1st Lect.
2.10.18

· mail, web
· tutorial warning

Real analysis · sequences, series of reals – infinite sums
· functions ~~#~~of reals

· not only how to solve problems, ~~but~~ $\boxed{\text{why}}$ solution works
[difference from high school : you all know
formula for roots of quadratic eq., Pyth. theorem
Q: - who would be able to explain why they work ?)
Tools for other subjects: analysis of algorithms ...

Logic & proofs

· proposition ~~#~~ = statement, sentence
– ~~which~~ is True ~~or~~ or False
[we might not be able to decide, no one knows whether π^π is a rational number]

examples: NO : 5+13 , n is even
YES : 5+13 = 7 , 4 is even, every ~~#~~ natural number n is even

$\forall n \in \mathbb{N}$: n is even
$\exists n \in \mathbb{N}$: n is even

there exist a natural number ~~#~~ n which is even

Negation · ~~#~~ every proposition can be negated
· negation of a true proposition is a false proposition (not an alternative fact)
· neg. of a false proposition is a true prop.
[if this does not work you are not negating properly]

· P proposition, negation $\neg P$

Logical connectives · and $\wedge$, &
· or $\vee$
· implication $\Rightarrow$
"if - then"

2 is even and 2 is a prime
2 is even or 2 is odd
2 is even or 2 is prime

true regardless of relationship ~~whether Alice is~~ between A and b

If Alice is a sister of Bob's mother, then Alice is Bob's aunt.

Note: ~~from the fact that it...~~ if the first part of the statement is false, we cannot conclude anything about the second part (Alice can be Bob's father's sister)

- Equivalence "$\Leftrightarrow$" „if and only if"

Alice is Bob's mother $\Leftrightarrow$ Bob is Alice's son

[true ~~...~~ unless something strange with genders is happening]

- Quantifiers
  - universal $\forall$ „(for) all / (for) every"
  - existential $\exists$ „there exists"

  $\exists!$ „there is exactly one"

  - ~~...~~
  - $\forall$ child C $\exists!$ woman W ~~...~~ such that: W is a mother of C (true)
  - $\exists$ woman W $\forall$ child C : W is a mother of C (not true)

- we always quantify over some set (in the previous cases over sets of all women, children, resp.), $\forall x \in \mathbb{R} : x^2 \geq 0$ often over set of all natural numbers ... ~~...~~

I will not elaborate on how to negate etc.
- Ask if something is unclear
- Attend mathematical skills if needed

Proofs
- direct ~~...~~. Sum of two even integers is an even integer.

~~i.e. if ... even integers x, y ...~~

Proof. x, y even, therefore $\exists$ integers a, b such that $x = 2a$, $y = 2b$

Then, $x + y = 2a + 2b = 2(a+b)$, ~~...~~

since $a+b$ is integer $\underbrace{2(a+b)}_{=x+y}$ is an even ~~...~~.

~~indirect~~ Proof by contrapositive

"$A \Rightarrow B$" we prove "$\neg B \Rightarrow \neg A$" instead

For $\forall n \in \mathbb{N}$: If n ~~≥0~~ $\in \mathbb{N}$ ~~and~~ $4^n - 1$ is prime, then n is odd.

Contra ~~Coun~~terpositive: $\forall n \in \mathbb{N}$: n is even $\Rightarrow$ $4^n - 1$ is not a prime

Proof n even, thus $\exists k \in \mathbb{N}: n = 2k$

Then $4^n - 1 = 4^{2k} - 1 = (4^k - 1)(4^k + 1)$, $4^k \geq 4$, $\boxed{4^k - 1,\ 4^k + 1 \geq 1}$

$\Rightarrow 4^n - 1$ not a prime (has two factors > 1)

[Q: works if we replace 4 by 2 ?]

Proof by contradiction

- start with a negation of the statement and reach a conclusion which we know is false

Example:

Theorem (irrationality of $\sqrt{2}$)

There is no fraction $\frac{a}{b}$, where $a, b \in \mathbb{Z}$, $b \neq 0$ such that $\left(\frac{a}{b}\right)^2 = 2$.

