LECTURE 1, 2/16/2022

SETS, FUNCTIONS, REAL NUMBERS

• *What does the mathematical analysis analyze?* Infinite processes and operations. Let us have a look at two paradoxes.

$$S = 1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} + \cdots + \underbrace{\frac{1}{n} - \frac{1}{n}}_{=0} + \cdots = 0\ ,$$

but also, after reordering the summands,

$$S = 1 + \frac{1}{2} - 1 + \frac{1}{3} + \frac{1}{4} - \frac{1}{2} + \cdots + \underbrace{\frac{1}{2n-1} + \frac{1}{2n} - \frac{1}{n}}_{=\frac{1}{2n(2n-1)}>0} + \cdots > 0\ ?$$

Then we have the following infinite table with entries -1, 0 and 1

1	-1	0	0	0	$\ldots$	$\sum = 0$
0	1	-1	0	0	$\ldots$	$\sum = 0$
0	0	1	-1	0	$\ldots$	$\sum = 0$
0	0	0	1	-1	$\ldots$	$\sum = 0$
0	0	0	0	1	$\ldots$	$\sum = 0$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\sum = 1$	$\sum = 0$	$\sum = 0$	$\sum = 0$	$\sum = 0$	$\ldots$	$\sum = 1 \setminus 0$

?

in which the sum of row sums differs from the sum of column sums.

• *Review of logical and set-theoretic notation.* Logical connectives: $\varphi \vee \psi$ ... or, $\varphi \wedge \psi$ ... and, $\varphi \Rightarrow \psi$ ... implication, $\varphi \iff \psi$ ... equivalence, $\neg\varphi$ ... negation. For example, it always holds that

$$\neg(\varphi \vee \psi) \iff \neg\varphi \wedge \neg\psi\ .$$

Hence brackets and binding strength of each connective are also important. Quantifiers: $\forall\, x:\ \ \varphi(x)$ ... for every x it holds that $\varphi(x)$, $\exists\, x:\ \ \varphi(x)$ ... there is an x such that $\varphi(x)$ holds. For example, it always holds that

$$\neg(\exists\, x:\ \varphi(x)) \iff \forall\, x:\ \neg\varphi(x)\ .$$

We denote the empty set by $\emptyset$ and $x \in A$ means that the set x is an element of the set A. A set M may be written down either by listing its elements, like in

$$M = \{a,\, b,\, 2,\, \{\emptyset,\, \{\emptyset\}\},\, \{a\}\}$$

(how many of them does M have?), or by specifying these elements by some property. For example (here $\mathbb{N} := \{1, 2, 3, \dots\}$),

$$M = \{n \in \mathbb{N} \mid \exists\, m \in \mathbb{N}:\ n = 2 \cdot m\}$$

is the set of (all) even natural numbers.

Relations between sets: $A \subset B \overset{\text{def}}{\iff} \forall\, x:\ \ x \in A \Rightarrow x \in B$ ... A is a subset of B, $\neg\exists\, x:\ \ x \in A \wedge x \in B$ ... A and B are disjoint, $A = B \iff (\forall\, x:\ \ x \in A \iff x \in B)$ is the *axiom of extensionality* that determines equality of two sets.

Operations with sets: $A \cup B := \{x \mid x \in A \vee x \in B\}$ is their union, $A \cap B := \{x \in A \mid x \in B\}$ is their intersection, $\bigcup A := \{x \mid \exists\, b \in A:\ \ x \in b\}$ is the sum of A, $\bigcap A := \{x \mid \forall\, b \in A:\ \ x \in b\}$ is the intersection of A, $A \setminus B := \{x \in A \mid x \notin B\}$ is the set difference of A and B, and

$$\mathcal{P}(A) := \{X \mid X \subset A\}$$

is the *power set* of the set A.

- *Ordered pairs and functions.* For two sets A and B, the set

$$(A,\, B) := \{\{B,\, A\},\, \{A\}\}$$

is the *(ordered) pair* of A and B. It always holds that

$$(A,\, B) = (A',\, B') \iff A = A' \wedge B = B'\ .$$

It is possible to define the ordered triple of sets A, B and C by

$$(A,\, B,\, C) := (A,\, (B,\, C))\ ,$$

and similarly the ordered quadruple (A, B, C, D) etc., but it is better to set

$$(A,\, B,\, C) := \{(1,\, A),\, (2,\, B),\, (3,\, C)\}$$

etc. The *Cartesian product* of sets A and B is the set

$$A \times B := \{(a,\, b) \mid a \in A,\, b \in B\}\ .$$

Any subset $C \subset A \times B$ is a *(binary) relation* between A and B. Instead of $(a, b) \in C$ we write $a\,C\,b$, for instance $2 < 5$. If $A = B$, we speak of a relation on the set A.

