Lecture 1

Reference: Judson, Chapter 1

One of the main aims of this course is make you familiar with formal mathematical notation and teach you how to write rigorous proofs. The foundation of the modern mathematical language lies in the *set theory*. Thus we start this course with recalling basic notions of sets and maps between sets.

Sets & Quantifiers

Recall that a *set* is denoted by curly brackets $\{\dots\}$. Elements of a set must by **distinct**. The following important sets have special reserved notation.

- $\mathbb{N} = \{1, 2, 3, \dots\}$ is the set of all **positive** integers. Sometimes we call $\mathbb{N}$ the set of *natural* numbers.
- $\mathbb{Z} = \{\dots, -2, -1, 0, -1, 2, \dots\}$ is the set of all integers.
- $\mathbb{Q} = \left\{ \frac{m}{n} \,\middle|\, m \in \mathbb{Z}, n \in \mathbb{N} \right\}$ is the set of rational numbers.
- $\mathbb{R} = (-\infty, +\infty)$ is the set of real numbers.

There are many ways to describe a given set.

Example 1

We can specify a set by listing all its elements,

$$A = \{1, 2, 3\}.$$

Or as a set of elements satisfying certain properties:

$$A = \{a \in \mathbb{Z} \mid 1 \leqslant a \leqslant 3\}.$$

In the plain English the last definition will be read as

set A is the set of all integers a such that $1 \leqslant a$ and $a \leqslant 3$.

We can also give a descriptive definition

$$B = \{\text{odd integers}\}$$

or equivalently write

$$B = \{2n + 1 \mid n \in \mathbb{Z}\}.$$

The latter will be read as

B is the set of numbers of the form $2n + 1$ where n ranges over all the integers

Definition 1: Quantifiers

Throughout this course we will be often using quantifier notations. Please make sure you remember and understand them.

- $\forall$ (upside-down A) means *'for all'* or *'for any'*. For example '$\forall x \in \mathbb{R}$ we have $x^2 \geqslant 0$' means 'for all $x \in \mathbb{R}$ we have $x^2 \geqslant 0$'.
- $\exists$ (mirrored E) means *'there exists'*. For example '$\exists\ C \in \mathbb{R}$ such that $\forall x \in \mathbb{R}$ $x^2 > C$' means 'there exists $C \in \mathbb{R}$ such that for all $x \in \mathbb{R}$ $x^2 > C$'.
- ! means *'unique'*. For example '$\forall y > 0$ $\exists! x > 0$ such that $x^2 = y$' means 'for all $y > 0$ there exists a unique $x > 0$ such that $x^2 = y$'.

Recall also the following notation regarding mutual relation of sets and elements.

- $a \in A$ means that element a belongs to the set A;
- $B \subset A$ (or $B \subseteq A$) means that set B is a subset of the set A, i.e.,

  $$\forall b \in B \text{ we have } b \in A.$$

  Clearly $A \subset A$ and $A = B$ if and only if $A \subset B$ and $B \subset A$;
- $B \subsetneq A$ means that B is a **proper** subset of A, i.e., $B \subset A$ but $B \neq A$.
- $\emptyset$ is the empty set, i.e., the set with no elements in it.

Operations with sets

Now we describe several important operations which allow to produce new sets from given sets.

Definition 2: Union

The **union** of two sets A and B is the set

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

consisting of all elements belonging to either A or B.

Definition 3: Intersection

The **intersection** of two sets A and B is the set

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

consisting of all elements belonging to both A and B.

We can define the unions of intersections of multiple sets in an obvious way:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n, \quad \bigcap_{i=1}^{n} A_i = A_1 \cap \cdots \cap A_n.$$

Definition 4: Difference

Difference of sets A and B is the set

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

Note that unlike unions and intersections, the difference is not *symmetric*, i.e., in general $A \backslash B \neq B \backslash A$.

Definition 5: Cartesian Product

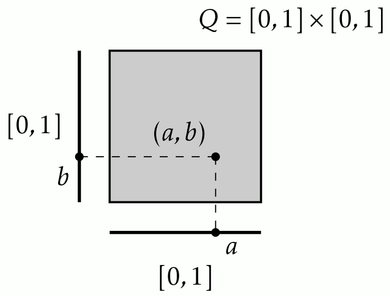
Given two sets A and B the **Cartesian product** of A and B is

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

is the set consisting of all the pairs (a, b).

Example 2

Let Q be the square in the plane with the vertices $(0,0)$, $(1,0)$, $(1,1)$, $(0,1)$. Then $Q = [0,1] \times [0,1]$. In general, if is helpful to think of the Cartesian product of two sets as of a *square*.



Maps

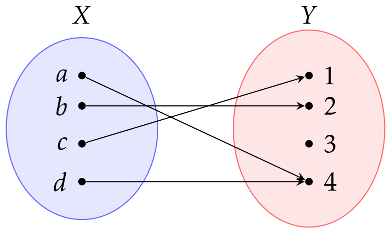
Informally, a map f from set A to set B is a *rule* which assigns an element $b \in B$ to each element $a \in A$. In this case we write

$$f\colon A \to B, \quad f(a) = b.$$

Under a map $f\colon A \to B$ **every** element $a \in A$ is assigned with a **unique** element $f(a) \in B$.

If sets A and B are finite and 'small' we could represent a map explicitly using a *mapping diagram*:

Figure 1: Mapping diagram



Often the notion **function** is used as a synonym of **map**.

Example 3

Define a map $f\colon \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = x^2.$$

For every set A, there is a distinguished map

$$\mathrm{id}_A\colon A \to A, \quad \mathrm{id}_A(a) = a \; \forall a \in A,$$

called **identity map**. It sends any element $a \in A$ to itself.

