INDUCTION AND RECURSION David Pierce Bern, 2008

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 $\mathbf{F}_2$.

Ch. 8 **R** has the **least upper bound property.**

Ch. 28 **R** is constructed from **Q**.

Ch. 2 The **natural numbers** are 1, 2, 3, . . . ; these compose **N**.

"Basic assumptions" about the natural numbers are the

- principle of **mathematical induction,**
- **well-ordering** principle, and
- principle of **"complete" induction,** namely $A = \mathbf{N}$ if $1 \in A$ and

$$\{1, \dots, k\} \subseteq A \implies k + 1 \in A.$$

From each "basic assumption," the others can be proved. **No!**

The “basic assumptions” are *not* equivalent.

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

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 $\mathbf{Z}/(2)$: the transitive closure of $x \mapsto x+1$ is not an ordering.
- The proper subset $\boldsymbol{\omega}$ of $\boldsymbol{\omega}+\boldsymbol{\omega}$ 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 $\mathbf{N}$.

Why not *define* $\mathbf{N}$ by quantification over all supersets of $\mathbf{N}$? That is,

$$\mathbf{N} = \bigcap \{X \subseteq \mathbf{R} \colon 1 \in X \;\&\; \forall y \; (y \in X \Rightarrow y+1 \in X)\}.$$

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 Σ... it is sufficient to show,

ρ. that $A \mathfrak{Z} \Sigma$, and $[A \subseteq \Sigma]$

σ. that the transform of every common element of A_o and Σ is likewise element of Σ." $[\phi[A_o \cap \Sigma] \subseteq \Sigma]$

"71... the essence of a **simply infinite system** N consists in the existence of a transformation ϕ of N and an element 1 which satisfy the following conditions **α, β, γ, δ**:

α. $N' \mathfrak{Z} N$. $[\phi[N] \subseteq N]$

β. $N = 1_o$. $[N = \bigcap\{X \subseteq N : 1 \in X \ \& \ \phi[X] \subseteq X\}]$

γ. The element 1 is not contained in N'. $[1 \notin \phi[N]]$

δ. The transformation ϕ is similar." [ϕ is injective]

These are the **'Peano axioms'** before Peano.

“126. Theorem of the **definition by induction.** If there is given a... transformation θ of a system Ω into itself, and besides a determinate element ω in Ω, then there exists one and only one transformation ψ of the number-series N, which satisfies the conditions

I. $\psi(N)\ \mathfrak{Z}\ \Omega$ $\qquad [\psi[N] \subseteq \Omega]$

II. $\psi(1) = \omega$

III. $\psi(n') = \theta\psi(n)$, where n represents every number.”

That is, from $(\mathbf{N}, \phi, 1)$ to (Ω, θ, ω) 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,

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

Peano (1889) acknowledges Dedekind.

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

$$a + (b + 1) = (a + b) + 1. \tag{$*$}$$

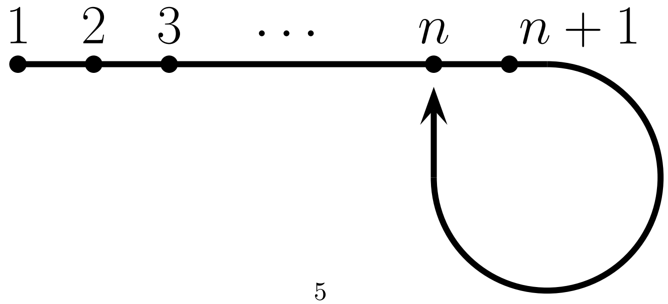
This defines *instances* of $a + (b + 1)$; assuming:

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 $(*)$ holds for all a and b in $\mathbf{N}$, because of (3).

Dedekind's (126) gives addition satisfying $(*)$ 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,

$$a \times 1 = a, \qquad a \times (b+1) = a \times b + a,$$

is justified by induction alone. However:

Theorem. *The identities*

$$a^1 = a, \qquad a^{b+1} = a^b \times a \tag{$\dagger$}$$

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

In $\mathbf{Z}/(6)$:

n	n^2	n^3	n^4	n^5	n^6
2	4	2	4	2	4
3	3	3	3	3	3
4	4	4	4	4	4
5	1	5	1	5	1

In $\mathbf{Z}/(3)$:

n	n^2	n^3	$n^3 \times n$	n^4
2	1	2	1	2

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 $(\mathbf{N}, 0, \sigma)$:

(i) σ is injective;

(ii) $0 \notin \sigma_*(\mathbf{N})$;

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

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

$$f^0 = 1_X, \qquad f^{\sigma n} = f \circ f^n.$$

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'.

See also Burris, *Logic for Mathematics and Computer Science* (1998).

A more general setting: SENTENTIAL LOGIC

Cf. Thomas Forster, *Logic, Induction, and Sets* (2003).

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

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

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

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 $\phi\colon \mathcal{V} \to \mathbf{F}_2$, we extend to all of $\mathcal{S}$ by

$$\phi(\sim X) = 1 + \phi(X), \qquad \phi((X \Rightarrow Y)) = 1 + \phi(X) + \phi(X)\phi(Y).$$

Also **Detachment** is given recursively by

$$
\begin{aligned}
D(X, U) &= U, \qquad \text{if } U \in \mathcal{V}, \\
D(X, \sim Y) &= \sim Y, \\
D(X, (Y \Rightarrow Z)) &= \begin{cases} Z, & \text{if } X = Y, \\ (Y \Rightarrow Z), & \text{otherwise.} \end{cases}
\end{aligned}
$$

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

$$
\begin{gathered}
(X \Rightarrow (Y \Rightarrow X)), \\
((\sim X \Rightarrow \sim Y) \Rightarrow (Y \Rightarrow X)), \\
((X \Rightarrow (Y \Rightarrow Z)) \Rightarrow ((X \Rightarrow Y) \Rightarrow (X \Rightarrow Z))).
\end{gathered}
$$

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

Hence the non-triviality of decision problems.

ALGEBRAIC CHARACTERIZATIONS

Let Σ be a set, and $n\colon \Sigma \to \boldsymbol{\omega}$.

An **algebra** with **signature** Σ is a pair

$$(A, s \mapsto s^{\mathfrak{A}})$$

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

The **term algebra** on B with signature Σ is the set of strings obtained by closing B under each function

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

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

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

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

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