MATH 301

INTRODUCTION TO PROOFS

Sina Hazratpour
Johns Hopkins University
Fall 2021

- integers
- rational numbers
- real numbers

Relevant sections of the textbook

- Section B.2. (incomplete!)

Quotients by relations

Recall from problem 5 of homework #4 that for each a binary relation R on a set X we can construct a set X/R whose elements are R-classes

$$[x]_R = \{y \in X \mid R(x, y)\}$$

for all $x \in X$.

Quotients by relations

Recall from problem 5 of homework #4 that for each a binary relation R on a set X we can construct a set X/R whose elements are R-classes

$$[x]_R = \{y \in X \mid R(x, y)\}$$

for all $x \in X$. Now collect all such R-classes into one set:

$$X/R =_{\text{def}} \{\, [x]_R \mid x \in X\}$$

Quotients by relations

Recall from problem 5 of homework #4 that for each a binary relation R on a set X we can construct a set X/R whose elements are R-classes

$$[x]_R = \{y \in X \mid R(x, y)\}$$

for all $x \in X$. Now collect all such R-classes into one set:

$$X/R =_{\text{def}} \{\, [x]_R \mid x \in X\}$$

We call the set X/R the quotient of X by the relation R.

Example

Consider the set of natural numbers with the usual ordering $\leqslant : \mathbb{N} \to \mathbb{N} \to \mathbf{2}$ *defined for* $m \in \mathbb{N}$ *recursively by*

$m \leqslant 0$ *if and only if* $m = 0$, *and*

$m \leqslant \mathrm{succ}(n)$ *if and only if* $m = \mathrm{succ}(n)$ *or* $m \leqslant n$.

Example

Consider the set of natural numbers with the usual ordering $\leqslant : \mathbb{N} \to \mathbb{N} \to \mathbf{2}$ *defined for* $m \in \mathbb{N}$ *recursively by*

$m \leqslant 0$ *if and only if* $m = 0$*, and*

$m \leqslant \mathrm{succ}(n)$ *if and only if* $m = \mathrm{succ}(n)$ *or* $m \leqslant n$*.*

We have classes $[n]$ *forming a chain in the subset relation ordering:*
$[0] \supset [1] \supset [2] \supset \ldots.$

Example

Consider the set of natural numbers with the usual ordering $\leqslant : \mathbb{N} \to \mathbb{N} \to \mathbf{2}$ *defined for* $m \in \mathbb{N}$ *recursively by*

$$m \leqslant 0 \text{ if and only if } m = 0, \text{ and}$$

$$m \leqslant \mathrm{succ}(n) \text{ if and only if } m = \mathrm{succ}(n) \text{ or } m \leqslant n.$$

We have classes $[n]$ *forming a chain in the subset relation ordering:* $[0] \supset [1] \supset [2] \supset \ldots$. *Note that* $0 \leqslant 1$ *but* $[0] \neq [1]$.

So far R is just a general binary relation. In general we do not have that

Proposition

Prove that if R is reflexive then $\forall x \in X,\ x \in [x]$.

So far R is just a general binary relation. In general we do not have that

Proposition

Prove that if R is reflexive then $\forall x \in X,\ x \in [x]$.

Proposition

Prove that if R is transitive then $\forall x, y \in X, R(x, y) \wedge R(y, x) \Rightarrow [x] = [y]$.

So far R is just a general binary relation. In general we do not have that

Proposition

Prove that if R is reflexive then $\forall x \in X,\ x \in [x]$.

Proposition

Prove that if R is transitive then $\forall x, y \in X, R(x, y) \wedge R(y, x) \Rightarrow [x] = [y]$.

Proposition

Prove that if R is symmetric and transitive then
$\forall x, y \in X,\ R(x, y) \Rightarrow [x] = [y]$.

Proposition

Prove that if R is reflexive, symmetric and transitive then
$\forall x, y \in X,\ R(x, y) \Leftrightarrow [x] = [y]$.

Suppose we have a graph G. Define a relation R on vertices of G by imposing that

$$R(a, b) \Leftrightarrow \text{ there is an edge from } a \text{ to } b.$$

Suppose we have a graph G. Define a relation R on vertices of G by imposing that

$$R(a, b) \Leftrightarrow \text{there is an edge from } a \text{ to } b.$$

- What is a class $[a]$ for a vertex a?

