

Lemma 3.2 (1) For any  $n, m \in \mathbb{N}$   
 exactly one of  $m \in m$  or  $n = m$   
 or  $m \in n$  holds

(2) For all  $n, m \in \mathbb{N}$   
 $m \in m \Leftrightarrow n \notin m$

(3) For any  $n, m \in \mathbb{N}$  we have  
 either  $n \notin m$  or  $n = m$  or  $m \notin n$

(4)  $\in$  (or equivalently  $\notin$ ) is a linear  
 ordering on  $\mathbb{N}$ .

Treatment of binary relations in  $\mathbb{Z}$

For a set  $A$  a relation on  $A$  is a  
 subset of  $A^2 = A \times A$

Remark A function  $f: A \rightarrow A$  is a  
 binary relation on  $A$ .

If  $R \subseteq A^2$  and  $\langle a, b \rangle \in R$  for  $a, b \in A$ ,  
 we write this also as  $a R b$ .

$\subseteq A^2$  is a (partial) ordering on  $A$  if

- ①  $a \notin a$  (i.e.  $\langle a, a \rangle \notin \subseteq$ ) for all  $a \in A$
- ② for all  $a, b, c$ ,  $a \subseteq b$  and  $b \subseteq c$  imply  $a \subseteq c$  (the relation is transitive)

$\subseteq \subseteq A^2$  is a linear ordering if

$\subseteq$  satisfies ① ② and  
 partial ordering

③ for all  $a, b \in A$  one of  $a \subseteq b, a = b,$   
 $b \subseteq a$  holds.

Remark ① If  $\subseteq$  is a partial ordering, the  
 $a \subseteq b$  implies  $b \not\subseteq a$  [if  $a \subseteq b, b \subseteq a$   
 then ② implies  $a \subseteq a$  which contradicts ①]

Thus the conditions  $a \subseteq b, a = b, b \subseteq a$  are exclusive.

② Let  $\subseteq = \{ \langle a, b \rangle \in \mathbb{N}^2 \mid a \in b \}$  (4) claims that  $\subseteq$

(which is  $= \{ \langle a, b \rangle \in \mathbb{N}^2 \mid a \notin b \}$ )  
 is a linear ordering on  $\mathbb{N} = \mathbb{N}$

proof (1): done last time.

(2): Suppose  $n, m \in \mathbb{N}$ ,  
 if  $m \in m$  then  $m \subseteq m$  by Lemma 3.1, (2),  
 $m \neq m$  by Lemma 3.1, (3). Thus we have  
 $n \notin m$

Remark + Exercise For a tfae:

- (a)  $\subseteq$  is transitive
- (b) For any  $b$ ,  $b \in a \Rightarrow b \subseteq a$

If  $n \notin m$  then  $n \neq m$  and  $m \notin m$  [ if  $m \in m$  then  $m \in m \notin m$ . Hence  $m \in m$  a contradiction to Lemma 3.1(3),

By (1), it follows that  $m \in m$ .

(3): clear by (1) and (2)

(4):  $\in \uparrow \mathbb{N} = \neq \uparrow \mathbb{N}$  by (2)

$\in \uparrow \mathbb{N}$  is transitive since  $\in \uparrow \mathbb{N} = \neq \uparrow \mathbb{N}$

$a \neq a$  by Lemma 3.1(3) for all  $a \in \mathbb{N}$

and the linearity (3) is just (1).  $\square$

Lemma 4.1 ( $\rho: \mathbb{N} \rightarrow \mathbb{N}; n \mapsto m \cup \{m\}$ )

$\rho(m)$  is a successor of  $m$  w.r.t  $\in \uparrow \mathbb{N}$   
 For all  $m \in \mathbb{N}$  (i.e.  $m \in \rho(m) = m \cup \{m\}$  and for any  $m$  with  $m \in m$  then  $\rho(m) \in m$  or  $\rho(m) = m$ )

Proof  $m \in \rho(m) = m \cup \{m\}$  is clear  
 Suppose  $m \in m$ . Then we have either  $\rho(m) \in m$  or  $\rho(m) = m$  or  $m \in \rho(m)$  by Lemma 3.2(1).  
 $m \notin \rho(m)$  [ if  $m \in \rho(m)$  then  $m \in m$  or  $m = m$   
 $\downarrow$   $\downarrow$   
 $m \in m$   $\Downarrow$   $m \in m$  ]

So we have  $\rho(m) \in m$  or  $\rho(m) = m$  as desired!  $\square$

Notation  $\in \uparrow \mathbb{N}$  is also denoted by  $<$   
 $\rho(m)$  by  $m+1$

Lemma 4.2 There is a unique function

$\text{add}: \mathbb{N}^2 \rightarrow \mathbb{N}$  with  
 (1)  $\text{add}(\langle m, 0 \rangle) = m$   
 (2)  $\text{add}(\langle m, m+1 \rangle) = \text{add}(\langle m, m \rangle) + 1$

Proof we first prove the uniqueness. Suppose that  $\text{add}: \mathbb{N}^2 \rightarrow \mathbb{N}$  is as above

