Mathematical Logic
Lecture 10
16.12.2022

Chapter 7. Number sets

We will give the definition of natural numbers, integers, rational numbers.

A. Natural numbers

We introduce nat. numbers by using axioms of set theory.

Axiom of regularity: if X is a set, then $X \notin X$

Axiom of infinity: There exists a set Y which satisfies the following properties:

- $\emptyset \in Y$.
- if X is a set such that $X \in Y$, then $X^+ \in Y$,

where $X^+ := X \cup \{X\}$ is called the successor of X.

Def 1) A set Y satisfying the above conditions is called an inductive set

~1930 2). The set of natural numbers is the smallest inductive set

i.e.: $\mathbb{N} := \bigcap_{Y \text{ inductive}} Y$

Rem: We have $\mathbb{N} = \{\emptyset, \emptyset^+ = \{\emptyset\}, \{\emptyset\}^+ = \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots\}$

not.: $\emptyset = 0$, $\{\emptyset\} = 1 = 0^+$, $\{\emptyset, \{\emptyset\}\} = 2 = 1^+$, ...

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

We relate this def of $\mathbb{N}$ to the older axioms of Peano ~1889

Giuseppe Peano.

Theorem: The triple $(\mathbb{N}, \underset{\emptyset}{\overset{\shortparallel}{0}}, s)$ satisfies the Peano axioms

(1) 0 is a natural number

(2) if n is a natural number then $s(n)$ is also a natural number

(3) 0 is not a succesor of any natural number

(4) If $n \neq m$, then $s(n) \neq s(m)$ (i.e. s is injective

(5) $\forall S$ set, $S \subseteq \mathbb{N}$, if S satisfies the conditions:

(a) $0 \in S$

(b) $\forall n$ if $n \in S$ then $s(n) \in S$.

then $S = \mathbb{N}$.

Rem (3), (5) $\Longrightarrow$ $\operatorname{Im} s = \mathbb{N} \setminus \{0\} =: \mathbb{N}^*$

Thm. 2 The Peano axioms determine the triple $(\mathbb{N}, 0, s)$ uniquely, up to a unique isomorphism.

More precisely: assume that $(\mathbb{N}', 0', s')$ is another triple satisfying the Peano axioms (1) — (5).

Then $\exists!$ bijective function $f : \mathbb{N} \to \mathbb{N}'$ s.t. $f(0) = 0'$, and the following diagram is commutative:

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

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

Operations with nat numbers

addition: we define recursively (by induction) a function $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\begin{cases} \bullet\ n + 0 \overset{def}{=} n \\ \bullet\ n + s(m) \overset{def}{=} s(n+m) \end{cases}$$

Rem take $m = 0$
$s(m) = 1$
$\Rightarrow n+1 = s(n)$

multiplication $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\begin{cases} \bullet\ n \cdot 0 \overset{def}{=} 0 \\ \bullet\ n \cdot s(m) \overset{def}{=} nm + n \end{cases}$$

ordering $m \leq n \overset{def}{\Longleftrightarrow} \exists\, p \in \mathbb{N}$ st $n = m + p$
"$<$" $p \in \mathbb{N}^*$

($m < n \Leftrightarrow m \leq n$ and $m \neq n$).

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

1). $(\mathbb{N}, +, \cdot)$ is a semiring $\begin{cases} (\mathbb{N}, +) \text{ comm monoid} \\ (\mathbb{N}, \cdot) \text{ — '' —} \\ \text{"}\cdot\text{" is distri wrt } + \end{cases}$

2). $(\mathbb{N}, \leq)$ is well-ordered; the rel is compat with the oper.

- $m < n \Rightarrow m + p < n + p$
- $m < n,\ p \neq 0 \Rightarrow mp < np$.

3) Archimedean property:

$\forall m \in \mathbb{N},\ \forall p \in \mathbb{N}^*\ \exists\, n \in \mathbb{N}$ st $n \cdot p > m$.

Proof HW and seminar.

B. The set of integers

<u>Problem</u> – equations of the form $7+x=4$ do not have solution in $\mathbb{N}$.

– $(\mathbb{N},+)$ is not a group

we want to define
$$x = 4-7 = 3-6$$

<u>Def.</u> 1). On the set $\mathbb{N}\times\mathbb{N}$, we define the rel.:
$$(m,n)\sim(p,q) \overset{def}{\Longleftrightarrow} m+q = n+p.$$
(this is an equivalence relation (HW).)

2). The set of integers is the <u>quotient set</u>
$$\mathbb{Z} := \mathbb{N}\times\mathbb{N}/\sim \;= \{\widetilde{(m,n)} \mid m,n\in\mathbb{N}\}.$$
where $\widetilde{(m,n)} = \{(m',n') \mid (m,n)\sim(m',n')\}$.

<u>Operation on $\mathbb{Z}$</u>

- $\widetilde{(m,n)} + \widetilde{(p,q)} \overset{def}{=} \widetilde{(m+p,\, n+q)}$
- $\widetilde{(m,n)}\cdot\widetilde{(p,q)} \overset{def}{=} \widetilde{(mp+nq,\, mq+np)}$
- $\widetilde{(m,n)} < \widetilde{(p,q)} \overset{def}{\Longleftrightarrow} m+q < n+p$ in $\mathbb{N}$

<u>Theorem.</u> The structure $(\mathbb{Z},+,\cdot,\leq)$ satisfies:

(1) $(\mathbb{Z},+,\cdot)$ is an <u>integral domain</u>.
$$\left\{\begin{array}{l} \left.\begin{array}{ll}(\mathbb{Z},+) & \text{ab. grp.}\\ (\mathbb{Z},\cdot) & \text{com, monoid}\\ \text{"}\cdot\text{" distr. w.r.t. "}+\text{"} & \end{array}\right\} \text{comm ring} \\ a,b\neq 0 \Rightarrow ab\neq 0 \\ (\nexists \text{ divisors of zero}).\end{array}\right.$$

(2). "$\leq$" total order, compat with oper:

$a<b \Rightarrow a+c < b+c$

$a<b,\ c>0 \Rightarrow ac < bc$

$a<b,\ c<0 \Rightarrow ac > bc$

(3). <u>Archimedean property</u>: $\forall a \in \mathbb{Z}$, $\forall b \in \mathbb{Z}$, $b > 0$,

$\exists\, n \in \mathbb{N}$ s.t. $nb > a$.

