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.

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ is the set of natural numbers.
- $\mathbb{Z} = \{\ldots -2, -1, 0, 1, 2, \ldots\}$ 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.

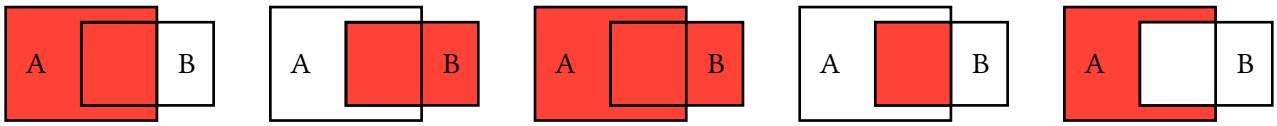


Figure 1: From left to right: A, B, $A \cup B$, $A \cap B$, $A - B$

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 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 $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$ 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

$$\begin{aligned} S_{m+1} &= (m+1) + \tfrac{m(m+1)}{2} \\ &= \tfrac{2(m+1)}{2} + \tfrac{m(m+1)}{2} \\ &= \tfrac{m^2+3m+2}{2} \\ &= \tfrac{(m+1)(m+2)}{2}. \end{aligned}$$

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

$$\begin{aligned} 0 + \quad & 1 + \ldots + (n-2) + (n-1) + n \\ n + (n-1) + \ldots + \quad & 2 + \quad 1 + 0 \end{aligned}$$

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 $0 \leq r < b$.

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

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

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 $0 \leq r, r' < b$, we have $-b < r - r' < b$; thus $r - r' = 0$, i.e. $r = r'$. Again using $(\blacklozenge)$ we see that $bq = bq'$ and since $b \neq 0$ 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 $0 \leq r < b$ 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

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

We prove two things:

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

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

- With notation as in the statement of Proposition 3.4.1, 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 Proposition 3.4.1 to conclude that $P(n)$ holds $\forall n \in \mathbb{N}$. This proves the Proposition.

■

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 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.

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:

  (♣) 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 (♣) 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 $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ...\right\}$ 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 $b = 1, 2, -2$.

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

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

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

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."

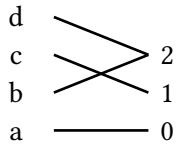
Example 4.1.3:

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

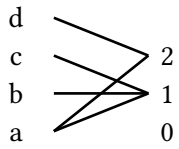
Notice that formally, f corresponds to the subset

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

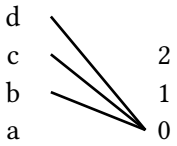
We can represent this function using the following diagram:



(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 $1/2, 2/4, -3/-6, \ldots$ and we do not know if $f(.5)$ should be $1, 2, -3, \ldots$

(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

$$f(A) = \{b \in B \mid \exists a \in A, f(a) = b\}.$$

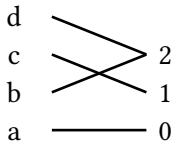
More generally, for a subset $A_1 \subseteq A$, the image of A_1 is the subset of B defined by $f(A_1) = \{b \in B \mid \exists a \in A_1, f(a) = b\}$.

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

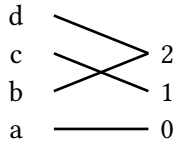
$$\forall x \in B, \exists a \in A, f(a) = x.$$

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:

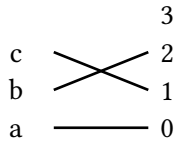
(a). For $A = \{a, b, c, d\}$ and $B = \{0, 1, 2\}$ consider again the function $f : A \to B$ described by the following diagram.



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 function $f : A \to B$ 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 bijective 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 bijection.

Example 4.5.2:

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

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

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.

5. Week 5 [2025-09-29]

5.1. Cardinality of sets

In this sections we want to look at the question of whether two sets can be identified and in particular at whether they have the same number of elements. We will see that the concept "having the same number of elements" makes sense not only for finite sets but also for infinite ones.

Over the years, we have all developed some intuition for the concepts of "more", "less" and "the same" based on our experience with finite sets. For infinite sets, the answers to some questions may be different from what we would expect from this intuition. For a start, with our definition, it will not be true that all infinite sets have the same number of elements. On the other hand, while the set of integers strictly contains the set of natural number and the set of rational numbers strictly contains the integers, we will see that all these sets have the same number of elements. The real numbers on the other hand have many more elements. Let us start with a definition:

Definition 5.1.1: We say that two sets A, B have the same cardinality if and only if there is a bijection between the two, in which case we write $|A| = |B|$.

5.2. Cadinality of finite sets

Definition 5.2.1: For $n \in \mathbb{N}$, we define the set I_n as follows:

$$I_0 = \emptyset$$

and for $n > 0$ by

$$I_n = I_{n-1} \cup \{n-1\}$$

.

Of course, $I_n = \{0, 1, 2, ..., n-1\}$.

Definition 5.2.2:

For a set A and a natural number $n \in \mathbb{N}$, we say that a set A is finite of cardinality n if there is a bijection between A and the set I_n just defined.

We then say that $|A| = n$. In particular, $|\emptyset\ | = 0$.

We say that a set A is infinite if it is not finite.

Proposition 5.2.3:

Let $n \in \mathbb{N}$ and suppose that A is a finite set of cardinality n. If $b \notin A$ then $A \cup \{b\}$ is a set of cardinality $n + 1$.

Proof: Since $|A| = n$, there is a bijection $\varphi : I_n \to A$. Now define $\psi : I_{n+1} \to A \cup \{b\}$ by the rule

$$\psi(m) = \begin{cases} \varphi(m) \text{ if } m < n+1 \\ b \text{ if } m = n+1. \end{cases}$$

We define $\mu : A \cup \{b\} \to I_{n+1}$ by the rule

$$\mu(a) = \begin{cases} \varphi^{-1}(a) \text{ if } a \in A \\ n+1 \text{ if } a = b \end{cases}$$

Note that μ is well-define since for any element $a \in A \cup \{b\}$, either $a \in A$ or $a = b$ but not both.

It is straightforward to check that $\mu \circ \psi = \mathrm{id}_{I_n}$ and that $\psi \circ \mu = \mathrm{id}_{A \cup \{b\}}$. ■

Proposition 5.2.4: Let $M, n \in \mathbb{N}$ and consider the set

$$B_n(M) = \{b \in \mathbb{N} \mid M \leq b < M + n\}.$$

Then $|B_n(M)| = n$.

Notice that $I_n = B_n(0)$.

Proof: In fact, we will give two proofs. Either of these proofs establishes the result; we provide both here to illustrate different techniques!

For the first proof, define

$$f : I_n \to B_n(M) \text{ by } f(a) = a + M$$

and

$$g : B_n(M) \to I_n \text{ by } g(a) = a - M.$$

First, these two maps are well defined. We need to see that the images are in the corresponding codomains:

An element a of I_n is a natural number with $0 \leq a < n$. Then $f(a) = a + M$ is a natural number with $M = 1 + M \leq a + M < n + M$ so that $a + M \in B_n(M)$.

Similarly, an element b of $B_n(M)$, is a natural number with $M \leq b < M + n$. Then $b - M$ is a natural number with $0 = M - M \leq b - M < n = M + n - M$ so that $b - M \in I_n$.

We check that the two functions are inverse of each other:

$$g \circ f(a) = g(f(a)) = g(a + M) = (a + M) - M = a$$

and

$$f \circ g(b) = f(g(b)) = f(b - M) = (b - M) + M = b.$$

Thus f and g are inverse bijections; in particular, f is a bijection between $B_n(M)$ and I_n so indeed $|B_n(M)| = n$.

For the second proof, notice that $B_0(M) = \emptyset$ and for $n \in \mathbb{N}$, $n > 0$ we have

$$B_n(M) = B_{n-1}(M) \cup \{M + n - 1\}.$$

We now prove by induction on n that $|B_n(M)| = n$.

For the base case, since $B_0(M) = \emptyset$, we indeed know that $|B_0(M)| = 0$.

For the induction step, let $k \in \mathbb{N}$ and suppose that $|B_k(M)| = k$. We must show that $|B_{k+1}(M)| = k+1$.

Since

$$B_{k+1}(M) = B_k(M) \cup \{M+k\}$$

and since $M + k \notin B_k(M)$, it follows from Proposition 5.2.3 that $|B_{k+1}(M)| = k+1$ as required.

Thus the formula $|B_n(M)| = n$ follows by induction.

■

Proposition 5.2.5: Let $m, n \in \mathbb{N}$ and let A, B be finite sets of cardinality m and n respectively. Then the disjoint union $A \bigsqcup B$ is finite of cardinality $m+n$.

Proof: Since $|A| = m$ and $|B| = n$, there are bijections

$$\varphi : I_m \to A \text{ and } \psi : I_n \to B.$$

Let us write $\iota_A : A \to A \bigsqcup B$ and $\iota_B : B \to A \bigsqcup B$ for the inclusion mappings.

We now define a mapping $\Phi : I_{m+n} \to A \bigsqcup B$ by the rule

$$\Phi(k) = \begin{cases} \iota_A(\varphi(k)) \text{ if } k < m \\ \iota_B(\psi(k-m)) \text{ otherwise} \end{cases}.$$

Notice for $k \in I_{m+n}$ with $m \leq k$ that $k - m \in I_n$, so the definition is meaningful.

On the other hand we define a mapping $\Psi : A \bigsqcup B \to I_{m+n}$ as follows:

any $x \in A \bigsqcup B$ has exactly one of the following forms:

- $x = \iota_A(a)$ for $a \in A$: in this case, define $\Psi(x) = \varphi^{-1}(a) \in I_m \subseteq I_{m+n}$.
- $x = \iota_B(b)$ for $b \in B$: in this case, define $\Psi(x) = \psi^{-1}(b)) + m \in I_{m+n}$.

When $x = \iota_B(b)$ notice that $\psi^{-1}(b) \in I_n$ so that $\psi^{-1}(b) + m$ is indeed in I_{m+n}.

For $k \in I_{m+n}$ we argue that $\Psi(\Phi(k)) = k$.

- if $k < m$ then $\Psi(\Phi(k)) = \Psi(\iota_A(\varphi(k))) = \varphi^{-1}(\varphi(k)) = k$
- if $m \leq k$ then $\Psi(\Phi(k)) = \Psi\left(\iota_{b(\psi(k-m))}\right) = \psi^{-1}(\psi(k-m)) + m = k - m + m = k$

For $x \in A \bigsqcup B$ we argue that $\Phi(\Psi(x)) = x$.

- if $x = \iota_A(a)$ for $a \in A$ then

  $$\Phi(\Psi(x)) = \Phi(\varphi^{-1}(a)) = \iota_A(\varphi(\varphi^{-1}(a))) = \iota_A(a) = x$$

  since $\varphi^{-1}(a) < m$.
- if $x = \iota_B(b)$ for $b \in B$ then

  $$\Phi(\Psi(x)) = \Phi(\psi^{-1}(b) + m) = \iota_B(\psi(\psi^{-1}(b) + m - m)) = \iota_B(\psi(\psi^{-1}(b))) = \iota_B(b) = x.$$

■

Remark 5.2.6: Suppose that $f : X \to Y$ is a bijection and let $x \in X$. Then f determines by restriction a bijection

$$X \setminus \{x\} \to Y \setminus \{f(x)\}.$$

Proposition 5.2.7: Let A be a finite set of cardinality n. If $n > 0$ and if $x \in A$, then the set

$$A \setminus \{x\} = \{a \in A \mid a \neq x\}$$

has cardinality $n - 1$.