Assume that such a fraction a/b exists.

Proof: WLOG (= Without loss of generality) assume that $\frac{a}{b}$ is irreducible (i.e., a and b are coprime), b positive

- $\left(\frac{a}{b}\right)^2 = 2$ thus $\overset{(b \neq 0)}{a^2 = 2b^2}$ thus $2 \mid a^2$ thus $2 \mid a$

$\Rightarrow$ a is even $a = 2c$ for some $c \in \mathbb{Z}$, $a^2 = 4c^2$

Thus $4c^2 = 2b^2 \quad | : 2$

$2c^2 = b^2 \Rightarrow$ thus b is even $\lightning$ a, b coprime

Proof by induction

~~Statem~~ Proposition $\forall n \in \mathbb{N} : V(n)$

We show · $V(1)$ is true [sometimes we need ~~n~~ also $V(2)$:]

$\forall n \in \mathbb{N}: \underbrace{V(n)}_{\text{induction hypothesis (IH)}} \Rightarrow V(n+1)$ → domino effect

Strong induction: $\forall n \in \mathbb{N}: \left(\forall k \in \mathbb{N}, k \leq n \; V(n)\right) \Rightarrow V(n+1)$ $\quad V(n) =$ „n is odd" „$n^2 \geq 0$"

Example

Theorem (Bernoulli inequality)

For every real $x \geq -2$ and a natural number n,

$V(n)$: $(1+x)^n \geq 1+nx$.

Proof (induction)

$n=1$: $LS = (1+x)^1 = 1+x = RS$ ✓

$n=2$: $LS = (1+x)^2 = 1+2x+x^2 \geq 1+2x = RS$ ✓ (as $x^2 \geq 0$)

We show $\forall n \in \mathbb{N}: V(n) \Rightarrow V(n+2)$

[so $V(1) \Rightarrow V(3) \Rightarrow V(5) \dots$, $V(2) \Rightarrow V(4) \Rightarrow \dots$]

Assume $(1+x)^n \geq 1+nx$)

Then $(1+x)^{n+2} = (1+x)^n \cdot (1+x)^2 \overset{\text{ind. hyp.} + ⊛}{\geq} (1+nx)(1+x)^2$

$= (1+nx)(1+2x+x^2) = 1+2x+x^2+nx+2nx^2+nx^3$

$= \underbrace{1+x(n+2)}_{RS} + \underbrace{x^2}_{\geq 0} + \underbrace{x^2}_{\geq 0}\underbrace{n}_{\geq 0}\underbrace{(2+x)}_{\geq 0}$

⊛ true because $(1+x)^2 \geq 0$, in general, $a \geq b \not\Rightarrow ac \geq bc$ (e.g. $c=-1$) ■

Theorem: Every natural number $n > 1$ is divisible by some prime.

Proof. $n = 2$: $2 \mid 2$, 2 prime ✓

ind. hyp for n: $\forall k \overset{>1}{\leq} n$: k is divisible by a prime

· Let D be a set of divisors of $n+1$ different from 1 and $n+1$

$D = \emptyset$: $n+1$ is a prime, $n+1 \mid n+1$ ✓

$D \neq \emptyset$: take $d \in D$, $1<d\leq n$, by IH d is divisible by a prime $p \Rightarrow n+1$ is div. by p

2nd lecture

9.10.18

Sets & functions

- sets = collections of elements (possibly inf. many, possibly 0)
- $\subset (\subseteq)$ „subset", $\cup$, $\cap$ $\quad \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \ldots$

$A_1 \ldots A_n$ sets $\quad \bigcup_{i=1}^{n} A_i = A_1 \cap A_2 \ldots$

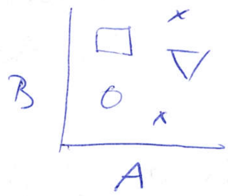
- $\setminus$ $\quad A \setminus B =$ ~~A~~ elements in A which are not in B
- $P(X)$ set of subsets
- kartesian product $A \times B = \{(a,b) \mid a \in A, b \in B\}$