Suppose we have a graph G. Define a relation R on vertices of G by imposing that

$$R(a, b) \Leftrightarrow \text{ there is an edge from } a \text{ to } b.$$

- What is a class $[a]$ for a vertex a?
- Show that if $R(a, b) \wedge R(b, a)$ then it is not necessarily true that $[a] = [b]$.

Suppose we have a graph G. Define a relation R on vertices of G by imposing that

$$R(a, b) \Leftrightarrow \text{ there is a path from } a \text{ to } b.$$

Suppose we have a graph G. Define a relation R on vertices of G by imposing that

$$R(a, b) \Leftrightarrow \text{ there is a path from } a \text{ to } b.$$

- What is a class $[a]$ for a vertex a?

Suppose we have a graph G. Define a relation R on vertices of G by imposing that

$$R(a, b) \Leftrightarrow \text{ there is a path from } a \text{ to } b.$$

- What is a class $[a]$ for a vertex a?
- Show that if $R(a, b) \wedge R(b, a)$ then $[a] = [b]$.

Proposition

Prove that the function $q\colon X \to X/R$ assigning to each x in X the class $[x]$ in X/R is a surjection.

The universal mapping property of quotient construction

Proposition

Let R be a symmetric and transitive relation on a set X. For any set Y, precomposing with q yields a bijection

$$(X/R \to Y) \cong \{f\colon X \to Y \mid \forall x, y \in X,\ R(x, y) \Rightarrow f(x) = f(y)\}$$

Recall that a relation R on a set A is called an equivalence if it satisfies the following conditions:

- **reflexivity**: $\forall a \in A,\ R(a,a)$,
- **symmetry**: $\forall a,b \in A,\ R(a,b) \to R(b,a)$, and
- **transitivity**: $\forall a,b,c \in A,\ R(a,b) \Rightarrow R(b,c) \Rightarrow R(a,c)$.

Recall that a relation R on a set A is called an equivalence if it satisfies the following conditions:

- **reflexivity**: $\forall a \in A,\ R(a, a)$,
- **symmetry**: $\forall a, b \in A,\ R(a, b) \to R(b, a)$, and
- **transitivity**: $\forall a, b, c \in A,\ R(a, b) \Rightarrow R(b, c) \Rightarrow R(a, c)$.

We usually denote an equivalence relation by the symbol $\sim$ (instead of R).

Quotients by equivalence relations

For each equivalence $\sim$ on a set X we can construct a set $X/\sim$ whose elements are equivalence classes

$$[x]_\sim = \{y \in X \mid x \sim y\}$$

for all $x \in X$.

Quotients by equivalence relations

For each equivalence $\sim$ on a set X we can construct a set $X/\sim$ whose elements are equivalence classes

$$[x]_\sim = \{y \in X \mid x \sim y\}$$

for all $x \in X$. Now collect all such equivalence classes into one set:

$$X/\sim \,=_{\text{def}} \{[x]_\sim \mid x \in X\}$$

Quotients by equivalence relations

For each equivalence $\sim$ on a set X we can construct a set $X/\sim$ whose elements are equivalence classes

$$[x]_\sim = \{y \in X \mid x \sim y\}$$

for all $x \in X$. Now collect all such equivalence classes into one set:

$$X/\sim \, =_{\text{def}} \{[x]_\sim \mid x \in X\}$$

We call the set $X/\sim$ the quotient of X by equivalence relation $\sim$.

For an equivalence relation $\sim$, the surjection $q\colon X \to X/\sim$ has an extra nice property:

$$q(x) = q(y) \Leftrightarrow R(x, y)$$

Example of quotient by an equivalence relation

Consider the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$. where

$$(m, n) \sim (m', n') \Leftrightarrow m + n' = n + m' \, .$$

Prove that this relation is an equivalence.

Example of quotient by an equivalence relation

Consider the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$. where

$$(m, n) \sim (m', n') \Leftrightarrow m + n' = n + m' .$$

Prove that this relation is an equivalence.

The equivalence class $[(0,0)]$ is the set $\{(0,0),(1,1),(2,2),...\}$.