Proof: Since $|A| = n$, there is a bijection $\varphi : I_n \to A$. Write $k = \varphi^{-1}(x) \in I_n$.

Now notice that – with notation as in Proposition 5.2.4 –

$$I_n = I_k \bigsqcup \{k\} \bigsqcup B_{n-k-1}(k+1);$$

recall that

$$B_{n-k-1}(k+1) = \{m \in \mathbb{N} \mid k+1 \leq m < k+1+n-k-1\} = \{m \in \mathbb{N} \mid k+1 \leq m < n\}.$$

Thus

$$I_n \setminus \{k\} = I_k \bigsqcup B_{n-k-1}(k+1).$$

Now, according to Remark 5.2.6, φ determines by restriction a bijection

$$I_n \setminus \{k\} \to A \setminus \{x\}.$$

Thus

$$|A \setminus \{x\}| = |I_n \setminus \{k\}| = |I_k \bigsqcup B_{n-k-1}(k+1)| = (*)$$

Using Proposition 5.2.5 we know that $(*) = |I_k| + |B_{n-k-1}(k+1)|$; In turn, Proposition 5.2.4 shows that $|B_{n-k-1}(k+1)| = n - k - 1$. Thus we have proved that

$$|A \setminus \{x\}| = k + (n - k - 1) = n - 1,$$

as required.

■

Finally, we need to establish that cardinality is unambiguous. Namely, we prove that

Proposition 5.2.8: Let $m, n \in \mathbb{N}$ and let A and B be finite sets with $|A| = m$ and $|B| = n$. If there is a bijection between A and B then $m = n$.

Proof: We have proved that the composition of bijections is a bijection Proposition 4.5.9. Our assumptions give a bijection $I_m \xrightarrow{\sim} A$ and a bijection $I_n \xrightarrow{\sim} B$. Thus, there is a bijection $I_m \xrightarrow{\sim} I_n$.

Without loss of generality, we may and will suppose that $n \leq m$.

We proceed by induction on n.

If $n = 0$, then $I_n = \emptyset$. Since I_n and I_m are in bijection, there can be no elements in I_m, either. In other words, $I_m = \emptyset$ so that $m = 0$. This establishes the base-case of the induction.

Now suppose that $k \in \mathbb{N}$ and that we know the following: whenever $k \leq m$ and I_k and I_m are in bijection, then $k = m$.

Given $k + 1 \leq m$ and a bijection $\varphi : I_{k+1} \to I_m$, we must argue that $k + 1 = m$.

Well, the restriction of φ to the subset $I_k = I_{k+1} \setminus \{k + 1\}$ determines a bijection

$$\varphi' : I_k \to I_m \setminus \{\varphi(k + 1)\};$$

see Remark 5.2.6. It follows from Proposition 5.2.7 that the cardinality of $I_m \setminus \{\varphi(k + 1)\}$ is equal to $m - 1$; since φ' is a bijection, the cardinality of I_k is $m - 1$. Thus $k = m - 1$ so that $k + 1 = m$ as required.

Now the equality $m = n$ follows by induction. ■

Proposition 5.2.9: If A is a finite set with n elements and $B \subseteq A$, then B is a finite set with at most n elements and it has precisely n elements if and only if $B = A$.

Proof: As A is finite with n elements, there is a bijection between A and $I_n = \{0, 1, ..., n - 1\}$. Using this bijection, we can identify A with I_n and just assume that B is a subset of I_n.

What we need to do is define a bijection between B and a set $I_k = \{1, 2, ..., k\}$, for some $k \leq n$. Equivalently, we need to label the elements of B with numbers $1, 2, ..., k$ for some k We can do this as follows: we choose the smallest element $b_0 \in B$ and we will label it with 0, then we choose the smallest number in $b_1 \in B - \{b_0\}$ and we label it with 1 and so on. We keep going until we run out of elements in B.

Observe that

$$b_0 < b_1 < b_2 < ...$$

As $b_0 \in B \subseteq I_n = \{0, 1, ..., n - 1\}$, we have $1 \leq b_1$. From our choice of b_0 as the smallest element B , $0 \leq b_0 < b_1$, so $1 \leq b_1$. Similarly $k \leq b_k$ and because all the elements in B are in I_n, there are at most n elements b_k. So, we will run out of elements in B after at most n steps. Moreover, if we need all of the n steps, then $b_0 = 0, b_1 = 1, ..., b_{n-1} = (n - 1)$ and therefore $B = I_n$. ■

6. Week 6 [2025-10-06]

6.1. Cardinality of infinite sets

Definition 6.1.1: A set A is countable, or countably infinite, if there is a bijection between A and the set $\mathbb{N}$ of natural numbers.

Proposition 6.1.2: The set E of even natural numbers is countably infinite.

Proof: We will exhibit a bijection between E and $\mathbb{N}$. For this, define functions

$$f : \mathbb{N} \to E \text{ by the rule } f(a) = 2a$$

and

$$g : E \to \mathbb{N} \text{ by the rule } g(b) = e/2.$$

These functions are well defined as by definition, a natural number b is even if and only if there exists another natural number a such that $b = 2a$. So, for any natural number a, $2a$ is an even number and for every even number b, $b/2$ is a natural number. Moreover, the two functions are inverse of each other as

$$(g \circ f)(a) = g(f(a)) = g(2a) = 2a/2 = a$$

and

$$(f \circ g)(b) = f(g(b)) = f(b/2) = 2 \cdot (b/2) = b.$$

■

Proposition 6.1.3: The set $\mathbb{Z}$ of integers is countably infinite.

Proof: We will exhibit a bijection between $\mathbb{Z}$ and $\mathbb{N}$.

Our bijection will identify even natural numbers with non-negative integers, and odd natural numbers with negative integers.

Define

$$f : \mathbb{N} \to \mathbb{Z} \text{ by the rule } f(n) = \begin{cases} n/2 \text{ if } n = 2k \text{ is even} \\ -(n+1)/2 \text{ if } n = 2k+1 \text{ is odd} \end{cases}$$

and define

$$g : \mathbb{Z} \to \mathbb{N} \text{ by the rule } g(z) = \begin{cases} 2z \text{ if } z \geq 0 \\ -2z - 1 \text{ if } z < 0 \end{cases}$$

We check that the functions are mutually inverse:

For $z \in \mathbb{Z}$, if $z \geq 0$ then

$$(f \circ g)(z) = f(g(z)) = f(2z) = z$$

while if $z < 0$ then

$$(f \circ g)(z) = f(g(z)) = f(-2z-1) = -(-2z-1+1)/2 = z.$$

This shows that $f \circ g = \mathrm{id}_{\mathbb{Z}}$.

For $n \in \mathbb{N}$, if $n = 2k$ is even then

$$(g \circ f)(n) = g(f(n)) = g(n/2) = 2 \cdot (n/2) = n$$

while if $n = 2k+1$ is odd then

$$(g \circ f)(n) = g(f(n)) = g(-(n+1)/2) = -2(-(n+1)/2) - 1 = n+1-1 = n.$$

This shows that $g \circ f = \mathrm{id}_{\mathbb{N}}$. ■

Remark 6.1.4: Using the bijection described in the previous proof, note that

n	$f(n)$
0	0
1	−1
2	1
3	−2
4	2
5	−3
6	3
7	−4
8	4

z	$g(z)$
−4	7
−3	5
−2	3
−1	1
0	0
1	2
2	4
3	6
4	8

Proposition 6.1.5: If A is a countably infinite set and $B \subseteq A$, then B is either finite or countably infinite.

Proof: As A is countable, there is a bijection between A and $\mathbb{N}$. Using this bijection, we can identify A with $\mathbb{N}$ and just assume that B is a subset of $\mathbb{N}$.

What we need to do is to find a way to label the elements in B as $1, 2, ..., k, ...$ We proceed as in the proof of Proposition 5.2.9. Since B is a subset of $\mathbb{N}$, the well ordering principle permits us to choose the smallest element $b_0 \in B$. If $b_0, b_1, ..., b_m$ have been chosen we choose b_{m+1} to be the small element of $B \setminus \{b_0, b_1, ..., b_m\}$.

Observe that

$$b_0 < b_1 < b_2 < ...$$

If after n steps, $B \setminus \{b_0, b_1, ..., b_{n-1}\} = \emptyset$, then $B = \{b_0, ..., b_{n-1}\}$ is finite of cardinality n.

Otherwise, notice that (♣) $\{b_i \mid i \in \mathbb{N}\} \not\subseteq I_m$ for any $m \in \mathbb{N}$.

we claim that $B = \{b_i \mid i \in \mathbb{N}\}$ so that B is countably infinite.

Clearly $\{b_i \mid i \in \mathbb{N}\} \subseteq B$ by construction. To prove the other inclusion, we proceed by contradiction.

Thus we suppose that $B \setminus \{b_i \mid i \in \mathbb{N}\}$ is non-empty. By the well-ordering principle, there is a smallest element $c \in B \setminus \{b_i \mid i \in \mathbb{N}\}$.

In view of (♣), $\{b_i \mid i \in \mathbb{N}\} \not\subseteq I_c$ so $\exists j \in \mathbb{N}, c < b_j$. But this is a contradiction since b_j was chosen to be the smallest element of $B \setminus \{b_0, ..., b_{c-1}\}$ and $c \in B \setminus \{b_0, ..., b_{c-1}\}$.

This contradiction proves that $B = \{b_i \mid i \in \mathbb{N}\}$ so that B is indeed countably infinite, as required. ■

Proposition 6.1.6: Let X and Y be sets and suppose that $f : X \to Y$ is a surjective function. If X is countably infinite, then Y is countably infinite or finite.

Proof: We first show that there is a "right inverse" to f; i.e. a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.

Indeed, to define g, for each $y \in Y$ we *choose* some element x of the inverse image $f^{-1}(\{y\})$. Since f is surjective, such a choice is always possible.

Since $f(g(y)) = y$ by definition, indeed $f \circ g = \mathrm{id}_Y$.

Now, note that g is an *injective* function. This follows from a homework problem, and may be proved as follows.

Suppose that $y_1, y_2 \in Y$ and that $g(y_1) = g(y_2)$. To see that g is injective, we must argue that $y_1 = y_2$.

But

$$g(y_1) = g(y_2) \Rightarrow f(g(y_1)) = f(g(y_2)) \Rightarrow (f \circ g)(y_1) = (f \circ g)(y_2) \Rightarrow y_1 = y_2$$

Since g is injective, the Proposition follows by applying Proposition 6.1.5 to the subset

$$g(Y) \subseteq X.$$

■

Proposition 6.1.7: Suppose that X and Y are countably infinite sets. Then the cartesian product

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

is countably infinite.

Proof: By hypothesis, there is a bijection between X and $\mathbb{N}$, and a bijection between Y and $\mathbb{N}$. Thus we can identify $X \times Y$ with $\mathbb{N} \times \mathbb{N}$, and our task is to prove that $\mathbb{N} \times \mathbb{N}$ is countably infinite.

For each $n \in \mathbb{N}$, consider the set D_n of elements $(i, j) \in \mathbb{N} \times \mathbb{N}$ for which $i + j = n$. Thus

$$D_n = \{(i, j) \in \mathbb{N} \times \mathbb{N} \mid i + j = n\}.$$

There are $n+1$ elements in D_n, namely

$$D_n = \{(0,n),(1,n-1),(2,n-2),...,(n-2,2),(n-1,1),(n,0)\}$$

To give a bijection between $\mathbb{N}\times\mathbb{N}$ and $\mathbb{N}$, our task is to label all the elements in $\mathbb{N}\times\mathbb{N}$.