$A \times B \times C = \{(a,b,c) \mid \ldots\}$

! $A \cup B = B \cup A$, $A \cap B = B \cap A$ but $A \setminus B \neq B \setminus A$

$A \times B \neq B \times A$

Binary relations $R \subset A \times B$



Function

- a binary relation ~~such~~ $f \in A \times B$ is a function if $\forall a \in A \; \exists! \, b \in B : (a,b) \in f$
- usually we use different notation and write

$f : A \to B$ domain co-domain, $f(a) = b \in$ image of a

$a \ldots$ preimage of b (might not be unique)

- f injective:

$\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

- f surjective: $\forall b \in B \; \exists a \in A : f(a) = b$
- f is a bijection: surjective & injective

= one-to-one

ev

A finite: $f : A \to A$ inj. $\Leftrightarrow$ surj

$f : \mathbb{N} \to \mathbb{N}$ give examples

Another type of binary relation is

PARTIAL ORDER ~~S~~ on ~~X~~. relation ~~only~~ on ~~A~~ $\times$ ~~A~~, ~~relation~~ ~~A~~ (product of a set with itself)

Def. by example

- examples $\leq$ for $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$

$\subseteq$ for sets [some pairs of sets are ordered, some not]

divisibility for ~~...~~ $\mathbb{N}$

- I expect you will have exact def. in DM, unless ~~...~~ you had it already

We will almost always consider $\leq$ on $\mathbb{R}$, but let me state the following definition for a general partial order $\leq$ on some set X

Def

$x \in X$ is an upper bound of $A \subseteq X$ if $\forall a \in A: a \leq x$

a lower bound of $A \subseteq X$ if $\forall a \in A: a \geq x$

NOTE: x might not belong to A!

Example: $X = \mathbb{R}$, $A = \{\frac{1}{n} \mid n \in \mathbb{N}\}$

- upper bounds: 1 and all bigger
- lower bounds: 0 and all smaller

(is there some lower bound > 0? NO, we will discuss in a while)

$x \in X$ is a supremum of $A \subseteq X$ if it is a smallest upper bound, that is, x is an upper bound of A and for any other upperbound x' of A, $x' \geq x$

~~Example~~: We write $\sup A = x$

Ex.: $\sup\{\frac{1}{n} \mid n \in \mathbb{N}\} = 1$

an infimum of $A \subseteq X$ if it is a largest lower bound, that is, x is an upper bound of A and for any other upper bound x' of A, $x' \leq x$

We write $\inf A = x$

Ex. We guessed that $\inf\{\frac{1}{n} \mid n \in \mathbb{N}\} = 0$

Proof: Clearly, 0 is a lower bound.

We want to show that every other lower bound x' is ≤ 0.

For contradiction, assume that $x' > 0$ is a lower bound. We find n s.t. $\frac{1}{n} < x'$, getting a contradiction.

~~Consider a number~~ Consider $n = \left\lceil \frac{1}{x'} \right\rceil + 1$

- $n \in \mathbb{N}$, so $\frac{1}{n} \in \{\frac{1}{n} \mid n \in \mathbb{N}\}$
- moreover, $n > \frac{1}{x'}$, so $x' > \frac{1}{n}$ $\lightning$ with assumption that x' is a lower bound

NOTE: sup belongs to the set, inf does not

A set $A \subseteq X$ is
- **bounded from above** if there exists an upper bound
- **bounded from below** if there exists a lower bound
- **bounded** = b. from above & below

Ex. $\{\frac{1}{n} \mid n \in \mathbb{N}\}$ bounded

$\{n \mid n \in \mathbb{N}\}$ b. from below, not from above

NOTE:
- sup. & inf are unique, up./low. bounds are not
- bounded set has upper & lower bound but not necessarily sup & inf!