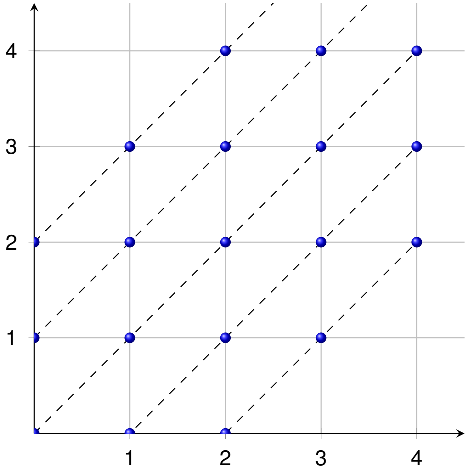
Example of quotient by an equivalence relation

Consider the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$. where

$$(m, n) \sim (m', n') \Leftrightarrow m + n' = n + m' \, .$$

Prove that this relation is an equivalence.

The equivalence class $[(0, 0)]$ is the set $\{(0, 0), (1, 1), (2, 2), ...\}$. What is the equivalence class $[(0, 1)]$?



4
3
2
1
1
2
3
4

Integers

We define the set $\mathbb{Z}$ of integers as the quotient $\mathbb{N} \times \mathbb{N} / \sim$.

Integers

We define the set $\mathbb{Z}$ of integers as the quotient $\mathbb{N} \times \mathbb{N} / \sim$.

- In other words, a pair (m, n) represents the would-be integer $m - n$.

Integers

We define the set $\mathbb{Z}$ of integers as the quotient $\mathbb{N} \times \mathbb{N}/\sim$.

- In other words, a pair (m, n) represents the would-be integer $m - n$.
- In this case, there are *canonical representatives* of the equivalence classes: those of the form $(n, 0)$ or $(0, n)$.

Addition on integers

We can define the operation of addition on $\mathbb{Z}$ by an assignment $+_\sim : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ which assigns to the pair $([(m, n)], [(m', n')])$ the class $[(m + m', n + n')]$.

Exercise

Show that the assignment $+_\sim$ is well-defined, i.e. it defines a function.

Addition on integers

We can define the operation of addition on $\mathbb{Z}$ by an assignment $+_\sim : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ which assigns to the pair $([(m,n)],[(m',n')])$ the class $[(m+m',n+n')]$.

Exercise

Show that the assignment $+_\sim$ is well-defined, i.e. it defines a function.

Exercise

- *Show that for all integers a we have $0+a=a=a+0$.*
- *Show that for all integers a,b,c we have $(a+b)+c=a+(b+c)$.*
- *Show that for all integers a,b we have $a+b=b+a$.*

We can define the operation of multiplication on $\mathbb{Z}$ by an assignment $\cdot_\sim : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ which assigns to the pair $([(m, n)], [(m', n')])$ the class $[(m \cdot m', n \cdot n')]$.

Exercise

Show that the assignment $\cdot_\sim$ is well-defined, i.e. it defines a function.

We can define the operation of multiplication on $\mathbb{Z}$ by an assignment $\cdot_\sim : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ which assigns to the pair $([(m, n)], [(m', n')])$ the class $[(m \cdot m', n \cdot n')]$.

Exercise

Show that the assignment $\cdot_\sim$ is well-defined, i.e. it defines a function.

Exercise

- *Show that for all integers a we have $0 + a = a = a + 0$.*
- *Show that for all integers a, b, c we have $(a + b) + c = a + (b + c)$.*
- *Show that for all integers a, b we have $a + b = b + a$.*

Every function $f\colon A \to B$ gives rise to an equivalence relation $\sim_f$ on A defined by

$$a \sim_f b \Leftrightarrow f(a) = f(b)\,.$$

Every function $f\colon A \to B$ gives rise to an equivalence relation $\sim_f$ on A defined by

$$a \sim_f b \Leftrightarrow f(a) = f(b)\,.$$

That is to say that $a \sim_f b$ if a, b are in the same fibre of f.

Every function $f : A \to B$ gives rise to an equivalence relation $\sim_f$ on A defined by

$$a \sim_f b \Leftrightarrow f(a) = f(b)\,.$$

That is to say that $a \sim_f b$ if a, b are in the same fibre of f.

Exercise

Show that the relation above is indeed an equivalence relation.

