0 \cdot (0+1)/2 = 0$. This confirms $P(0)$.

We now confirm that $\forall m, P(m) \Rightarrow P(m+1)$. Let $m \in \mathbb{N}$ and suppose that $P(m)$ holds. Thus we know that

$$S_m = \frac{m(m+1)}{2}$$

We must prove that $P(m+1)$ holds. Notice that by definition, we have

$$S_{m+1} = (m+1) + S_m.$$

Using the induction hypothesis $P(m)$, we can replace S_m in the right-hand side to find that

$$S_{m+1} = (m+1) + \frac{m(m+1)}{2}$$
$$= \frac{2(m+1)}{2} + \frac{m(m+1)}{2}$$
$$= \frac{m^2 + 3m + 2}{2}$$
$$= \frac{(m+1)(m+2)}{2}.$$

This confirms that $P(m+1)$ holds. Now $P(n)$ holds for each n by Proposition 3.1.2. ∎

In fact, we can give a proof of Proposition 3.3.1 without using induction, as follows

Proof: *Alternate proof.*

We write this sum S_n twice, once in ascending order and once in descending order

$$0 + \quad 1 + \ldots + (n-2) + (n-1) + n$$
$$n + (n-1) + \ldots + \quad 2 + \quad 1 + 0$$

If we add each term in the second row to the one above it, we get always n. There are $n + 1$ terms in S_n. So twice S_n is $n(n + 1)$. Then $S_n = n(n + 1)/2$.

∎

Proposition 3.3.2: Let $n \in \mathbb{N}$. Then $4^n - 1$ is divisible by 3.

Proof: We proceed by induction on n.

We must first prove the *base case*, namely the case $n = 0$. When $n = 0$, we have $4^n - 1 = 1 - 1 = 0$. Now we know that $0 = 0 \times 3$ so indeed $3 \mid 0 = 4^0 - 1$.

We now suppose that $m \in \mathbb{N}$ and that $4^m - 1$ is divisible by 3. We must prove that $4^{m+1} - 1$ is divisible by 3.

Well,

$$4^{m+1} - 1 = 4 \cdot 4^m - 1 = 4 \cdot 4^m - 4 + 4 - 1 = 4(4^m - 1) + (4 - 1) \quad (\clubsuit)$$

If $4^m - 1 = 3a$ we see that

$$(\clubsuit) \quad = 4 \cdot 3a + 3 = 3(4a + 1)$$

which confirms that $3 \mid 4^{m+1} - 1$.

Now it follows by Proposition 3.1.2 that $3 \mid 4^n - 1$ for every $n \in \mathbb{N}$. ∎

3.4. Strong induction

Proposition 3.4.1: (**Strong mathematical induction principle**) Let $P(n)$ be a family of propositions indexed by $n \in \mathbb{N}$.

For $n \in \mathbb{N}$ write $Q(n)$ for the proposition

$$\forall k \in \mathbb{N}, k \leq n \Rightarrow P(k);$$

thus $Q(n)$ is the proposition that $P(k)$ holds for every $k \leq n$.

Assume the following:

   (a). $P(0)$ is true, and
   (b). $\forall m, Q(m) \Rightarrow P(m + 1)$

Then $P(n)$ holds for every $n \in \mathbb{N}$.

Proof: We proceed as before; thus let $S = \{n \in \mathbb{N} \mid P(n) \text{ fails to hold}\}$. To prove the proposition, we must show that S is empty.

We give a proof by contradiction; thus we suppose that S is non-empty. Using Fact 3.1.1, we write $n \in S$ for the *smallest* element of S.

In view of (a), we know that $0 \notin S$ so that $0 < n$ and thus $n = m + 1$. For any $k \leq m$ we have $k \notin S$ so that $P(k)$ holds. By definition, this means that $Q(m)$ holds. Now by (b), $Q(m) \Rightarrow P(m + 1)$.

SO on the one hand $P(m + 1)$ holds, but on the other hand, $n = m + 1 \in S$ so that $P(m + 1)$ does not hold. This contradiction proves that $S = \emptyset$; thus, the Proposition holds.

∎

Remark 3.4.2: The difference between induction and strong induction is that in the second step, we are using more than the statement for the previous natural number, we are using it for all the previous natural numbers. In carrying out the proof, we need to be careful that we only use statements that we have checked or assumed.

We are going to use the strong induction principle to prove that "division with remainder" works for integers. In other words, we are going to show for $a, b \in \mathbb{Z}$ with $b > 0$ that there are unique integers $b, q \in \mathbb{Z}$ such that $a = bq + r$ and $0 \le r < b$.

First, let's establish the *uniqueness*.

Proposition 3.4.3: Let $b \in \mathbb{Z}$ with $b > 0$, and let $q, r, q', r' \in \mathbb{Z}$. Suppose that

$$(\blacklozenge) \quad bq + r = bq' + r'$$

and that

$$0 \le r < b \text{ and } 0 \le r' < b.$$

Then $q = q'$ and $r = r'$.