(0) the above definitions do not depend on the choice of representatives.

<u>Proof</u> HW + seminar.

<u>Rem</u>. 1). we need to check:

$$\left.\begin{array}{l}(m,n) \sim (m',n')\\ (p,q) \sim (p',q')\end{array}\right\} \overset{?}{\Longrightarrow} \begin{array}{l}(m+p,\, n+q) \sim (m'+p',\, n'+q')\\ (mp+nq,\, mq+np) \sim (m'p'+n'q',\, m'q'+n'p')\end{array}$$

2). the funct. $f : \mathbb{N} \to \mathbb{Z}$, $f(n) = \widehat{(n,0)}$ is a strictly increasing morphism

We identify $\underset{\underset{\mathbb{N}}{\cap}}{n} = \widehat{(n,0)} \in \mathbb{Z}$

then: $\widehat{(m,n)} = f(m) - f(n) = m - n$

C. The set of rational numbers

<u>Problem</u>. - equation of the form $7x = 4$ do not have solutions in $\mathbb{Z}$

- $(\mathbb{Z}, +, \cdot)$ is not a <u>field</u> = ~~camp~~ corp comutativ

we enlarge $\mathbb{Z}$ in order to get a field.

we want to form "fractions" $x = \frac{4}{7} = \frac{8}{14} \ldots$

$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b$

Def. 1) On the set $\mathbb{Z}\times\mathbb{Z}^*$ we define the relation "$\sim$":

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

(this is an equiv relation: HW!).
(R, T, S)

2). The <u>set of rational numbers</u> is the quotient set

$$\mathbb{Q} := \mathbb{Z}\times\mathbb{Z}^*/_\sim = \{ \widehat{(a,b)} \mid (a,b)\in\mathbb{Z}\times\mathbb{Z}^* \}$$

where $\widehat{(a,b)} = \{(a',b')\in\mathbb{Z}\times\mathbb{Z}^* \mid (a,b)\sim(a',b')\}$

$\parallel$ not

$\frac{a}{b}$.

$\frac{a}{b} < \frac{c}{d} \Leftarrow \frac{ad}{bd} < \frac{cb}{bd}$

<u>Operations in $\mathbb{Q}$</u>

- $\widehat{(a,b)} + \widehat{(c,d)} \overset{def}{=} \widehat{(ad+bc\ ,\ bd)}$
- $\widehat{(a,b)} \cdot \widehat{(c,d)} \overset{def}{=} \widehat{(ac\ ,\ bd)}$
- $\widehat{(a,b)} < \widehat{(c,d)} \overset{def}{\iff} (ad-bc)bd < 0$ in $\mathbb{Z}$

<u>Theorem</u> The structure $(\mathbb{Q}, +, \cdot, \leq)$ satisfies:

(0) the above definition do not depend on the choice of representatives.

(1) $(\mathbb{Q}, +, \cdot)$ is a <u>field</u> $\begin{cases} (\mathbb{Q},+) \text{ abelian group.} \\ (\mathbb{Q}^*,\cdot) \text{ abelian gr} \\ \text{"}\cdot\text{" is distr. w.r.t. } + \end{cases}$

http://paperkit.net

(2). "$\leq$" is a total order $(R, T, A + \text{total})$, compatible with the operations:

$$\forall x, y, z \in \mathbb{Q} \text{ we have: } \begin{cases} x<y \Rightarrow x+z < y+z \\ x<y,\ z>0 \Rightarrow xz < yz \\ x<y,\ z<0 \Rightarrow xz > yz \end{cases}$$

(3) Archimedean property:

$$\forall x \in \mathbb{Q} \ \forall y \in \mathbb{Q},\ y>0 \ \exists n \in \mathbb{N} \text{ s.t. } ny > x$$

(4). The map $f : \mathbb{Z} \to \mathbb{Q}$, $f(a) = \widehat{(a,1)} = \frac{a}{1}$

is a strictly increasing ring morphism:

$$\begin{cases} \cdot\ a<b \Rightarrow f(a) < f(b) \\ \cdot\ f(a+b) = f(a) + f(b) \\ \cdot\ f(ab) = f(a) f(b) \end{cases}$$

Remark. 1). We identify $\underset{\mathbb{Z}}{\underset{\cap}{a}} = f(a) = \frac{a}{1} \in \mathbb{Q}$

We denote $\widehat{(a,b)} = \underbrace{\frac{a}{b}}_{\text{fraction}}$, so $\frac{a}{b} = f(a) \cdot f(b)^{-1}$

$\left(\text{ie } \frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b}\right)$

2). $\lim_{n\to\infty} \frac{1}{n} = 0$: $\forall \varepsilon > 0 \ \exists N = N_\varepsilon$ s.t. $\forall n > N_\varepsilon$ we have $\frac{1}{n} < \varepsilon$

$\Updownarrow$

$n \cdot 1 > \frac{1}{\varepsilon}$

this is a consequence of the fact that $\mathbb{R}$ is Archimedean!

Homework: ex. 87 – 93