Lecture 2

Recall:

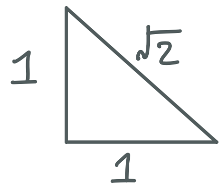
Natural Numbers $\mathbb{N} = \{1, 2, 3, \dots\}$

Integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Rational Numbers $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$

Real Numbers $\mathbb{R} = ?$

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \overbrace{\mathbb{Q} \subsetneq \mathbb{R}}^{\text{not obvious}}$$



Prop: $\sqrt{2} \notin \mathbb{Q}$

Moral: there are useful numbers missing from $\mathbb{Q}$.

To prove this, we will first prove a lemma

Lemma: Let $x \in \mathbb{Z}$. If x^2 is even, then x is even.

Pf: Assume, for the sake of contradiction, that x is odd, so $\exists\, y \in \mathbb{Z}$ so that $x = 2y+1$.

Then $x^2 = (2y+1)^2 = \overbrace{\underbrace{4y^2+2y}_{\text{even}}+1}^{\text{odd}}$.

So x^2 is odd, which is a contradiction. $\square$

Question: how is proof by contradiction related to proving the contrapositive?

For this lemma...

<u>Lemma</u>: Let $x \in \mathbb{Z}$. If $\overbrace{x^2 \text{ is even}}^{P}$, then $\underbrace{x \text{ is even}}_{Q}$.

Proving "If P, then Q" is equivalent to proving the contrapositive "If $\underbrace{\neg Q}_{x \text{ is odd}}$, then $\underbrace{\neg P}_{x^2 \text{ is odd}}$".

Pf that $\sqrt{2} \notin \mathbb{Q}$:

Assume, for the sake of contradiction, that $\sqrt{2} \in \mathbb{Q}$, so $\exists\, m, n \in \mathbb{Z}$ with $n \neq 0$ so that $\sqrt{2} = \frac{m}{n}$.

We may choose m and n so they aren't both even. ☼

Squaring both sides, we obtain

$$2 = \frac{m^2}{n^2} \implies \underbrace{2n^2 = m^2}_{(*)}.$$

Since m^2 is even, lemma ensures m is even, so $\exists\, y \in \mathbb{Z}$ so that $m = 2y$.

Substituting into $(*)$, $2n^2 = (2y)^2 = 4y^2 \implies n^2 = 2y^2$; so n^2 is even, and our lemma ensures n is even.

This contradicts ☼. Therefore $\sqrt{2} \notin \mathbb{Q}$. $\square$

So what is $\mathbb{R}$?

In order to define $\mathbb{R}$, we will begin by defining what it means to be an <u>ordered field</u>

Def: (field): A set F is a <u>field</u> if it has two operations (addition and multiplication) that satisfy the following properties $\forall a,b,c \in F$:

(A1) $a+(b+c)=(a+b)+c$ — associativity

(A2) $a+b=b+a$ — commutativity

(A3) $\exists$ an element in F called 0 s.t. $\forall a \in F$, $a+0=a$ — identity

(A4) for each $a \in F$, $\exists$ an element called $-a \in F$ s.t. $a+(-a)=0$ — inverse

(m1) $a(bc)=(ab)c$ — associativity

(m2) $ab=ba$ — commutativity

(m3) $\exists$ an element in F called 1 s.t. $1 \neq 0$ and $\forall a \in F$, $a \cdot 1 = a$ — identity

(m4) for each $a \in F$, $a \neq 0$, $\exists$ an element called $\frac{1}{a}$ s.t. $a \cdot \frac{1}{a} = 1$. — inverse

(DL) $a(b+c)=ab+ac$ — distributive law

Remark: $\mathbb{N}$ and $\mathbb{Z}$ aren't fields
$\mathbb{Q}$ is a field
$M_n(\mathbb{R})$ isn't a field, for $n \geq 2$

Using the definition of a field, you can rigorously prove familiar algebraic properties.

Thm: If F is a field, then $\forall\, a,b \in F$:
(i) If $a+c=b+c$, then $a=b$
(ii) $a \cdot 0 = 0$

Pf:
First, we will show (i). By (A4), there exists $-c \in F$ s.t. $c+(-c)=0$. Thus,

$$a+c=b+c \implies (a+c)+(-c) = (b+c)+(-c)$$

$$\overset{(A1)}{\implies} a+(c+(-c)) = b+(c+(-c))$$

$$\overset{(A4)}{\implies} a+0 = b+0$$

$$\overset{(A3)}{\implies} a=b$$

We now show (ii). By (A3), $0+0=0$, so

$$a\cdot(0+0)=a\cdot 0 \overset{(D2)}{\Longrightarrow} a\cdot 0+a\cdot 0=a\cdot 0$$

$$\overset{(A3)}{\Longrightarrow} a\cdot 0+a\cdot 0=a\cdot 0+0$$

$$\overset{(A2)}{\Longrightarrow} a\cdot 0+a\cdot 0=0+a\cdot 0$$

$$\overset{(i)}{\Longrightarrow} a\cdot 0=0 \qquad \square$$