Proof: Using ($\blacklozenge$) we see that $b(q - q') = r' - r$ which shows that $b \mid r' - r$. Since $0 \le r, r' < b$, we have $-b < r - r' < b$; thus $r - r' = 0$, i.e. $r = r'$. Again using ($\blacklozenge$) we see that $bq = bq'$ and since $b \ne 0$ we conclude that $q = q'$. ∎

Proposition 3.4.4: (**Division with remainder for $\mathbb{N}$**) Given $n, b \in \mathbb{N}, b > 0$, there exist unique natural numbers q, r with $0 \le r < b$ such that $n = bq + r$.

We are going to give the proof twice. The first time, we will emphasize how the proof follows Proposition 3.4.1.

Proof:

Fix $b \in \mathbb{N}$ with $b > 0$.

The uniqueness statement follows from Proposition 3.4.3; it remains to show the *existence* of q, r.

We are going to prove the existence using strong induction on n.

What this means is that we consider the family of propositions

$$P(n): \quad \exists q, r \in \mathbb{N}, 0 \le r < b \text{ and } n = bq + r.$$

We prove two things:

- We show that $P(0)$ holds:

  For this, we take $q = r = 0$ and note that $0 \le 0 < b$ and $0 = b \cdot 0 + 0$.

- With notation as in the statement of <u>Proposition 3.4.1</u>, we show for all $m \in \mathbb{N}$ that $Q(m) \Rightarrow P(m+1)$.

  So we suppose that $Q(m)$ holds; i.e. we suppose for $k \leq m$ that $P(k)$ holds.

  We now treat two cases: in the first case, $m + 1 < b$ and in the second case, $b \leq m + 1$.

  If $m + 1 < b$ then $P(m+1)$ is true since we can take $q = 0$ and $r = m + 1$. Then

  $$m + 1 = b \cdot 0 + m + 1 \text{ and } m + 1 < b.$$

  We are left with the case $b \leq m + 1$. In this case, notice that $0 \leq m + 1 - b$ so that $m + 1 - b \in \mathbb{N}$. We now apply the induction hypothesis. Notice since $b > 0$, $m + 1 - b < m + 1$; i.e. $m + 1 - b \leq m$. By the induction hypothesis $Q(m)$ we know that $P(m + 1 - b)$ holds. Thus we may find $q, r \in \mathbb{N}$ for which

  $$m + 1 - b = b \cdot q + r \text{ and } 0 \leq r < b.$$

  Now we see that $m + 1 = b \cdot (q + 1) + r$ and $0 \leq r < b$, which proves that $P(m+1)$ holds.

We now apply <u>Proposition 3.4.1</u> to conclude that $P(n)$ holds $\forall n \in \mathbb{N}$. This proves the Proposition.

$\blacksquare$

Let's repeat that proof; this time, we use natural language and avoid naming the various propositions.

Proof:

Fix $b \in \mathbb{N}$ with $b > 0$.

The uniqueness statement follows from <u>Proposition 3.4.3</u>; it remains to show the *existence* of q, r.

We are going to prove the existence using strong induction on n.

We prove two things:

- We prove that the statement is correct when $n = 0$.

  For this, we take $q = r = 0$ and note that $0 \leq 0 < b$ and $0 = b \cdot 0 + 0$.

- For the induction step, we fix m and assume the following:

  ($\clubsuit$) for each $0 \leq k < m$, we can write $k = qb + r$ with $q, r \in \mathbb{N}$ and $0 \leq r$.

  We must prove that division with remainder works for $n = m + 1$.

  We now treat two cases: in the first case, $m + 1 < b$ and in the second case, $b \leq m + 1$.

  If $m + 1 < b$, take $q = 0$ and $r = m + 1$. Then

  $$m + 1 = b \cdot 0 + m + 1 \text{ and } m + 1 < b$$

  which confirms that division with remainder holds for $n = m + 1$ in this case.

  We are left with the case $b \leq m + 1$. Notice that $0 \leq m + 1 - b$ so that $m + 1 - b \in \mathbb{N}$. We now apply the induction hypothesis. Notice since $b > 0$, $m + 1 - b < m + 1$; i.e. $k = m + 1 - b \leq m$. By the induction hypothesis ($\clubsuit$) we may find $q, r \in \mathbb{N}$ for which

  $$k = m + 1 - b = b \cdot q + r \text{ and } 0 \leq r < b.$$

Now we see that $m + 1 = b \cdot (q + 1) + r$ and $0 \leq r < b$, as required.

The proposition now follows by [Proposition 3.4.1](#).

∎

Corollary 3.4.4.1: (**Division with remainder for $\mathbb{Z}$**) Given $z, b \in \mathbb{Z}, b > 0$, there exist unique integers q, r with $0 \leq r < b$ such that $z = bq + r$.

Proof: Again, the uniqueness statement follows from [Proposition 3.4.3](#); it remains to show the *existence* of q, r.

From [Proposition 3.4.4](#), we already know the result if $z \geq 0$. Assume then $z < 0$; then $-z > 0$. Hence, from [Proposition 3.4.4](#), there exist natural numbers q', r' with $0 \leq r' < b$ such that $-z = bq' + r'$.