There are several important properties which a map might satisfy.

Definition 6: Bijection, injection and surjection

A map $f\colon A \to B$ is called **injective** if it does not *glue* elements together, i.e.,

$$\forall x, y \in A: \quad \text{If } f(x) = f(y), \text{ then } x = y.$$

A map $f\colon A \to B$ is called **surjective** if its image is the whole B, i.e.,

$$\forall b \in B, \; \exists a \in A \text{ such that } f(a) = b.$$

A map which is injective and surjective is called **bijective**.

Problem 1: Change exactly one arrow in the Figure 1 to make the map bijective. In how many ways you can do it?

Example 4

Function $f(x) = x^2$ defines a map $f\colon \mathbb{R} \to \mathbb{R}$. This map not injective, since $f(1) = f(-1) = 1$. It is also not surjective, since $f(x)$ never takes the value -1.
The map $g\colon \mathbb{R} \to \mathbb{R}$ defined by the function $g(x) = x^3$ is on the contrary bijective.

If we have two maps

$$f\colon A \to B, \quad g\colon B \to C,$$

the we can form a new map $(g \circ f)$ called the **composition** of f and g:

$$(g \circ f)\colon A \to C, \quad (g \circ f)(a) := g(f(a)).$$

NB: Note that maps in a composition $g \circ f$ are applied **from right to left** — order in which you take composition is important!

Definition 7: Inverse map

Map $g\colon B \to A$ is the **inverse** of the map $f\colon A \to B$ if

$$(g \circ f) = \mathrm{id}_A, \text{ and } (f \circ g) = \mathrm{id}_B.$$

The inverse map is denoted by f^{-1}.

Example 5

Map

$$g\colon [0, +\infty) \to [0, +\infty), \quad g(x) = \sqrt{x}$$

is the inverse of the map

$$f\colon [0, +\infty) \to [0, +\infty), \quad f(x) = x^2$$

When does a map admits an inverse? The following theorem answers this question.

Theorem 1

Map $f\colon A \to B$ **admits an inverse** if and only if f is **bijective**. In this case the inverse is unique.

NB: Whenever we encounter **if and only if** claim, a proof in **two directions** is required!

Proof. Direction $\Rightarrow$.
Assume that f admits an inverse $g\colon B \to A$. We are about to prove that f is injective and bijective.

- (f is injective). Indeed, assume that $f(x) = f(y)$ for some $x, y \in A$. Apply g to both sides of this identity, then

  $$x = \mathrm{id}_A(x) = (g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y) = \mathrm{id}_A(y) = y.$$

  So f is injective

- (f is surjective). Take any $b \in B$. Then

  $$f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b,$$

  so b is in the range of f, and therefore f is surjective.

Direction $\Leftarrow$.
Let us define function $g\colon B \to A$. Given any $b \in B$ we can find $a \in A$ such that $f(a) = b$, since f is surjective. Then we define

$$g(b) = a.$$

It remains to check that g is indeed the inverse map.

- Check that $(f \circ g) = \mathrm{id}_B$. Take any $b \in B$. Then by definition of g, we have $f(g(b)) = b$. Therefore indeed $(f \circ g)(b) = b$.
- Check that $(g \circ f) = \mathrm{id}_A$. Take any $a \in A$. Then we want to check that
$$(g \circ f)(a) = a.$$
We already know that
$$f(g(f(a))) = f(a),$$
since $f \circ g = \mathrm{id}_B$. Now, as f is injective the latter implies
$$g(f(a)) = a,$$
as required.

□

Equivalence relations

Definition 8: Equivalence relation

Equivalence relation on a set A is a subset $R \subset A \times A$ satisfying the following properties

- (reflexive) for any $a \in A$ we have $(a, a) \in R$
- (symmetric) if $(a, b) \in R$, then $(b, a) \in R$.
- (transitive) if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

If we have $(a, b) \in R$ we will write '$a \sim b$' and say 'a is equivalent to b'.

Example 6

1. $R = \{(a, a) \mid a \in A\}$. In other words, any element a is equivalent only to itself.
2. $R = \{(a, b) \mid a, b \in A\}$. In other words, any element $a \in A$ is equivalent to any other element $b \in A$.
3. Take $R = \mathbb{Z}$ and define $R = \{(m, n) \mid m - n \text{ is even}\} \subset \mathbb{Z} \times \mathbb{Z}$.

If $a \in A$ and $\sim$ is an equivalence relation, we can form an equivalence class
$$[a] = \{b \in A \mid b \sim a\}.$$

Proposition 1

Let $\sim$ be an equivalence relation on the set A. Then any two equivalence classes $[a]$, $[b]$ either coincide element-wise, or do not intersect.

Proof. Exercise. □

The above exercise allows to define a new set consisting of the equivalence classes:

Definition 9

The set of *equivalence classes in A* ***modulo*** *an equivalence relation* $\sim$ is defined as
$$A/\sim \; = \; \{[a] \mid a \in A\}.$$

There is a natural map
$$A \to A/\sim, \quad a \mapsto [a]$$
sending each element to its equivalence class.

Problem 2: When is the natural map $A \to A/\sim$ surjective? injective? bijective?

Example 7

Going back to Example 6, we see that
If $R = \{(a,a) \mid a \in A\}$ then $A/\sim$ is the same as A
If $R = \{(a,b) \mid a, b \in A\}$ then $A/\sim$ has only one element
Finally, in the last example $\mathbb{Z}/\sim$ consists of two elements: class of odd integers and class of even integers.