I Number systems

I.1 basic set theory

Definition: A set is collection of objects called elements or members. A set with no elements is called the empty set and is denoted by $\emptyset$ (sometimes also by $\{\}$)

Example: $A := \{1,2,3\}$ $B := \{4,5,6\}$ $C := \emptyset$

$:=$ $\Leftrightarrow$ definition

- If an element x belongs to the set X, we write $x \in X$.
- If it doesn't belong, we write $x \notin X$.
- Writing an element several times in a set, doesn't change it.

Definition: The set A is a subset of a set B if

$\forall x \in A : x \in B$ = "for each element x of A, one has that $x \in B$"

$\forall$ for each, conditions, one uses $!$ to list conditions

Notation: $\subset$ or $\subseteq$

$E = \{1,2\} \subseteq \{1,2,3\}$ $\quad \{1,2\} \in \{1,\{1,2\}\}$

$\{1,2\} \not\subseteq \{2,\{1,2\}\}$

Definition: Let A and B be two sets.

We define:

a) the union of A and B, denoted by $A \cup B$ by

$A \cup B := \{x \mid x \in A \text{ or } x \in B\}$

b) the intersection of A and B, denoted by $A \cap B$ by

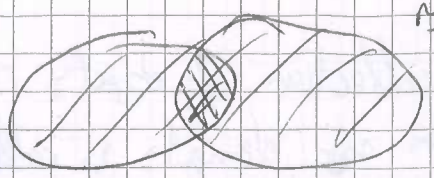
$A \cap B := \{x \mid x \in A \text{ and } x \in B\}$

c) a complement of B relative to A is

$A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}$

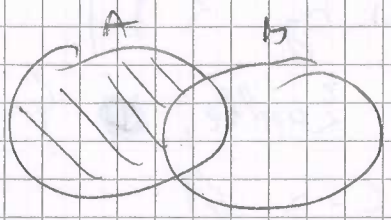
• We say that A and B are disjoint if $\emptyset = A \cap B$

Venn diagram

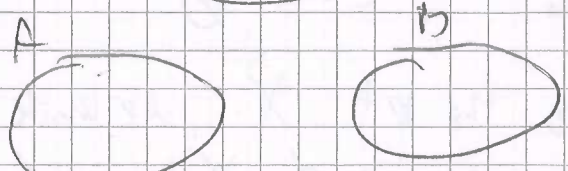


//// $A \cup B$

XXX $A \cap B$



$A \setminus B$



$A \cap B = \emptyset$

De Morgan laws:

(Exercise) $A, B \subseteq C$

$$(A \cap B)^c = A^c \cup B^c$$

$$(A \cup B)^c = A^c \cap B^c$$

ex

• We can take a union of more than ~~one~~ (two) sets

I index set, A_i sets for $i \in I$

$$\bigcup_{i \in I} A_i := \{ x \mid \exists\, i \in I \text{ s.t. } x \in A_i \}$$

(exists)

$$\bigcap_{i \in I} A_i := \{ x \mid \forall\, i \in I \text{ s.t. } x \in A_i \}$$

(For all)

~~De Morgan laws~~ $A_i \subseteq$

$i \in I$, $A_i \subseteq B$ B a set

$$\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c \qquad \left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} A_i^c.$$

I-2 Natural numbers. $\mathbb{N}$

(positive integers)

I-2-1

Peano axioms

① There is an element $1 \in \mathbb{N}$.

② Each element $n \in \mathbb{N}$ admits a unique successor $n^+ \in \mathbb{N}$ (successor operation)

③ If $n \neq m$, then $n^+ \neq m^+$ (different)

④ 1 is not a successor of any $n \in \mathbb{N}$

⑤ Each subset $S \subseteq \mathbb{N}$ which contains 1 and such that for every integer $n \in S$, one has that $n^+ \in S$ is equal to $\mathbb{N}$.

Theorem: (Principle of mathematical induction)

Suppose that $P(n)$ is a property depending on an integer n.

(Example: $3 \mid n$, $n^3 + 1 + 2n = (n+1)^2$)

Assume: 1) $P(1)$ is true. (basis)

2) Suppose that if $P(n)$ is true, then $P(n^+)$ is true. (induction step)

Then $P(n)$ is true $\forall n \in \mathbb{N}$.

Proof: Let $S \subseteq \mathbb{N}$ be the subset of $\mathbb{N}$ given by the $n \in \mathbb{N}$ for which $P(n)$ is true.

$$S := \{ n \in \mathbb{N} \mid P(n) \text{ is true} \}$$

1) We have that $1 \in S$.

2) We have that if $n \in S$, then $n^+ \in S$. But by Peano axiom ⑤, we obtain $S = \mathbb{N}$. So the statement is true. For all $n \in \mathbb{N}$.