Therefore, $z = b(-q') + (-r')$. Here $-q' \in \mathbb{Z}$. If $0 \leq r' < b$, multiplying with -1 that is a negative number we reverse the inequalities. Therefore $-b < -r' \leq 0$. If $r' = 0$, this is what we need. If r' is not 0, $-b < -r' < 0$. we can add b to these inequalities to give us $0 < b - r' < b$. From $z = b(-q') + (-r')$, we also have $z = b(-q' - 1) + (b - r')$. Then

$$q = -q' - 1 \text{ and } r = b - r'$$

work in the statement of the corollary.

∎

Corollary 3.4.4.1.1: Let $n \in \mathbb{Z}$. If n is not even, then $\exists q \in \mathbb{Z}, n = 2q + 1$.

Proof: Use [Corollary 3.4.4.1](#) to write $n = 2q + r$ for unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < 2$.

Thus $r \in \{0, 1\}$. One sees at once that n is even if and only if $r = 0$ ∎

Remark 3.4.1: The corollary shows that n is odd (i.e. not even) if and only if n has the form $2q + 1$ for some $q \in \mathbb{Z}$.

3.5. Sequences

Definition 3.5.1: A sequence $a_n, n \in \mathbb{N}$ is a family of numbers, where the members of the family are indexed by the natural numbers.

Example 3.5.2:
  (a). The sequence $\{0, 1, 2, ...\}$ is given by $a_n = n$ for $n \in \mathbb{N}$.
  (b). The sequence $\{1, -1, 1, -1, ...\}$ is given by $a_n = (-1)^n$ for $n \in \mathbb{N}$.
  (c). The sequence $\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ...\}$ is given by $a_n = \frac{1}{n+1}$ for $n \in \mathbb{N}$.

One can sometimes give a *recursive* definition of a sequence.

Example 3.5.3:
  (a). Consider the sequence defined recursively by the requirements: $a_0 = 0$ and $a_n = a_{n-1} + 1$ for $n > 0$.

   Let's prove that this sequence satisfies $a_n = n$ for each $n \in \mathbb{N}$. We use *induction* − i.e. [Proposition 3.1.2](#) − to prove that $a_n = n$ for each n.

We most confirm first that $a_0 = 0$; this is true by assumption.

Finally, we must confirm for $m \in \mathbb{N}$ that $a_m = m$ implies that $a_{m+1} = m+1$. But the recursively relation we are assuming implies this; indeed, it shows that

$$a_{m+1} = a_m + 1 = m + 1$$

as required. Now [Proposition 3.1.2](#) implies that $a_n = n$ for every $n \in \mathbb{N}$

- Consider the sequence defined recursively by the requirements $a_0 = 1$ and $a_n = (-1) \cdot a_{n-1}$ for $n > 0$.

  This sequence is given by the formula $a_n = (-1)^n$. Indeed, we again give a proof by induction.

  In the base, case we know $a_0 = 1 = (-1)^0$ by assumption.

  For $m \in \mathbb{N}$, if we know that $a_m = (-1)^m$, our recursive relation we assume then gives

  $$a_{m+1} = (-1) \cdot a_m = (-1) \cdot (-1)^m = (-1)^{m+1}.$$

  Thus [Proposition 3.1.2](#) confirms for each $n \in \mathbb{N}$ that $a_n = (-1)^n$.

(a). If a sequence b_n satisfies the two conditions

  $$b_0 = 3, \text{ and } b_n = 2b_{n-1} \text{ for } n > 0,$$

  then $b_n = 3 \cdot 2^n$:

  Proceed by induction.

  In the base case, we have $b_0 = 3 = 3 \cdot 2^0$ by assumption.

  Let $m \in \mathbb{N}$ and suppose that $b_m = 3 \cdot 2^m$. We must argue that $b_{m+1} = 3 \cdot 2^{m+1}$.

  Our assumption implies that

  $$b_{m+1} = 2b_m = 2 \cdot 3 \cdot 2^m = 3 \cdot 2^{m+1}$$

  as required. Thus [Proposition 3.1.2](#) implies that $b_n = 2 \cdot 3^n$ for each $n \in \mathbb{N}$.

(b). Consider the *Fibonacci* sequence F_n defined by $F_0 = F_1 = 1$ and $F_i = F_{i-1} + F_{i-2}$ for $i \geq 2$. In this case, it is less clear how to write down a formula for F_n!

Sometimes we can check that a sequence satsifies a recurrence relationship. FOr example:

Example 3.5.4:

(a). Let's consider the sequence $a_n = 2^n$ and show that

  $$a_n = 6 \cdot a_{n-2} - a_{n-1} \text{ for each } n \in \mathbb{N} \text{ with } n \geq 2.$$

  Indeed, let $n \in \mathbb{N}$ with $n \geq 2$ and compute:

  $$6 \cdot a_{n-2} - a_{n-1} = 6 \cdot 2^{n-2} - 2^{n-1} = 2^{n-2}(6-2) = 2^{n-2} \cdot 4 = 2^n = a_n.$$

(b). Show that the sequence $b_n = (-3)^n$ satisfies the recurrence

  $$b_n = 6 \cdot b_{n-2} - b_{n-1} \text{ for } n \geq 2$$

  .