Since

$$\mathbb{N} = \bigsqcup_{n\in\mathbb{N}} D_n$$

we will accomplish this by first labeling the element of D_0 with 0, the elements of D_1 with 1 and 2, the elements of D_2 with $3,4,5$ and so forth.

Note that the labels for the elements in D_n must begin at the number

$$|D_0| + |D_1| + ... + |D_{n-1}| = \sum_{i=0}^{n-1}(i+1) = \sum_{j=1}^{n} j = n(n+1)/2.$$

Here is concrete description of this labeling:

Define

$$f : \mathbb{N}\times\mathbb{N} \to \mathbb{N} \text{ by } f(i,j) = i + (i+j)(i+j+1)/2.$$

To define the inverse function

$$g : \mathbb{N} \to \mathbb{N}\times\mathbb{N}$$

notice that $n(n+1)/2$ is an increasing function of n that is unbounded. Thus for any $m\in\mathbb{N}$ we can find a unique natural number $n\in\mathbb{N}$ for which

$$n(n+1)/2 \leq m < (n+1)(n+2)/2.$$

We define

$$g(m) = (m - n(n+1)/2, n - m + n(n+1)/2)$$

We now check that $g\circ f = \mathrm{id}_{\mathbb{N}\times\mathbb{N}}$. Let $(i,j)\in\mathbb{N}\times\mathbb{N}$ and write $n = i+j$. We must argue that $g\circ f)(i,j) = (i,j)$. Using the definitions we find

$$\begin{aligned}(g\circ f)(i,j) &= g(i + (i+j)(i+j+1)/2) \\ &= g(i + n(n+1)/2) \\ &= (i + n(n+1)/2 - n(n+1)/2, n - (i + n(n+1)/2) + n(n+1)/2) \\ &= (i, n-i) = (i,j)\end{aligned}$$

as required..

Finally, we show that $f\circ g = \mathrm{id}_{\mathbb{N}}$. Let $m\in\mathbb{N}$ and find the unique $n\in\mathbb{N}$ for which $n(n+1)/2 \leq m < (n+1)(n+2)/2$. We must confirm that $(f\circ g)(m) = m$. Using definitions, we have:

$$\begin{aligned}(f\circ g)(m) &= f(m - n(n+1)/2, n - m + n(n+1)/2) \\ &= m - n(n+1)/2 + n(n+1)/2 \\ &= m\end{aligned}$$

as required. ■

Remark 6.1.8: Some values of the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. In the table, the first row contains values of i and the first column contains values of j. The remaining entries are the values $f(i, j)$.

i \ j	0	1	2	3	4	5	6	7	8	9	10
0	0	2	5	9	14	20	27	35	44	54	65
1	1	4	8	13	19	26	34	43	53	64	76
2	3	7	12	18	25	33	42	52	63	75	88
3	6	11	17	24	32	41	51	62	74	87	101
4	10	16	23	31	40	50	61	73	86	100	115
5	15	22	30	39	49	60	72	85	99	114	130
6	21	29	38	48	59	71	84	98	113	129	146
7	28	37	47	58	70	83	97	112	128	145	163
8	36	46	57	69	82	96	111	127	144	162	181
9	45	56	68	81	95	110	126	143	161	180	200
10	55	67	80	94	109	125	142	160	179	199	220

Corollary 6.1.8.1: The set of non-negative rational numbers $\mathbb{Q}_{\geq 0}$ is countably infinite.

Proof: A non-negative rational number may be expressed uniquely in the form n/m where $(n, m) \in \mathbb{N} \times \mathbb{N}$, $m \neq 0$ and n and m have no common divisor.

Thus $\mathbb{Q}_{\geq 0}$ may be identified with a subset of $\mathbb{N} \times \mathbb{N}$. In view of Proposition 6.1.5, we know that $\mathbb{Q}_{\geq 0}$ is either finite or countably infinite.

Since $\mathbb{N} \subset \mathbb{Q}_{\geq 0}$, we know that $\mathbb{Q}_{\geq 0}$ is not finite, and the Corollary is proved. ■

Remark 6.1.1: An alternative line of argument is to note that there is a surjective mapping $\mathbb{N} \times \mathbb{N}_{>0} \to \mathbb{Q}_{\geq 0}$ given by $(m, n) \mapsto m/n$. Now apply Proposition 6.1.6.

Corollary 6.1.1.1: The set $\mathbb{Q}$ of rational numbers is countably infinite.

Proof: Note that $\mathbb{Q}$ is the disjoint union

$$\mathbb{Q} = \mathbb{Q}_{\geq 0} \bigsqcup \mathbb{Q}_{<0}.$$

According to Corollary 6.1.8.1, there is a bijection $\varphi : \mathbb{Q}_{\geq 0} \xrightarrow{\sim} \mathbb{N}$.

The mapping $x \mapsto -x$ puts $\mathbb{Q}_{<0}$ with an infinite subset of $\mathbb{Q}_{\geq 0}$, so by Proposition 6.1.5 there is a bijection $\psi : \mathbb{Q}_{<0} \xrightarrow{\sim} \mathbb{N}$.

Now consider the mapping

$$\Phi : \mathbb{Q} = \mathbb{Q}_{\geq 0} \bigsqcup \mathbb{Q}_{<0} \to \mathbb{N} \times \mathbb{N}$$

given by

$$f(x) = \begin{cases} (\varphi(x), 0) \text{ if } x \geq 0 \\ (0, \psi(x)) \text{ otherwise.} \end{cases}$$

Then Φ is one-to-one so that $\mathbb{Q}$ identifies with an infinite subset of the countably infinite set $\mathbb{N} \times \mathbb{N}$; thus $\mathbb{Q}$ is countably infinite. ■

Theorem 6.1.1: The infinite set $\mathbb{R}$ is not countably infinite.

Proof: You will show for homework that $\mathbb{R}$ is in bijection with the open interval $(0,1)$. So the result will follow if we show that $(0,1)$ is not countably infinite.

Note that an $x \in (0,1)$ may be represented as a decimal expression. For example, the decimal expression $x = 0.519\overline{6}$ is the number

$$x = \frac{5}{10} + \frac{1}{100} + \frac{9}{1000} + 6\left(\sum_{i=4}^{\infty} \frac{1}{10^i}\right)$$

If the interval $(0,1)$ were countable, we could order all the decimals expressions between 0 and 1 and put them in correspondence with the positive natural numbers $\mathbb{N}_{>0}$.

So, we suppose that $(0,1) = \{a_i \mid i \in \mathbb{N}_{>0}\}$.

We are going to show that there is at least one real number $y \in (0,1)$ not in our list. We are going to construct y be specifying the decimal digits of y.

To define the nth decimal digit of y, we look at the nth decimal digit of the element a_n in our list.

If that digit is some number $b < 9$, we use $b+1$ as the nth decimal digit of y.

If that digit is $a = 9$, we use 0 as the nth of y.

For example, if our list begins

a_1	0.123123123...
a_2	0.121221222...
a_3	0.123456789...
a_4	0.345189237...
a_5	0.116722298...
a_6	0.336721498...
a_7	0.000999835...

then the decimal expansion of y would begin

$$y = 0.2342320...$$

We notice for each n that the n-th decimal digit of y is different from the nth decimal digit of a_n. Thus $y \neq a_n$. Since this holds for each n, $y \notin \{a_i \mid i \in \mathbb{N}\}$.

Also, y is strictly between 0 and 1:if it were identically 0, it would mean that in the original list, the nth digit of a_n is equal to 9 for each n. But many decimals between 0 and 1 have no decimal digits of 9 at all, so the original list was incomplete.

Similarly, if the new number were $0.999999\ldots = 1$, it would mean that a_n has 0 as its nth decimal digit. But many decimals between 0 and 1 have no 0's at all, so the original list was incomplete. This contradiction completes the proof that the interval of the real line $(0, 1)$ is not countable and therefore $\mathbb{R}$ itself is not countable.

■

6.2. Counting problems; products and unions of sets.

Proposition 6.2.1: Assume that A, B are finite sets. Then $A \cup B$ is finite and

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof: We can write B as the union of disjoint subsets

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

Thus Proposition 5.2.5 shows that $|B| = |B \cap A| + |B \setminus A|$.

Thus we have

$$(*) \quad |B \setminus A| = |B| - |B \cap A|.$$

Now, we can write $A \cup B$ as the union of disjoint subsets

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

Since this union is disjoint, we find

$$|A \cup B| = |A| + |B \setminus A|.$$

Now substituting $(*)$, we arrive at the formula

$$|A \cup B| = |A| + |B| - |B \cap A|$$

as required. ■

Example 6.2.2: At a certain large gathering, twenty percent of attendees wear a blue T-shirt and ten percent wear a blue baseball hat while only four percent wear both.

This means that $20 + 10 - 4 = 26$ percent wear at least one of the two blue articles.

6.3. Products

Recall that the cartesian product of two sets is the set of pairs with the first element in the first set, the second in the second set. – see Definition 1.2.4.8.

We just saw that the disjoint union of two sets has cardinality equal to the sum of the two cardinalities. In a similar way, we are going to see now that the cartesian product has cardinality equal to the product of the two cardinalities

Proposition 6.3.1: Assume that A, B are finite sets of cardinality m and n respectively. Then $A \times B$ is finite of cardinality mn.

Proof: From our assumptions, there are bijections

$$f : I_m \to A \text{ and } g : I_n \to B.$$

We now define a function

$$h : A \times B \to I_{mn} \text{ by } h(a, b) = m \cdot g(b) + f(a).$$

We claim that h is a bijection.

We first show that h is one-to-one. For this, let $(a,b),(a',b') \in A \times B$ and suppose that $h(a,b) = h(a',b')$. We must argue that $(a,b) = (a',b')$.

By assumption we know that

$$(*) \quad m \cdot g(b) + f(a) = m \cdot g(b') + f(a').$$

Since $f(a), f(a') \in I_m$, the remainder upon division of $h(a,b)$ by m is $f(a)$ and the remainder upon division of $h(a',b')$ by m is $f(a')$.

Since $h(a,b) = h(a',b')$ by assumption, these remainders are equal by Proposition 3.4.4. Thus $f(a) = f(a')$ and since f is a bijection, we conclude that $a = a'$.

Now $(*)$ shows that $m \cdot g(b) = m \cdot g(b')$ so that $g(b) = g(b')$. Since g is a bijection, conclude that $b = b'$.

Thus $(a,b) = (a',b')$ and we have proved that h is one-to-one.

We now prove that h is onto. Given $x \in I_{mn}$, divide x by m to obtained

$$x = qm + r \text{ where } q, r \in \mathbb{N}, 0 \leq r < m$$

as in Proposition 3.4.4.

Note that

$$0 \leq x = qm + r < mn.$$

Thus

$$qm < mn \Rightarrow q < n.$$

In particular, $q \in I_n$ and $r \in I_m$. Now set Let $b = g^{-1}(q)$ and $a = f^{-1}(r)$ and it is easy to see that

$$h(a,b) = x.$$

This proves that h is onto and completes the proof that h is a bijection. We now conclude that $|A \times B| = mn$ as required. ■

7. Week 7 - [2025-10-14]

7.1. Relations

The mathematical concept of relation expresses a sort of connection between two objects. This connection can be one directional only or bi-directional; for example, the relation between child and parent would be of the first type, the relation among siblings would be of the second.