$m+1$  is the smallest element of  $\mathbb{N}$  higher than  $m$  i.e. for any  $m$  with  $m < m$  either  $m+1 < m$  or  $m+1 = m$

and  $\text{add}^*: \mathbb{N}^2 \rightarrow \mathbb{N}$  with  
 (1)\*  $\text{add}^*(\langle m, 0 \rangle) = m$   
 (2)\*  $\text{add}^*(\langle m, m+1 \rangle) = \text{add}^*(\langle m, m \rangle) + 1$

We show that, for all  $m \in \mathbb{N}$   
 (\*)<sub>m</sub> for all  $m \in \mathbb{N}$   $\text{add}(\langle m, m \rangle) = \text{add}^*(\langle m, m \rangle)$   
 We show (1)\* and (2)\*  $\rightarrow$  (\*)<sub>m</sub>

For (1):  
 $\text{add}(\langle m, 0 \rangle) = m = \text{add}^*(\langle m, 0 \rangle)$   
 (1) (1)\*

For ①: assume  $(*)_m$

$$\text{add}(\langle n, m+1 \rangle) = \text{add}(\langle n, m \rangle) + 1$$

$$\stackrel{\text{②}}{=} \text{add}^*(\langle n, m \rangle) + 1 = \text{add}^*(\langle n, m+1 \rangle)$$

$(*)_m$   $\text{②}^*$

To show the existence we show that for all  $m \in \mathbb{N}$  there is a unique function

$$\text{add}_m : \mathbb{N} \times \{m, m+1\} \rightarrow \mathbb{N} \text{ with ① ②}$$

[Note  $m+1 = \{n \in \mathbb{N} \mid n \leq m\}$  by Lemma 4.3] and that

⊗ for  $m < m'$  we have  $\text{add}_m \subseteq \text{add}_{m'}$

The uniqueness is proved similarly to the uniqueness of add

Lemma 4.3(4) For any

$m \in \mathbb{N}$  we have  $m \subseteq \mathbb{N}$ .

② If  $m \in \mathbb{N}$  then  $m = \{n \in \mathbb{N} \mid n < m\}$

proof ①: Let  $X = \{m \in \mathbb{N} \mid m \subseteq \mathbb{N}\}$

Then  $\emptyset \in X$ , if  $m \in X$  then  $m \in \mathbb{N}$  (and  $n \in \mathbb{N}$ )

so  $m+1 = m \cup \{m\} \in \mathbb{N}$  and  $m \cup \{m\} \subseteq \mathbb{N}$

Thus  $m+1 \in X$ , Thus  $X = \mathbb{N}$ .

②: If  $m \in \mathbb{N}$  then  $m \in \mathbb{N}$ , hence  $m \in \{n \in \mathbb{N} \mid n < m\}$

if  $m \in \{n \in \mathbb{N} \mid n < m\}$  then trivially  $m \in m$ .  $\square$

③:  $m+1 = \{n \in \mathbb{N} \mid n < m+1\}$ : by ②

$$= \{n \in \mathbb{N} \mid n < m \text{ or } m = n\} = (m+1 = m \cup \{m\})$$

④  $\text{add}_0$  can be defined as

$$\{\langle \langle m, 0 \rangle, n \rangle \in \mathbb{N}^2 \times \mathbb{N} \mid m \in \mathbb{N}\} = \{\langle m \in \mathbb{N}^2 \times \mathbb{N} \mid \text{there is } n \in \mathbb{N} \text{ s.t. } m = \langle \langle n, 0 \rangle, n \rangle\}$$

(3)  $m+1 = \{n \in \mathbb{N} \mid n \leq m\}$

Suppose that  $\text{add}_m$  has been defined

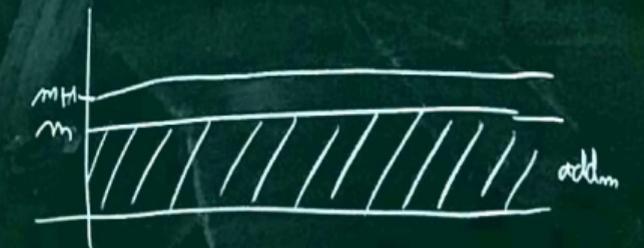
then let  $\text{add}_{m+1} = \text{add}_m \cup \{\langle \langle n, m+1 \rangle, \text{add}_m(\langle n, m \rangle) + 1 \rangle \mid n \in \mathbb{N}\}$

Since  $\text{add}_{m+1} \supseteq \text{add}_m$

⊗ is also satisfied.

Finally we define

$$\text{add} = \bigcup_{m \in \mathbb{N}} \text{add}_m = (*)$$



$(*) =$

$$\{\langle \langle n, m \rangle, l \rangle \in \mathbb{N}^2 \times \mathbb{N} \mid \text{there is some } m' \in \mathbb{N} \text{ s.t. } \langle \langle n, m \rangle, l \rangle \in \text{add}_{m'}\}$$

This add is as desired.  $\square$

Similarly we can show the unique existence

mult.  $\mathbb{N}^2 \rightarrow \mathbb{N}$  with

$$\text{mult}(m, 0) = 0$$

$$\text{mult}(n, m+1) = \text{add}(\text{mult}(n, m), m)$$