Definition 1 (function) *A function (or a map) f from a set A to a set B is any ordered triple*

$$(A,\, B,\, f)$$

such that $f \subset A \times B$ and for every $a \in A$ there is exactly one $b \in B$ with $a\,f\,b$. We write that $f\colon A \to B$ and $f(a) =\ b$.

The set A is the *definition domain* of the function f and B is its *range*. The element b is the *value* of f on the *argument* a. For $C \subset A$, resp. $C \subset B$, the set

$$\begin{aligned} f[C] &:= \{f(a) \mid a \in C\} \subset B\ , \text{ resp.} \\ f^{-1}[C] &:= \{a \in A \mid f(a) \in C\} \subset A\ , \end{aligned}$$

is the *image* of C in f, resp. the *preimage* of C in f.

• *Families of functions, operations with functions.* A *sequence* (in a set X) is a function

$$a\colon \mathbb{N} \to X\ .$$

We write $(a_n) = (a_1, a_2, \dots) \subset X$ and $a_n := a(n)$, $n \in \mathbb{N}\,(= \{1, 2, \dots\})$. A *word* (over an alphabet X) is a function

$$u\colon [n] \to X$$

for some $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$, where $[n] := \{1, 2, \dots, n\}$ and $[0] := \emptyset$. For $n = 0$ also $u = \emptyset$. We write $u = a_1 a_2 \dots a_n$, where $a_i := u(i)$ for $i \in [n]$. A *(binary) operation* (on a set X) is a function

$$o\colon X \times X \to X\ .$$

Instead of $o((a, b)) = c$ we write $a\,o\,b = c$, for instance $1 + 1 = 2$.

A function $f\colon X \to Y$ is *injective* (an *injection*) if for every $a, b \in X$ one has that $a \neq b \Rightarrow f(a) \neq f(b)$. It is *onto* (or *surjective*, a *surjection*) if $f[X] = Y$. It is *one-to-one* (or *bijective*, a *bijection*) if it is injective and onto. It is *constant* if there is a $c \in Y$ such that $f(a) = c$ for every $a \in X$. A function $f\colon X \to X$ is an *identity function* if $f(a) = a$ for every $a \in X$.

If $f\colon X \to Y$ is an injection, the *inverse (function)* of f is the function $f^{-1}\colon f[X] \to X$ given by $f^{-1}(y) = x \iff f(x) = y$. For two functions

$$g\colon X \to Y \text{ and } f\colon Y \to Z$$

their *composition* (or the *composed function*) is the function

$$f \circ g = f(g)\colon X \to Z$$

given by $f(g)(a) := f(g(a))$, $a \in X$.

- *Linear orders, infima and suprema.*

Definition 2 (linear order) *A linear order on a set A is any relation $<$ on A that is $(a, b, c \in A)$*

1. *irreflexive:* $\forall\, a:\ a \not< a$,
2. *transitive:* $\forall\, a, b, c:\ a < b \wedge b < c \Rightarrow a < c$ *and*
3. *trichotomic:* $\forall\, a, b:\ a < b \vee b < a \vee a = b$.

Note that 1 and 2 imply that in 3 always exactly one possibility occurs. The notation $a \le b$ means that $a < b \vee a = b$, $a > b$ means that $b < a$, and similarly for $a \ge b$. We write $(A, <)$ or $(A, <_A)$ to invoke a linear order on A.

Let $(A, <)$ be a linear order on A and let $B \subset A$. We say that B is *bounded from above* if there is an $a \in A$ such that $b \le a$ for every $b \in B$. Then a is an *upper bound* of B. Boundedness from below and lower bounds are defined similarly. The set of all upper (resp. lower) bounds of B is denoted by $U(B)$ (resp. $L(B)$). The *maximum* (or the *largest element*) of B, which need not exist, is a $b \in B$ such that $\forall\, b' \in B:\ b' \le b$. The *minimum* (or the *least* *element*) of B is defined similarly. These elements are denoted as $\max(B)$ and $\min(B)$.

> **Definition 3 (supremum and infimum)** *Suppose that $(A, <)$ is a linear order on A and $B \subset A$. If $U(B) \neq \emptyset$ and $\min(U(B))$ exists, we call it the supremum of B and denote it by*
>
> $$\sup(B) := \min(U(B)) \ .$$
>
> *If $L(B) \neq \emptyset$ and $\max(L(B))$ exists, we call it the infimum of B and denote it by*
>
> $$\inf(B) := \max(L(B)) \ .$$

For example, in the standard linear order of real numbers $\min((0,1))$ does not exist, $\min([0,1)) = 0$, $\inf((0,1)) = \inf([0,1)) = 0$ and $\sup(\mathbb{N})$ does not exist because $U(\mathbb{N}) = \emptyset$.

