Why do we learn and teach foundations wrongly?

According to Spivak’s *Calculus* (2d ed., 1980):

Ch. 1 **Numbers** have twelve “simple and obvious properties”.

Ch. 27 These are the defining properties of an **ordered field**.

Ch. 1 Without ordering, one cannot prove $1 + 1 \neq 0$: consider $\mathbb{F}_2$.

Ch. 8 $\mathbb{R}$ has the **least upper bound property**.

Ch. 28 $\mathbb{R}$ is constructed from $\mathbb{Q}$.

Ch. 2 The **natural numbers** are 1, 2, 3, ...; these compose $\mathbb{N}$.

“Basic assumptions” about the natural numbers are the

- principle of **mathematical induction**, 
- **well-ordering** principle, and
- principle of **“complete” induction**, namely $A = \mathbb{N}$ if $1 \in A$ and $\{1, \ldots, k\} \subseteq A \implies k + 1 \in A$.

From each “basic assumption,” the others can be proved. **No!**
The “basic assumptions” are not equivalent.

1. Induction is about \((\mathbb{N}, 1, x \mapsto x + 1)\).
2. Well-ordering is about \((\mathbb{N}, \leq)\).
3. “Complete” induction (à la Spivak) is about \((\mathbb{N}, \leq, 1, x \mapsto x + 1)\).

Each is logically distinguishable from the others by appropriate models (as \(\mathbf{F}_2\) shows the field-axioms do not imply \(1 + 1 \neq 0\)):

- Only induction works in \(\mathbb{Z}/(2)\): the transitive closure of \(x \mapsto x + 1\) is not an ordering.
- The proper subset \(\omega\) of \(\omega + \omega\) is closed under 0 and \(x \mapsto x \cup \{x\}\), but the transitive closure of the latter is a well-ordering.

Induction involves quantification over all subsets of \(\mathbb{N}\).

Why not define \(\mathbb{N}\) by quantification over all supersets of \(\mathbb{N}\)? That is,

\[
\mathbb{N} = \bigcap \{X \subseteq \mathbb{R} : 1 \in X \land \forall y (y \in X \Rightarrow y + 1 \in X)\}.
\]

Then induction, well-ordering, and complete induction follow from this.
Dedekind gets things straight in *The Nature and Meaning of Numbers* (1887, 1893):

“59. Theorem of **complete induction.** In order to show that the chain $A_o$ [that is, $\bigcap\{X: A \subseteq X \& \phi[X] \subseteq X\}$] is part of any system $\Sigma$...it is sufficient to show,

- $\rho.$ that $A \nexists \Sigma$, and $[A \subseteq \Sigma]$
- $\sigma.$ that the transform of every common element of $A_o$ and $\Sigma$ is likewise element of $\Sigma$.”

“71...the essence of a **simply infinite system** $N$ consists in the existence of a transformation $\phi$ of $N$ and an element 1 which satisfy the following conditions $\alpha, \beta, \gamma, \delta$:

- $\alpha.$ $N' \nexists N$. $[\phi[N] \subseteq N]$
- $\beta.$ $N = 1_o$. $[N = \bigcap\{X \subseteq N: 1 \in X \& \phi[X] \subseteq X\}]$
- $\gamma.$ The element 1 is not contained in $N'$. $[1 \notin \phi[N]]$
- $\delta.$ The transformation $\phi$ is similar.” $[\phi$ is injective$]$
“126. Theorem of the **definition by induction**. If there is given a... transformation $\theta$ of a system $\Omega$ into itself, and besides a determinate element $\omega$ in $\Omega$, then there exists one and only one transformation $\psi$ of the number-series $N$, which satisfies the conditions

I. $\psi(N) \not\in \Omega$ \\
[\(\psi[N] \subseteq \Omega\)] \\
II. $\psi(1) = \omega$ \\
III. $\psi(n') = \theta \psi(n)$, where $n$ represents every number.”

That is, from $(N, \phi, 1)$ to $(\Omega, \theta, \omega)$ there is a unique homomorphism.

“130. Remark... it is worth while to call attention to a circumstance in which [**definition by induction (126)**] is essentially distinguished from the theorem of **demonstration by induction** [(59)], however close may seem the relation between the former and the latter...”

In particular,

- $\mathbb{Z}/(2)$ allows demonstration by induction; but
- there is no homomorphism from $\mathbb{Z}/(2)$ into $\mathbb{Z}/(3)$. 
Peano (1889) acknowledges Dedekind.

For every $a$ in $\mathbb{N}$, there is a successor $a + 1 \in \mathbb{N}$. Then Peano defines

$$a + (b + 1) = (a + b) + 1.$$  \hfill (\ast)

This defines *instances* of $a + (b + 1)$; assuming:

1. that $b + 1$ uniquely determines $b$;
2. that $a + b$ is already defined;
3. that $a + (b + 1)$ is *not* already defined.

By induction, all $a + b$ can be defined. But it is not immediate that (\ast) holds for all $a$ and $b$ in $\mathbb{N}$, because of (3).

Dedekind’s (126) gives addition satisfying (\ast) immediately.

