

## 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  $\bar{X} \notin \bar{X}$

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

<sup>1930</sup> 2) The set of natural numbers is the smallest inductive set

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

Rem we have  $\mathbb{N} = \{ \emptyset, \emptyset^+, \{\emptyset\}^+, \{\emptyset, \{\emptyset\}\}^+, \dots \}$   
not:  $\parallel \quad \parallel \quad \parallel$   
 $0 \quad 1 = 0^+ \quad 2 = 1^+ \dots$

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

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

Theorem 1 The triple  $(\mathbb{N}, 0, \Delta)$  satisfies the Peano axioms

- (1)  $0$  is a natural number
- (2) If  $n$  is a natural number then  $\Delta(n)$  is also a natural number
- (3)  $0$  is not a successor of any natural number
- (4) If  $n \neq m$ , then  $\Delta(n) \neq \Delta(m)$  (i.e.  $\Delta$  is injective)
- (5) If  $S$  is a set,  $S \subseteq \mathbb{N}$ , if  $S$  satisfies the conditions:
  - (a)  $0 \in S$
  - (b) If  $n$  if  $n \in S$  then  $\Delta(n) \in S$ .
 then  $S = \mathbb{N}$ .

Remark (3), (5)  $\implies \text{Im } \Delta = \mathbb{N} \setminus \{0\} =: \mathbb{N}'$

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

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

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

$$\begin{array}{ccc}
 \mathbb{N} & \xrightarrow{\Delta} & \mathbb{N} \\
 f \downarrow & & \downarrow f \\
 \mathbb{N}' & \xrightarrow{\Delta'} & \mathbb{N}'
 \end{array}
 \quad \text{i.e.} \quad f \circ \Delta = \Delta' \circ f$$

## Operations with nat numbers

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

$$\begin{cases} \bullet n + 0 \stackrel{\text{def}}{=} n \\ \bullet n + \Delta(m) \stackrel{\text{def}}{=} \Delta(n+m) \end{cases}$$

Prop take  $m=0$   
 $\Delta(m) = 1$   
 $\Rightarrow n+1 = \Delta(n)$

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

$$\begin{cases} \bullet n \cdot 0 \stackrel{\text{def}}{=} 0 \\ \bullet n \cdot \Delta(m) \stackrel{\text{def}}{=} nm + n \end{cases}$$

ordering  $m \leq n \stackrel{\text{def}}{=} \exists p \in \mathbb{N} \text{ s.t. } n = m+p$   
 $<$   $p \in \mathbb{N}^+$   
 $(m < n \Leftrightarrow m \leq n \text{ and } m \neq n)$

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

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

2).  $(\mathbb{N}, \leq)$  is well-ordered ; the rel is compat with  $+$  and  $\cdot$   
 $\bullet m < n \Rightarrow m+p < n+p$   
 $\bullet m < n, p \neq 0 \Rightarrow mp < np$

3) Archimedean property :

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

Proof HW and semir.

## B. The set of integers

Problem - eqs like of the form  $7+x=4$  do not have solution in  $\mathbb{N}$ . we want to define  
-  $(\mathbb{N}, +)$  is not a group  $x = 4-7 = 3-6$

Def. 1). On the set  $\mathbb{N} \times \mathbb{N}$ , we define the rel.:

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

(this is an equivalence rel. (hw).)

2). the set of integers is the quotient set

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

$$\text{where } \widetilde{(m, n)} = \{ (m', n') \mid (m, n) \sim (m', n') \}.$$

Operation on  $\mathbb{Z}$

$$\bullet \quad \widetilde{(m, n)} + \widetilde{(p, q)} \stackrel{\text{def}}{=} \widetilde{(m+p, n+q)}$$

$$\circ \quad \widetilde{(m, n)} \cdot \widetilde{(p, q)} \stackrel{\text{def}}{=} \widetilde{(mp+nq, mq+np)}$$

$$\bullet \quad \widetilde{(m, n)} < \widetilde{(p, q)} \stackrel{\text{def}}{\iff} m+q < n+p \text{ in } \mathbb{N}$$

Thm. The structure  $(\mathbb{Z}, +, \cdot, <)$  satisfies:

- (1)  $(\mathbb{Z}, +, \cdot)$  is an integral domain.  
(2)  $<$  is a total order, compat with oper:
- $a < b \implies a+c < b+c$   
 $a < b, c > 0 \implies ac < bc$   
 $a < b, c < 0 \implies ac > bc$

$\left. \begin{array}{l} (\mathbb{Z}, +) \text{ ab. grp.} \\ (\mathbb{Z}, \cdot) \text{ comm. monoid} \\ \cdot \text{ distrib. wrt. } + \end{array} \right\} \text{conv. prop.}$   
 $a, b \neq 0 \implies ab \neq 0$   
( $\exists$  divisors of zero).

(3) Archimedean propy:  $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, b > 0,$   
 $\exists n \in \mathbb{N}$  s.t.  $nb > a$ .

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

Pro of HW + lemma.

Rem. 1). we need to check:

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

2). the func.  $f: \mathbb{N} \rightarrow \mathbb{Z}, f(n) = \widetilde{(n, 0)}$  is a strictly increasing morphism

We identify  $\mathbb{N} = \widetilde{(n, 0) \mid n \in \mathbb{Z}}$

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

## C. The set of rational numbers

Problem. - e.g.  $\forall x \in \mathbb{Z}$  does not have solutions in  $\mathbb{Z}$

-  $(\mathbb{Z}, +, \cdot)$  is not a field = corp. complete

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

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

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

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

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

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

2). The set of rational numbers is the quotient set

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

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

|| not

$$\frac{a}{b}$$

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

Operations in  $\mathbb{Q}$

$$\bullet \quad \widetilde{(a, b)} + \widetilde{(c, d)} \stackrel{\text{def}}{=} \widetilde{(ad + bc, bd)}$$

$$\bullet \quad \widetilde{(a, b)} \cdot \widetilde{(c, d)} \stackrel{\text{def}}{=} \widetilde{(ac, bd)}$$

$$\bullet \quad \widetilde{(a, b)} < \widetilde{(c, d)} \stackrel{\text{def}}{\iff} (ad - bc)bd < 0$$

$\iff \mathbb{Q}$

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

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

(1)  $(\mathbb{Q}, +, \cdot)$  is a field  $\left\{ \begin{array}{l} (\mathbb{Q}, +) \text{ abelian group.} \\ (\mathbb{Q}^*, \cdot) \text{ abelian group.} \\ \cdot \text{ is distrib. w.r.t. } + \end{array} \right.$

(2).  $\leq$  is a total order, compatible with the operations:  
 $(\mathbb{R}, +, \cdot)$

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

(3) Archimedean property:

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

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

is a strictly increasing ring morphism:

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

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

We don't  $\widehat{(a, b)} = \frac{a}{b}$ , so  $\frac{a}{b} = f(a) \cdot f(b)^{-1}$   
 fraction (i.e.  $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b}$ )

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

this is a consequence of the

fact that  $\mathbb{R}$  is Archimedean!

$$\Downarrow$$

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