- *Ordered fields.* We need them to define real numbers.

Definition 4 (ordered field) *An ordered field F is an algebraic structure*

$$F = (F,\, 0_F,\, 1_F,\, +_F,\, \cdot_F,\, <_F)$$

on a set F that has two distinct distinguished elements 0_F and 1_F in F, two operations $+_F$ and $\cdot_F$ on F and a linear order $<_F$ on F, and is such that the following axioms hold ($a, b, c \in F$).

1. $\forall\, a : \;\; a +_F 0_F = a \wedge a \cdot_F 1_F = a$ *(the element 0_F is neutral in $+_F$, and the element 1_F in $\cdot_F$).*
2. *Both operations $+_F$ and $\cdot_F$ are associative and commutative.*
3. $\forall\, a, b, c : \;\; a \cdot_F (b +_F c) = (a \cdot_F b) +_F (a \cdot_F c)$ *(the distributive law holds).*
4. $\forall\, a \,\exists\, b : \;\; a +_F b = 0_F$, $\forall\, a \neq 0_F \,\exists\, b : \;\; a \cdot_F b = 1_F$ *(inverse elements exist).*
5. $\forall\, a, b, c : \; a <_F b \Rightarrow a +_F c <_F b +_F c$, $\forall\, a, b : \; a,\, b >_F 0_F \Rightarrow a \cdot_F b > 0_F$ *($<_F$ respects both operations).*

The axioms 1–4 are the axioms of a *field*. An example of an ordered field is the *fractions* (or *rational numbers*) $\mathbb{Q}$:

$$\mathbb{Q} := \{m/n \mid m,\, n \in \mathbb{Z},\, n \neq 0\}\ ,$$

where $\mathbb{Z} := \{\ldots, -1, 0, 1, \ldots\}$ are the *integers*. Another example is

$$\mathbb{Q}(\sqrt{2}) := \{r + s\sqrt{2} \mid r,\, s \in \mathbb{Q}\}\ .$$

These ordered fields differ, the equation $x^2 = 2$ is insoluble in $\mathbb{Q}$ (we prove it below) but it has a solution in $\mathbb{Q}(\sqrt{2})$.

- *Incompleteness of the ordered field* $\mathbb{Q}$.

Definition 5 (completeness) *An ordered field is complete if every nonempty subset of it that is bounded from above has a supremum.*

We show that the ordered field $\mathbb{Q}$ is not complete, it follows from the next theorem. For its proof we recall the *principle of induction*—every nonempty set $X \subset \mathbb{N}$ has the least element.

Theorem 6 ($\sqrt{2} \notin \mathbb{Q}$) *In the field of rational numbers, the equation*

$$x^2 = 2$$

has no solution.

Proof. We assume the contrary that $(a/b)^2 = 2$ for some $a, b \in \mathbb{N}$. Thus

$$a^2 = 2b^2$$

and by the principle of induction we may assume that the number a in the equation is minimum. The number a^2 is even, therefore also a is even and $a = 2c$ for some $c \in \mathbb{N}$. But then

$$(2c)^2 = 2b^2 \rightsquigarrow 4c^2 = 2b^2 \rightsquigarrow b^2 = 2c^2 \ .$$

Since $b < a$, we have obtained a solution of the displayed equation that has on the left-hand side a number that is smaller than a. This is a contradiction. $\square$

Corollary 7 (incompleteness of $\mathbb{Q}$) *The ordered field*

$$\mathbb{Q} = (\mathbb{Q},\ 0,\ 1,\ +,\ \cdot,\ <)$$

of fractions is not complete.

Proof. We show that the set of fractions

$$X := \{r \in \mathbb{Q} \mid r^2 < 2\}$$

is nonempty and bounded from above but its supremum does not exist. The first two properties are clear, $\frac{4}{3} \in X$ and $x < 2$ for every $x \in X$. For contrary we take the fraction $s := \sup(X)$. If $s^2 > 2$, there is a fraction $r > 0$ such that $s - r > 0$ and still $(s - r)^2 > 2$. But then $s - r > x$ for every $x \in X$, which contradicts the fact that s is the least upper bound of X. If $s^2 < 2$, there is a fraction $r > 0$ such that still $(s + r)^2 < 2$. Then $s + r \in X$, which contradicts the fact that s is an upper bound of X. By trichotomy it must be that $s^2 = 2$. But this is impossible by the previous theorem. □

- *The complete ordered field* $\mathbb{R}$.

