Section 1: natural numbers

We want to *rigorously* go over the calculus material. Before integration and differentiation, we need to describe *numbers*.

$$\begin{tikzcd} \boxed{\text{Natural numbers}} \arrow[d] \\ \boxed{\text{Integers}} \arrow[d] \\ \boxed{\text{Rational numbers}} \arrow[d] \\ \boxed{\text{Real numbers}} \end{tikzcd}$$

We use *set theory* to describe the set $\mathbb{N} = \{1, 2, 3, \ldots\}$[1] of *natural numbers*, and their "good" (useful) properties.

[1] $0 \notin \mathbb{N}$

Peano Axioms (Postulates), pp. 1-2 of textbook

- **(N1)** $\mathbb{N}$ contains a *distinguished element* 1.
- **(N2)** Every $n \in \mathbb{N}$ has its *successor* in $\mathbb{N}$, denoted by $\mathbf{S}(n)$ (the book denotes the successor by $n+1$).
- **(N3)** 1 is not a successor of any element of $\mathbb{N}$.
- **(N4)** If m and n have the same successor, then $m = n$.
- **(N5)** If $A \subset \mathbb{N}$ is such that $1 \in A$, and $\mathbf{S}(n) \in A$ whenever $n \in A$, then $A = \mathbb{N}$.

The *successor map* $\mathbf{S}$ is *injective* (can you give a definition of injectivity?).

If $\mathbf{S}(n) = \mathbf{S}(m)$, then $n = m$, by (N4).

Is $\mathbf{S}$ is *surjective*? No: by (N3), no $k \in \mathbb{N}$ satisfies $\mathbf{S}(k) = 1$.

More about Peano Axioms

(N1) $\mathbb{N}$ contains a *distinguished element* 1.

(N2) Every $n \in \mathbb{N}$ has its *successor* in $\mathbb{N}$, denoted by $\mathbf{S}(n)$ (the book denotes the successor by $n+1$).

(N3) 1 is not a successor of any element of $\mathbb{N}$.

(N4) If m and n have the same successor, then $m = n$.

(N5) If $A \subset \mathbb{N}$ is such that $1 \in A$, and $\mathbf{S}(n) \in A$ whenever $n \in A$, then $A = \mathbb{N}$.

What are elements of $\mathbb{N}$ with no predecessors? 1 is the only one.

- 1 is not a successor of anything.
- Suppose, for the sake of contradiction, that $m \in \mathbb{N} \backslash \{1\}$ has no predecessor. Let $A = \mathbb{N} \backslash \{m\}$. Then (i) $1 \in A$, and (ii) if $n \in A$, then $n+1 \in A$. By (N5), $A = \mathbb{N}$, a contradiction.

Uniqueness of $\mathbb{N}$

Theorem (Uniqueness of $\mathbb{N}$)

Suppose X is a set with a distinguished element $1'$ and the successor map $\mathbf{S}'$, satisfying (N1-5). Then there exists a bijection $\Phi : \mathbb{N} \to X$ so that $\Phi(1) = 1'$, and, for every n, $\Phi(\mathbf{S}(n)) = \mathbf{S}'(\Phi(n))$.

Example of a set X satisfying the Peano Axioms.

Let $X = \{0, 1, 2, \ldots\}$ (non-negative integers), $1' = 0$, $\mathbf{S}'(x) = x + 1$.
Check: (N1-5) hold.

Define $\Phi : \mathbb{N} \to X : n \mapsto n - 1$. Then $\Phi(1) = 0 = 1'$, and

$$\Phi(\mathbf{S}(n)) = \mathbf{S}(n) - 1 = (n + 1) - 1 = (n - 1) + 1 = \mathbf{S}'(\Phi(n)).$$

All five Peano Axioms are needed to describe $\mathbb{N}$

Example of a family satisfying (N1-4), failing (N5).

Let $X = \{(a, b) : a \in \mathbb{N}, b \in \{1, 2\}\}$.

Distinguished element: $\mathbf{1} = (1, 1)$.

Successor map: $(a, b) + 1 := (a + 1, b)$.

$A = \{(a, 1) : a \in \mathbb{N}\}$ contains $\mathbf{1}$, and $n \in A \Rightarrow n + 1 \in A$.

However, $A \neq X$. So, (N5) fails; you can check that the other four axioms hold.

Mathematical induction: theory

Theorem (Principle of mathematical induction)

Suppose $(P_n)_{n \in \mathbb{N}}$ is a list of statements, and

1. *P_1 is true.*
2. *If $n \in \mathbb{N}$, and P_n is true, then P_{n+1} is true.*

Then P_n is true for any $n \in \mathbb{N}$.

