11.12.2018

LECTURE 11

Number sets

We are going to construct the sets $\mathbb{N}$ -(natural numbers), $\mathbb{Z}$(integers), $\mathbb{Q}$(rational numbers)

I. Natural numbers

- we introduce natural numbers by using the axioms of set theory:

Axiom of regularity

If x is a set, then $x \notin x$

Axiom of infinity

There exists at least a set y with the following property:

$\emptyset \in y$ and if x is a set s.t. $x \in y$

then $x^+ \in y$, where $^+ := x \cup \{x\}$ is called the successor of x

Def: A set y satisfying the above property is called an inductive set.

Def: The set $\mathbb{N}$ of natural numbers is the intersection of all inductive sets

$$\boxed{\mathbb{N} \stackrel{def.}{=\!=} \bigcap_{y \text{ is inductive}} y}$$

Remark

$$\mathbb{N} = \{ \underset{0}{\underset{\shortparallel}{\emptyset}}, \underset{1}{\underset{\shortparallel}{\emptyset^+}} = \{\emptyset\}, \underset{2}{\underset{\shortparallel}{\{\emptyset\}^+}} = \{\emptyset, \{\emptyset\}\}, \underset{3}{\underset{\shortparallel}{\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}}} \dots \}$$

We denote $s : \mathbb{N} \to \mathbb{N}$ $s(n) = n^+$ the successor function

Theorem The triple $(\mathbb{N}, 0, s)$ satisfies the Peano axioms

(1) 0 is a natural number

(2) If n is a natural number, then (sn) is a natural

(3) if n is a natural number, then $(sn) \neq 0$

(4) if $m \neq n$, then $s(m) \neq s(n)$

(5) principle of mathematical induction

If the subset $S \in \mathbb{N}$ satisfies:

1) $0 \in S$
2) if $n \in S$, then $s(n) \in S$

then $S = \mathbb{N}$

Remark

s is an inj. function

$\operatorname{Im} s = \mathbb{N}^* = \mathbb{N} \setminus \{0\}$

Theorem 2

The Peano axioms determine the triple $(\mathbb{N}, 0, s)$ uniquely up to a unique isomorphism. More precisely, if $(\mathbb{N}', 0', s')$ is another triple satisfying the Peano axioms $(1^\circ - 5^\circ)$ then there $\exists!$ function $f : \mathbb{N} \longrightarrow \mathbb{N}'$ s.t.

(a) f is bijective

(b) $f(0) = 0'$

(c) the following diagram is commutative:

$$\begin{tikzcd}
\mathbb{N} \arrow[r, "f"] \arrow[d, "s"'] & \mathbb{N}' \arrow[d, "s'"] \\
\mathbb{N} \arrow[r, "f"'] & \mathbb{N}'
\end{tikzcd}$$

i.e. $s' \circ f = f \circ s$

Operations with natural numbers

These are defined recursively (by induction)

addition $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$: $\begin{cases} m + 0 \overset{\text{def}}{=} m \\ m + s(n) = s(m+n) \end{cases}$

(in particular, we have $m + 1 = s(m)$)

multiplication $\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ $\quad m \cdot 0 \overset{\text{def}}{=} 0$

$m \cdot s(n) \overset{\text{def}}{=} mn + m$

(in particular $m \cdot 1 = 0 + m = \ldots = m$)
(needs proof by induction)

the relation „<" $m < n \overset{\text{def}}{\Longleftrightarrow} \exists p \in \mathbb{N}^*$ s.t. $n = m+p$.

Theorem 3 The structure $(\mathbb{N}, \cdot, +, \leq)$ is:

1) a semiring (assoc. and commut.)
2) well-ordered + compatibility:
   $m < n \Rightarrow m+p < n+p$
   $m < n$, $p \neq 0 \Rightarrow mp < np$
3) Archimedean $\forall m, p \in \mathbb{N}$, $p \neq 0$
   $\exists n \in \mathbb{N}$ s.t. $np > m$

II Integers

Motivation: - in $\mathbb{N}$, equations of the form $x+5=3$ do not have solutions. we need to define $3-5=4-6$. More abstractly, we want to extend the semiring $\mathbb{N}$ to a ring.

Consider the set: $\mathbb{N}\times\mathbb{N} = \{(m,n) \mid m,n \in \mathbb{N}\}$

On the set we define the relation „$\sim$"

$$(m,n) \sim (p,q) \overset{\text{def}}{\Longleftrightarrow} m+q = n+p$$

Then „$\sim$" is an equivalence relation on $\mathbb{N}\times\mathbb{N}$ (ex!)
(R, T, S)

so we might consider the quotient set.

