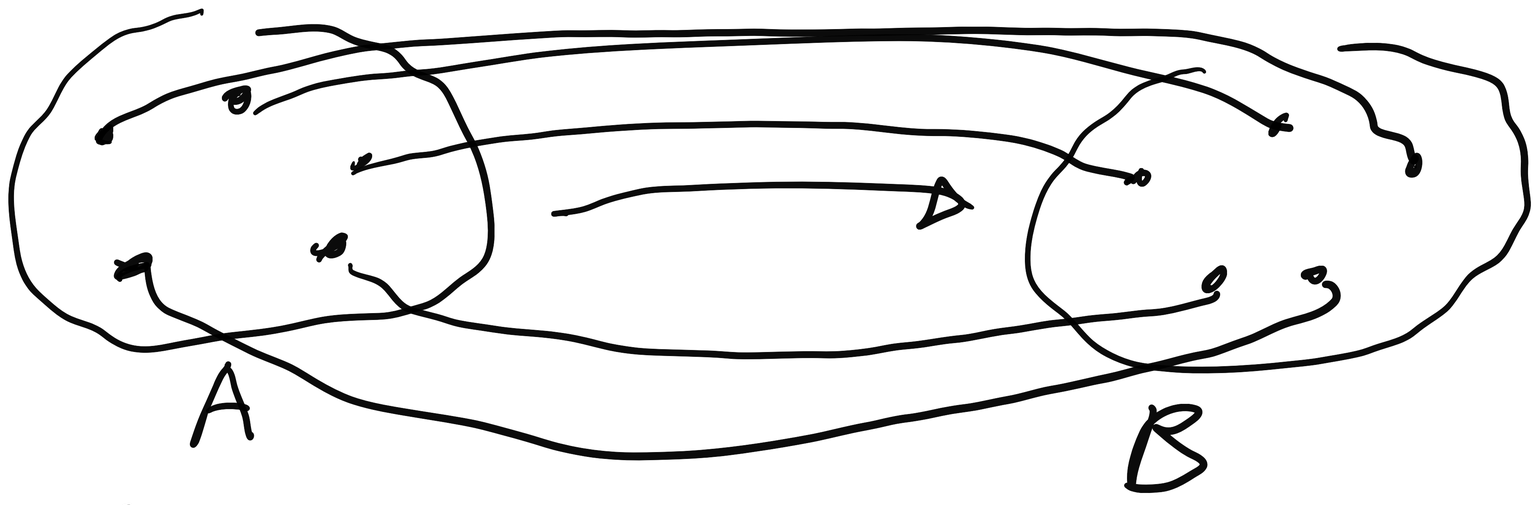
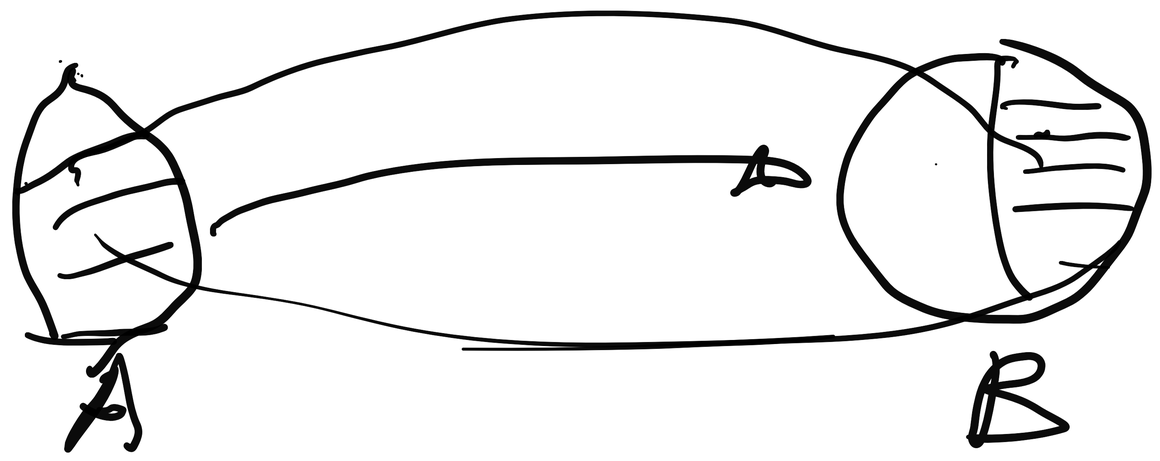
f :



idea of bijective function

$A \subset B$ $A \neq B$



$\mathbb{O}$

$f: \mathbb{N} \longrightarrow \mathbb{O} = \{\text{odd numbers}\}$

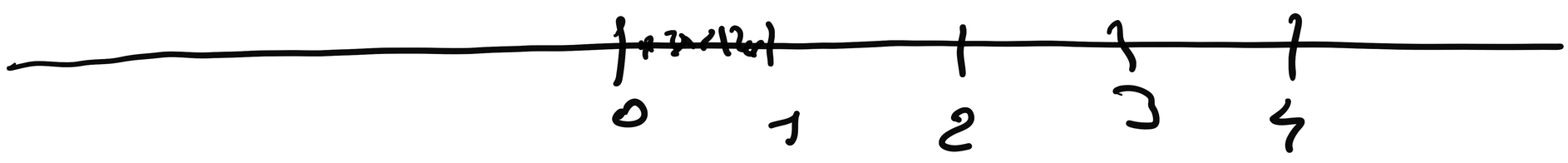
$n \longmapsto f(n) = 2n+1$

Definition: a set E that can be put in one-to-one correspondence is called "countable"

