ANALYSIS I EXTENSION LECTURE
3.ARITHMETIC ON $\mathbb{N}$

ASILATA BAPAT

Addition

How can we make sense of "$1+2=3$" if $1=\{\varnothing\}$ and $2=\{\varnothing,\{\varnothing\}\}$? The strategy is to define a function of "addition of m" for every $m \in \mathbb{N}$.

Theorem. *For every $m \in \mathbb{N}$, there exists a function $S_m \subseteq \mathbb{N}\times\mathbb{N}$ such that*

(1) $S_m(0)=m$

(2) $\forall n \in \mathbb{N}$, $S_m(n^+)=(S_m(n))^+$

Proof. First we show that there exists at least one <u>relation</u> $S'_m \subseteq \mathbb{N}\times\mathbb{N}$ with the "right" properties. Then we show that S'_m is a function. Define

$$S_m := \left\{ R \subseteq \mathbb{N}\times\mathbb{N} \;\middle|\; (0,m)\in R \text{ and if } (n,x)\in R \text{ then } (n^+,m^+)\in R \right\}$$

$S_m \neq \varnothing$ because $\mathbb{N}\times\mathbb{N}\in S_m$. Set

$$S'_m := \bigcap_{R\in S_m} R$$

S'_m is the smallest relation with the properties. We will **show that S'_m is indeed a function.** It has the required properties by construction.

(1) <u>We need to show Domain(S'_m) $=\mathbb{N}$.</u>

Let $p(n)$ be true if $\exists x$ s. t. $(n,x)\in S'_m$. It is obvious that $p(0)$ is true because $(0,m)\in S'_m$. Suppose $p(n)$ is true if $\exists x\in\mathbb{N}$ s. t. $(n,x)\in S'_m$. So $\forall R\in S_m$, $(n,x)\in R \implies (n^+,x^+)\in R \implies (n^+,x^+)\in S'_m \implies p(n^+)$ is true. So by induction, Domain$(S'_m)=\mathbb{N}$.

(2) <u>We need to show that if $(n,x),(n,y)$ are both in S'_m, then $x=y$.</u>

Let $p(n)$ be true: $\forall r\in n$, there exists a unique $x\in\mathbb{N}$ s. t. $(r,x)\in S'_m$. Note that $p(0)$ is vacuously true.

Suppose $p(n)$ is true, we want to show $p(n^+)$ is also true. Let $r\in n^+=n\cup\{n\}$. This means that $r=n$ or $r\in n$. If $r\in n$, we already know the statement is true; If $r=n$, suppose that $(n,a)\in S'_m$ and $(n,b)\in S'_m$.

Claim. *At most one of (n,a) and (n,b) can have a "predecessor" in S'_m.*

Suppose $(p_1,x_1)\in S'_m$ and $(p_2,x_2)\in S'_m$ s. t. $(p_1^+,x_1^+)=(n,a)$ and $(p_2^+,x_2^+)=(n,b)$. Since $p_1^+=p_2^+=n$, we have $p_1=p_2$ and $p_1\in n \implies (p_1,x_1)\in S'_m$ and $(p_2,x_2)\in S'_m$ imply $x_1=x_2$. So, $a=x_1^+$ and $b=x_2^+ \implies a=b$. If $a\neq b$, either $\nexists(p_1^+,x_1^+)=(n,a)$ or $\nexists(p_2^+,x_2^+)=(n,b)$.

Suppose (WLOG) $\nexists p_1$ s. t. $(p_1^+, x_1^+) = (n, a)$ and $(p_1, x_1) \in S'_m$, then we can <u>remove</u> (n, a) from S'_m by defining $S''_m := S'_m - (n, a)$ and we get a smaller relation with the same properties! This cannot happen because S'_m is the intersection of all R, which implies $S'_m \subset S''_m$

So, by (1) and (2), $\exists! a$ s. t. $(n, a) \in S'_m$, and so $p(n^+)$ also is true $\implies$ S'_m is a function with the desired properties S_m. $\square$

We can now prove the following facts:

(1) $\forall n \in \mathbb{N}$, $S_1(n) = n^+$.