The mathematical definition is defined as follows:

Definition 7.1.1: Let A and B be sets. A relation from A to B is defined to be a subset R of the cartesian product $A \times B$.

For $a \in A$ and $b \in B$ we write $a \sim b$ if and only if $(a, b) \in R$.

Example 7.1.2:

(a). Let A be the set of all students enrolled in some class at Tufts in the Fall of 2025, B the set of all course being offered this Fall. Consider the set of pairs

$$R = \{(a, b) \mid a \text{ is enrolled in class } b\}$$

that is, students are related to the courses they are enrolled in. Then for any of member of our class, the proposition

"your name" $\sim$ Math 65

holds.

(b). Let $A = \mathbb{R}_{>0} = (0, \infty)$ be the set of positive real numbers, and let $B = \mathbb{Z}$ be the set of all integers.

Consider the set of pairs

$$R = \{(a, b) \in \mathbb{R}_{>0} \times \mathbb{Z} \mid b \leq a \leq b + 1\}$$

that is, every real number is related to the integers that are at most one unit apart from it. Then

$$1.3 \sim 1, \quad 1.3 \sim 2 \quad \text{but} \quad 1.3 \nsim 5.$$

(c). Any function $f : A \to B$ is a relation.

In fact, $a \sim b$ if and only if $b = f(a)$. The relation $R \subseteq A \times B$ has the form

$$R = \{(a, f(a)) \mid a \in A\}$$

and is called the graph of the function f.

There are many relations from A to B that are not functions.

(d). Let $A = \{a, b, c\}, B = \{1, 2, 3\}$.

Then $R_1 = \{(a, 1), (b, 1), (c, 3)\}$ is the graph of a function.

But $R_2 = \{(a, 1), (a, 2), (b, 3), (c, 3)\}$ is a relation which is not the graph of a function as a appears twice as the first term of a pair.

Similarly, $R_3 = \{(a,1),(b,3)\}$ is a relation which is not the graph of a function as c does not appear as the first term of a pair.

(e). For a function $\mathbb{R} \to \mathbb{R}$, this definition of graph is the graph in the plane $\mathbb{R}^2$ that you are familiar with. The condition that for every $a \in A$, a appears in one and only one pair $(a,b) \in R$ is a translation of the vertical line test.

For example, the graph of $f : \mathbb{R} \to \mathbb{R}$ given by the rule $f(x) = 2x + 1$ is the line in the plane $\mathbb{R}^2$ with slope 2 and y-intercept 1.

We now focus on relations from a set to itself – i.e. the case in which $A = B$. We then simply describe a relation from A to A as a relation on A.

Here are some properties that such a relation may or may not satisfy:

Definition 7.1.3: Let A be a set and let $\sim$ be a relation on A.
- The relation is reflexive if $\forall x \in A, x \sim x$.
- The relation is symmetric if $\forall x, y \in A, x \sim y \Rightarrow y \sim x$.
- The relation is antisymmetric if $\forall x, y \in A, x \sim y$ and $y \sim x \Rightarrow x = y$.
- The relation is transitive if $\forall x, y, z \in A, x \sim y$ and $y \sim z \Rightarrow x \sim z$.

Definition 7.1.4: Let A be a set and $\sim$ a relation on A. Then $\sim$ is an equivalence relation provided that it is
- reflexive,
- symmetric, and
- transitive.

Example 7.1.5:

(a). Define a relation on the set of current Tufts students as follows: for students x and y, $x \sim y$ if and only if x and y are both enrolled in the same section of some course.

This relation is reflexive and symmetric but not necessarily transitive. For example, x and y might be enrolled in Math 65, y and z might both be enrolled in Comp 40, but it is entirely possible that x and z have no courses in common.

(b). Define another relation on the set of current Tufts students as follows: for students x and y, $x \sim y$ if and only if x and y are enrolled in precisely the same courses.

Then this relation is an equivalence relation.

(c). Consider the following relation R on the set $A = \{a,b,c\}$:

$$R = \{(a,a),(a,b),(b,b),(b,a),(c,c)\}$$

- The relation is reflexive as it contains $(a,a),(b,b),(c,c)$.
- The relation is symmetric: the only pairs $(x,y), x \neq y$ in the relation are $(a,b),(b,a)$; thus the condition that $x \sim y$ implies $y \sim x$ is satisfied. (or equivalently that $(x,y) \in R \Rightarrow (y,x) \in R$).

- The relation is transitive: the only pairs $(x, y), x \neq y$ in the relation are $(a, b), (b, a)$, that is $a \sim b$ and $b \sim a$ which implies if the relation is transitive $a \sim a$.

  Also $b \sim a$ and $a \sim b$ implies if the relation is transitive $b \sim b$. As the relation contains both (a, a) and (b, b), it is transitive

As the relation is reflexive, symmetric and transitive, it is an equivalence relation.

(d). Consider the set $S = \mathbb{Z}$ of all integers. Choose a **fixed** integer n. Consider the relation defined for $z_1, z_2 \in \mathbb{Z}$ by

$$z_1 \sim z_2 \Leftrightarrow \exists k \in \mathbb{Z}, z_1 - z_2 = nk.$$

We check that it this an equivalence relation by checking that it satisfies the three required properties:

- reflexive: Let $z \in \mathbb{Z}$. Then $z - z = 0 = n \cdot 0$ for so that $z \sim z$.
- symmetric: Let $z_1, z_2 \in \mathbb{Z}$ and suppose that $z_1 \sim z_2$. Thus, we may find $k \in \mathbb{Z}$ with $z_1 - z_2 = nk$ We must argue that $z_2 \sim z_1$. But $z_2 - z_1 = (-z_1 - z_2) = -nk = n \cdot (-k)$ Since $-k \in \mathbb{Z}$, we see that $z_2 \sim z_1$ be definition, as required. This proves that $\sim$ is symmetric.
- transitive: Let $z_1, z_2, z_3 \in \mathbb{Z}$ and suppose that $z_1 \sim z_2$ and $z_2 \sim z_3$. To prove transitivity, we must show that $z_1 \sim z_3$.

  By definition of the relation, there are $k_1, k_2 \in \mathbb{Z}$ such that

  $$z_1 - z_2 = nk_1 \text{ and } z_2 - z_3 - nk_2.$$

  Adding these two equations, one obtains

  $$z_1 - z_3 = (z_1 - z_2) + (z_2 - z_3) = nk_1 + nk_2 = n(k_1 + k_2)$$

  As $k_1 + k_2 \in \mathbb{Z}$, the definition of our relation implies that $z_1 \sim z_3$ and therefore the relation is transitive.

This relation is usually denoted using the symbol $\equiv$. For $z_1, z_2 \in \mathbb{Z}$, the symbol $z_1 \equiv z_2 (\mathrm{mod}\, n)$ means what we have been writing as $z_1 \sim z_2$; read

$z_1 \equiv z_2 (\mathrm{mod}\, n)$

aloud as

"z_1 is congruent to z_2 modulo n."

Note e.g. that $13 \equiv 1 (\mathrm{mod}\, 12)$; thus the identifications made when doing "clock arithmetic" amounts to "congruence mod 12".

(e). Let $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ be the set of pairs of integers with the second one not being zero. Define a relation $\sim$ on A as follow: $(a, b) \sim (c, d)$ if and only if $ad = bc$.

We carefully check the three properties of an equivalence relation for $\sim$. As A is a set of pairs, the relation relates two pairs.

- reflexive: Let $(a, b) \in A$. We must argue that $(a, b) \sim (a, b)$. We know that $ab = ba$ by the commutative property of the product of integers.

  Hence, by definition of the relation, $(a, b) \sim (a, b)$. This proves that $\sim$ is reflexive.

- symmetric: Let $(a,b),(c,d) \in A$ and suppose that $(a,b) \sim (c,d)$. We must show that $(c,d) \sim (a,b)$.

  By definition of $\sim$, we know that $ad = bc$. Hence, $cb = da$. Therefore, by definition we have $(c,d) \equiv (a,b)$. This shows that $\sim$ is symmetric.

- transitive: let $(a,b),(c,d),(e,f) \in A$ and suppose that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$. We must show that $(a,b) \sim (e,f)$.

  By definition of $\sim$, we know that $ad = bc$ and $cf = de$.

  Multiplying the first equation with f and the second with b, we obtain $adf = bcf$ and $bcf = bde$. Therefore, $adf = bde$.

  This equation is equivalent to $d(af - be) = 0$. As by assumption, $d \neq 0$, we find that $af - be = 0$ or so that $af = be$.

  By definition of $\sim$, this means that $(a,b) \sim (e,f)$; thus $\sim$ is transitive.

Observe that for integers a, b, c, d with b and d non-zero, the two rational numbers a/b and c/d are equal if and only if $(a,b) \sim (c,d)$.

7.2. Equivalence classes for our examples

Let A be a set and let $\sim$ be an equivalence relation on A.

Definition 7.2.1: For $a \in A$, the equivalence class of a – denoted $[a]$ – is the subset of A defined by

$$[a] = \{x \in A \mid x \sim a\}.$$

Sometimes the equivalence class $[a]$ of a is called the coset of a for the equivalence relation.

Example 7.2.2: Let's look at the equivalence classes for the examples in Example 7.1.5.

(a). Since this relation was not an equivalence relation, we haven't defined equivalence classes in this case.

(b). In this example, there are many equivalence classes. There is precisely one for each choice of course schedule. Popular schedules will correspond to larger equivalence classes.

(c). For the relation R on $A = \{a,b,c\}$, there are two equivalence classes; they are

$$[a] = [b] = \{a,b\} \text{ and } [c] = \{c\}.$$

(d). For the relation on $\mathbb{Z}$ defined by "congruence modulo n", there are precisely n equivalence classes.

Given any integer $z \in \mathbb{Z}$, there are unique integers $z = qn + r$. Then

$$z - r = nq \text{ with } 0 \leq r < n.$$

Notice that that $z \equiv r \pmod{n}$ so that $z \in [r]$.

This shows that every z is in exactly one of the equivalence classees

$$[0], [1], [2], \ldots, [n-1].$$

(e). The set of equivalence classes may be identified with the set of rational numbers.

Note that every fraction a/b is equivalent to a fraction in lowest terms.

8. Week 8 – week of [2025-10-20]

8.1. Properties of equivalence classes

Definition 8.1.1: Let A be a set and let A_i be a collection of subsets of A for i in some index set I. The A_i form a partition of A if every element of A belongs to one and only one of the sets A_i.

Put another way,

$$A = \cup_{i\in I} A_i \text{ and } \forall i,j \in I, i \neq j \Rightarrow A_i \cap A_j = \emptyset.$$

Given a set A and an equivalence relation $\sim$ recall that the equivalence class of an element $a \in A$ is the set

$$[a] = \{x \in A \mid x \sim a\}$$

Proposition 8.1.2: Let A be a set with an equivalence relation $\sim$. Then the equivalence classes form a partition of A.

More precisely, the following hold:

(a). for each $a \in A$, $a \in [a]$.

(b). two equivalence classes are either disjoint or equal.

Remark 8.1.3: b. is equivalent to

$$\forall a, b \in A, [a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$$

and also equivalent to $\forall a, b \in A, [a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$.

