Last time:  defined a relation ~ on \( \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \)

- checked that ~ is an equivalence relation
- defined \( \mathbb{Q} = \text{set of equivalence classes of } ~ \)
  \( \mathbb{Q} : = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / ~ \)
- notation: \( \frac{a}{b} \) = equivalence class of \( (a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \)
- defined \( + : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q} \)
  \( \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \)
  and checked that + is well defined
- stated and didn't prove: \( \cdot : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q} \)
  \( \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \)
  is also well-defined.

Easy to see: (i) \( \forall \frac{a}{b} \in \mathbb{Q}, \frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + 0 \cdot b}{b \cdot 1} = \frac{a}{b} \)

(ii) \( \forall \frac{a}{b} \in \mathbb{Q}, \frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b} \)

(iii) + is associative and commutative

(iv) \( \cdot \) is associative and commutative

(v) \( \cdot \) distributes over +:

\( \frac{a}{b} - \left( \frac{c}{d} + \frac{e}{f} \right) = \frac{a \cdot d + c \cdot d + a \cdot b - c \cdot f - e \cdot b}{b \cdot d + f} \)

(vi) \( \frac{a}{b} + \left( -\frac{a}{b} \right) = \frac{ab + (-ca) \cdot b}{b^2} = \frac{(a + (-a))b}{b^2} = \frac{0 \cdot b}{b^2} = 0 \cdot \frac{1}{b} \)
  there are additive inverses in \( \mathbb{Q} \).

(vii) if \( \frac{a}{b} \neq \frac{0}{1} \) (i.e. if \( a \neq 0 \)) then \( \frac{b}{a} \) makes sense

\( \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1} \).

\( \Rightarrow \forall x \in \mathbb{Q}, x \neq 0, \exists \ x^{-1} \ s.t. \ x \cdot x^{-1} = \frac{1}{1} \).

(i)-(vi) \( \Rightarrow \mathbb{Q} \) is a commutative ring with unity

(vii) \( \Rightarrow \mathbb{Q} \) is a field.

Unfinished business from previous two lectures:

Proposition 6.1 (division algorithm for \( \mathbb{Z} \)): \( \forall a, d \in \mathbb{Z}, \ d \geq 1, \)

\( \exists \) unique \( q, r \in \mathbb{Z} \) such that

1. \( a = q \cdot d + r \)
2. \( 0 \leq r < d \)
Proof (existence of $r$ and $d$)

We use a version of well-ordering principle:

"any nonempty subset of $\mathbb{N} \cup \{0\}$ has a least element."

- if $a = 0$, take $q = 0$, $r = 0$. Then $0 = 0 \cdot d + 0$ and $0 < d$.
- if $d = 1$, let $q = a$, $r = 0$ Then $a = a \cdot 1 + 0$ and $0 < 1$.

Now assume $a \neq 0$, $d > 1$ and consider

$$X = \{ a - td | t \in \mathbb{Z}, a - td \geq 0 \}.$$

Claim $X \neq \emptyset$. Reason: if $a > 0$, $a - 0 \cdot d = a \in X$

- if $a < 0$, $a - ad = a(1-d) > 0$ since $a < 0$ and $1-d < 0

$$\Rightarrow a - ad \in X.$$

By well-ordering principle $\exists r = \text{least element of } X.$

Since $r \in X$, $\exists q \in \mathbb{Z}$ st. $r = a - q \cdot d = a - q \cdot d + r$.

Since $r \in X$, $r > 0$. We now argue that $r < d$

Suppose not, $r \geq d$. Then

$$0 \leq r - d = a - q \cdot d - d = a - (q+1) d

\Rightarrow r - d \in X.$$

On the other hand, since $d > 0$, $r - d < r$.

This contradicts the fact that $r \in X$ is least.

Conclusion: $r < d$

This proves existence of $r, d \in \mathbb{Z}$ with $a = q \cdot d + r, 0 \leq r < d$.

(uniquneness). Suppose $\exists q_1, q_2, r_1, r_2 \in \mathbb{Z}$ st.

$$a = q_1d + r_1 = q_2d + r_2, \quad 0 \leq r_1, r_2 < d.$$

Then either $r_1 < r_2$ or $r_2 < r_1$. Say $r_2 < r_1$. Then

$$0 \leq r_1 - r_2 = (a - q_1d) - (a - q_2d) = (q_2 - q_1) d.$$

Since $r_1, r_2 < d$, $d > r_1 - r_2 = (q_2 - q_1) d$

The only non-negative integer multiple of $d$ which is less than $d$

is $0$. $\Rightarrow (q_2 - q_1) d = 0$.

Since $d \neq 0$, cancellation law $\Rightarrow q_2 - q_1 = 0$.

$\Rightarrow r_1 - r_2 = 0 \cdot d = 0$.

$\therefore q_2 = q_1$ and $r_1 = r_2.$
Functions.

Informally, a function $f$ from a set $A$ to a set $B$ assigns to each element of $A$ one element $f(a) \in B$.

We write $f : A \rightarrow B$

$\text{A}$ is the domain of $f$

$\text{B}$ is the range of $f$ (also called codomain or target).

Example 1: $f : \mathbb{R} \rightarrow \mathbb{R}, \quad f(x) = x^2$.

Non-example: $h : [0, \infty) \rightarrow \mathbb{R}, \quad h(x) = \pm \sqrt{x}$

The set $\{ x \in \mathbb{R} \mid x \geq 0 \}$.

$h$ is not a function: it assigns to 4 both 2 and -2.

Formally, there are two ways to proceed:

1) "function" is an undefined notion, just like "set" or "is an element of".

2) given a function $f : A \rightarrow B$, we have a relation

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

Not every relation $R \subseteq A \times B$ can be a graph of a function; $R$ has to pass "the vertical line test".

$$(a, b), (a, b') \in R \Rightarrow b = b'$$

The set $\uparrow^y R = \{ (x, y) \in \mathbb{R}^2 \mid y = \pm \sqrt{x} \}$

fails the vertical line test and so is not the graph of a function.

The book defines a function $f : A \rightarrow B$ to be a relation $R \subseteq A \times B$ st.

$$(a, b), (a', b') \in R \text{ and } a = a' \Rightarrow b = b'$$
But then it tells you not to think of functions as relations.

Most of the time we think of functions as rules.

Ex For every set $A \neq \emptyset$ we have the identity function $I_A : A \to A$.

\[ I_A(a) = a. \]

(In terms of relations $I_A \sim \{(a, a) \in A \times A \mid a = a'\}.$)

Ex Let $\sim$ be an equivalence relation on a set $X$.

Let $X/\sim$ = set of equivalence classes of elements of $X$

\[ = \{[a] \mid a \in X\}. \]

We have a function $\pi : X \to X/\sim$, $\pi(a) = [a]$.

Functions can be composed: if $f : A \to B$, $g : B \to C$

are two functions, their composite is $g \circ f : A \to C$

defined by

\[ (g \circ f)(a) = g(f(a)). \]

Ex $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sin x$  $g : \mathbb{R} \to \mathbb{R}$, $g(u) = u^2$

\[ (g \circ f)(x) = (\sin x)^2 \]

\[ (f \circ g)(u) = \sin(u^2). \]

Theorem 1.7.3 Composition of functions is associative:

$\forall f : A \to B$, $\forall g : B \to C$, $\forall h : C \to D$

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

Proof $\forall a \in A$

\[ (h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))) \]

\[ = (h \circ g)(f(a)) = ((h \circ g) \circ f)(a). \]