Indeed, let $n \in \mathbb{N}$ with $n \geq 2$ and compute:

$$6 \cdot b_{n-2} - b_{n-1} = 6 \cdot (-3)^{n-2} - (-3)^{n-1} = (-3)^{n-2}(6 - (-3)) = 9 \cdot (-3)^{n-2} = (-3)^n = b_n.$$

Example 3.5.5: Let's consider sequences a_n which satisfies the recurrence relation

$$(\clubsuit) \quad a_n = a_{n-1} + 4a_{n-2} - 4a_{n-3}$$

(a). If the sequences a_n and b_n both satisfy $(\clubsuit)$ then for any real numbers s, t so does the sequence c_n where $c_n = s \cdot a_n + t \cdot b_n$ for $n \in \mathbb{N}$.

Indeed, let $n \in \mathbb{N}$. Our assumptions mean for $n \geq 3$ that

$$a_n = a_{n-1} + 4a_{n-2} - 4a_{n-3}$$

and

$$b_n = b_{n-1} + 4b_{n-2} - 4b_{n-3}.$$

But then

$$\begin{aligned}
c_n &= s \cdot a_n + t \cdot b_n = s \cdot (a_{n-1} + 4a_{n-2} - 4a_{n-3}) + t \cdot (b_{n-1} + 4b_{n-2} - 4b_{n-3}) \\
&= (s \cdot a_{n-1} + t \cdot b_{n-1}) + 4(s \cdot a_{n-2} + t \cdot b_{n-2}) - 4(s \cdot a_{n-3} + t \cdot b_{n-3}) \\
&= c_{n-1} + 4c_{n-2} - 4c_{n-3}.
\end{aligned}$$

(b). For a real number $b \neq 0$, the sequence $a_n = b^n$ satsifes $(\clubsuit)$ if $b = 1, 2, -2$.

$$\begin{aligned}
b^n = b^{n-1} + 4b^{n-2} - 4b^{n-3} &\Leftrightarrow b^n - b^{n-1} - 4b^{n-2} + 4b^{n-3} = 0 \\
&\Leftrightarrow b^{n-3}(b^3 - b^2 - 4b + 4) = 0
\end{aligned}$$

As we are assuming $b \neq 0$, this means $b^3 - b^2 - 4b + 4 = 0$. We can factor

$$b^3 - b^2 - 4b + 4 = (b - 1)(b - 2)(b + 2).$$

Therefore, $b = 1, b = -2, b = 2$ are solutions of the stated form. (In fact, these are the only solutions).

(c). For any real numbers $\alpha, \beta, \gamma \in \mathbb{R}$ there is a sequence a_n for which

$$a_0 = \alpha, a_1 = \beta, a_2 = \gamma$$

and $(\clubsuit)$ holds.

Indeed, define the sequence $a_n = c_0 + c_1 2^n + c_2(-2)^n$ where c_0, c_1, c_2 are real numbers.

It follows from observation (a) above that a_n satisfies $(\clubsuit)$.

Now we have

$$a_0 = c_0 + c_1 + c_2$$

$$a_1 = c_0 + 2c_1 - 2c_2$$

$$a_2 = c_0 + 4c_1 + 4c_2$$

So we must solve the system of linear equations

$$c_0 + c_1 + c_2 = \alpha$$
$$c_0 + 2c_1 - 2c_2 = \beta$$
$$c_0 + 4c_1 + 4c_2 = \gamma$$

Or equivalently we must solve the matrix equation

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & -2 \\ 1 & 4 & 4 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$$

This matrix equation has a (unique) solution $\begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix}$ since

$$\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & -2 \\ 1 & 4 & 4 \end{pmatrix} = 12.$$

4. **Week 4 - [2025-09-22]**

4.1. **Functions**

Functions are the way in which sets relate to each other. We begin our discussion of functions with the definition:

> **Definition 4.1.1**: A function consists of three pieces of data: a set A called the domain, a set B called the codomain and rule f that assigns to each element x of the set A one and only one element $f(x)$ of the set B.
>
> We write $f : A \to B$ as notation for a function.
>
> When the domain and codomain can be inferred from context, we sometimes just refer to the function using the name f.

Remark 4.1.2: Here is a more precise definition: a function $f : A \to B$ is a subset $R \subseteq A \times B$ of the cartesian product $A \times B$ with the property that for each $x \in A$, $\exists! y \in B$ such that $(x, y) \in R$.

This definitions makes precise what is meant by a "rule" that "assigns to each $x \in A$ an element $f(x)$ of B."

Example 4.1.3:

(a). Let $A = \{a, b, c, d\}$, let $B = \mathbb{Z}$, and let f be the rule defined by $f(a) = 0$, $f(b) = 2$, $f(c) = 1$, $f(d) = 2$.