Proof:

(a). Let $a \in A$. Since $\sim$ is reflexive, we know that $a \sim a$. But implies by definition that $a \in [a]$ as required.

(b). Let $a, b \in A$ and suppose that $[a] \cap [b] \neq \emptyset$. We must prove that $[a] = [b]$.

Fix $x \in [a] \cap [b]$. Then by definition $a \sim x$ and $b \sim x$. Since $\sim$ is symmetric, find that

$$a \sim x \text{ and } x \sim b \text{ so that by transitivity } a \sim b.$$

We now show that $[a] = [b]$. For this, we first prove that $[a] = [b]$. Let $c \in A$. Then

$$c \in [a] \Leftrightarrow a \sim c$$

and since $\sim$ is transitive and since $b \sim a$, we deduce $b \sim c$ so that $c \in [b]$.

THis proves $[a] \subseteq [b]$. A symmetric argument (reverse the roles of a and of b) shows that $[b] \subseteq [a]$ and the proof is complete.

■

The Proposition says that an equivalence relation gives a way to classify the elements of the set. We put every element in A in a single equivalence class, just as we would sort a jumble of objects into piles by throwing every object in one of the piles.

The converse of the Proposition is also true:

Proposition 8.1.4: Let A be a set and let A_i for $i \in I$ be a partition of A. I.e.

$$A = \cup_{i\in I} A_i \text{ and } \forall i, j \in I, i \neq j \Rightarrow A_i \cap A_j = \emptyset.$$

Define a relation of A as follows: for $a, a' \in A$ then $a \sim a'$ if and only if there exists some $i \in I$ such that $a \in A_i$ and $a' \in A_i$.

Then $\sim$ is an equivalence relation.

Proof: As the A_i give a partition, every element in A is in one of the A_i. Therefore, the element is related to itself; i.e. $\sim$ is reflexive.

As being in the same subset is a relation that is symmetric and transitive, this shows that $\sim$ is an equivalence relation. ■

Example 8.1.5: For an integer n, we saw previously the relation $\equiv (\mathrm{mod}\, n)$ on $\mathbb{Z}$. Recall for $a, b \in \mathbb{Z}$ that $a \equiv b (\mathrm{mod}\, n)$ means that $a - b = nk$ for some $k \in \mathbb{Z}$.

We saw that ther are n equivalence classes, namely $[0], [1], \ldots, [n-1]$.

Proposition 8.1.2 tells us that the classes for a partition. In particular, if $0 \leq i, j < n$ and $i \neq j$ then $[i] \cap [j] = \emptyset$.

We usually write $[i]_n$ to indicate the equivalence class of $i \in \mathbb{Z}$ for the relation of "congruence modulo n."

The set of all equivalence classes for this relation is denoted $\mathbb{Z}_n$.

The set of equivalence classes is a new set a life of its own. For example, as we have seen in the set of rational numbers $\mathbb{Q}$ is the set of equivalence classes of an equivalence relation defined on the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, otherwise known as the set of fractions.

Working with equivalence classes is often important. It is also tricky if the only way we have of getting hold of an equivalence class is by taking a representative of that equivalence class. For example, let x, y be rational numbers $x, y \in \mathbb{Q}$. We want to define their sum and product using what we already know from addition and product of integers.

This is normally done as follows: as x, y are rational, we can find integers $a, b, c, d \in \mathbb{Z}, b \neq 0, d \neq 0$ such that x can be represented by a/b and y can be represented by c/d. Then we say that $x + y$ is the rational number represented by $(ad + bc)/bd$ and xy is the rational number represented by ac/bd. We need to make sure that this makes sense.

For example, both $1/2$ and $2/4$ represent the same rational number that we will call x. Both $15/25$ and $3/5$ represent the same rational number that we will call y.

Then we want $x + y$ to be represented by both

$$\frac{1\times 25+2\times 15}{2\times 25}=\frac{55}{50} \text{ and } \frac{2\times 5+4\times 3}{4\times 5}=\frac{22}{20}$$

which is OK as both fractions represent the same rational number.

Similarly, we want xy to be represented by both

$$\left(\frac{1}{2}\right)\times\left(\frac{2}{25}\right)=\frac{1\times 15}{2\times 25}=\frac{15}{50}, \text{and } \left(\frac{2}{4}\right)\times\left(\frac{3}{5}\right)=\frac{2\times 3}{4\times 5}=\frac{6}{20}.$$

which is OK since

$$\frac{15}{50}=\frac{6}{20} \text{ as } 15\times 20=2^2\times 3\times 5=50\times 6.$$

In general, if we want the sums and products of rational numbers to be well defined in terms of the operations with the corresponding fractions, we need the following result:

Proposition 8.1.6: Let $a_1,a_2,c_1,c_2\in\mathbb{Z}$ and $b_1,b_2,d_1,d_2\in\mathbb{Z}\setminus\{0\}$ be such that $\frac{a_1}{b_1}$ and $\frac{a_2}{b_2}$ are equivalent fractions – i.e. $a_1b_2=a_2b_1$ – and such that $\frac{c_1}{d_1}$ and $\frac{c_2}{d_2}$ are equivalent fractions – i.e. $c_1d_2=c_2d_1$. Then

$$\frac{a_1d_1+c_1b_1}{b_1d_1} \text{ and } \frac{a_2d_2+c_2b_2}{b_2d_2}$$

are equivalent fractions, and

$$\frac{a_1c_1}{b_1d_1} \text{ and } \frac{a_2c_2}{b_2d_2}$$

are equivalent fractions.

Proof: We look at addition first. We start with the two equations

$$a_1b_2=a_2b_1 \text{ and } c_1d_2=c_2d_1.$$

We multiply the first equation by d_1d_2 and the second one by b_1b_2 to obtain $a_1b_2d_1d_2=a_2b_1d_1d_2$ and $c_1d_2b_1b_2=c_2d_1b_1b_2$ Adding the left hand sides and right hand sides of the two equations and using the distributive property, we obtain

$$b_2d_2(a_1d_1+c_1b_1)=a_1b_2d_1d_2+c_1d_2b_1b_2=a_2b_1d_1d_2+c_2d_1b_1b_2=b_1d_1(a_2d_2+c_2b_2)$$

which says that the two fractions

$$\frac{a_1d_1+c_1b_1}{b_1d_1} \text{ and } \frac{a_2d_2+c_2b_2}{b_2d_2}$$

are equivalent. Thus addition of rational numbers is well defined.

Similarly, start again from

$$a_1b_2=a_2b_1 \text{ and } c_1d_2=c_2d_1$$

and multiplying the left and right hand sides of these equations, we obtain

$$a_1 b_2 c_1 d_2 = a_2 b_1 c_2 d_1.$$

This shows that the fractions

$$\frac{a_1 c_1}{b_1 d_1} \text{ and } \frac{a_2 c_2}{b_2 d_2}$$

are equivalent. Thus multiplication of rational numbers is well defined.

■

Example 8.1.7: We define addition on $\mathbb{Z}_n$ as follows

$$[a]_n + [b]_n = [a+b]_n \text{ for } a, b \in \mathbb{Z}.$$

We need to check that this rule makes sense: An equivalence class can be represented by many different integers.

We need to verify that the elements we pick to represent the equivalence classes do not change the definition of the operation. Let us assume that $[a_1]_n = [a_2]_n$ and $[b_1]_n = [b_2]_n$.

Recall that two equivalence classes are the same if the representative elements are related.

From our definition of the equivalence relation

$$\exists k \in \mathbb{Z}, a_1 - a_2 = nk, \exists l \in \mathbb{Z}, b_1 - b_2 = nl$$

Adding these two equations we obtain

$$(a_1 + b_1) - (a_2 + b_2) = n(k+l).$$

As $k+l$ is the sum of two integers, it is again an integer. Then, from the definition of the equivalence relation, this tells us that $a_1 + b_1 \equiv a_2 + b_2 (\mathrm{mod}\, n)$. or equivalently $[a_1 + b_1]_n = [a_2 + b_2]_n$. Therefore, the definition $[a]_n + [b]_n = [a+b]_n$ defines the sum of cosets in an unambiguous way, it does not matter if we change the integer so long as we stay inside each of the equivalence classes, we still get the same equivalence class for the sum.

We now define a product on $\mathbb{Z}_n$ as follows

$$[a]_n [b]_n = [ab]_n \text{ for } a, b \in \mathbb{Z}.$$

We check that this is well defined. Let us assume that

$$[a_1]_n = [a_2]_n \text{ and } [b_1]_n = [b_2]_n \text{ for } a_i, b_i \in \mathbb{Z}.$$

Then,

$$\exists k \in \mathbb{Z}, a_1 - a_2 = nk \text{ and } \exists l \in \mathbb{Z}, b_1 - b_2 = nl.$$

We can rewrite these equations as

$$\exists k \in \mathbb{Z}, a_1 = a_2 + nk \text{ and } \exists l \in \mathbb{Z}, b_1 = b_2 + nl.$$

Multiplying these two equations we obtain

$$a_1 b_1 = a_2 b_2 + n a_2 l + nk b_1 + n^2 kl = a_2 b_2 + n(a_2 l + b_2 k + nkl).$$

As a_1, b_1, k, l, n are integers,$a_2 l + b_2 k + nkl$ is also an integer. Then, from the definition of the equivalence relation, this tells us that

$$a_1 b_1 \equiv a_2 b_2 (\mathrm{mod}\, n)$$

or equivalently $[a_1 b_1]_n = [a_2 b_2]_n$. Therefore, the rule $[a]_n [b]_n = [ab]_n$ defines the product of cosets in an unambiguous way.

Example 8.1.8: As we have an addition and product in $\mathbb{Z}_n$, we can consider solutions to equations.

(a). Let us solve the equation $[2]_8 + [x] = [6]_8$ for the unknown $[x]$. We can add $[-2]_8$ to both sides. Using the definition of addition of cosets we find that

$$[x]_8 = [0 + x]_8 = [-2 + 2 + x]_8 = [-2]_8 + [2]_8 + [x]_8 = [-2]_8 + [6]_8 = [-2 + 6]_8 = [4]_8$$

So, $[x]_8 = [4]_8$. The solution is unique in $\mathbb{Z}_8$ but not in $\mathbb{Z}$. If we are interested in the set of integers x that satisfy the equation, then x is any element in the set

$$\{4 + 8k \mid k \in \mathbb{Z}\}.$$

(b). Let us solve the equation $[5]_{10}[x]_{10} = [0]_{10}$. We do not have a way to divide in $\mathbb{Z}_{10}$, so the best strategy in this case is to translate this equation into an equation in $\mathbb{Z}$ which can be simplified:

$$\exists k \in \mathbb{Z} \text{ such that } 5x = 10k \Rightarrow \exists k \in \mathbb{Z} \text{ such that } x = 2k.$$

So, x can be any even integer and $[x]_{10}$ can take any of the values

$$[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}.$$

Example 8.1.9: Let us fix a modulus $n \in \mathbb{N}$ and work in $\mathbb{Z}_n$. We pointed out already that in general we can't divide in $\mathbb{Z}_n$. But sometimes we can!

Suppose that $a \in \mathbb{Z}$ and that there are integers $u, v \in \mathbb{Z}$ such that

$$au + nv = 1.$$

Since $au - 1 = nv$ we see that $au \equiv 1 (\mathrm{mod}\, n)$. In other words,

$$[a]_n \cdot [u]_n = [au]_n = [1]_n.$$

Thus $[u]_n$ is a *multiplicative inverse* for the element $[a]_n \in \mathbb{Z}_n$.