Image factorization

Proposition

Suppose $f\colon A \to B$ is a function. We can factor f into a surjection followed by a bijection followed by an injection.

$$\begin{tikzcd}
A \arrow[rrr, "f"] \arrow[dr, twoheadrightarrow, "q"'] & & & B \\
& C \arrow[r, "g"'] & D \arrow[ur, rightarrowtail, "i"'] &
\end{tikzcd}$$

that is there are functions q, g, i such that $f = i \circ g \circ q$, where q is a surjection, g is a bijection, and i is an injection.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. As shown before, q is surjective and i is injective.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. As shown before, q is surjective and i is injective. We define g to be the assignment which takes an equivalence class $[x]$ to the element $f(x) \in B$.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. As shown before, q is surjective and i is injective. We define g to be the assignment which takes an equivalence class $[x]$ to the element $f(x) \in B$. Note that g is well-defined, since if $[x] = [y]$ then $x \sim_f y$ and therefore, by the definition of $\sim_f$, we have $f(x) = f(y)$.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. As shown before, q is surjective and i is injective. We define g to be the assignment which takes an equivalence class $[x]$ to the element $f(x) \in B$. Note that g is well-defined, since if $[x] = [y]$ then $x \sim_f y$ and therefore, by the definition of $\sim_f$, we have $f(x) = f(y)$. We now show that g is a bijection.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. As shown before, q is surjective and i is injective. We define g to be the assignment which takes an equivalence class $[x]$ to the element $f(x) \in B$. Note that g is well-defined, since if $[x] = [y]$ then $x \sim_f y$ and therefore, by the definition of $\sim_f$, we have $f(x) = f(y)$. We now show that g is a bijection. g is injective since for every $x, y \in A$, if $g([x]) = g([y])$ then $f(x) = f(y)$ and therefore, $[x] = [y]$.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. As shown before, q is surjective and i is injective. We define g to be the assignment which takes an equivalence class $[x]$ to the element $f(x) \in B$. Note that g is well-defined, since if $[x] = [y]$ then $x \sim_f y$ and therefore, by the definition of $\sim_f$, we have $f(x) = f(y)$. We now show that g is a bijection. g is injective since for every $x, y \in A$, if $g([x]) = g([y])$ then $f(x) = f(y)$ and therefore, $[x] = [y]$. Also, g is surjective: given b in $f_*(A)$ there is some $a \in A$ such that $b = f(a) = g([a])$.

Proof.

We have to construct the sets C, D and a surjection q, a bijection g and an injection i. Now we define C to be $A/\sim_f$, and we define D to be the image $f_*(A)$ of A under f. We also define q to be the obvious quotient map and i to be the obvious inclusion. As shown before, q is surjective and i is injective. We define g to be the assignment which takes an equivalence class $[x]$ to the element $f(x) \in B$. Note that g is well-defined, since if $[x] = [y]$ then $x \sim_f y$ and therefore, by the definition of $\sim_f$, we have $f(x) = f(y)$. We now show that g is a bijection. g is injective since for every $x, y \in A$, if $g([x]) = g([y])$ then $f(x) = f(y)$ and therefore, $[x] = [y]$. Also, g is surjective: given b in $f_*(A)$ there is some $a \in A$ such that $b = f(a) = g([a])$. $\square$

Our factorization diagram becomes

$$\begin{tikzcd}
A \arrow[rrr, "f"] \arrow[dr, two heads, "q"'] & & & B \\
& A/\sim \arrow[r, "g"'] & f_*(A) \arrow[ur, tail, "i"'] &
\end{tikzcd}$$

Our factorization diagram becomes

$$\begin{tikzcd} A \arrow[rrr, "f"] \arrow[dr, two heads, "q"'] & & & B \\ & A/\sim \arrow[r, "g"'] & f_*(A) \arrow[ur, tail, "i"'] & \end{tikzcd}$$

In fact, $g \circ q = p \colon X \to \mathbf{Im}(f)$.

Definition

For a function $f\colon X \to X$, define

$$\mathrm{Fix}(f) =_{\mathrm{def}} \{x \in X \mid f(x) = x\}\,.$$

We call $\mathrm{Fix}(f)$ *the set of fix-points of* f.

Definition

For a function $f : X \to X$, define

$$\mathrm{Fix}(f) =_{\text{def}} \{x \in X \mid f(x) = x\} .$$

We call $\mathrm{Fix}(f)$ *the set of fix-points of f.*

Definition

A function r is called an idempotent if $r \circ r = r$.

Definition

For a function $f\colon X \to X$, define

$$\mathrm{Fix}(f) =_{\mathrm{def}} \{x \in X \mid f(x) = x\}\,.$$

We call $\mathrm{Fix}(f)$ the set of fix-points of f.

