MATH 301

INTRODUCTION TO PROOFS

Sina Hazratpour
Johns Hopkins University
Fall 2021

- Relations
- Functions

Relevant sections of the textbook

- Chapter 3
- Chapter 5

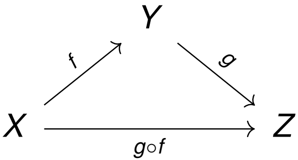
Recall: Compositionality of functions

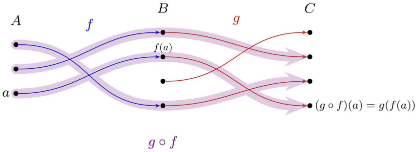
For any set X, we can define a function $\mathrm{id}\colon X \to X$ by letting $\mathrm{id}(x)$ to be the same as x. This function is called the identity function on X.

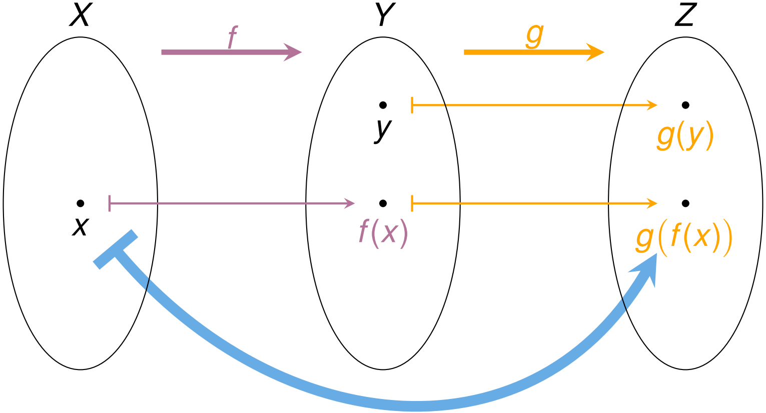
More interestingly, let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions. We can define a new function $k\colon X \to Z$ by letting

$$k(x) =_{\mathrm{def}} g(f(x))$$

The function k is called the composition of f and g which we also call "f composed with g" (or "g after f") and which we denote by $g \circ f$.







$$\lambda y.g(y) \circ \lambda x.f(x) = \lambda x.g\,[f(x)/y]$$

$$\lambda y.log_2 y \circ \lambda x.2^x = \lambda x.log_2 y\,[2^x/y] = log_2 2^x = x$$

The composition of function introduced above has two important properties:

unitality for any function $f\colon X \to Y$, we have $f \circ \mathrm{id}_X = f$ and $\mathrm{id}_Y \circ f = f$.

associativity for any functions $f\colon W \to X$, $g\colon X \to Y$ and $h\colon Y \to Z$, we have

$$h \circ (g \circ f) = (h \circ g) \circ f\,.$$

For any function $f\colon X \to Y$, we define as subset of $X \times Y$ known as the graph of f.

$$\mathbf{Gr}(f) = \{(x, y) \mid f(x) = y\}$$

Define functions h, i, and p as follows:

$$h = \lambda x.(x, f(x)) \tag{1}$$

$$i = \lambda (x, y).(x, y) \tag{2}$$

$$p = \lambda (x, y).y \tag{3}$$

Exercise

Show that the functions f, h, i, and p fit into the following square of sets and functions commutes:

$$\begin{array}{ccc} \mathbf{Gr}(f) & \xrightarrow{\;i\;} & X \times Y \\ {\scriptstyle h}\uparrow & & \downarrow{\scriptstyle p} \\ X & \xrightarrow[f]{} & Y \end{array}$$

Composition of relations

Given a relation R on X and Y and a relation S on Y and Z we can compose them to get a relation $S \circ R$ on X and Z defined as follows:

$$x(S \circ R)z \iff \exists y \in Y\,(xRy \wedge yRz)$$

Exercise

Let B be the “brothership” relation (xBy means x is a brother of y) and S be the “sistership” relation. Show that the composite relation $S \circ B$ is not equivalent to B.

Exercise

- *Prove that if both R and S are partial orders then $S \circ R$ is a partial order.*
- *Prove that if both R and S are equivalence relations then $S \circ R$ is an equivalence relation.*

Exercise

Show that for any equivalence relation R on a set X we have

1. $R \circ R = R$.
2. $R \circ R \circ \ldots \circ R = R$

Composition of functions from compositions of relations

Theorem

Suppose $f\colon X \to Y$ and $g\colon Y \to Z$ are functions. Consider the corresponding relations R_f and R_g. The relation corresponding to the composite function $g \circ f$ is equivalent to the composite relations $R_g \circ R_f$, that is,

$$\forall x \in X \forall z \in Z \left(x \, R_{g \circ f} \, z \iff x \, (R_g \circ R_f) \, z \right)$$

Isomorphisms of sets

Definition

An isomorphism between two sets X and Y is a pair of function

$$f: X \to Y \text{ and } g: Y \to X$$

such that $g \circ f = \mathrm{id}_X$, and $f \circ g = \mathrm{id}_Y$.

We can think of functions f and g above as no data-loss “processes”, e.g. conversion of files to different format without data being lost.