For example, let $n = 25$ and let $a = 19$. Then

$$19 \cdot 4 + 25 \cdot (-3) = 76 - 75 = 1.$$

Thus

$$[19]_{25} \cdot [4]_{25} = [1]_{25}.$$

We can now solve the equation

$$[19]_{25} \cdot y + [1]_{25} = [6]_{25}.$$

Indeed, we find that

$$[19]_{25} \cdot y = [6]_{25} + [-1]_{25} = [5]_{25};$$

since $[4]_{25} = [19]_{25}^{-1}$ we see that

$$y = [4]_{25} \cdot [5]_{25} = [20]_{25}.$$

On the other hand, sometimes elements in $\mathbb{Z}_n$ really have no multiplicative inverse. For example, $[5]_{25} \in \mathbb{Z}_{25}$ has no multiplicative inverse. We can confirm this statement by checking that the equation

$$(*) \quad [5]_{25} \cdot y = 1$$

has no solution y in $\mathbb{Z}_{25}$.

To see that $(*)$ has no solution, suppose $[u]_{25}$ were a multiplicative inverse for some $u \in \mathbb{Z}$. Then $[1]_{25} = [5]_{25} \cdot [u]_{25} = [5u]_{25}$. This means there is $k \in \mathbb{Z}$ for which $1 - 5u = 25k$.

This last equation implies that

$$1 \equiv 0 (\mathrm{mod}\, 5)$$

– i.e. that $[0]_5 = [1]_5$ – which is nonsense since $\{[0], [1], \ldots, [4]\}$ are distinct. This contradiction confirms that $(*)$ has no solutions.

The arithmetic properties of addition and product in $\mathbb{Z}_n$ is called modular arithmetic. Modular arithmetic is widely used in cryptography and error correction. Instead of checking that two numbers are the same, it is easier to check that their cosets are the same in $\mathbb{Z}_n$ for some n; the advantage is that the set $\mathbb{Z}_n$ is *finite*.1

9. Week 09 [2025-10-27]

9.1. Limits of sequences

Remember that a sequence of numbers (integers, rational, real, complex...) is a collection of numbers indexed by $\mathbb{N}$:

$$(a_n)_{n\in\mathbb{N}}.$$

We considered sequences when we were talking about recursion, we were then using an inductive process to define a sequence.

Sequences play an important role in the study of Calculus. In fact, we are going to use a certain sequences – called Cauchy sequences – to give a definition of real numbers.

A more formal definition of sequence would be

Definition 9.1.1: A sequence of rational numbers is a function $a : \mathbb{N} \to \mathbb{Q}$.

A sequence of real, resp. complex, numbers is a function $a : \mathbb{N} \to \mathbb{R}$, resp. $a : \mathbb{N} \to \mathbb{C}$.

When considering sequences, we typically write a_n for the value of a at n rather than $a(n)$. And we often just write a_n for a sequence (a_n), where it is to be understood that the index variable n ranges over the set $\mathbb{N}$.

You are familiar from Calculus with the concept of convergence of sequences, although you may not have defined it formally. The intuitive idea of a sequence with limit L is that the values of a_n come arbitrarily close to L. Being "arbitrarily close" means that the distance from a_n to L can be made smaller than any fixed positive number by requiring n to be large.

As distance in the number line is measured by the absolute value, we can formalize this as follows:

Definition 9.1.2: A sequence a_n of rational (resp. real, complex) numbers is said to converge to $L \in \mathbb{Q}$ (resp. $L \in \mathbb{R}$ or $L \in \mathbb{C}$) provided that the following holds:

for every $\varepsilon > 0$, there is $m \in \mathbb{N}$ such that

More succinctly:

$$\forall \varepsilon > 0, \exists m \in \mathbb{N}, \forall n \in \mathbb{N}, n \Rightarrow m \Rightarrow |a_n - L| < \varepsilon.$$

When the sequence (a_n) converges to a value L, we say that the limit of the sequence is L and write

$$\lim_{n\to\infty} a_n = L.$$

Remark 9.1.3: Here is a point-of-view on the definition: imagine you are trying to persuade an official that your sequence converges to L. When you interact with them, the official decides on some error tolerance – this is the ε in the definition.

The official then requires you to show that the sequence is "eventually within ε of the limit." The way to do this is to argue that for a suitable value of m, all the terms a_m, a_{m+1} ... of the sequence are within the error tolerance of L. More precisely, you must ensure that

$$|a_m - L| < \varepsilon, \quad |a_{m+1} - L| < \varepsilon, \quad \text{etc}$$

Since you have to be ready for any official, you need to be able to handle an arbitrary ε.

Example 9.1.4:

A main tool that we use is the following: for any real number r, there is a natural number m with $m \geq r$. This is known as the Archimedean property of the real numbers.

Another important tool is the triangle inequality which says that for real numbers a, b we have

$$|a + b| \leq |a| + |b|.$$

(a). The sequence $a_n = (n+3)/(n+2) \in \mathbb{Q}$ has limit 1: compute the difference between a_n and 1.

$$|a_n - 1| = \left|\frac{n+3}{n+2} - 1\right| = \left|\frac{n+3-(n+2)}{n+2}\right| = \frac{1}{n+2}$$

Let $\varepsilon > 0$ in $\mathbb{Q}$. Using the archimedean property, we may choose m so that $m \geq \dfrac{1}{\varepsilon} - 2$. Then,

$$\forall n \geq m, |a_n - 1| = \frac{1}{n+2} \leq \frac{1}{m+2} \leq \varepsilon.$$

This confirms that

$$\lim_{n\to\infty} \frac{n+3}{n+2} = 1.$$

(b). The sequence

$$a_0 = 1, a_1 = -1, a_2 = 1, a_3 = -1, \ldots, a_n = (-1)^n$$

does not convergence. Evidently, the sequence alternates between 1 and -1 (the even terms are 1 and the odd terms are -1.)

If the sequence had a limit L, the even terms of the sequence can be made arbitrarily close to L and the same for the odd numbers.

One then uses the so-called *triangular inequality* which says that the distance between the two points is at most the sum of the distances of the two to a third point.

This would force 1 to be arbitrarily close to -1.

Let's write this down more carefully:

Assume that (a_n) had a limit L. Then, for $\varepsilon = 1/2$, there exists some $m \in \mathbb{N}$ such that for all $n \geq m$, $|a_n - L| < 1/2$.

Choose $n \geq m$, with n even. Then

$$\begin{aligned} 2 = |\ 1 - (-1)| = |a_n - a_{n+1}| &= |(a_n - L) + (L - a_{n+1})| \\ &\leq |a_n - L| + |L - a_{n+1}| \leq 1/2 + 1/2 = 1 \end{aligned}$$

which is a contradiction.

(c). Consider the sequence of rational numbers

$$a_0 = 0, a_1 = 0.3, a_2 = 0.33, a_3 = 0.333, a_4 = 0.3333, a_5 = 0.3333, a_6 = 0.333333, \ldots$$

The general term a_n has zero for the integral part, the first n digits after the decimal point are threes and the remaining digits are zero.

The limit of this sequence is $1/3 \in \mathbb{Q}$. To see this, notice that for each n, $1/3 - a_n$ has zero integral part and the first n digits equal to zero.

Therefore,

$$|a_n - 1/3| < \frac{1}{10^n}.$$

Then

$$|a_n - 1/3| < \varepsilon \quad \text{if} \quad \frac{1}{10^n} < \varepsilon$$

.

Thus we must choose m to be a natural number with the property that

$$m \geq \frac{-\ln \varepsilon}{\ln 10}.$$

(d). You have probably been told that π is an irrational number. Let's use π to construct a sequence of rational numbers.

The sequence of rational numbers

$$a_0 = 3, a_1 = 3.1, a_2 = 3.14, a_3 = 3.141, a_4 = 3.1415, a_5 = 3.14159, a_6 = 3.141592, \ldots$$

and in general a_n has the first n digits of the decimal expansion of π and zeros afterwards. We claim: the limit of this sequence does not exist in $\mathbb{Q}$.

Indeed, assume the limit $L \in \mathbb{Q}$ did exist. For each j, choose

$$\varepsilon = \frac{1}{10^{j+1}}.$$

Then there exists some m such that for all $n \geq m$ we have

$$|a_n - L| \leq \frac{1}{10^{j+1}}.$$

It follows that the first j digits of L agree with the first j digits of π.

This would be true for every j. Therefore, $L = \pi \notin \mathbb{Q}$.

In fact, the limit of the sequence is the real number π.

9.2. First results about limits

Proposition 9.2.1:

Consider a sequence a_n of rational or real numbers.

(a). The limit if it exists is unique: If $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a_n = L'$, then $L = L'$.

(b). Any constant sequence $a_n = a, \forall n$ converges to $L = a$.

(c). Multiplication with scalars is compatible with limits: If $\lim_{n\to\infty} a_n = L$ and $c \in \mathbb{Q}$ or $c \in \mathbb{R}$, then $\lim_{n\to\infty}(ca_n) = cL$.

(d). Addition of sequences is compatible with limits: If $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$, then $\lim_{n\to\infty}(a_n + a'_n) = L + L'$.

(e). Product of sequences is compatible with limits: If $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$, then $\lim_{n\to\infty}(a_n a'_n) = LL'$.

Proof:

(a). Assume that $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a_n = L'$. If $L \neq L'$, then $|L - L'| = b > 0$. Choose $0 < \varepsilon < b/2$. There exist $m, m' \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \varepsilon$, and if $n \geq m'$, then $|a_n - L'| < \varepsilon$. Take $n \geq \max(m, m')$. Then using the triangle inequality, we find that

$$b = |L - L'| = |(L - a_n) + (a_n - L')| \leq |L - a_n| + |a_n - L'| \leq \varepsilon + \varepsilon = 2\varepsilon < b$$

which is a contradiction.

(b). Any constant sequence with $a_n = a$ for each n satisfies $|a_n - L| = |a - a| = 0 < \varepsilon$ for any positive ε. Therefore, it converges to $L = a$ by definition of limit.

(c). Assume that $\lim_{n\to\infty} a_n = L$ and let c be a rational number. If $c = 0$, the required result is immediate. Thus we may suppose $c \neq 0$. To rpove that $\lim_{n\to\infty} ca_n = cL$, choose $\varepsilon > 0$. From the convergence of the sequence, there exist $m \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \frac{\varepsilon}{|c|}$. Then also

$$|ca_n - cL| = |c\|a_n - L| \leq |c|\ \frac{\varepsilon}{|}c|) = \varepsilon$$

showing that $\lim_{n\to\infty}(ca_n) = cL$.

(d). Assume that $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$. Choose $\varepsilon > 0$. Thus $\frac{\varepsilon}{2} > 0$. From the convergence of the sequences, there exist $m, m' \in \mathbb{N}$ such that if $n \geq m$, then $|a_n - L| < \frac{\varepsilon}{2}$, and if $n \geq m'$, then $|a'_n - L'| < \frac{\varepsilon}{2}$. Take $n \geq \max(m, m')$, then using the triangle inequality we find that

$$|(a_n + a'_n) - (L + L')| = |(a_n - L) + (a'_n - L')| \leq |a_n - L| + |a'_n - L'| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

showing that $\lim_{n\to\infty}(a_n + a'_n) = L + L'$.