Example: $1 + 2 + \dots + n = \frac{n \cdot (n+1)}{2}$ $\forall n \in \mathbb{N}$.

$P(1)$ is true, because $1 = \frac{1 \cdot 2}{2} = 1$. (we will define shortly formally what means $+$ and $\cdot$)

$P(n) \Rightarrow P(n+1)$ ...

We write $2 := 1^+$, $3 := 2^+ = (1^+)^+$, $4 := 3^+ = (2^+)^+ = ((1^+)^+)^+$

We have an ordering of $\mathbb{N}$ $\forall n : n < n^+$.

$1 < 2 < 3 < 4 < \dots$

↑ Peano

We write $m < n$ if n is obtained from m by applying the succ operation finitely many times.

Transitivity: if $m < n$, $n < k$, then $m < k$.

Irreflexivity: $m \not< m$.

not Peano

Trichotomy: Given $m, n \in \mathbb{N}$, we have that exactly one of the following is valid $m = n$, $m < n$ or $n < m$.

We write $m > n$ if $n < m$

bigger

We write $m \leq n$ if $m < n$ or $m = n$.

~~Theorem~~ (well ordering of $\mathbb{N}$)

Theorem: Every non-empty subset $S \subseteq \mathbb{N}$ has a minimal element. (that is, an element $a \in S$ s.t. $\forall n \in S$ one has $a \leq n$)

Proof: Suppose that $S \subseteq \mathbb{N}$ is a subset without a minimal element. We will show that S is empty. Let $B := S^c = \mathbb{N} \setminus S$. Showing $B = \emptyset$ is the same as showing $S = \mathbb{N}$. Note $1 \in B$, as otherwise 1 would belong to S and hence would be a minimal element. If $1, 2, \dots n \in B$, then $n^+ \in B$ as otherwise n^+ would be the minimal element of S.

By principle of mathematical induction $B = \mathbb{N}$ so $S = \emptyset$. ∎

Remarks: Variations of mathematical induction: (1) Suppose basis begin from 17. Suppose Strong induction

Assume $P(1)$ is true. Assume whenever $P(1) \dots P(n)$ are true then

$P(n+1)$ is true. Proof: $Q(n) = P(1) \dots P(n)$ hold.

from $Q(n)$ and $Q(n) \Rightarrow Q(n+1)$ are both true.

* Different base: $P(n)$ true $\forall n \geq m$ $P(n)$ true $\Rightarrow P(n+1)$ true then $P(n)$ true for all $n \geq m$

I-2-2 Operations in $\mathbb{N}$

Definition: For $n, m \in \mathbb{N}$ we define:

addition $n + m := \underbrace{((n^+)^+ \dots)}_{m\text{-times}} \in \mathbb{N}$

multiplication:

$$n \cdot m = \underbrace{n + n + \dots + n}_{m \text{ times}} \in \mathbb{N} \quad (\text{or } \cdot)$$

$n^+ = n + 1$.

Basic properties:

1) $n + m = m + n$ commutativity of addition
2) $n \cdot m = m \cdot n$ commutativity of multiplication.
3) $(n+m)+\ell = n+(m+\ell)$ 4) $(nm)\ell = n(m\ell)$
   associativity for addition ~> for multiplication.
5) $n \cdot 1 = 1 \cdot n = n$ (neutral element for multiplication)
6) $n(m+\ell) = nm + n\ell$ distributivity
7) $a < b \quad \forall c \in \mathbb{N} \quad a + c < b + c$ Proof: $c = 1$ ... $a+1 < b+1$ ... $a+c < b+c \Rightarrow a+c^+ < b+c^+$ ... $a+c < b+c \Rightarrow a+c^+ < b+c+1$ by induction
8) $a < b \quad \forall c \in \mathbb{N} \quad ac < bc$.

I-3 Integers

Definition: Define element 0 by setting it to be neutral element for addition. We write $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$

We define $0^+ = 1$. Define predecessor $\overset{-}{n}$ of $n \in \mathbb{N}$ to be s.t. $(n^-)^+ = n$

~~**Definition:** For each element $n \in \mathbb{N}$, we define $-n$ to be the inverse of n for addition. $n + (-n) = (-n) + n = 0$.~~

~~We define ...~~

~~**Definition:** We define ...~~

Definition: We define $\mathbb{Z} := \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$.

We extend successor to $\mathbb{Z}$ by declaring for $n \in \mathbb{N}$ that $n^+ = n+1$, $0^+ = 1$, $(-n)^+ = -n+1$.

Each element $n \in \mathbb{Z}$ has a unique successor and predecessor.

Def: For each element $n \in \mathbb{N}$ we define $-n$ as an inverse element to n with respect to addition.

