Lecture 2

Tuesday, September 29, 2020 12:05 PM

Lecture 2: Axioms & Properties of $\mathbb{Z}$ and $\mathbb{N}$

§1. Axioms for $\mathbb{Z}$

assume to be true

$\mathbb{Z}$ a set with two operations $+$ and $\cdot$.
integers (Zahlen) sum product

(A1) $+$ is commutative, associative $\forall n,m,p \in \mathbb{Z}$: $(n+m)+p = n+(m+p)$,
$\cdot$ is commutative, associative and distributive property. $\forall n,m,p \in \mathbb{Z}$: $m\cdot(n+p) = m\cdot n + m\cdot p$.

exists

(A2) $\exists\, 0 \in \mathbb{Z}$ s.t. $\forall m \in \mathbb{Z}$ we have $m+0=m$.

(A3) $\exists\, 1 \in \mathbb{Z}$ s.t. $1 \neq 0$ and $\forall m \in \mathbb{Z}$ we have $m\cdot 1 = m$.

(A4) For each $m \in \mathbb{Z}$ $\exists\, (-m) \in \mathbb{Z}$ s.t. $m + (-m) = 0$.
depends

(A5) Let $m,n,p \in \mathbb{Z}$ s.t. (1) $m \neq 0$ (2) $m\cdot n = m\cdot p$ then $n = p$.

§2. Properties of $\mathbb{Z}$: your task is to deduce the statements in Prop. 16 through 1.27 from the axioms.

↳ e.g. we don't yet know 0 is unique, 1 is unique, is $0+m=m$?

Prop. 1.9.: Let $m,n,p \in \mathbb{Z}$ (given). $\boxed{\text{If } m+n = m+p,}$ then $\boxed{n=p}$. ← conclusion
assumption start use Axioms ↳ end

Proof: By (A4) $\exists(-m)$ s.t. $m+(-m)=0$. Since $\boxed{m+n = m+p}$ we can sum $(-m)$ on both sides and obtain $(m+n+(-m)) = m+p+(-m)$. (*)

Now we use A1 (commutative addition) so rewrite (*) as $n+m+(-m) = p+m+(-m)$.

Then (A4) implies $n+0 = p+0$. By (A2) $n+0=n$ and $p+0=p$. $\boxed{\text{Thus } n=p}$. ∎

§3. Axiom for $\mathbb{N}$.

note that $0 \in \mathbb{Z}$ but no order (no $\leq, \geq$) yet.
↳ add axiom to define $\mathbb{N}$.

Axiom (2.1): $\exists\, \mathbb{N} \subseteq \mathbb{Z}$ (in) a subset s.t.

(i) If $m,n \in \mathbb{N}$ then $m+n \in \mathbb{N}$. (ii) If $n,m \in \mathbb{N}$, then $n\cdot m \in \mathbb{N}$.

(iii) $0 \notin \mathbb{N}$ (iv) $\forall m \in \mathbb{Z}$, then $m \in \mathbb{N}$, $m = 0$ OR $-m \in \mathbb{N}$. ($\exists$ by (A4))

Remarks (1) we'll use A2.1 to introduce an order in $\mathbb{Z}$ and then do INDUCTION

(2) A2.1(iv) does not say that only one happens (of $m \in \mathbb{N}$, $m=0$, $-m \in \mathbb{N}$). Rather uniqueness follows from Axioms. (PROOF BY CONTRADICTION)
↳ PROOF OF Prop. 2.2. shows only one is true