Notice that formally, f corresponds to the subset

$$R = \{(a, 0), (b, 2), (c, 1), (d, 2)\} \subseteq A \times \mathbb{Z}.$$

We can represent this function using the following diagram:
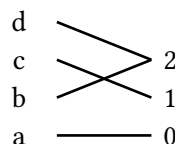
(b). With the same domain and codomain, the rule $f(a) = 1$, $f(a) = 2$, $f(b) = 1$, $f(c) = 1$ and $f(d) = 2$ *does not determine a function*, since f assigns two different values to the element $a \in A$.

(c). Again with the same domain and codomain, the rule $f(b) = 0$, $f(c) = 0$, $f(d) = 0$ *does not determine a function*, since the value $f(a)$ is not specified.

Often we specify functions using *formulas*. For example:

Example 4.1.4:

(a). There is a function $f : \mathbb{R} \to \mathbb{R}$ given by the rule $f(x) = x^2$ for $x \in \mathbb{R}$.

(b). In fact, the same rule can define different functions. For example, there is a function

$$f : \mathbb{Q} \to \mathbb{R}_{\geq 0} \text{ given by } f(x) = x^2.$$

When giving a function with a rule, It is important to make sure that the rule makes sense. Sometimes an expression is not defined for some values of the intended domain, as when trying to divide by 0 or taking the square root of a negative real number. Another sometimes-overlooked problem is that when we list the elements in the domain, they can be listed in several ways and the assignment rule would give different outputs depending on what representation you choose. Examples below should clarify these difficulties:

Example 4.1.5:

(a). In an elementary school, assign to each classroom the color of the T-shirt of a child in that class on the first day of school. If we do not specify the child this would not give a well defined function if different children in the same classroom wear T-shirts of different colors.

(b). The assignment $f : \mathbb{Q} \to \mathbb{Z}$ given by $f(m/n) = m$ is not a well defined function. Indeed, 0.5 is a rational number that can be represented by $1/2, 2/4, -3/-6, \dots$ and we do not know if $f(.5)$ should be $1, 2, -3, \dots$

(c). The assignment $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(m/n) = 2m/5n$ is a well defined function. We need to check that the definition is independent of the way we represent a rational number as a fraction. Assume $a/b = c/d$. By definition, this means that $ad = bc$. Multiplying both sides of this equality by 10, we can write this as $(2a)(5d) = (5b)(2c)$ which tells us that $2a/5b = 2c/5d$. So our assignment is not ambiguous and we get a well defined function from the set of rational numbers to itself

(d). The assignment $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \sqrt{x}$ is not a function as the value of f at a negative number is not defined.

(e). The assignment $f : \mathbb{C} \to \mathbb{C}$ given by $f(x) = \sqrt{x}$ is not a well defined function as every complex number (except for 0) has two different square roots! Unlike the real case, we cannot "choose the positive root". For example, the two square roots of $-i$ are

$$\frac{-1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i, \qquad \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i.$$

Neither seems "more positive" than the other.

4.2. Properties of functions

> **Definition 4.2.1**: Given a function $f : A \to B$ and a function $g : B \to C$, the ==composition== of the two functions f, g is the function
>
> $$g \circ f : A \to C$$
>
> given by the rule $(g \circ f)(a) = g(f(a)), \forall a \in A$.

Note in particular that we can only compose two functions if the codomain of the first is the domain of the second. Then, the composition is obtained by applying the two functions one after the other.

Example 4.2.2: Consider the following sets:
- A is a set of friends, $A = \{$ Alice, Bob, Chris $\}$,
- B is a set of possible household pets, $B = \{$ cat, dog, bunny $\}$
- $C = \mathbb{Q} \geq 0)$ is the set of non-negative rational numbers.

Consider functions

- $f : A \to B$ where $f(x)$ representing the preferred pet of friend x.

- $g : B \to C$ where $g(y)$ represents the cost per week, in dollars, to own the pet y.

For $x \in A$, $(g \circ f)(x)$ represents the anticipated costs for pet-ownership by the friend x.

Notice that the composition $f \circ g$ is not defined. The domain of g is the set of pets. If y is a pet, then $g(y)$ is a non-negative rational number, and $f(g(y))$ is not meaningful, since the domain of f is the set of friends (Alice, Bob, Chris).

Example 4.2.3: Consider the two functions $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x + 2$ and $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = 3x$. In this case, as the domain and codomain are the same, it makes sense to compose the two functions in any order.

$$(f \circ g)(x) = f(g(x)) = f(3x) = 3x + 2,$$

$$(g \circ f)(x) = g(f(x)) = g(x + 2) = 3(x + 2) = 3x + 6$$

We see that even when it makes sense to compose functions in both orders, usually $f \circ g$ and $g \circ f$ will differ.

4.3. Image and pre-image

> **Definition 4.3.1**: Let $f : A \to B$ be a function. The ==image== or ==range== of f is the subset of B defined by
>
> $$f(A) = \{b \in B \mid \exists a \in A, f(a) = b\}.$$
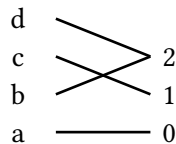>
> More generally, for a subset $A_1 \subseteq A$, the ==image== of A_1 is the subset of B defined by $f(A_1) = \{b \in B \mid \exists a \in A_1, f(a) = b\}$.
>
> For a sbuset $B_1 \subseteq B$, the ==inverse image== or ==pre-image== of B_1 is the subset of A defined by
>
> $$f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}.$$

Example 4.3.2:

(a). For $A = \{a, b, c, d\}$ and $B = \{0, 1, 2\}$ consider the function $f : A \to B$ described by the following diagram.