We extend $\mathbb{Z} := \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$ negative integers

We define addition on $\mathbb{Z}$ as follows:

1) addition with zero: $\forall a \in \mathbb{Z} : a+0 = 0+a = a$

2) addition of negative integers: For $m, n \in \mathbb{N}$:

$(-m) + (-n) = -(m+n)$

3) Addition of a negative and positive integer

For $m, n \in \mathbb{N}$:

$$m + (-n) = (-n) + m = \begin{cases} k & \text{if } m = n+k \text{ for some } k \in \mathbb{N} \\ 0 & \text{if } m = n \\ -k & \text{if } n = m+k \text{ for some } k \in \mathbb{N}. \end{cases}$$

We define $m, n \in \mathbb{Z}$ $m - n = m + (-n)$.

Properties: For $n \in \mathbb{Z}$: $n^- = n - 1$.

Multiplication: For $m, n \in \mathbb{N}$, define $m \cdot (-n) = (-m) \cdot n = -(mn)$

$(-m) \cdot (-n) = mn$

For every $a \in \mathbb{Z}$ $a \cdot 0 = 0 \cdot a = 0$.

Properties: 1) $+$ and $\cdot$ are commutative.

2) $+$ and $\cdot$ are associative.

3) 1 is neutral element for multiplication and 0 for addition.

4) Distributivity $n(m+k) = nm + nk$. $m, n, k \in \mathbb{Z}$

Every element has an inverse

We define $a<b$ if there exists $n \in \mathbb{N}$ s.t. $b = a+n$

We obtain that

$$\cdots < -2 < -1 < 0 < 1 < 2 < 3 < \cdots$$

Set $a>b$ if $b<a$

1) irreflexivity $a \not< a$ $\forall a \in \mathbb{Z}$ ($1-1+1=0$)

2) trichotomy if $a,b \in \mathbb{Z}$ then $a<b$ or $a=b$ or $a>b$

Properties: ~~If $a \in \mathbb{Z}$~~ and $a,b \in \mathbb{Z}$ s.t. $a<b$

then $a+c < b+c$ $a,b,c \in \mathbb{Z}$

3) transitivity if $a<b$ and $b<c$ then $a<c$

4) if $a,b,c \in \mathbb{Z}$, $a<b$,

$a+c < b+c$ | $a<b$ then $b = a+m$ with $m \in \mathbb{N}$.

$(a+c)+m = a+(c+m) = a+(m+c)$

$= (a+m)+c$

$= b+c$

hence $b+c > a+c$.

5) if $a,b,c \in \mathbb{Z}$

$a<b$ if $c>0$ then $ac < bc$

if $c<0$ then $ac > bc$.

Define

We define $a \leq b$ if $a<b$ or $a=b$. $a \geq b$ if $b \leq a$.

Exercise: State and prove properties analogous to the above

1) reflexivity $a \leq a$ $\forall a \in \mathbb{Z}$ 3) transitivity

2) $\forall a,b$ $a \leq b$ or $b \leq a$ 4) $a,b,c \in \mathbb{Z}$ $a \leq b$

$a+c \leq b+c$

5) $a,b,c \in \mathbb{Z}$ $a \leq b$ if $c \geq 0$ then $ac \leq bc$

if $c \leq 0$ then $ac \geq bc$

I-4 Rational numbers $\mathbb{Q}$

I-4-1

Not all rational numbers have inverse for multiplication. (a does not have an inverse b s.t. $ab=1$, $b \in \mathbb{Z}$)

Example: 2 does not have an inverse for multiplication.

Proof: Assume on the contrary that 2 does have an inverse for multiplication.

$\exists m = 1$. Then $m \neq 0$, because $2 \cdot 0 = 0$. If $m > 0$

then $m \geq 1$. We have that $2m = m + m \geq 1 + m > m \geq 1$

which is not possible as $2m = 1$. So $m < 0$, hence $m \leq -1$

We have that $2m = m + m \leq -1 + m < m \leq -1$, a contradiction

Hence, 2 does not have a multiplicative inverse.

Definition We construct $\mathbb{Q}$ as follows:

$$\mathbb{Q} := \left\{ \frac{m}{n} \mid m \in \mathbb{Z},\ n \in \mathbb{Z} - \{0\} \right\}$$

where $\frac{m}{n} = \frac{a}{b}$ if and only if $m \cdot b = n \cdot a$.

$m \in$ numerator

$n \in$ denominator.

Definition: Addition $\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$ $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$.

Subtraction $\frac{a}{b} - \frac{c}{d}$

additive Inverse $-\frac{a}{b} := \frac{-a}{b}$.

Subtraction $\frac{a}{b} - \frac{c}{d} := \frac{a}{b} + \left(\frac{-c}{d}\right) = \frac{ad - bc}{bd}$

Multiplication $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Division $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, $\frac{c}{d} \neq 0$

$\frac{a}{b} / \frac{c}{d} := \frac{ad}{bc}$.