Def the set of integers is

$$\boxed{\mathbb{Z} := \mathbb{N}\times\mathbb{N}/_{\sim} = \{\widetilde{(m,n)} \mid m, n \in \mathbb{N}\}}$$

where $\widetilde{(m,n)} = \{(p,q) \in \mathbb{N}\times\mathbb{N} \mid (m,n) \sim (p,q)\}$ is the class of the pair (m,n)

Operations in $\mathbb{Z}$

„+": $\widetilde{(m,n)} + \widetilde{(p,q)} \overset{\text{def}}{=} \widetilde{(m+p, n+q)}$

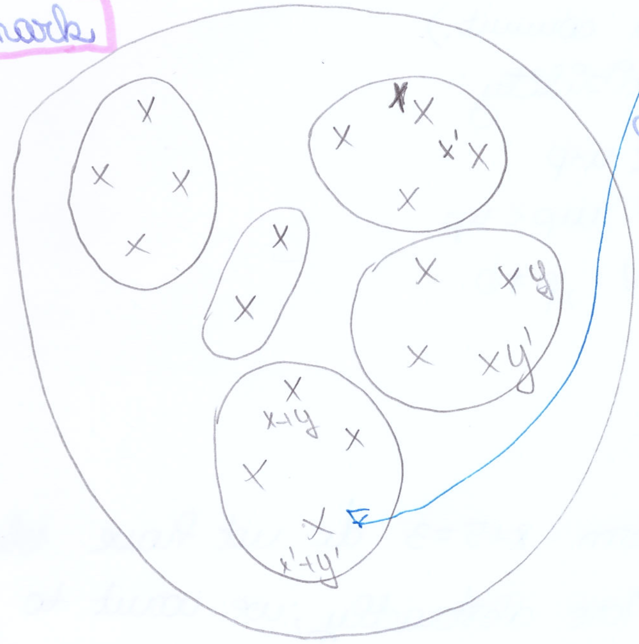
„$\cdot$": $\widetilde{(m,n)} \cdot \widetilde{(p,q)} \overset{\text{def}}{=} \widetilde{(mp+nq, mq+np)}$

„<": $\widetilde{(m,n)} < \widetilde{(p,q)} \overset{\text{def}}{\Longleftrightarrow} m+q < n+p$.

Theorem

1) the above definition do not depend on the choice of representant

Remark



if $x'+y'$ is not here then the def is not correct! (it must be in the same class as $x+y$)

In our case:

- if $(m,n)\sim(m',n')$ and $(p,q)\sim(p',q')$ then we must show that $(m+p, n+q)\sim(m'+p', n'+q')$
- the same for „$\cdot$", „$\leq$"

2) the structure $(\mathbb{Z},+,\cdot,\leq)$ is:

(a) an integral domain
(b) totally ordered (+compat)
(c) Archimedean

Remark

The function $f:\mathbb{N}\to\mathbb{Z}$ $f(n)=\widetilde{(n,0)}$ is a strictly increasing homomorphism of semirings:

We identify n with $\widetilde{(n,0)}$, and then we have:

$$\widetilde{(m,n)} = m-n = m+(-n)$$

III. Rational numbers

Motivation - equations of the form $3x=5$ do not have solutions in $\mathbb{Z}$, we need to define $\frac{5}{3}=\frac{10}{6}$. More abstractly,

- we want to extend ring $\mathbb{Z}$ to a field (= corp commutative)

The construction

On the set $\mathbb{Z}\times\mathbb{Z}^* = \{(a,b) \mid a,b\in\mathbb{Z},\ b\neq 0\}$ we define the relation „$\sim$" as follows:

$$(a,b)\sim(c,d) \overset{def}{\Longleftrightarrow} ad=bc$$

The „$\sim$" is an equivalence relation on $\mathbb{Z}*\mathbb{Z}^*$

Def: The set of rational numbers is:

$$\boxed{\mathbb{Q} := \mathbb{Z}*\mathbb{Z}^*/_{\sim} = \{\widetilde{(a,b)} \mid a,b\in\mathbb{Z},\ b\neq 0\}}$$

where $\widetilde{(a,b)} = \{(c,d)\in\mathbb{Z}*\mathbb{Z}^* \mid (a,b)\sim(c,d)\}$ is the class of the pair (a,b)

Notation $\widetilde{(a,b)} = \frac{a}{b}$ (fraction)

numerator denominator

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc$$

Operations with rationals:

„$+$": $\widetilde{(a,b)} + \widetilde{(c,d)} \stackrel{def.}{=} \widetilde{(ad+bc,\, bd)}$

„$\cdot$": $\widetilde{(a,b)} \cdot \widetilde{(c,d)} \underset{def.}{=} \widetilde{(ac, bd)}$

„$<$": $\widetilde{(a,b)} \cdot \widetilde{(c,d)} \underset{def}{=} (ad-bc)\,bd < 0$

Theorem 1) The above definitions do not depend on the choice of representatives.

2) The structure $(\mathbb{Q}, +, \cdot, \leq)$ is

(a) a field with $\widetilde{(a,b)}^{-1} = \widetilde{(b,a)}$
$\quad\ \neq 0 \quad \neq 0$

(b) totally ordered (+ compatibility conditions)

(c) Archimedean

$(\forall a,b\in\mathbb{Q}\quad b>0 \qquad \exists n\in\mathbb{N}.$
s.t. $n\cdot b > a$ $)$

Remark

The function $f:\mathbb{Z}\to\mathbb{Q}$ $\quad f(a) = \widetilde{(a,1)} = \frac{a}{1}$ is a strictly increasing homomorphism of rings.

We identify a with $\frac{a}{1}$

we have $\frac{a}{b} = \left(\frac{a}{1}\right)\cdot\left(\frac{1}{b}\right) = f(a)\cdot f(b)^{-1} = a\cdot b^{-1}$