(e). Assume that $\lim_{n\to\infty} a_n = L$, $\lim_{n\to\infty} a'_n = L'$. Choose $\varepsilon > 0$.

From the convergence of the sequences, there exist $m, m' \in \mathbb{N}$ such that

$$n \geq m \Rightarrow |a_n - L| < \frac{\varepsilon}{2(|L'|+1)}$$

and

$$n \geq m' \Rightarrow |a'_n - L'| < \min\left(\frac{\varepsilon}{2(|L|+1)}\right), 1).$$

Then also

$$|a'_n| = |(a'_n - L') + L| \leq |a'_n - L'| + |L'| < 1 + |L'|.$$

Take $n \geq \max(m, m')$. Using the triangle inequality, we see tha

$$\begin{aligned} |(a_n a'_n) - (LL')| &= |(a_n - L)a'_n + L(a'_n - L')| \\ &\leq |a_n - L\|a'_n| + |L\|a'_n - L'| \\ &\leq \frac{\varepsilon}{2(|L'|+1)}(|L'|+1) + \frac{\varepsilon}{2(|L|+1)}|L| < \varepsilon; \end{aligned}$$

this shows that $\lim_{n\to\infty}(a_n.a_n') = LL'$.

■

9.3. Cauchy sequences

We now want to introduce Cauchy sequences.

For our discussion, the importance of Cauchy sequences lies in the following observation: If a_n is a Cauchy sequence of rational numbers, the sequence a_n behaves like a convergent sequence in the sense that its terms are very close to each other, but it might fail to converge to an element of $\mathbb{Q}$.

Definition 9.3.1: A sequence (a_n) of real or rational numbers is said to be a Cauchy sequence if for any $\varepsilon > 0$, there exists some $m \in \mathbb{N}$ such that for all $n_1, n_2 \geq m$,

$$|a_{n_1} - a_{n_2}| < \varepsilon.$$

Note that the statement of the condition that a sequence is Cauchy does not depend on knowledge of a limit for the sequence.

Example 9.3.2:

(a). Let $a_n = 1/n$ for $n \in \mathbb{N}_{>0}$. Then a_n is a Cauchy sequence.

Indeed, let $\varepsilon > 0$. We must find m such that $n_1, n_2 \geq m$ implies that $|a_{n_1} - a_{n_2}| < \varepsilon$.

We take $m \geq 2/\varepsilon$. Notice that for any $n \geq m$ we have $|a_n| = |1/n| < \varepsilon/2$.

Now we see that if $n_1, n_2 \geq m$, then

$$|a_n - a_m| = \left|\frac{1}{n} - \frac{1}{m}\right| \leq \left|\frac{1}{n}\right| + \left|\frac{1}{m}\right| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

(b). The sequence of rational numbers

$$a_0 = 3, a_1 = 3.1, a_2 = 3.14, a_3 = 3.141, a_4 = 3.1415, a_5 = 3.14159, a_6 = 3.141592, \ldots$$

where in general a_n has the first n digits of the decimal expansion of π and zeros afterwards.

This is a Cauchy sequence: if we want to make

$$\left|a_{n_1} - a_{n_2}\right| < \frac{1}{10^m},$$

it suffices to take $n_1, n_2 \geq m$ because then the first m digits of a_{n_1}, a_{n_2} will be the same.

Proposition 9.3.3: Let a_n be a sequence of rational or real numbers.

(a). If a_n converges, then a_n is a Cauchy sequence.

(b). If a_n and a'_n are Cauchy sequences, then $a_n + a'_n$ is a Cauchy sequence.

(c). If a_n is a Cauchy sequence, then its terms are bounded: there exists $B > 0$ such that $|a_n| < B$ for every $n \in \mathbb{N}$.

(d). If a_n and a'_n are Cauchy sequences, then $a_n \cdot a'_n$ is a Cauchy sequence.

Proof:

(a). Assume that $\lim_{n\to\infty} a_n = L$. To prove that a_n is Cauchy, let $\varepsilon > 0$. We must find m such that $n_1, n_2 \geq m \Rightarrow |a_n - a_m| < \varepsilon$.

We use the m obtained from the definition of convergence for $\varepsilon/2$; thus we know that $n \geq m \Rightarrow |a_n - L| < \varepsilon/2$.

Now if $n_1, n_2 \geq m$ then

$$\begin{aligned} |a_n - a_m| &= |a_n - L + L - a_m| \\ &\leq |a_n - L| + |a_m - L| \\ &\leq \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon; \end{aligned}$$

this proves that a_n is Cauchy.

(b). Assume that a_n and a'_n are Cauchy. To show that $a_n + a'_n$ is Cauchy, let $\varepsilon > 0$.

Since a_n is Cauchy, there is $m \in \mathbb{N}$ such that $n_1, n_2 \geq m$ implies that $\left|a_{n_1} - a_{n_2}\right| < \varepsilon/2$. Since a'_n is Cauchy, there is $m' \in \mathbb{N}$ such that $n_1, n_2 \geq m'$ implies that $\left|a'_{n_1} - a'_{n_2}\right| < \varepsilon/2$.

Let $M = \max(m, m')$. If $n_1, n_2 \geq M$ then we find that

$$\begin{aligned} \left|\left(a_{n_1} + a'_{n_1}\right) - \left(a_{n_2} + a'_{n_2}\right)\right| &= \left|a_{n_1} - a_{n_2} + a'_{n_1} - a'_{n_2}\right| \\ &\leq \left|a_{n_1} - a_{n_2}\right| + \left|a'_{n_1} - a'_{n_2}\right| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Thus $a_n + a'_n$ is indeed Cauchy.

(c). Assume that a_n is Cauchy. Then there is some $m \in \mathbb{N}$ with the property that $n_1, n_2 \geq m \Rightarrow \left|a_{n_1} - a_{n_2}\right| < 1$.

In particular, for $n \geq m$ we see that

$$|a_n| = |a_n - a_m + a_m| \leq |a_n - a_m| + |a_m| \leq 1 + |a_m|.$$

Now set

$$A = \max(|a_0|, |a_1|, ...|a_{m-1}|, 1 + |a_m|).$$

Then for and n we see that $|a_n| \leq A$ as required.

(d). Suppose that a_n and a'_n are Cauchy seqeuences.

Use c. to find a bound A such that $|a_n| \leq A$ and $|a'_n| \leq A$ for all $n \in \mathbb{N}$.

We prove that $a_n \cdot a'_n$ is Cauchy. Let $\varepsilon > 0$.

Since a_n and a'_n Cauchy, we can choose m so that

$$n_1, n_2 \geq m \Rightarrow \left|a_{n_1} - a_{n_2}\right| < \frac{\varepsilon}{2A} \quad \text{and} \quad \left|a'_{n_1} - a'_{n_2}\right| < \frac{\varepsilon}{2A}.$$

Now, for $n_1, n_2 \geq m$ we see that

$$\begin{aligned}
\left|a_{n_1} \cdot a'_{n_1} - a_{n_2} \cdot a'_{n_2}\right| &= \left|\left(a_{n_1} - a_{n_2}\right)a'_{n_1} + a_{n_2}\left(a'_{n_1} - a'_{n_2}\right)\right| \\
&\leq \left|a_{n_1} - a_{n_2}\right|\left|a'_{n_1}\right| + \left|a_{n_2}\right|\left|a'_{n_1} - a'_{n_2}\right| \\
&\leq A\left|a_{n_1} - a_{n_2}\right| + A\left|a'_{n_1} - a'_{n_2}\right| \\
&< A \cdot \frac{\varepsilon}{2A} + A \cdot \frac{\varepsilon}{2A} = \varepsilon.
\end{aligned}$$

This completes the proof that $a_n a'_n$ is Cauchy.

■

9.4. Construction of the real numbers

The natural numbers $\mathbb{N}$ have an inductive (or recursive) description: there is a natural number 0, and for each natural number n, there is a successor natural number $n+1$. This amounts to a *construction* of natural numbers.

In homework, you saw how to define the integers $\mathbb{Z}$ give $\mathbb{N}$. Namely, you consider the set S of pairs (a,b) where $a,b \in \mathbb{N}_{>0}$ with the equivalence relation $(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$. Then $\mathbb{Z}$ is the set of equivalence classes in S.

Similarly, we saw how to define rational numbers $\mathbb{Q}$ given $\mathbb{Z}$. Namely, you consider the set D of pairs (a,b) where $a,b \in \mathbb{Z}$ and $b \neq 0$, with the equivalence relation $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Then $\mathbb{Q}$ is the set of equivalence classes in D.

We now want to give an analogous definition of real numbers $\mathbb{Q}$.

Let A be the set of all Cauchy sequences a_n where $a_n \in \mathbb{Q}$ for each $n \in \mathbb{N}$.

We define a relation $\sim$ on A by the rule:

$$a_n \sim a'_n \text{ if and only if } \lim_{n\to\infty} a_n - a'_n = 0.$$

Proposition 9.4.1: The relation $\sim$ on the set A of Cauchy sequences of rational numbers is an equivalence relation.

Proof:

- reflexive: for $a_n \in A$, we know that $a_n \sim a_n$ since $\lim_{n\to\infty} a_n - a_n = \lim_{n\to\infty} 0 = 0$.
- symmetric: Let $a_n, b_n \in A$ and assume that $a_n \sim b_n$. Then

$$\begin{aligned}\lim_{n\to\infty} a_n - b_n = 0 &\Rightarrow \lim_{n\to\infty} (-1)(b_n - a_n) = 0\\ &\Rightarrow (-1)\lim_{n\to\infty} b_n - a_n = 0\\ &\Rightarrow \lim_{n\to\infty} b_n - a_n = 0.\end{aligned}$$

  Thus $b_n \sim a_n$.
- transitive: Let $a_n, b_n, c_n \in A$ and assume that $a_n \sim b_n$ and $b_n \sim c_n$. Our hypothesis means that $\lim_{n\to\infty} a_n - b_n = 0$ and $\lim_{n\to\infty} b - n - c_n = 0$.

  Now,

$$\begin{aligned}\lim_{n\to\infty} a_n - c_n &= \lim_{n\to\infty} a_n - b_n + b_n - c_n\\ &= \lim_{n\to\infty} (a_n - b_n) + \lim_{n\to\infty} (b_n - c_n)\\ &= 0 + 0 = 0.\end{aligned}$$

  This shows that $a_n \sim c_n$ and confirms that $\sim$ is transitive.

■

Definition 9.4.2: The real numbers $\mathbb{R}$ are defined to be set of equivalence classes of A for the relation $\sim$.

Example 9.4.3: Recall that we can represent a real number $0 \leq x \leq 1$ by its decimal expansion:

$$x = 0.d_1d_2d_3... \text{ with } d_i \in \{0, 1, ..., 9\}.$$

What this means is that

$$x = \sum_{i=1}^{\infty} \frac{d_i}{10^i}.$$

Consider the *partial sums* a_n of this series:

$$a_n = \sum_{i=1}^{n} \frac{d_i}{10^i} \text{ for } n \in \mathbb{N}_{>0}.$$

Thus $x = \lim_{n\to\infty} a_n$ so that x is the limit of the Cauchy sequence a_n.

From the standpoint of our definition of $\mathbb{R}$, we view the equivalence class $[a_n]$ as the same thing as the number x.