Theorem 8 (existence of $\mathbb{R}$) *There exists a unique (see the next theorem) complete ordered field*

$$\mathbb{R} = (\mathbb{R},\ 0_{\mathbb{R}},\ 1_{\mathbb{R}},\ +_{\mathbb{R}},\ \cdot_{\mathbb{R}},\ <_{\mathbb{R}})\ .$$

We call it the field of real numbers.

Recall the axiom of completeness: if $X \subset \mathbb{R}$ is nonempty and there is a $y \in \mathbb{R}$ such that $x \le_{\mathbb{R}} y$ for every $x \in X$, then the set of such numbers y has the least element. We shall omit the lower indices

$\mathbb{R}$ for the neutral elements, operations and the linear order. Every ordered field contains as its prime field (the smallest subfield) a copy of $\mathbb{Q}$.

We explain how the completeness of an ordered field makes it in a sense unique. A bijection $f\colon F \to G$ between two ordered fields is their *isomorphism* if $f(0_F) = 0_G$, $f(1_F) = 1_G$ and for every $x, y \in F$ it holds that

$$f(x +_F y) = f(x) +_G f(y),\ f(x \cdot_F y) = f(x) \cdot_G f(y)$$

and

$$x <_F y \iff f(x) <_G f(y)\ .$$

Theorem 9 (uniqueness of $\mathbb{R}$) *Every two complete ordered fields are isomorphic.*

Corollary 10 ($\sqrt{2} \in \mathbb{R}$) *In the field of real numbers, the equation*

$$x^2 = 2$$

has a solution.

Proof. We take a set similar to that in the proof of Corollary 7,

$$X := \{a \in \mathbb{R} \mid a^2 < 2\}\ .$$

By Theorem 8 it has a supremum $s := \sup(X) \in \mathbb{R}$. The same arguments as in that proof show that neither $s^2 < 2$ nor $s^2 > 2$. Hence $s^2 = 2$. $\square$

In a future lecture we prove a far-reaching generalization of the previous result. In the next proposition continuity of a function roughly means (later we will see a precise definition) that a small change in the argument of a function results in a small change of the value.

Proposition 11 (the Bolzano–Cauchy Theorem) *Let $a \leq b$ be real numbers and*

$$f\colon [a,\, b] \to \mathbb{R}$$

be a continuous function such that $f(a)f(b) \leq 0$. Then there is a number $c \in [a, b]$ such that $f(c) = 0$.

• *Countable and uncountable sets, uncountability of* $\mathbb{R}$. A set X is *infinite* if there exists an injection $f\colon \mathbb{N} \to X$. If X is not infinite, it is *finite*. One can show that for every finite set X there is a surjection $f\colon \mathbb{N} \to X$.

Definition 12 ((un)countable sets) *We define the following kinds of sets.*

1. *X is countable if there is a bijection $f\colon \mathbb{N} \to X$.*
2. *A set is at most countable if it is finite or countable.*
3. *A set is uncountable if it is not at most countable.*

Theorem 13 ($\mathbb{Q}$ is countable) *The set of fractions is countable.*

Proof. For a fraction $\frac{m}{n} \in \mathbb{Q}$ in lowest terms, which means that $n \in \mathbb{N}$ and that the numerator $m \in \mathbb{Z}$ and the denominator n are coprime (i.e., the largest $k \in \mathbb{N}$ dividing simultaneously m and n

is $k = 1$), we define the norm $\|\frac{m}{n}\| := |m| + n \in \mathbb{N}$ and sets

$$Z_j := \{z_{1,j} < z_{2,j} < \cdots < z_{k_j,j} \mid z_{i,j} \in \mathbb{Q},\ \|z_{i,j}\| = j\},\ j \in \mathbb{N}\ .$$

For example,

$$Z_5 = \{-\tfrac{4}{1} < -\tfrac{3}{2} < -\tfrac{2}{3} < -\tfrac{1}{4} < \tfrac{1}{4} < \tfrac{2}{3} < \tfrac{3}{2} < \tfrac{4}{1}\} \text{ and } k_5 = 8\ .$$

