To do analysis we need
- natural numbers \( \mathbb{N} = \{1, 2, 3, \ldots\} \), a.k.a. positive integers
- integers \( \mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\} \)
- rational numbers \( \mathbb{Q} = \{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\} \)
- real numbers \( \mathbb{R} \)

One can construct \( \mathbb{N} \) using finite sets + set theory
- construct \( \mathbb{Z} \) out of \( \mathbb{N} \) + algebra
- construct \( \mathbb{Q} \) out of \( \mathbb{Z} \) + algebra
- construct \( \mathbb{R} \) out of \( \mathbb{Q} \) + metric topology/analysis

Alternatively (this is what the textbook does)
One writes down the characteristic properties of \( \mathbb{N} \)
(Peano axioms)

First, a definition
(Given a natural number \( n \) we call \( n+1 \) its successor)

<table>
<thead>
<tr>
<th>Successor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intuition: start with 1; it has the successor 2, which has the successor 3, ... keep on going; get all natural numbers this way</td>
</tr>
</tbody>
</table>

Peano axioms for \( \mathbb{N} \)

\( N_1 \) 1 belongs to \( \mathbb{N} \)
\( N_2 \) If \( n \) belongs to \( \mathbb{N} \) its successor \( n+1 \) belongs to \( \mathbb{N} \)
\( N_3 \) \( 1 \) is not a successor of any natural number: \( \forall n \in \mathbb{N} \) so that \( n+1 \neq 1 \)
N4. If $n+1 = m+1$ then $n = m$.

N5. If $S \subseteq \mathbb{N}$ a subset with (a) $1 \in S$ and (b) $n \in S \implies n+1 \in S$ then $S = \mathbb{N}$.

Comment: One can use N1-N5 to construct/define $+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (addition of positive numbers).

The textbook and we won't do it.

Comment 2. Axiom/property N5: "*Induction*"

Recall a typical formulation:

- Suppose that for each $n \in \mathbb{N}$ we have a statement $P_n$.
- Moreover suppose that
  
  (Ii) $P_1$ is true
  
  (Iii) if $P_n$ is true then $P_{n+1}$ is true (i.e., $P_n \implies P_{n+1}$)

- Conclusion: $P_n$ is true for all $n$.

Example $P_n$: $| \sin nx | \leq n | \sin x |$ for all $x \in \mathbb{R}$

Is $P_n$ true for all $n$?

\(P_1\): $| \sin 1 \cdot x | \leq 1 \cdot | \sin x |$ \quad \text{yes.}

\(P_n \implies P_{n+1}\):

\[ | \sin (n+1) x | = (| \sin (nx + x) | = | \sin nx \cos x + \cos nx \sin x | \leq | \sin nx \cos x | + | \cos nx \sin x | \]

\[= (| \sin nx | \cdot | \cos x | + | \cos nx | \cdot | \sin x |) \leq n | \sin x | + | \sin x | \]

\[\leq | \sin nx | + | \sin x | \leq n | \sin x | + | \sin x | \]

\[\implies \leq (n+1) | \sin x |. \quad \text{So yes.} \]

Conclusion: $| \sin nx | \leq n | \sin x |$ for all $n$. 
Example 6 \mid 7^n - 1 for all n \in \mathbb{N}.

Proof \(P_1\) 6 \mid (7^1 - 1) \checkmark

\((P_n \lor P_{n+1})\) Suppose 6 \mid (7^n - 1). Then

\[7^{n+1} - 1 = 7 \cdot 7^n - 1 = (6+1)7^n - 1 = 6 \cdot 7^n + (7^n - 1)\]

Since 6 \mid 6 \cdot 7^n and since 6 \mid (7^n - 1) by assumption

6 \mid (6 \cdot 7^n + (7^n - 1)) = 7^{n+1} - 1. So \(P_n \lor P_{n+1}\)

Conclusion 6 \mid 7^k - 1 for all k \in \mathbb{N}.

Why is \(\mathbb{N}\) “better” than \(\mathbb{N}\)?