Ex. $X = \mathbb{Q}$

$A = \{a \in \mathbb{Q} \mid a^2 < 2\}$

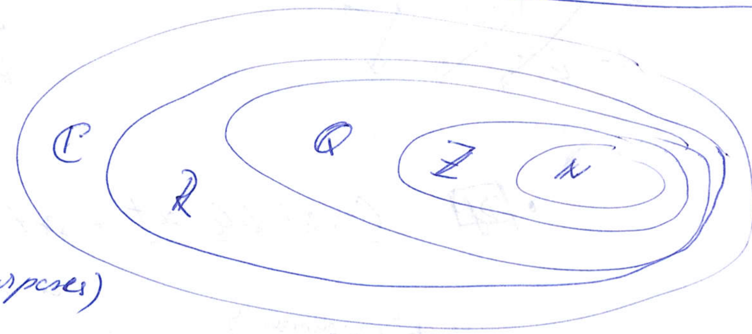
intuitively: sup A should be $\sqrt{2}$, but we know that $\sqrt{2} \in \mathbb{Q}$, ~~[illegible]~~

[one should still show that no rational number is sup, but we ~~[illegible]~~ need to know a bit more to prove it]

„ $\mathbb{Q}$ are incomplete "

Numbers

We will be satisfied with informal definitions (formal are unnecessary complicated for our purposes)



- natural numbers $\mathbb{N} = \{1, 2, \dots\}$ — equation $x + 5 = 2$ does not have a solution in $\mathbb{N}$
- integers $\mathbb{Z} = \mathbb{N} \cup \{0, -1, -2, \dots\}$ — eg. $2x + 5 = 2$ does not have a sol.
- rationals = fractions $\mathbb{Q} = \underbrace{\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\} / \sim}$ „equivalence classes"
  - fractions $\frac{a}{b}, \frac{c}{d}$ are equivalent (equal) if $a \cdot d = b \cdot c$ = they represent the same rational number
  - decimal expansion
    - finite or periodic
    - not unique: $0,\overline{9} = 0{,}999\ldots = 1$

$x^2 = 2$ has no solution in $\mathbb{Q}$

• reals $\mathbb{R}$ • „filling the gaps bettween rational numbers" • dec. exp. except $0,\dots\bar{9}$

• no solution to $x^2 = -1$

• complex numbers $\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$ i = imaginary unit, $i^2 = -1$

(we will not really use them)

3rd lecture 16.10

Size of infinite sets

• are there more integers (or reals) than natural numbers ?

• intuitively: yes (they are a superset) / No all are inf / all different sizes

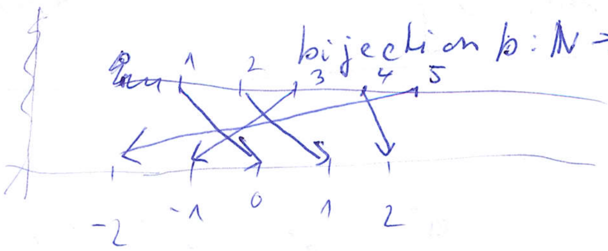
Definition: Sets have the same cardinality (= size), if there exists a bijection between them.

Finite sets: Imagine you need to find out if there is the same number of men and women in a dancing hall. Solution: ask them to form pairs, see if there is anyone left.

The same for infinite sets:

• cardinality of $\mathbb{N}$ and $\mathbb{Z}$ is the same

bijection $b:\mathbb{N}\to\mathbb{Z}$



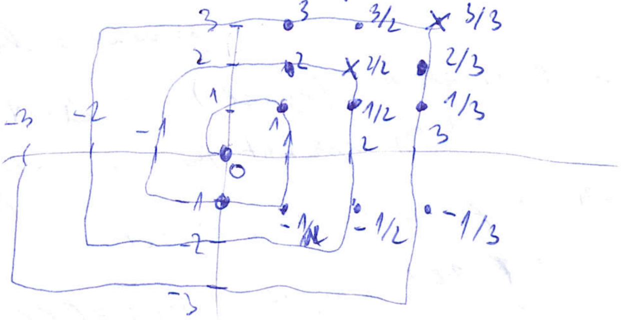
$b(1) = 0$
$b(2k) = k$
$b(2k+1) = -k$

• Df **Countable set** = set such that there exists a bijection $b:\mathbb{N}\to$ the set (i.e., we can label the elements of the set by nat. numbers)

• „smallest" cardinality of an infinite set

• $\mathbb{N}, \mathbb{Z}$ are countable

• is $\mathbb{Q}$ countable?, YES consider irreducible fractions in the grid $\mathbb{Z}\times\mathbb{Z}$: walk in the spiral starting from 0, assign number n to the n-th fraction you meet



NOTE: if a set is countable, every its inf. subset is countable (shift bijection by one for every missing element)

• is $\mathbb{R}$ countable ? NO

Theorem (Cantor 1873) Set of real numbers is uncountable.