(2) $\forall n \in \mathbb{N}$, $S_0(n) = n$.

(3) $\forall m, n, k \in \mathbb{N}$, we have $S_{S_m(n)}(k) = S_m\left(S_n(k)\right)$ (associativity)

(4) $\forall m, n \in \mathbb{N}$, we have $S_m(n) = S_n(m)$ (commutativity)

All properties are proved by induction.

Proof of (1) Let $p(n)$ be true if $S_1(n) = n^+$. $S_1(0) = 1 = 0^+$. So $p(0)$ is true. Suppose $p(n)$ is true. Then

$$S_1(n^+) = [S_1(n)]^+ = (n^+)^+$$

So $p(n^+)$ is true $\to$ induction.

Proof of (2) Let $p(n)$ be true if $S_0(n) = n$. $p(0)$ is true because $S_0(0) = 0$. Let $p(n)$ be true. Then

$$S_0(n^+) = [S_0(n)]^+ = n^+$$

So $p(n+)$ also is true $\to$ induction.

Proof of (3) Let $p(k)$ be true if $\forall m, n$ we have $S_{S_m(n)}(k) = S_m\left(S_n(k)\right)$. For $k = 0$, $S_{S_m(0)} = S_m(n)$; $S_m(S_n(0)) S_m(n) = S_{S_m(0)}$. So $p(0)$ is true. Suppose $p(k)$ is true. Then

$$S_{S_m(n)}(k^+) = \left[S_{S_m(n)}(k)\right]^+ = \left[S_m(S_n(k))\right]^+ = S_m\left[(S_n(k))^+\right] = S_m\left(S_n(k^+)\right)$$

So $p(k^+)$ is true$\to$ induction.

Proof of (4) Let $p(n)$ be true $\forall m \in n$, we have $S_m(n) = S_n(m)$. For $n = 0$, $S_m(0) = m = S_0(m)$. So $p(0)$ is true. Suppose $p(n)$ is true.

$$S_m(n^+) = [S_m(n)]^+ = [S_n(m)]^+ = S_n(m^+) = S_n(S_1(m)) = S_{S_n(1)}(m) = S_{S_1(n)}(m) = S_{n^+}(m)$$

So $p(n^+)$ is true $\to$ induction.

There are some more properties of $\mathbb{N}$.

(1) If $m, n \in \mathbb{N}$, $m \in n$ iff $m \subsetneq n$.

(2) If $m, n \in \mathbb{N}$, we say that $m < n$ if $m \in n$, and $m \leq n$ if $m \in n$ or $m = n$. Then $\forall M, N \in \mathbb{N}$, exactly one of the following is true (Trichotomy):

$$m < n \ \underline{\text{or}}\ n < m \ \underline{\text{or}}\ m = n$$

(3) For every $m, n\mathbb{N}$, we have $m \leq n$ iff there is a unique $k \in \mathbb{N}$ such that $m + k = n$

(4) For every $m, n, k \in \mathbb{N}$, if $n + m = n + k$ then $m = k$ (Cancellation).

Subtraction and Multiplication

Definition (Subtruction)**.** Given $m, n\mathbb{N}$, such that $m \leq n$, define $n - m$ to be the unique $k \in \mathbb{N}$ such that $m + k = n$

Remark. This satisfies the usual properties.

Multiplication is defined similarly to addition. Fix $m \in \mathbb{N}$, then $\exists$ a function $P_m : \mathbb{N} \mapsto \mathbb{N}$ with the following properties:

(1) $P_m(0) = 0$

(2) $P_m(n^+) = P_m(n) + m$

(Proved analogously to S_m)
We eventually write $P_m(n)$ as $m \cdot n$ or mn.

Multiplication satisfies the following properties: $\forall m, n, k \in \mathbb{N}$

(1) $P_m(0) = 0$

(2) $P_1(n) = n$

(3) $P_m(n) = P_n(m)$ (commutativity)

(4) $P_m\left(P_n(k)\right) = P_{P_m(n)}(k)$ (associativity)

(5) $P_m(n + k) = P_m(k) + P_n(k)$ (distributivity)