Both sets have an operation + which is associative. In \(\mathbb{Z}\) an equation

\[a + x = b\]

always has a solution: \(x = b + (-a)\)

(In \(\mathbb{N}\) such an \(x\) need not exist: \(\# x \in \mathbb{N}\),

\[4 + x = 2\]

Four properties of +: \(\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}\).

\[A_1\quad a + (b + c) = (a + b) + c\]

for all \(a, b, c \in \mathbb{Z}\)

\[A_2\quad a + b = b + a\]

\[A_3\quad \exists 0\] so that \(0 + n = n = n + 0\) for all \(n \in \mathbb{Z}\).
For each $a \in \mathbb{Z}$ there is be $\mathbb{Z}$ so that $a + b = 0$.

(equivalently: for equation $a + x = 0$ has a solution
One usually writes $-a$ for such $b$.

Comments 1) A1 and A2 hold for $N$; A3 and A4 do not.

2) If $S$ is a set with an operation $+: S \times S \rightarrow S$

satisfying A1, A2, A3, A4, $S$ is called an **abelian group**.

So A1-A4 say: "$\mathbb{Z}$, $+$, 0) is an abelian group"

There are many more abelian groups:

$(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$ are also abelian groups.

$N$ and $\mathbb{Z}$ have another operation $\cdot$ (times).

It "plays well" with addition. Here are the properties of $\cdot$:

\[ M_1 \] $a \cdot (bc) = (ab) \cdot c \quad \forall a, b, c$

\[ M_2 \] $a \cdot b = b \cdot a \quad \forall a, b$

\[ M_3 \] There is 1 so that $1 \cdot a = a$ for all $a$.

\[ DL \] $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Comment: M1, M2, M3, DL (together with A1-A4) say:

"$\mathbb{Z}$ is a commutative ring"

More pedantically:

"$(\mathbb{Z}, +, 0, \cdot, 1)$ is a commutative ring"
However in \( \mathbb{Z} \), for \( a \neq 1 \):
\[
a \cdot x = 1
\]
has no solutions. Thus \( \mathbb{Q} \) and \( \mathbb{R} \) are "better".

For any \( a \neq 0 \), \( \exists x \) so that \( ax = 1 \).

**Comments:** Such solution \( x \) is usually denoted by \( a^{-1} \).

- A commutative ring \((\mathbb{R}, +, 0, \cdot)\) so that
- \( M_4 \) also holds is called a field.

**Examples:** \( \mathbb{Q}, \mathbb{R} \) are fields, \( \mathbb{Z} \) is not.

**Why is \( \mathbb{Q} \) "better" than \( \mathbb{R} \)?**

**Proposition** The equation \( x^2 = 2 \) has no solutions in \( \mathbb{Q} \).

**Comments:** We'll see later that it does have real solutions; they are called \( \pm \sqrt{2} \).

- Our proof uses the following property of 2:
  
  \[(*)\]  
  \[
  \text{If } 2 \text{ divides } n \cdot m \ (n, m \in \mathbb{Z}) \text{ then either } 2 \text{ divides } n \text{ or } 2 \text{ divides } m.
  \]

**Proof** Suppose \( \frac{p}{q} \in \mathbb{Q} \) solves \( x^2 = 2 \), where \( p, q \in \mathbb{Z} \). May assume: \( p \) and \( q \) are relatively prime, i.e., no common factors.
Then \( \left( \frac{p}{q} \right)^2 = 2 \Rightarrow p^2 = 2q^2 \)

\[ \Rightarrow 2 \mid p^2 = p \cdot p \Rightarrow 2 \mid p \text{ or } 2 \mid q \text{ i.e. } 2 \mid p. \]

\[ \Rightarrow p = 2n \text{ for some } n \in \mathbb{N}. \]

\[ \Rightarrow (2n)^2 = 2q^2 \]

\[ \Rightarrow 2n^2 = q^2 \]

\[ \Rightarrow 2 \mid q^2 \quad (\ast) \quad 2 \mid q. \]

**Contradiction:** We assumed \( p \neq q \) have no common factors.

**Conclusion:** There is no \( \frac{p}{q} \in \mathbb{Q} \) so that \( \left( \frac{p}{q} \right)^2 = 2 \).