Definition

The sets X and Y are said to be isomorphic in case there exists an isomorphism between them. In this case, we use the notation $X \cong Y$.

Exercise

Show that for any set A, it is isomorphic to $\emptyset$ if and only if A does not have any elements. Can you prove this without the LEM?

Previously, we defined the cartesian product $A \times B$ of two sets A and B to consists of all the pairs (a, b) where $a \in A$ and $b \in B$. Now, we show that if we have more two sets the order of forming products does not matter.

Exercise

1. *For all sets A, B, C we have*

$$(A \times B) \times C \cong (A \times B) \times C$$

For this reason, we use $A \times B \times C$ to denote either sets.

Exercise

Show that two finite sets are isomorphic if and only if they have the same number of elements.

Exercise

Show that for any function $f\colon X \to Y$, *we have*

$$\mathbf{Gr}(f) \cong X\,.$$

A remark on disjoint unions

We introduced the operation of taking disjoint union of two sets as follows:

$$A \sqcup B = \{\mathrm{inl}(x) \mid x \in A\} \cup \{\mathrm{inr}(x) \mid x \in B\}$$

Exercise

Show that

$$A \sqcup B \cong (\{0\} \times A) \cup (\{1\} \times B)$$

Inspired by this fact we define the disjoint union of a family $\{A_i \mid i \in I\}$ of sets to be

$$\bigsqcup_{i \in I} A_i = \bigcup_{i \in I} \{i\} \times A_i \,.$$

An element of $\bigsqcup_{i \in I} A_i$ is a pair (i, a) where $i \in I$ and $a \in A_i$.

Inverse of a relation

We can always define an inverse to a relation:

Definition

For a relation R on X and Y we define the inverse of R to be a relation R^{-1} on Y and X defined by

$$yR^{-1}x \Leftrightarrow xRy$$

Exercise

Show that if a relation R is functional then it is not necessarily the case that R^{-1} is functional.

Arithmetic of sets

We define the operation of addition on sets as follows: For sets X and Y let the sum $X + Y$ be defined by their disjoint union $X \sqcup Y$.

Exercise

1. *Show that the addition operation on sets is both commutative and associative.*
2. *Show that the empty set is the unit (aka neutral element) of addition of sets.*

Exercise

Show that $\underline{m} + \underline{n} \cong \underline{m+n}$ *for all natural numbers* m *and* n*.*

Exercise

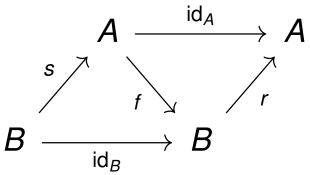
1. *Show that if S and S' are isomorphic, then for all sets X, we have $X + S \cong X + S'$.*
2. *Prove that for any singleton S, we have $\mathbb{N} + S \cong \mathbb{N}$.*

Sometimes, when the context precludes risk of confusion, we use the notation 1 for any singleton set. Therefore, we can simplify the last statement in above to

$$\mathbb{N} + 1 \cong \mathbb{N}.$$

Definition

- *A* *retract* *(aka* *left inverse**) of function* $f: A \to B$ *is a morphism* $r: B \to A$ *such that* $r \circ f = \mathrm{id}_A$*. In this case we also say A is a retract of B.*
- *A* *section* *(aka* *right inverse**) of function* $f: A \to B$ *is a morphism* $s: B \to A$ *such that* $f \circ s = \mathrm{id}_B$*.*



Example

- *The circle is a retract of punctured disk.*
- *The maps from the infinite helix to the circle has a section, but no continuous section.*

Injections

Definition

A function $f\colon X \to Y$ is injective (or one-to-one) if

$$\forall a, b \in X \left(f(a) = f(b) \Rightarrow a = b \right)$$

An injective function is said to be an injection.

Surjections

Definition

A function $f\colon X \to Y$ is surjective (aka onto) if

$$\forall y \in Y,\ \exists x \in X,\ f(x) = y$$

holds. A surjective function is said to be a surjection.

Proposition

1. *A function with a retract is injective.*
2. *A function with a section is surjective.*

Injection and retracts

Does every injection have a retract?

Injection and retracts

No. Consider the function $\emptyset \to \mathbf{1}$.

Injection and retracts

Proposition

Let $f : X \to Y$ be a function. If f is injective and X is inhabited, then f has a retract.

Injection and retracts

Proof.

Suppose that f is injective and X is inhabited. Since X is inhabited, we get always fix an element of it, say $x_0 \in X$. Now, define $r\colon Y \to X$ as follows.

$$r(y) = \begin{cases} x & \text{if } y = f(x) \text{ for some } x \in X \\ x_0 & \text{otherwise} \end{cases}$$

Note that r is well-defined since if for some y, the there are elements x and x' such that $y = f(x) = f(x')$, then, by injectivity of f, we have $x = x'$, and therefore, the value of r is uniquely determined.

To see that r is a retract of f, let $x \in X$. Letting $y = f(x)$, we see that y falls into the first case in the specification of r, so that $r(f(x)) = g(y) = a$ for some $a \in X$ for which $y = f(a)$. But, $f(x) = y = f(a)$, and by injectivity of f we have $x = a$. Therefore, for every $x \in X$,

Injection and retracts

Was this proof constructive?

Questions

Time for your questions!