We see that $f(\{a, b\}) = \{0, 2\}$ and $f^{-1}(\{2\}) = \{b, d\}$.

(b). Consider a function $f : \mathbb{R} \to \mathbb{R}$. Then $f^{-1}(\{0\})$ is exactly the set of $x \in \mathbb{R}$ for which $f(x) = 0$ – sometimes these x are called the *roots* of f.

(c). Consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. The image or range of this function is the set of non-negative real numbers $[0, \infty)$.

If we take the open interval in the real line $(-2, 2) = A_1$, then its image is the half closed interval $f(A_1) = (0, 4)$.

Computing the inverse images of some sets, we have

$$f^{-1}(\{4\}) = \{2, -2\} \text{ and } f^{-1}(\{-4\}) = \emptyset.$$

4.4. Injective or one-to-one functions, and surjective or onto functions

Definition 4.4.1: A function $f : A \to B$ is one-to-one or injective if

$$\forall a_1, a_2 \in A, a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2).$$

In words: f is injective if distinct elements of A are always mapped to distinct elements of B.

Sometimes one says that an injective function is an injection.

Remark 4.4.2: It is often useful to use the *contrapositive* of this definition. Taking the contrapositive of the definition, we see that f is injective if and only if the following holds:

$$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2.$$

Definition 4.4.3: A function $f : A \to B$ is onto or surjective if $f(A) = B$. In other words, f is surjective provided that
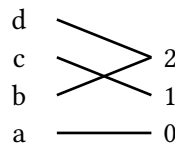
$$\forall x \in B, \exists a \in A, f(a) = x.$$

In words, f is surjective if every element of the codomain is the image of some element in the domain.

Sometimes one says that a surjective function is a surjection.

Example 4.4.4:

(a). For $A = \{a, b, c, d\}$ and $B = \{0, 1, 2\}$ consider again the function $f : A \to B$ described by the following diagram.

Then f is onto since every element of B appears on the right-hand side of a connecting arrow in the diagram.

But f is not one-to-one since $f(b) = f(d) = 2$ while $b \neq d$.

(b). With $A = \{a, b, c\}$ and $B = \{0, 1, 2, 3\}$ consider the function $g : A \to B$ described by the diagram
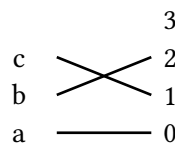
Then g is one-to-one. But g is not onto since $3 \notin f(A)$.

(c). The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is neither one to one nor onto. Indeed, $f(2) = f(-2) = 4$, shows that f is not one-to-one. As there is no real number x for which $x^2 = -1$, $-1 \notin f(\mathbb{R})$ so f is not onto.

(d). Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(z) = 3z + 2$.

Then f is one-to-one. Indeed, suppose that $a_1, a_2 \in \mathbb{Z}$ and that $f(a_1) = f(a_2)$. We must argue that $a_1 = a_2$.

Since $f(a_1) = f(a_2)$, we know $3a_1 + 2 = 3a_1 + 2$. Subtracting 2 from both sides of the equation and dividing by 3, $a_1 = a_2$, showing that f is one to one..

On the other hand, f is not onto. We must find an integer which is not in the image $f(\mathbb{Z})$ of f.

For this, we will show that $1 \notin f(\mathbb{Z})$. We prove this by contradiction; thus, we suppose that for $a \in \mathbb{Z}$ we have $f(a) = 1$.

We have $3a + 2 = 1 \Rightarrow 3a = -1 \Rightarrow a = -1/3$.

But the rational number $-1/3$ is not an integer. This contradiction proves that f is not onto.

(e). Now consider $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = 3x + 2$.

The argument in the preceding example again shows that g is one-to-one.

But now g is onto. Indeed, for $x \in \mathbb{R}$, we may form

The same proof we gave in (b) shows that f is an injective function $\mathbb{R} \to \mathbb{R}$.

To see that f is surjective, let $y \in \mathbb{R}$. We must find $x \in \mathbb{R}$ for which $f(x) = y$; i.e. we must solve the equation $3x + 2 = y$ for x. We find that

$$3x = y - 2 \Rightarrow x = (y - 2)/3.$$

We see that $f((y - 2)/3) = y$ which confirms that f is surjective.

Remark 4.4.5:

(a). When writing a proof that a function $f : A \to B$ is *onto*, you should expect to start writing your proof as follows:

"Let $b \in B$. We must find $a \in A$ so that $f(a) = B$."

You should really write all that, at least for now! Though of course the name of the co-domain – and the name of the element of the co-domain – can vary.

Then you need to give some argument about why you can find a suitable element a.

(b). When writing a proof that a functtion $f : A \to B$ is *one-to-one* you should expect to start one of two ways:

First:

"Let $a_1, a_2 \in A$ and suppose that $f(a_1) = f(a_2)$. To show that f is one-to-one, we must argue that $a_1 = a_2$.""