Following Kalmár, Landau (1929) shows implicitly that addition *can* be defined with induction alone. Hence it can be defined on finite structures:
Likewise, the recursive definition of multiplication,

\[ a \times 1 = a, \quad a \times (b + 1) = a \times b + a, \]
is justified by induction alone. However:

**Theorem.** The identities

\[ a^1 = a, \quad a^{b+1} = a^b \times a \]

hold on \( \mathbb{Z}/(n) \) if and only if \( |n| \in \{0, 1, 2, 6\} \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( n^2 )</th>
<th>( n^3 )</th>
<th>( n^4 )</th>
<th>( n^5 )</th>
<th>( n^6 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

In \( \mathbb{Z}/(6) \): 

\[
\begin{array}{cccccc}
2 & 3 & 4 & 4 & 4 & 4 \\
5 & 1 & 5 & 1 & 5 & 1 \\
\end{array}
\]

In \( \mathbb{Z}/(3) \):

\[
\begin{array}{cccccccc}
\hline
n & n^2 & n^3 & n^3 \times n & n^4 \\
\hline
2 & 1 & 2 & 1 & 2 \\
\end{array}
\]

**Alexandre Borovik:** Detecting a failure of \((\dagger)\) modulo \( pq \) gives a 1/4 chance of factorizing \( pq \). See *A Dialogue on Infinity*,

http://dialinf.wordpress.com/
Mac Lane & Birkhoff, *Algebra* (1st ed. 1967):

P. 35  ‘Peano Postulates’ for \((\mathbb{N}, 0, \sigma)\):

(i) \(\sigma\) is injective;

(ii) \(0 \notin \sigma(\mathbb{N})\);

(iii) if \(0 \in U\), and \(n \in U \Rightarrow \sigma(n) \in U\), then \(U = \mathbb{N}\).

P. 36  Natural numbers index iterates of an operation \(f\) on a set \(X\):

\[
f^0 = 1_X, \quad f^{\sigma n} = f \circ f^n.
\]

P. 38  Any two of the Postulates have a model in which the third fails.

P. 67  The possibility of recursive definitions is the Peano–Lawvere Axiom (or Dedekind–Peano Axiom in Lawvere & Rosebrugh 2003); this is logically equivalent to the three ‘Peano Postulates’.

A more general setting: SENTENTIAL LOGIC

Let $\mathcal{V}$ be a set $\{ P, P', P'', P''', \ldots \}$ of sentential variables.

Let $\mathcal{S}$ be the set of sentences generated from $\mathcal{V}$ by closing under

$$X \xleftarrow{N} \sim X \quad \text{and} \quad (X, Y) \xleftarrow{C} (X \Rightarrow Y).$$

Then $\mathcal{S}$ admits proof by induction, as e.g. in showing that parentheses come in pairs.

Moreover, $N$ and $C$ are injective, and

$$\mathcal{S} = \mathcal{V} + C[\mathcal{S}] + C[\mathcal{S} \times \mathcal{S}]$$

(disjoint union). Therefore $\mathcal{S}$ admits definition by recursion.

For example, truth assignments are so defined: If $\phi : \mathcal{V} \rightarrow F_2$, we extend to all of $\mathcal{S}$ by

$$\phi(\sim X) = 1 + \phi(X), \quad \phi((X \Rightarrow Y)) = 1 + \phi(X) + \phi(X)\phi(Y).$$
Also Detachment is given recursively by

\[ D(X, U) = U, \quad \text{if } U \in V, \]
\[ D(X, \sim Y) = \sim Y, \]
\[ D(X, (Y \Rightarrow Z)) = \begin{cases} 
Z, & \text{if } X = Y, \\
(Y \Rightarrow Z), & \text{otherwise.}
\end{cases} \]

Let the set \( \mathcal{T} \) of theorems be the subset of \( \mathcal{S} \) generated by closure under \( D \) of some axioms, perhaps

\[ ((X \Rightarrow (Y \Rightarrow X)), \]
\[ (((X \Rightarrow (Y \Rightarrow (X \Rightarrow Z)))) \Rightarrow ((X \Rightarrow (Y \Rightarrow Z)) \Rightarrow ((X \Rightarrow (Y \Rightarrow (X \Rightarrow Z))))). \]

Then \( \mathcal{T} \) admits proof by induction, but not definition of functions by recursion.

Hence the non-triviality of decision problems.
ALGEBRAIC CHARACTERIZATIONS

Let $\Sigma$ be a set, and $n: \Sigma \to \omega$.

An algebra with signature $\Sigma$ is a pair

$$(A, s \mapsto s^A)$$

or $\mathfrak{A}$, where $A$ is a nonempty set, $s$ ranges over $\Sigma$, and $s^A: A^n(s) \to A$.

The term algebra on $B$ with signature $\Sigma$ is the set of strings obtained by closing $B$ under each function

$$(t_1, \ldots, t_{n(s)}) \mapsto st_1 \cdots t_{n(s)}.$$ 

Call this algebra $\text{Tm}_\Sigma(B)$.

An algebra $\mathfrak{A}$ with signature $\Sigma$ admits

- **proof by induction**, if $\mathfrak{A} \cong \text{Tm}_\Sigma(\emptyset)/\mathcal{I}$ for some congruence $\mathcal{I}$;
- **definition by recursion**, if $\mathfrak{A} \cong \text{Tm}_\Sigma(\emptyset)$.

Again, http://dialinf.wordpress.com/