The rational numbers

What can we do w/ \( \mathbb{Q} \) that we cannot do w/ \( \mathbb{Z} \)?

- multiplicative inverses:
  \[ \exists \ 5^{-1} \]
  \[ \forall x \in \mathbb{Q} \setminus \{0\} \exists x^{-1} \in \mathbb{Q} \text{ s.t.} \ x \cdot x^{-1} = 1 \]

We can solve eq’ns \( x \in \mathbb{Q} \)

\[ m \cdot x = n \text{ has a sol’n for} \ m \in \mathbb{Q} \setminus \{0\}, \ n \in \mathbb{Q} \]

(also for \( m = n = 0 \))

Invert division?

Idea: Record pairs of integers so that

\( (m, 1) \) represents \( m \in \mathbb{Z} \)

\( (1, m) \) represents a sol’n to \( m \cdot x = 1 \).

\( \Delta \) should not allow \( 0 \) in second coord.
Define \( \mathbb{Q} = \left( \mathbb{Z} \times \left( \mathbb{Z} \times \mathbb{Z} \right) \right) / \sim \)

where \( (a, b) \sim (a', b') \) when

\[ \exists c \in \mathbb{Z} \text{ s.t. } a = ac', b = bc' \]

or \( a = a'c, b = b'c \).

Write \([a, b]\) for the equivalent class of \((a, b)\).

\([6, 21] = [10, 35]\)

\((a, b) \sim (a', b') \) if \( \exists (a'', b'') \) s.t.

\( a = ca'', b = cb'' \)

or \( a = d a'', b = d b'' \).

Note: “Lowest terms” corresponds to closest to origin in an equivalent class. (W/ positive second coord)

Get representative of \([a, b]\) \ w/ \( a \in \mathbb{Z}, b > 0 \)
Arithmetic  \[ [m,n] \cdot [p,q] = [m \cdot p, n \cdot q] \]
\[ [m,n] + [p,q] = [(m \cdot q)+(p \cdot n), n \cdot q] \]
Check: well-defined.  \[ \text{Convention: takes precedence over +} \]

Thus \( (\mathbb{Q}, +, \cdot) \)

has the following properties:

1) \( +, \cdot \) are commutative, associative binary ops

2) \( \exists \) additive identity \( 0 = [0,1] \) s.t. \[ \forall m \in \mathbb{Q} \rightarrow m + 0 = m = 0 + m. \]

3) \( \exists \) multiplicative identity \( 1 = [1,1] \) s.t. \[ \forall m \in \mathbb{Q} \rightarrow m \cdot 1 = m = 1 \cdot m, \text{ and } 0 \neq 1. \]

4) There are additive inverses for all \( m \in \mathbb{Q} \)

5) There are multiplicative inverses for all \( m \in \mathbb{Q} \setminus \{0\} \)

6) Distributivity: \( \forall m,n,p \in \mathbb{Q} \rightarrow m \cdot (n+p) = (m \cdot n)+(m \cdot p) \)

\[ \text{class notes Page 64} \]
Defn: A field is a set $F$ equipped w/ binary operations $+$, $\cdot$ s.t. properties 
1 - 6 of $\mathbb{Q}$ hold w/ $\mathbb{Q}$ replaced by $F$.

* $\mathbb{Q}$ is a field

* $\mathbb{R}$ will be a field

* $\mathbb{C}$ is a field

* $\mathbb{Z}$ are not a field (no mult inverses)

* $\mathbb{Z}/n\mathbb{Z}$ satisfy 1 - 4 & 6

5 does not hold for, e.g., $\mathbb{Z}/6\mathbb{Z}$: only $[1], [5]$ have inverses

Fact: If $n = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. 

$$[m,n] = \frac{m}{n}$$ in $\mathbb{Q}$.