Then you need to give an argument that $f(a_1)$ and $f(a_2)$ are equal.

Alternately, you can begin as follows:

"Let $a_1, a_2 \in A$ and suppose that $a_1 \neq a_2$. To show that f is one-to-one, we must argue that $f(a_1) \neq f(a_2)$".

Then you need to give the appropriate argument!

4.5. Bijections

Let us look at functions that are both one to one and onto; such functions allow us to identify two sets.

> **Definition 4.5.1**: A function $f : A \to B$ is <mark>bijective</mark> if it is both one-to-one and onto, i.e. if it is both injective and surjective.
>
> Equivalently, f is bijective provided that
>
> $$\forall b \in B, \exists! a \in A \text{ with } f(a) = b.$$
>
> In words, a function is a bijection if every element in the co-domain is the image of one and only one element in the domain.
>
> Sometimes we say that a bijective function is a <mark>bijection</mark>.

Example 4.5.2:
  (a). For any set A, consider the identity function

$$\text{id}_A : A \to A \text{ given by id}_A(a) = a \text{ for each } a \in A.$$

  This function is a bijection.
  (b). We saw above that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x + 2$ is a bijection.

Bijections are functions that can be "undone" through composition with s suitable function:

Definition 4.5.3: A function $f : A \to B$ is invertible if there is a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$.

If f is invertible, we write $f^{-1} = g$ and call f^{-1} the inverse function to f.

Theorem 4.5.4: A function $f : A \to B$ is invertible if and only if f is bijective.

Proof: The main idea is that if f is a bijection, there is a natural way of choosing for each element in B one in A that allows you to go back.

($\Leftarrow$) : Assume that f is a bijection. Define $g : B \to A$ as follows: as f is onto, for every $b \in B$, there exists $a \in A$, $f(a) = b$. As f is one to one, this a is unique. Hence, we can define $g(b) = a$. As, by assumption, $f(a) = b$, it follows that $f(g(b)) = f(a) = b, \forall b \in B$. We ahve proved that, $f \circ g = \mathrm{id}_B$. Also, with the above notations, $\forall a \in A$, $g(f(a)) = g(b) = a$. Hence, $g \circ f = \mathrm{id}_A$ and we have proved that g is the inverse function to f so that f is invertible.

($\Rightarrow$) Assume that there exists a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. For any $b \in B$, $f(g(b)) = b$; this shows that f is onto. Assume $f(a_1) = f(a_2)$. Then $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$. Hence, f is one to one.

∎

Example 4.5.5:

(a). For any set A, we have $\mathrm{id}_A \circ \mathrm{id}_A = \mathrm{id}_A$ so that $\mathrm{id}_A^{-1} = \mathrm{id}_A$.

(b). The inverse function for the bijection $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 3x + 2$ for $x \in \mathbb{R}$ is the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(y) = (y - 2)/3$ for $y \in \mathbb{R}$.

(c).

Remark 4.5.6: An important observation is that to apply Theorem 4.5.4 to see that f is a bijection, you must confirm two conditions: $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$. Assuming only one of these conditions is insufficient in general.

For example, denote by $\mathbb{R}_{\geq 0} = [0, \infty)$ the set of real numbers greater than or equal to 0. Define

$$f : \mathbb{R} \to \mathbb{R}_{\geq 0} \text{ and } g : \mathbb{R}_{\geq 0} \to \mathbb{R} \text{ by } f(x) = x^2 \text{ and } g(x) = \sqrt{x}.$$

Then $f \circ g = \mathrm{id}_{\mathbb{R}_{\geq 0}}$ but neither f nor g is bijective.

Recall that for a function $f : A \to B$, we defined the inverse image of a subset $B_1 \subseteq B$ as

$$f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}.$$

Proposition 4.5.7: Assume that $f : A \to B$ is a bijection with inverse function $g = f^{-1} : B \to A$. Let $B_1 \subseteq B$ be any subset of B.

Assume now that f is a bijection and that $g : B \to A$ is the function satisfying $f \circ g = \mathrm{id}_B, g \circ f = \mathrm{id}_A$. Then, $f^{-1}(B_1) = g(B_1)$.

Proof: We need to prove the two inclusions We start with $f^{-1}(B_1) \subseteq g(B_1)$: take $a \in f^{-1}(B_1)$. By definition of $f^{-1}(B_1)$, $f(a) = b \in B_1$. By definition of g, $g(b) = a$. Hence $a \in g(B_1)$. As this is true for every $a \in f^{-1}(B_1)$, we conclude that $f^{-1}(B_1) \subseteq g(B_1)$.

Take now $a \in g(B_1)$. By definition of image of a set, there exists $b \in B_1$ such that $a = g(b)$. By definition of g, this means that $f(a) = b$. Hence, $f(a) \in B_1$. By definition of inverse image, this means that $a \in f^{-1}(B_1)$. As this is true for every $a \in g(B_1)$, we conclude that $g(B_1) \subseteq f^{-1}(B_1)$. ∎

Remark 4.5.8: The preceding result justifies our notational redundancy. When f is a bijection, taking the inverse-image of a set under f is the same as taking the image under the inverse functtion.