Definition

A function r is called an idempotent if $r \circ r = r$.

Exercise

Show that if $f\colon X \to X$ is idempotent, then $\mathrm{Fix}(f) \cong \mathbf{Im}(f)$.

Definition

For a function $f: X \to X$, define

$$\mathrm{Fix}(f) =_{\mathrm{def}} \{x \in X \mid f(x) = x\}\,.$$

We call $\mathrm{Fix}(f)$ *the set of fix-points of* f*.*

Definition

A function r is called an idempotent if $r \circ r = r$.

Exercise

Show that if $f: X \to X$ is idempotent, then $\mathrm{Fix}(f) \cong \mathbf{Im}(f)$*.*

Exercise

For an idempotent function $f: X \to X$, show that

$$X/\sim_f \;\cong\; \mathrm{Fix}(f) \cong \mathbf{Im}(f)$$

Exercise

Construct an idempotent $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ *such that* $\mathrm{Fix}(f)$ *is in bijection with the set of integers.*

Exercise

Suppose $r\colon A \to B$ is a retraction. Show that

$$B \cong A/\sim_r$$

Exercise

Suppose $r: A \to B$ *is a retraction. Show that*

$$B \cong A/\sim_r$$

Induction for integers

We identify a natural number n with the corresponding non-negative integer, i.e. with the image of $(n, 0) \in \mathbb{N} \times \mathbb{N}$ in $\mathbb{Z}$.

Induction for integers

We identify a natural number n with the corresponding non-negative integer, i.e. with the image of $(n, 0) \in \mathbb{N} \times \mathbb{N}$ in $\mathbb{Z}$.

Lemma

Suppose $P : \mathbb{Z} \to \mathbb{P}\mathrm{rop}$ *is a predicate over integers, and*

- $P(0)$ *holds,*
- $\forall n : \mathbb{N},\ P(n) \Rightarrow P(\mathrm{succ}(n))$*, and*
- $\forall n : \mathbb{N},\ P(-n) \to P(-\mathrm{succ}(n))$*.*

Then we have $\forall z : \mathbb{Z},\ P(z)$*.*

We constructed the integers $\mathbb{Z}$ as a quotient of $\mathbb{N} \times \mathbb{N}$, and observed that this quotient is generated by an idempotent.

We constructed the integers $\mathbb{Z}$ as a quotient of $\mathbb{N} \times \mathbb{N}$, and observed that this quotient is generated by an idempotent.

We construct the *field* of rationals $\mathbb{Q}$ along the same lines as well, namely as the quotient

$$\mathbb{Q} =_{\mathrm{def}} (\mathbb{Z} \times \mathbb{N})/\approx$$

where

$$(u, a) \approx (v, b) =_{\mathrm{def}} (u(b + 1) = v(a + 1)).$$

We constructed the integers $\mathbb{Z}$ as a quotient of $\mathbb{N} \times \mathbb{N}$, and observed that this quotient is generated by an idempotent.
We construct the *field* of rationals $\mathbb{Q}$ along the same lines as well, namely as the quotient

$$\mathbb{Q} =_{\text{def}} (\mathbb{Z} \times \mathbb{N})/\approx$$

where

$$(u, a) \approx (v, b) =_{\text{def}} (u(b+1) = v(a+1)).$$

In other words, a pair (u, a) represents the rational number $u/(1 + a)$.

We constructed the integers $\mathbb{Z}$ as a quotient of $\mathbb{N} \times \mathbb{N}$, and observed that this quotient is generated by an idempotent.

We construct the *field* of rationals $\mathbb{Q}$ along the same lines as well, namely as the quotient

$$\mathbb{Q} =_{\mathrm{def}} (\mathbb{Z} \times \mathbb{N})/{\approx}$$

where

$$(u, a) \approx (v, b) =_{\mathrm{def}} (u(b+1) = v(a+1)).$$

In other words, a pair (u, a) represents the rational number $u/(1+a)$.

Here too we have a canonical choice of representatives, namely fractions in lowest terms.

The arithmetic of rational numbers

We write down the arithmetical operations on $\mathbb{Q}$ so that we can compute with fractions.

The order on rational numbers

We equip $\mathbb{Q}$ with a total order.

Real numbers

Questions

Thanks for your attention!