Proof. Let $A = \{n \in \mathbb{N} : P_n \text{ holds }\}$. Then (1) $1 \in A$, and (2) if $n \in A$, then $n + 1 \in A$. By (N5), $A = \mathbb{N}$. ■

Mathematical induction: algorithm (from Section 1)

ALGORITHM FOR PROVING $P_1, P_2, \ldots$ BY INDUCTION:

1. *Basis for induction*: prove that P_1 holds.
2. *Induction step*: if $n \in \mathbb{N}$, and P_n [the *induction hypothesis*] holds, then P_{n+1} holds as well.

Then P_n holds for any $n \in \mathbb{N}$.

Example. Prove that, for any $n \in \mathbb{N}$, $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Notation: $\displaystyle\sum_{k=1}^{n} k = 1 + 2 + \ldots + n$.

We can use Peano Axioms to define addition (won't do this, for lack of time).

Prove: for any $n \in \mathbb{N}$, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

Proof by induction. P_n states that "$\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$."

Basis for induction. We need to verify P_1. This is easy: $1 = \frac{1(1+1)}{2}$.

Induction step. We need to show that, if $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, then $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$.

$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1)$, hence, by the induction hypothesis, $\sum_{k=1}^{n+1} k = \frac{n(n+1)}{2} + (n+1) = (n+1)\left(\frac{n}{2} + 1\right) = \frac{(n+1)(n+2)}{2}$, just as we wanted. ∎

Another example of mathematical induction

Prove that, for any $n \in \mathbb{N}$, $5 \mid 6^n - 1$.

$a \mid b$ means "a divides b."

Proof. Use induction; P_n reads "$5 \mid 6^n - 1$."

Basis for induction. Verify P_1: 5 divides $6^1 - 1 = 5$.

Induction step. Show that, if $5 \mid 6^n - 1$ (this is our induction hypothesis), then $5 \mid 6^{n+1} - 1$.
Need to connect $6^{n+1} - 1$ with $6^n - 1$.
Write $6^{n+1} - 1 = 6 \cdot 6^n - 1 = 6(6^n - 1) + 5$.
If $5 \mid 6^n - 1$, then $5 \mid 6(6^n - 1) + 5$. $\blacksquare$

The set $\mathbb{Z}$ of integers (Section 2)

This topic will be covered in the next lecture

We are not trying to *construct* $\mathbb{Z}$ from $\mathbb{N}$; however, we *describe* properties of $\mathbb{Z}$.

Addition: an operation $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, and $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Properties of addition on $\mathbb{Z}$

(A1) Associativity: for $a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$.

(A2) Commutativity: for $a, b \in \mathbb{Z}$, $a + b = b + a$.

(A3) Existence of neutral element: $\exists$ element $0 \in \mathbb{Z}$ s.t. $0 + a = a$ $\forall\, a \in \mathbb{Z}$.

(A4) Existence of opposite: $\forall\, a \in \mathbb{Z}\ \exists\ x \in \mathbb{Z}$ s.t. $a + x = 0$ (this x is denoted by $-a$).

Why is $\mathbb{Z}$ better than $\mathbb{N}$?

Properties of addition on $\mathbb{Z}$

(A1) Associativity: for $a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$.

(A2) Commutativity: for $a, b \in \mathbb{Z}$, $a + b = b + a$.

(A3) Existence of neutral element: $\exists$ element $0 \in \mathbb{Z}$ s.t. $0 + a = a$ $\forall\, a \in \mathbb{Z}$.

(A4) Existence of opposite: $\forall\, a \in \mathbb{Z}\ \exists\, x \in \mathbb{Z}$ s.t. $a + x = 0$ (this x is denoted by $-a$).

(A1), (A2) hold for $\mathbb{N}$ as well. However, (A3), (A4) fail for $\mathbb{N}$.
$\mathbb{Z}$ is "better" than $\mathbb{N}$.

If $+ : S \times S \to S$ satisfies (A1-4), then $(S, +, 0)$ is called an abelian (commutative) group.

Examples of abelian groups: $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$.

Uniqueness of 0 and $-a$; subtraction

Observation. The neutral element is unique.

Proof. If $0, 0'$ are neutral elements, then $0 = 0 + 0' = 0'$. ■

Observation. For $a \in \mathbb{Z}$, its opposite $-a$ is unique.

Proof. Suppose $a + x = 0 = a + x'$. Then
$x = x + 0 = x + (a + x') = (x + a) + x' = 0 + x' = x'$. ■

Observation. For $a, b \in \mathbb{Z}$, there exists a unique $x \in \mathbb{Z}$ s.t. $a + x = b$. We denote this x by $b - a$.

Proof. (1) Existence. Take $x = b + (-a)$, then
$x + a = \big(b + (-a)\big) + a = b + \big((-a) + a\big) = b + 0 = b$.

(2) Uniqueness. If $a + x = b$, then $(a + x) + (-a) = b + (-a)$.
LHS $= (x + a) + (-a) = x + \big(a + (-a)\big) = x + 0 = x$, so $x = b + (-a)$. ■

$\mathbb{N}$ has only addition, but no subtraction, due to the lack of (A3-4).