Be careful: when f is not a bijection, the symbol f^{-1} does not denote a function on the codomain of f.

Proposition 4.5.9: Let $f : A \to B$ and $g : B \to C$ be bijections. Then the composition

$$h = g \circ f : A \to C$$

is a bijection.

Proof: We first show that h is surjective. Let $c \in C$. Since g is surjective, we may choose $b \in B$ with $g(b) = c$. Since f is surjective, we may choose $a \in A$ with $f(a) = b$.

Now

$$h(a) = (g \circ f)(a) = g(f(a)) = g(b) = c$$

as required.

Now we show that h is one-to-one. Let $a_1, a_2 \in A$ and suppose that $h(a_1) = h(a_2)$.

Thus $g(f(a_1)) = g(f(a_2))$ and since g is injective, we may conclude that $f(a_1) = f(a_2)$. Finally, since f is injective, conclude that $a_1 = a_2$. This shows that h is injective and completes the proof that h is bijective. ∎

Remark 4.5.10: In the setting of [Proposition 4.5.9](#), notice that

$$h^{-1} = (g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

To confirm this, notice that

$$h \circ f^{-1} \circ g^{-1} = g \circ f \circ f^{-1} \circ g^{-1} = g \circ \mathrm{id}_B \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_C \,.$$

and that

$$f^{-1} \circ g^{-1} \circ h = f^{-1} \circ g^{-1} \circ g \circ f = f^{-1} \circ \mathrm{id}_B \circ f = f^{-1} \circ f = \mathrm{id}_A \,.$$

Example 4.5.11: In a previous example, we saw that the inverse of the function

$$f : \mathbb{R} \to \mathbb{R} \text{ given by } f(r) = 3r + 2 \text{ for } r \in \mathbb{R}$$

is given by the rule

$$g(x) = (x - 2)/3.$$

We can think of f as the composition of two functions: first, multiply by 3 and then add two.

If we define $f_1 : \mathbb{R} \to \mathbb{R}$ given as $f_1(r) = 3r$, and $f_2 : \mathbb{R} \to \mathbb{R}$ given as $f_2(s) = s + 2$, then $f = f_2 \circ f_1$.

The inverse of multiplying by 3 is dividing by 3 and the inverse of adding 2 is subtracting 2.

So, if $g_1(x) = x/3$, $g_2(y) = y - 2$, then g_1, g_2 are the inverses of f_1, f_2 respectively.

The composition $g = g_1 \circ g_2$ is subtracting 2 first and dividing by 3 afterwards which is exactly the effect of g, the inverse of f.

4.6. cancellation

Proposition 4.6.1: Let A, B be sets. Suppose that $f : A \to B$ is a function.
(a). Suppose that f is surjective. Prove that for any set C and any pair of functions

$$g_1 : B \to C \text{ and } g_2 : B \to C$$

such that $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$.
(b). Conversely, suppose that for every set C and for every pair of functions

$$g_1 : B \to C \text{ and } g_2 : B \to C,$$

the equality $g_1 \circ f = g_2 \circ f$ implies that $g_1 = g_2$. Prove that f is surjective.

Proof:

(a). We assume f to be surjective and we suppose that $g_1 \circ f = g_2 \circ f$. To see that $g_1 = g_2$, we must argue that $g_1(b) = g_2(b)$ for each $b \in B$. So we fix $b \in B$.

Since f is surjective, we may choose $a \in A$ for which $f(a) = b$. Since $g_1 \circ f = g_2 \circ f$, we find that

$$(g_1 \circ f)(a) = (g_2 \circ f)(a) \text{ so that } g_1(f(a)) = g_2(f(a)),$$

and thus $g_1(b) = g_2(b)$ as required.

(b). To prove that f is surjective, let $b_0 \in B$. We must argue that there is some $a \in A$ with $f(a) = b_0$.

We are going to proceed by contradiction. Thus, we suppose that b_0 is not contained in the image $f(A)$.

To use the hypothesis, let $C = \{0, 1\}$ be the set consisting of the two natural numbers 0 and 1. Now let $g_1 : B \to C$ be the constant function defined by

$$g_1(b) = 0 \text{ for all } b \in B,$$

and let $g_2 : B \to C$ be the function defined by the rule

$$g_2(b) = \begin{cases} 1 \text{ if } b = b_0 \\ 0 \text{ otherwise} \end{cases}$$

The function $g_1 \circ f : A \to C$ is the constant function $a \mapsto 0$. Since b_0 is not contained in the image $f(A)$, also $g_2 \circ f : A \to C$ is the constant function $a \mapsto 0$. Thus

$$g_1 \circ f = g_2 \circ f$$

and the hypothesis now implies that $g_1 = g_2$. But this is a contradiction, since $g_1(b_0) = 0 \neq 1 = g_2(b_0)$. This contradiction completes the proof that f is surjective.

■

Remark 4.6.2: Proposition 4.6.1 amounts to a characterization of surjective functions. A similar characterization for injective functions appears in the homework.