Here $\frac{0}{5} \notin Z_5$ because 0 and 5 are not coprime. Clearly, $j \neq j' \Rightarrow Z_j$ and $Z_{j'}$ are disjoint, every Z_j is finite (and $\neq \emptyset$) and $\bigcup_{j\in\mathbb{N}} Z_j = \mathbb{Q}$. The map $f\colon \mathbb{N} \to \mathbb{Q}$ is defined by

$$f(1) = z_{1,1},\ f(2) = z_{2,1},\ \ldots,\ f(k_1) = z_{k_1,1},\ f(k_1+1) = z_{1,2},\ \ldots$$

—the values of f first run through the k_1 sorted fractions in Z_1, then through the k_2 sorted fractions in Z_2, and so on. For $j \in \mathbb{N}$ the generic value equals

$$f(k_1 + k_2 + \cdots + k_{j-1} + i) = z_{i,j},\ i \in [k_j]\ ,$$

where for $j = 1$ we define this argument of f as i. It is easy to see that f is a bijection. □

We are going to prove the uncountability of real numbers. We obtain it as a consequence of the next fundamental set-theoretic result. It says that the power set $\mathcal{P}(X)$ is a much larger set than X.

Theorem 14 (Cantor's) *For no set X there exists a surjection*

$$f\colon X \to \mathcal{P}(X)$$

going from it onto its power set.

Proof. We assume for the contrary that X is a set and that $f\colon X \to \mathcal{P}(X)$ is a surjective map. We consider the subset

$$Y := \{x \in X \mid x \notin f(x)\} \subset X\ .$$

Since f is onto, there exist a $y \in X$ such that $f(y) = Y$. If $y \in Y$, by the definition of Y we have that $y \notin f(y) = Y$. If $y \notin Y = f(y)$, the element y has the property defining Y and therefore $y \in Y$. In both cases we get a contradiction. □

We denote by $\{0,1\}^{\mathbb{N}}$ the set of (all) sequences $(a_n) \subset \{0,1\}$.

Corollary 15 (on 0-1 sequences) *There is no surjection*

$$f\colon \mathbb{N} \to \{0,\,1\}^{\mathbb{N}}\ .$$

Proof. The map $g\colon \{0,1\}^{\mathbb{N}} \to \mathcal{P}(\mathbb{N})$, $g((a_n)) := \{n \in \mathbb{N} \mid a_n = 1\}$, is obviously a bijection. If the stated surjection f existed, the composite map $g \circ f$ would go from $\mathbb{N}$ onto $\mathcal{P}(\mathbb{N})$, which would contradict Theorem 14. □

Corollary 16 ($\mathbb{R}$ is uncountable) *The set of real numbers is uncountable.*

Proof. We again prove more — there is no surjection $f\colon \mathbb{N} \to \mathbb{R}$. We think of the real numbers as of infinite decimal expansions and take the set

$$X := \{0.a_1a_2\ldots \mid a_n \in \{0,\,1\}\} \subset \mathbb{R}$$

of those with only zeros and ones after the decimal point. Clearly, we have a bijection $g\colon X \to \{0,1\}^{\mathbb{N}}$. If the stated surjection f existed, we could easily obtain from it a surjection $f_0\colon \mathbb{N} \to X$ (we set $f_0(n) := f(n)$ if $f(n) \in X$, and $f_0(n) := 0.000\ldots$ else). But then the composite map $g \circ f_0$ would go from $\mathbb{N}$ onto $\{0,1\}^{\mathbb{N}}$, which would contradict Corollary 15. $\square$

• *Few words on* $\mathbb{C}$. We remind complex numbers and one fundamental property they possess. It is well known that

$$\mathbb{C} = \{a + bi \mid a,\, b \in \mathbb{R}\},\ i = \sqrt{-1}\ ,$$

and that $\mathbb{C}$ with the neutral elements $0_{\mathbb{C}} := 0 + 0i$ and $1_{\mathbb{C}} := 1 + 0i$ and the operations

$$(a + bi) +_{\mathbb{C}} (c + di) := (a +_{\mathbb{R}} c) + (b +_{\mathbb{R}} d)i$$

and

$$(a + bi) \cdot_{\mathbb{C}} (c + di) := (a \cdot_{\mathbb{R}} c -_{\mathbb{R}} b \cdot_{\mathbb{R}} d) + (a \cdot_{\mathbb{R}} d +_{\mathbb{R}} b \cdot_{\mathbb{R}} c)i$$

form a field. It has the following important property: so called Fundamental Theorem of Algebra holds for it.

Theorem 17 (FTA) *Every non-constant polynomial* $p(z)$ *in* $\mathbb{C}[z]$ *(with complex coefficients) has a root, a number* $z_0 \in \mathbb{C}$ *such that*

$$p(z_0) = 0\ .$$

THANK YOU FOR YOUR ATTENTION