Chapter 7. Number sets

We are going to define natural numbers, integers and rational numbers.

A. Natural numbers

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

The axiom of regularity: If X is a set, then $X \notin X$

The axiom of infinity: There exists a set Y with the following properties:

1° $\emptyset \in Y$

2° If the set X belongs to Y, then the set $X^+ \in Y$, where $X^+ := X \cup \{X\}$ is called the successor of X.

such a set Y is called an inductive set.

Def: The set of natural numbers is the smallest inductive set, i.e it's the intersection of all inductive sets.

$$\mathbb{N} = \bigcap_{Y \text{ inductive set}} Y \qquad \text{(John von Neumann)}$$

Rem: $\mathbb{N} = \{ \underbrace{\emptyset}_{0}, \underbrace{\emptyset^+ = \{\emptyset\}}_{1}, \underbrace{\emptyset^{++} = \{\emptyset\}^+ = \{\emptyset, \{\emptyset\}\}}_{2}, \ldots \}$,

$2^+ = \{\emptyset, \{\emptyset\}, \underbrace{\{\emptyset, \{\emptyset\}\}}_{3}, \ldots\}$

Theorem 1: The triple $(\mathbb{N}, 0, s)$, (where $s: \mathbb{N} \to \mathbb{N}$, $s(n) = n^+$ is called the successor function) satisfies the Peano axioms:

1) 0 is a natural number

(2) If n is a nat. number, then its successor $s(n)$ is a nat. numb.

(3) 0 is not a successor of a nat. number

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

(5) If a subset $S \subseteq \mathbb{N}$ satisfies the properties: (1° $0 \in S$, 2° $\forall n \in \mathbb{N}$, if $n \in S$ then $s(n) \in S$)

Then $S = \mathbb{N}$

Rem: Axiom (5) is a 2nd order formula because we quantify sets: $\forall S \ldots$

→ principle of mathematical induction.

Theorem 2: Peano's axioms determine the triple $(\mathbb{N}, 0, s)$ uniquely up to a unique isomorphism: i.e if $(\mathbb{N}, 0', s')$ is another triple satisfying Peano's axioms, the triple is a function $f: \mathbb{N} \to \mathbb{N}'$ s.t.

a) f is bijective

b) $f(0) = 0'$

c) $f(s(n)) = s'(f(n))$ $\forall n \in \mathbb{N}$

i.e the following diagram is commutative

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ f \downarrow & & \downarrow f \\ \mathbb{N}' & \xrightarrow[s']{} & \mathbb{N}' \end{array}$$

$f \circ s = s' \circ f$

Operations with natural numbers

- addition is defined by induction

$m + 0 \overset{\text{def}}{=} m$ $\qquad$ $m + 1 = s(m)$

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

- multiplications:

$m \cdot 0 \overset{\text{def}}{=} 0$ $\qquad$ $m \cdot 1 = m$

$m \cdot s(n) = m n + m$

· order relations

$$m < n \overset{\text{def}}{\iff} \exists p \in \mathbb{N},\ p \neq 0 \text{ s.t. } n = m + p$$

$$m \leq n \iff \exists p \in \mathbb{N} \text{ s.t. } n = m + p$$

Theorem: The structure $(\mathbb{N}, +, \cdot, \leq)$ satisfies the following properties:

- $(\mathbb{N}, +, \cdot)$ is a semiring $\begin{cases} (\mathbb{N}, +) \text{ comm. monoid} \\ (\mathbb{N}, \cdot) \text{ comm. monoid} \\ \text{"}\cdot\text{" is distributive w.r.t addition} \end{cases}$
- $(\mathbb{N}, \leq)$ is well-ordered, and "$\leq$" is compatible with $+, \cdot$:

$$\begin{cases} m < n \Rightarrow m + p < n + p \\ m < n,\ p \neq 0 \Rightarrow mp < np \end{cases}$$

- $\mathbb{N}$ is Archimedean:

$$\forall m \in \mathbb{N}\ \forall p \in \mathbb{N}^*,\ \exists n \in \mathbb{N} \text{ s.t. } np > m.$$