Proof: By contradiction. Take a subset of reals defined as follows $X = \{ 0,c_1c_2 \dots \mid c_i \in \{0,1\}\}$

• inf. decimal expansion from 0s and 1s

• we will show that X is not countable

• assume it is and let b be a bijection ~~f~~ $\mathbb{N} \to X$

so $b(k) = 0, c_{1,k}\, c_{2,k}\, c_{3,k} \dots$

• denote $\bar{c}_{m,k} = 1 - c_{m,k}$ (swaps 1 and 0)

• consider ~~a~~ number $p = 0, \bar{c}_{11}\, \bar{c}_{22}\, \bar{c}_{33} \dots$

• $p \in X$, but it differs from each $f(n)$ on n-th decimal place $\lightning$ b is a bijection as there is no $n \in \mathbb{N}$ such that $b(n) = p$.

set card. – finite
infinite – countable
– uncountable

Cantor diagonal method

• similarly, we can show that $P(\mathbb{N})$ = set of all subsets of $\mathbb{N}$ is uncountable

---

Properties of real numbers

• Field (algebraic) = set T with operations $+$ and $\cdot$ satisfying the following axioms:

(+) • commutativity ~~an~~ $\forall a,b \in T: a+b = b+a$

• associativity $\forall a,b,c \in T: a+(b+c) = (a+b)+c$

• existence of zero (neutral element) $\exists 0 \in T$ that: $a + 0 = a$

• existence of invers $\forall a \in T\ \exists b \in T: a+b = 0$

we write $\boxed{b = -a}$

(∗) • commutativity $\forall a,b \in T\quad a\cdot b = b \cdot a$

• associativity $\forall a,b,c \in T\quad a\cdot(b\cdot c) = (a \cdot b)\cdot c$

• existence of one (neutr. el.) $\exists 1 \in T\ \forall a \in T: 1 \cdot a = a$

• existence of invers $\forall a \in T, a \neq 0\ \exists b \in T: a \cdot b = 1$

we write $b = a^{-1} = \frac{1}{a}$

- distributivity: $\forall a,b,c \in F$ $(a+b)\cdot c = ac+bc$
- non-triviality: $0 \neq 1$

$\boxed{ex}$: uniqueness of $0, 1, -a, a^{-1}$ from axioms

- $\mathbb{R}$ is a field
- moreover: $\mathbb{R}$ is an <u>ordered</u> field, that is, there is <u>linear order</u> $\leq$ such that
  - $\forall a,b,c \in \mathbb{R}: a \leq b \Rightarrow a+c \leq b+c$
  - $\forall a,b \in \mathbb{R}: a \geq 0 \wedge b \geq 0 \Rightarrow a\cdot b \geq 0$
- is $\mathbb{Q}, \mathbb{Z}, \mathbb{N}$ field? $\mathbb{C}$?
- $\{0,1\}$ with operations mod 2
  - is it an ordered field? $\mathbb{Z}_2$ no

<u>Axiom of completeness</u>

$\forall X, Y \subseteq \mathbb{R}$ ~~sad tha~~ ~~su~~ such that $\forall x \in X\, \forall y \in Y: x \leq y$

$\exists c \in \mathbb{R}$ such that $\forall x \in X$ $x \leq c$ and $\forall y \in Y$ $c \leq y$.

NOTE: $\mathbb{Q}$ not complete
$X = \{q \mid q^2 < 2\}$
$Y = \{q \mid q^2 > 2\}$

<u>Theorem</u> $\mathbb{R}$ is the only ~~com~~ complete ordered field, up to isomorphism. [I.e.: we can rename elements, but they will be in 1-to-1 corresp. to $\mathbb{R}$.]