Example 9.4.4: Note that $\mathbb{Q} \subset \mathbb{R}$. Here are two ways of thinking about this containment:

- Any rational number $x \in \mathbb{Q}$ has a decimal expansion $x = \sum_{i=1}^{\infty} \frac{d_i}{10^i}$. In fact, the sequence of decimal digits d_i either terminates ($\exists m$ such that $i \geq m \Rightarrow d_i = 0$) or repeats. As in Example 9.4.3, we then see that x is the limit of the sequence of partial sums $a_n = \sum_{i=1}^{n} \frac{d_i}{10^i}$.
- For $x \in \mathbb{Q}$ the constant sequence c_n with $c_n = x$ for all $n \in \mathbb{N}$ is a Cauchy sequence with $\lim_{n\to\infty} c_n = x$.

In fact, $[a_n] = [c_n]$ so that both Cauchy sequences a_n and c_n represent $x \in \mathbb{Q} \subset \mathbb{R}$.

The next task is to show that operations of arithmetic are defined on the set of real numbers $\mathbb{R}$.

Suppose that $a_n, a'_n, b_n, b'_n \in A$ and assume that $a_n \sim b_n$ and $a'_n \sim b'_n$.

Proposition 9.4.5:
(a). $a_n + a'_n \sim b_n + b'_n$.
(b). $a_n \cdot a'_n \sim b_n \cdot b'_n$.

Proof: By hypothesis, we know that

$$(*) \lim_{n\to\infty} a_n - b_n = 0 \text{ and } \lim_{n\to\infty} a'_n - b'_n = 0.$$

(a). We must argue that $\lim_{n\to\infty} ((a_n + a'_n) - (b_n + b'_n)) = 0$. Using $(*)$ and Proposition 9.2.1 we find that

$$\lim_{n\to\infty} ((a_n + a'_n) - (b_n + b'_n)) = \lim_{n\to\infty} (a_n - b_n) + \lim_{n\to\infty} (a'_n - b'_n) = 0 + 0 = 0.$$

This proves that $a_n + a'_n \sim b_n + b'_n$ as required.

(b). We must argue that $\lim_{n\to\infty} (a_n \cdot a'_n - b_n \cdot b'_n) = 0$. To prove that this limit holds, let $\varepsilon \in \mathbb{Q}_{>0}$.

Since a'_n and b_n are Cauchy, we may use Proposition 9.3.3(c) to find a number $B \in \mathbb{Q}_{>0}$ such that $|a'_n| < B$ and $|b_n| < B$ for all $n \in \mathbb{N}$.

In view of $(*)$ we may find $m \in \mathbb{N}$ such that for any $n \geq m$ we have

$$|a_n - b_n| < \frac{\varepsilon}{2B} \text{ and } |a'_n - b'_n| < \frac{\varepsilon}{2B}.$$

Now, we see for $n \geq m$ that

$$\begin{aligned} |a_n \cdot a'_n - b_n \cdot b'_n| &= |(a_n - b_n) \cdot a'_n + b_n \cdot (a'_n - b'_n)| \\ &\leq |a_n - b_n| \cdot |a'_n| + |b_n| \cdot |a'_n - b'_n| \\ &\leq \frac{\varepsilon}{2B} \cdot B + B \cdot \frac{\varepsilon}{2B} = \varepsilon. \end{aligned}$$

This prove completes the proof of b.

■

For $[a_n], [a'_n]$ in $\mathbb{R} :=$equivalence classes of Cauchy sequences of rational numbers, we proved in Proposition 9.3.3 that $a_n + a'_n$ is a Cauchy sequence of rational numbers. We define

$$[a_n] + [a'_n] = [a_n + a'_n]$$

and the preceding proposition shows that this operation is well-defined.

Similarly, we proved in Proposition 9.3.3 that $a_n \cdot a'_n$ is a Cauchy sequence of rational numbers. We define

$$[a_n] \cdot [a'_n] = [a_n \cdot a_{n'}]$$

and the preceding proposition shows that this operation is well-defined.

Thus we have well-defined operations of addition and multiplication on $\mathbb{R}$.

We record the following, to give some sense of what should be checked.

Proposition 9.4.6:

(a). The operations of $+$ and $\cdot$ are associative and commutative.
(b). Multiplication distributes over addition.
(c). The element $1 \in \mathbb{R}$ which is the class of the constant sequence $1 \in \mathbb{Q}$ is a multiplicative identity for $\mathbb{R}$.
(d). The element $0 \in \mathbb{R}$ which is the class of the constant sequence $0 \in \mathbb{Q}$ is an additive identity for $\mathbb{R}$.

Leaving these aside, let's at least prove that a non-zero element of $\mathbb{R}$ has a multiplicative inverse.

We begin with a preliminary result:

Proposition 9.4.7: Let $[a_n] \in \mathbb{R}$ with $[a_n] \neq 0$.

(a). Then $\exists m$ such that $\forall n \geq m$ we have $a_n > 0$ or $\forall n \geq m$ we have $a_n < 0$.
(b). There is $\varepsilon_1 > 0$ and some $m \in \mathbb{N}$ such that $n \geq m \Rightarrow |a_n| > \varepsilon_1$.

Proof: Recall that $[a_n] = 0$ means that

$$\forall \varepsilon > 0, \exists m, n \geq m \Rightarrow |a_n| < \varepsilon.$$

Negating this condition, we see that $[a_n] \neq 0$ means that

$$(\clubsuit) \quad \exists \varepsilon_0 > 0, \forall m \in \mathbb{N}, \exists n_0 \geq m, |a_{n_0}| > \varepsilon_0.$$

(a). Now, assume that the statement of a. fails. This means that $\forall m \in \mathbb{N}$, $\exists k \geq m$ such that $a_k > 0$ and $\exists \ell \geq m$ such that $a_\ell < 0$.

Let $m \in \mathbb{N}$ be arbitrary, and choose n_0 as in ($\clubsuit$). If $a_{n_0} > 0$, we use the failure of the proposition to find some $n_1 \geq m$ for which $a_{n_1} < 0$, while if $a_{n_0} < 0$ we use the failure of the proposition to find some $n_1 \geq m$ for which $a_{n_1} > 0$.

Then

$$|a_{n_0} - a_{n_1}| = |a_{n_0}| + |a_{n_1}| \geq |a_{n_0}| > \varepsilon_0.$$

This condition shows that a_n is not a Cauchy sequence, which contradictions the the hypothesis. This contradiction proves a.

(b). Let $\varepsilon_0 > 0$ as in ($\clubsuit$), and let $\varepsilon_1 = \varepsilon_0/2$. Since a_n is a Cauchy sequence, we can find $m \in \mathbb{N}$ with the property that

$$n_1, n_2 \geq m \Rightarrow \left|a_{n_1} - a_{n_2}\right| < \frac{\varepsilon_0}{2}.$$

In particular, we see that

$$n_1, n_2 \geq m \Rightarrow \left|a_{n_1} - a_{n_2}\right| < \frac{\varepsilon_0}{2}.$$

Applying condition ($\clubsuit$) with m, we find $n_1 \geq m$ such that $|a_{n_1}| > \varepsilon_0$ i.e.

$$a_{n_1} > \varepsilon_0 \text{ or } a_{n_1} < -\varepsilon_0.$$

Now, for any $n_2 \geq m$ we have

$$-\frac{\varepsilon_0}{2} < a_{n_2} - a_{n_1} < \frac{\varepsilon_0}{2} \Rightarrow a_{n_1} - \frac{\varepsilon_0}{2} < a_{n_2} < a_{n_1} + \frac{\varepsilon_0}{2}.$$

Thus if $a_{n_1} > \varepsilon_0$ we see that

$$\frac{\varepsilon_0}{2} = \varepsilon_0 - \frac{\varepsilon_0}{2} < a_{n_1} - \frac{\varepsilon_0}{2} < a_{n_2},$$

while if $a_{n_1} < -\varepsilon_0$ we see that

$$a_{n_2} < a_{n_1} + \frac{\varepsilon_0}{2} < -\varepsilon_0 + \frac{\varepsilon_0}{2} = -\frac{\varepsilon_0}{2}.$$

In either case,

$$\left|a_{n_2}\right| > \frac{\varepsilon_0}{2} = \varepsilon_1$$

and the proof is complete.

■

Proposition 9.4.8: Given a real number $r \neq 0$, there is another real number r_1 with $r \cdot r_1 = 1$.

Proof: Let $r \neq 0$. Then there is a Cauchy sequence a_n of rational numbers with $r = [a_n]$. From Proposition 9.4.7 we can find m such that for all $n \geq m$, a_n is always positive or always negative. In particular, $a_n \neq 0$.

Define a sequence b_n by the rule

$$b_n = \begin{cases} 1 \text{ if } n \leq m \\ 1/a_n \text{ otherwise.} \end{cases}$$

Then for $n \geq m$ we have $a_n b_n = 1$ and this shows that $\lim_{n\to\infty} a_n b_n = 1$ so that $[a_n][b_n] = 1$.

It only remains to show that b_n is a Cauchy sequence.

For this, let $\varepsilon \in \mathbb{Q}_{>0}$, and use Proposition 9.4.7(b) to find $\varepsilon_1 > 0$ and $m_1 \in \mathbb{N}$ such that $n \geq m_1 \Rightarrow |a_n| > \varepsilon_1$.

Now use the condition that a_n is Cauchy applied to the positive number $\varepsilon \cdot \varepsilon_1^2$ to find $m \geq m_1$ such that

$$n_1, n_2 \geq m \Rightarrow |b_{n_1} - b_{n_2}| < \varepsilon \cdot \varepsilon_1^2.$$

Now, suppose that $n_1, n_2 \geq m$. Note that for $i = 1, 2$ that $|a_{n_i}| > \varepsilon_1 \Rightarrow \left|\frac{1}{a_{n_i}}\right| < \frac{1}{\varepsilon_1}$. Now we see that

$$\left|b_{n_1} - b_{n_2}\right| = \left|\frac{1}{a_{n_1}} - \frac{1}{a_{n_2}}\right| = \left|\frac{a_{n_2} - a_{n_1}}{a_{n_1} \cdot a_{n_2}}\right| < \frac{\varepsilon \cdot \varepsilon_1^2}{\varepsilon_1 \cdot \varepsilon_1} = \varepsilon.$$

This shows that b_n is Cauchy and completes the proof. ■

Finally, we would like to describe the order $\leq$ on $\mathbb{R}$.

We do this by first defining the absolute value.

For $x \in \mathbb{R}$, say $x = [a_n]$ for a rational Cauchy sequence a_n, construct the sequence $|a_n|$. This sequence is Cauchy and hence we may consider the class $[|a_n|]$. We define

$$|x| = [|a_n|].$$

We must check: if $a_n \sim a'_n$ then $[|a_n|] = [|a'_n|]$.

We now define a real number x to be non-negative if $|x| = x$.

And for $x, y \in \mathbb{R}$ we say that $x \geq y$ if and only if $x - y$ is non-negative. And we write $x > y$ if $x \geq y$ and $x \neq y$.

Proposition 9.4.9: For $x \in \mathbb{R}$, $x^2 \geq 0$.

Proof: Note for $y \in \mathbb{Q}$ that $y^2 \geq 0$ – i.e. $\left|y^2\right| = y^2$.

Now, write $x = [a_n]$ for a rational Cauchy sequence a_n. Then $x^2 = \left[a_n^2\right]$ and

$$\left|x^2\right| = \left[\left|a_n^2\right|\right] = \left[a_n^2\right] = x^2.$$

This shows that $\left|x^2\right| = x^2$ so that x^2 is non-negative. This means that $x^2 \geq 0$. ■