We identify $\mathbb{Z}$ as a subset of $\mathbb{Q}$

$$n = \frac{n}{1}.$$

Properties: 1) commutativity of $+$ and $\cdot$

2) associativity of $+$ and $\cdot$

3) distributivity $\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$

4) neutral element for addition: 0

— " — for multiplication: 1

5) Every element has a unique additive inverse

every element distinct from zero has a unique multiplicative inverse

: the inverse of $\frac{a}{b}$ is $\frac{b}{a}$ (Endlich, Proof: $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1} = 1$)

$ab \cdot 1 = ab$?

I - 4 - 2 Ordering of $\mathbb{Q}$

Lemma: Each $q \in \mathbb{Q}$ can be represented as a fraction $q = \frac{a}{b}$ with $b \in \mathbb{N}$.

Proof: We have that $q = \frac{c}{d}$ with $c \in \mathbb{Z}$ and $d \in \mathbb{Z} \setminus \{0\}$.
If $d > 0$, then set $b = d$ and $a = c$. We have $q = \frac{a}{b}$ with $b \in \mathbb{N}$. If $d < 0$, set $b = -d$ and $a = -c$.
We have that $q = \frac{c}{d} = \frac{-c}{-d} = \frac{a}{b}$ and $b \in \mathbb{N}$.

(in general $\frac{c}{d} = \frac{ck}{dk}$ for $k \in \mathbb{Z} - \{0\}$ because $cdk = dck$)

Definition We define $q_1 < q_2$ if $q_1 = \frac{a}{b}$ and $q_2 = \frac{c}{d}$ with $a, b, c, d \in \mathbb{Z}$ and $b, d \in \mathbb{N}$ if $ad < bc$. We define $q_1 > q_2$ if $q_2 < q_1$.
We define $q_1 \geq q_2$ if $q_1 > q_2$ or $q_1 = q_2$. (similarly for $\leq$)

Properties: 1) Irreflexivity $a \not< a$ 3) transitivity
2) trichotomy 4) $a < b$, $a, b \in \mathbb{Q}$, $c \in \mathbb{Q}$ $a + c < b + c$.
5) $a < b$, $a, b \in \mathbb{Q}$, $c > 0$ then $ac < bc$
$c < 0$ then $ac > bc$.

Properties of $\leq$ 1) Reflexive $a \leq a$, 2) trichotomy
3) transitivity 4) / 5) Analogous / 4.5 !

Proof of 5) $c>0$

$a = \frac{m}{n}$ $b = \frac{p}{q}$, $c = \frac{r}{s}$

with $m, n, p, q, r, s \in \mathbb{Z}$ and $n, q, s \in \mathbb{N}$

As $c>0$ $r>0$

$\frac{r}{s} > 0 = \frac{0}{1}$

$a < b \Rightarrow mq < pn$.

(implies) (multiply by rs)

$\Leftrightarrow r > 0$

(equivalent)

Properties in $\mathbb{Z}$.

$ac < bc \Leftrightarrow \frac{mr}{ns} < \frac{pr}{qs}$

$\Leftrightarrow mrqs < prns$.

Fact

Proposition: If $q \in \mathbb{Q} - \{0\}$, then $q^2 > 0$. ($q^2 = q \cdot q = q \cdot \ldots \cdot q$, n-times)

Note $a \neq 0$ as $\frac{a}{b} > 0$

Alt. use 5).

Proof: Write $q = \frac{a}{b}$, with $a \in \mathbb{Z}$, $b \in \mathbb{N}$. We have $q = \frac{a^2}{b^2}$

$b^2 \in \mathbb{N}$. We have that $q > 0 \Leftrightarrow \frac{a^2}{b^2} > \frac{0}{1} \Leftrightarrow a^2 \cdot 1 > b^2 \cdot 0$

$\Leftrightarrow a^2 > 0$.

a) If $a > 0$ then $a \in \mathbb{N}$ and $a^2 \in \mathbb{N}$ hence $a^2 > 0$.

If $a < 0$ then $a^2 = (-1)(-1) \cdot 1 \cdot a^2 = (-1) \cdot a \cdot (-1) \cdot a = \underbrace{(-a)}_{\in \mathbb{N}} \cdot \underbrace{(-a)}_{\in \mathbb{N}} \in \mathbb{N}$

hence $a^2 > 0$. If $a < 0$.

Fun Fact
$-a = (-1) \cdot a$
$a + (-a) = 0$
$(-a)\ a + (-1) \cdot a$
$= 1 \cdot a + (-1) \cdot a$
$= (1 + (-1)) \cdot a$
$= 0 \cdot a$

Hence $a^2 > 0$ and thus $q > 0$.