<u>~~Corollary~~ Consequence of the completeness axiom</u>

<u>Theorem</u> (existence of sup and inf of bounded set in $\mathbb{R}$)

Every non-empty subset of $\mathbb{R}$ bounded from above has supremum.
— // — from below has minimum.

<u>Proof</u>: Let X be nonempty, bounded from above.

We define $Y = \{y \in \mathbb{R} \mid \forall x \in X: x \leq y\}$, i.e. Y is a set of upper bounds of X

$Y \neq \emptyset$ since X is bounded from above.

By ax. of completeness $\exists c \in \mathbb{R}$ s.t. $\forall x \in X: x \leq c$, i.e, c is an upper bound and $\forall y \in Y: y \geq c$, i.e., c is the smallest upper bound = supremum.

Infimum analogously

Other important properties of numbers

Theorem (density of rational and irrational numbers)
$\forall a, b \in \mathbb{R}$ such that $a < b$, $\exists r \in \mathbb{Q}$ and $s \in \mathbb{R} \setminus \mathbb{Q}$ such that $a < r < b$ and $a < s < b$.

Proof: homework

Theorem (AG-inequality)
Let $a_1 \dots a_m \in \mathbb{R}^+$.
Then $$\frac{\sum_{i=1}^{m} a_m}{m} \geq \sqrt[m]{a_1 \dots a_m}.$$
Where $=$ holds if and only if $a_1 = a_2 = \dots = a_m$.

Let a_i
Arithmetic mean of $a_1 \dots a_m \in \mathbb{R}^+$ $= \frac{\sum_{i=1}^{m} a_i}{m}$

Geometric mean $= \sqrt[m]{a_1 \dots a_m}$

Absolute value $|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$

$|a-b|$ = „distance between a and b"
(length of interval $[a, b]$)

Triangle inequality $\forall a, b \in \mathbb{R}$: $|a| + |b| \geq |a+b|$

[usually Δ-ineq. says that sum of two sides of rectangle is bigger than the third side. We get the claim above by considering points $x, y, z \Rightarrow \Delta$-ineq. says
$$|x-y| + |y-z| \geq |x-z|$$
let $a = x - z$
$b = y - z$
$a + b = x - z$]

Infinite sequences and their limits

Def. Infinite sequence of elements of a nonempty set A (typically $A = \mathbb{R}, \mathbb{R}^+$) is a function $n \mapsto a_n$ from $\mathbb{N}$ to A. We denote such sequence $(a_n)_{n=1}^{\infty}$ or just (a_n), we say a_n is its n-th term.

[we can define finite sequence similarly but they are not so interesting, from now on sequence = inf. seq. unless said otherwise]

E.g. $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$; Fib seq. $a_1 = 1$, $a_2 = 1$, $a_3 = a_1 + a_2$, $a_n = a_{n-1} + a_{n-2}$

Def. Let $(a_n)_{n=1}^{\infty}$ be a sequence of reals.
A number $a \in \mathbb{R}$ is a limit of (a_n), we write

$$\lim_{n\to\infty} a_n = a \quad \text{if} \quad \forall \varepsilon > 0 \ (\varepsilon \in \mathbb{R}) \ \exists n_0 \in \mathbb{N} \ \forall n \in \mathbb{N}, n \geq n_0 : |a_n - a| < \varepsilon$$

Then we say that (a_n) converges and has proper limit.
Otherwise, we say that (a_n) diverges.

Def. We say that limit of (a_n) is ∞ if

$$\forall K \in \mathbb{R} \ \exists n_0 \in \mathbb{N} \ \forall n \in \mathbb{N}, n \geq n_0 : a_n > K$$

and is $-\infty$ if $\forall K \in \mathbb{R} \ \exists n_0 \in \mathbb{N} \ \forall n \in \mathbb{N} \ n \geq n_0 : a_n < K$

If limit of (a_n) is ∞ or $-\infty$, we say that (a_n) has improper limit (but diverges!)

I.e.
- converges = has proper limit — $1/n$, 1
- diverges
  - has improper limit — n
  - does not have limit at all — $(-1)^n$