Proof - HW

B. The set of integers

Problem: - equations of the form $5 + x = 2$ do not have solutions in $\mathbb{N}$

- $(\mathbb{N}, +)$ is not a group

We extend the notion of number.

idea: $x = 2 - 5 = 3 - 6 \iff 2 + 6 = 5 + 3$

Definition: On set $\mathbb{N} \times \mathbb{N} = \{(m, n) \mid m, n \in \mathbb{N}\}$. We define the relation "$\sim$":

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

The rel "$\sim$" is an equivalence relation (HW)

The set of integers is the quotient set

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

where $(m,n) := \{(p,q) \mid (m,n)\sim(p,q)\}$

Operations with integers:

- $\widetilde{(m,n)} + \widetilde{(p,q)} \overset{\text{def}}{=} \widetilde{(m+p, n+q)}$
- $\widetilde{(m,n)} \cdot \widetilde{(p,q)} \overset{\text{def}}{=} \widetilde{(mp+nq, mq+np)}$
- $\widetilde{(m,n)} < \widetilde{(p,q)} \overset{\text{def}}{\iff} m+q < n+p$

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

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

- integral domain (commuting with $1 = \widetilde{(1,0)}$, without divisors of $0 = \widetilde{(n,n)}$)
- totally ordered

compat with $+,\cdot$:
$$\begin{cases} a<b \Rightarrow a+c<b+c \\ a<b,\ c>0 \Rightarrow ac<bc \\ a<b,\ c<0 \Rightarrow a\cdot c>bc \end{cases}$$

- Archimedean:

$$\forall a\in\mathbb{Z}\ \forall b\in\mathbb{Z},\ b>0$$
$$\exists n\in\mathbb{N} \text{ s.t. } nb>a$$

Proof: HW!

C. The set of rationals

problem - equations of the form $5\cdot x=2$ do not have solutions in $\mathbb{Z}$
- $(\mathbb{Z},+,\cdot)$ is not a field (corp comutativ)

idea: - we add fractions

$$x = \frac{2}{5} = \frac{4}{10} \iff 2 \cdot 10 = 4 \cdot 5$$

Def: On the set $\mathbb{Z} \times \mathbb{Z}^* = \{(a,b) \mid a,b \in \mathbb{Z},\ b \neq 0\}$

We define the relation "$\sim$":

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

The rel. "$\sim$" is an equivalence relation (HW)

The set of rational numbers is the quotient set:

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

where $\widetilde{(a,b)} = \{(c,d) \mid (a,b) \sim (c,d)\}$

Operations in $\mathbb{Q}$:

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

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

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

- a field $\quad \widetilde{(a,b)}^{-1} = \widetilde{(b,a)}$
- totally ordered + compatibility:
  - $x < y \Rightarrow x + z < y + z$
  - $x < y,\ z > 0 \Rightarrow xz < yz$
  - $x < y,\ z < 0 \Rightarrow xz > yz$
- Archimedean:

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

Proof HW

Rem: $\lim_{n\to\infty} \frac{1}{n} = 0 \iff \forall \varepsilon > 0 \ \exists N_\varepsilon$ s.t. $\forall n > N_\varepsilon \quad \frac{1}{n} < \varepsilon$

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

Remark: $\mathbb{Q}$ extends $\mathbb{Z}$,

i.e. $\exists f : \mathbb{Z} \to \mathbb{Q}$

$f(a) = \widetilde{(a,1)}$ which is strictly increasing morphism

We identify $a \in \mathbb{Z}$ with $\widetilde{(a,1)} \in \mathbb{Q}$

Not $\frac{a}{b} = \widetilde{(a,b)}$

With this identification we have:

$$\frac{a}{b} = f(a) \cdot f(b)^{-1} = a \cdot b^{-1}$$

$$\parallel$$

$$\widetilde{(a,1)} \cdot \widetilde{(b,1)}^{-1} = \widetilde{(a,b)}$$

$$\parallel$$

$$\widetilde{(1,b)}$$