<u>Last time</u>: set theory

<u>Today</u>: Number systems. (involves "infinite" sets)

<u>Reference just for today</u>: Landau, <u>Foundations of analysis</u> (Canvas).

Peano's axioms.

There exists a set $\mathbb{N}$ with the following properties:

<u>P1.</u> $1 \in \mathbb{N}$

<u>P2.</u> There exists an injective function $S : \mathbb{N} \to \mathbb{N}$ s.t. $1 \notin S(\mathbb{N})$.

<u>P3.</u> If $A \subset \mathbb{N}$ is any subset s.t. $1 \in A$ and $n \in A \Rightarrow S(n) \in A$, then $A = \mathbb{N}$.

$$\mathbb{N} = \{1, \_, \_, \_\}.$$

From Peano's axioms, we can derive the

<u>Principle of mathematical induction</u>:

Let ϕ_n be a statement for each $n \in \mathbb{N}$. If ϕ_1 is true, and (ϕ_n is true) $\Rightarrow$ ($\phi_{S(n)}$ is true), then ϕ_n is true for all $n \in \mathbb{N}$.

Proof: Let $A = \{n \in \mathbb{N} \mid \phi_n \text{ is true}\}$.

Since ϕ_1 is true, $1 \in A$.

Since (ϕ_n is true) $\Rightarrow$ ($\phi_{S(n)}$ is true), we have

$$n \in A \implies S(n) \in A.$$

By P3, we have $A = \mathbb{N}$, i.e.

$$\phi_n \text{ is true for all } n \in \mathbb{N}. \quad \square$$

Definition: The function

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$
$$(m, n) \longmapsto m + n \qquad \text{(special notation)}$$

is defined inductively as follows:

- $m + 1 := S(m)$
- Supposing $m + n$ has been defined, let

$$m + S(n) = S(m+n).$$

Lemma 1. $m + 1 = 1 + m \quad \forall\, m \in \mathbb{N}$.

Pf: Induction on m:

Base case: $1 + 1 = S(1)$ by defn

$= 1 + 1$ ✓.

Induction step: Suppose $m+1 = 1+m$.

We have: $S(m)+1 = S(S(m))$ by defn. of $+$

$= S(m+1)$ "

$= S(1+m)$ by ind. hypoth.

$= 1+S(m)$ by defn of $+$.

By PMI, we're done. $\square$

Lemma 2. $S(m+n) = S(m)+n \quad \forall m,n \in \mathbb{N}$

Pf. Let $m \in \mathbb{N}$. We use induction on n:

Base case: $S(m+1) = S(S(m)) = S(m)+1$ ✓.

Induction step: Suppose $S(m+n) = S(m)+n$ for some $n \in \mathbb{N}$.

$S(m+S(n)) = S(S(m+n))$ by defn of $+$

$= S(S(m)+n)$ by ind. hyp.

$= S(m)+S(n)$ by defn of $+$.

By PMI, we conclude

$$S(m+n) = S(m)+n \quad \forall n \in \mathbb{N}.$$

Since $m \in \mathbb{N}$ was arbitrary, we're done $\square$

Theorem (Properties of addition)

(A1) If $m \in \mathbb{N}$, $n \in \mathbb{N}$ then $m + n \in \mathbb{N}$

(A2) $m + n = n + m \quad \forall\, m, n \in \mathbb{N}$

(A3) $(m+n)+p = m + (n+p) \quad \forall\, m, n, p \in \mathbb{N}$.

Pf: (A1) True since $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a function.

(A2) Let $m \in \mathbb{N}$, use induction on n.

Base case: Lemma 1.

Induction step: Suppose $m + n = n + m$.

$$\begin{aligned} m + S(n) &= S(m+n) && \text{by defn of } + \\ &= S(n+m) && \text{by induct. hyp.} \\ &= S(n) + m && \text{by Lemma 2.} \end{aligned}$$

By PMI, $m + n = n + m \;\forall\, n \in \mathbb{N}$.

Since $m \in \mathbb{N}$ was arbitrary, we're done

(A3) Exercise. (Not on HW) $\square$

<u>Definition</u>: The function $\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$$(m,n) \mapsto m \cdot n$$

is defined inductively as follows:

- $m \cdot 1 = m$
- $m \cdot S(n) = m \cdot n + m$

<u>Note</u>: $\Downarrow$ $m \cdot (n+1) = m \cdot n + m$ (Distributive prop.!)

<u>Theorem</u>. The function $\cdot$ satisfies:

(M1) $m \in \mathbb{N},\ n \in \mathbb{N} \Rightarrow m \cdot n \in \mathbb{N}$

(M2) $m \cdot n = n \cdot m$

(M3) $(m \cdot n) \cdot p = m \cdot (n \cdot p)$

(M4) $m \cdot 1 = m$.

See Landau for proofs.

We now want to e<u>xtend</u> the naturals

to allow other operations.

<u>P2.</u>

<u>Want</u>: $(m-n)$ = unique number s.t.

$$(m-n) + n = m.$$

$\rightsquigarrow$ negative #'s.

$$\mathbb{Z} = \underbrace{\mathbb{N} \sqcup \{0\} \sqcup \mathbb{N}}_{\text{disjoint union}}$$

$$= \{\underbrace{\ldots,-1}_{\text{neg. integers}},0,\underbrace{1,\ldots}_{\text{pos. integers}}\}$$

$\mathbb{N} \subset \mathbb{Z}$ is (by default) the positive integers.

Rational #'s? $\frac{2}{3} = \frac{4}{6} = \frac{8}{12} = \ldots$

$$\frac{p}{q} = \left\{ (m,n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \mid np = mq \right\}.$$

$$\frac{4}{6} = \left\{ \frac{2}{3}, \frac{-2}{-3}, \frac{4}{6}, \frac{-4}{-6}, \ldots \right\}$$

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\} \subset \mathcal{P}(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))$$

$$\mathbb{Z} \subset \mathbb{Q}$$

$$n \mapsto \frac{n}{1}.$$

<u>Definition:</u> The map $\frac{1}{(\cdot)} : \mathbb{Q} \setminus \{0\} \to \mathbb{Q} \setminus \{0\}$ is given by $\frac{p}{q} \longmapsto \frac{q}{p}$.

$$\frac{p}{q} + \frac{r}{s} := \frac{ps+qr}{qs}, \quad \frac{p}{q} \cdot \frac{r}{s} := \frac{p \cdot r}{q \cdot s}.$$

Theorem: The operations $+$ and $\cdot$ extend to $\mathbb{Q}$, satisfying (A1-3), (M1-4), (D), as well as

(A4) $0 + x = x$

(A5) $x + (-x) = 0$.

(M5) $x \cdot \left(\frac{1}{x}\right) = 1$.

Pf. See Landau. $\square$