$\{$ odd numbers $\}$ is countable
take $f(n)=2n+1$

$\{$ even numbers $\}$ ✱ ✱
take $f(n)=2n$

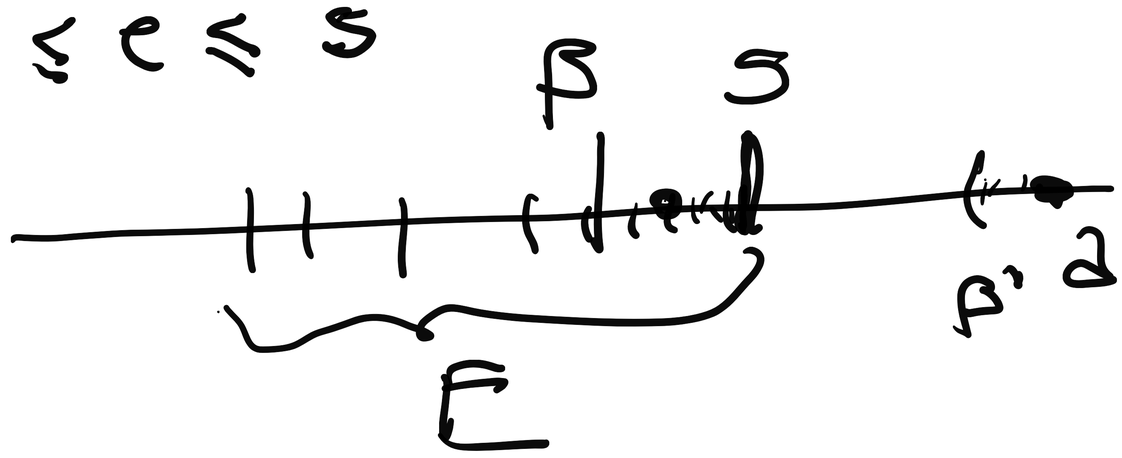
$\mathbb{Q} = \{$ rational numbers $\}$ is countable



Definition: E set, b is an lower upper bound for E if $e \leq a$ $\forall$ every $e \in E$ ($e \geq b$)

(E has de order $\leq$) "lower"

Definition: the "best" upper bound s is called a "Best" means if $\forall \beta < s$ then $\exists e$ s.t. $\beta \leq e \leq s$ (infimum i supremum of E.)



"Best" means if $\beta > i \Rightarrow \exists\ e \in E$ s.t. $i \leq e \leq \beta$

Example: $E = \left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\}$

$1 = \sup E$

If $\beta < 1$ $\exists\ n \in \mathbb{N}$ $\beta \leq \frac{1}{n} \leq 1$

take $n = 1$

$E \not\ni 0 = \inf E$

i) 0 is a lower bound of E

$0 \leq e$ $\forall e \in E$

i.e. $0 \leq \frac{1}{n}$ $\forall n \in \mathbb{N}$

ii) 0 is "the best" lower bound

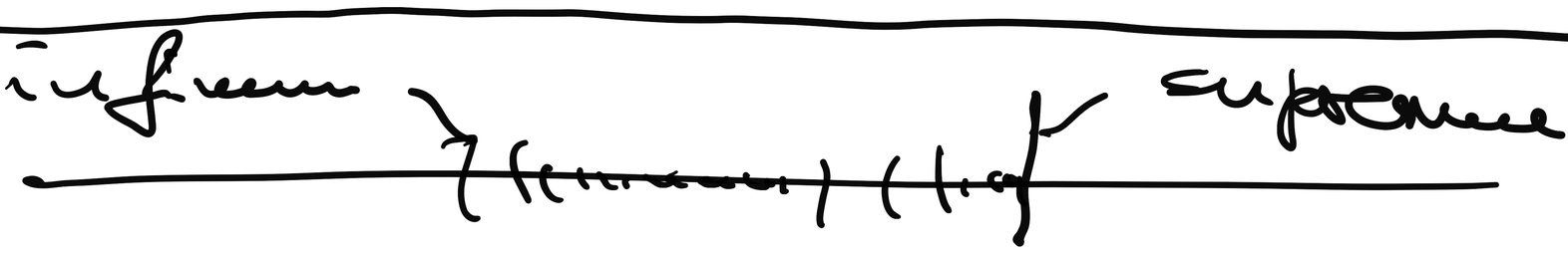
$\forall \beta > 0$ $\exists\ e \in E$ s.t. $0 \leq e \leq \beta$

i.e. $\exists n$ such that $0 \leq \frac{1}{n} \leq \beta$

$n \geq \frac{1}{\beta}$

Exercise $\left\{ 2 - \frac{1}{n^3} \;,\; n \in \mathbb{N} \atop n \neq 0 \right\}$

find, if any, infimum and supremum



Def $E \subseteq \mathbb{R}$ M is the maximum / m of E " minimum

if i) $M \in E$ $m \in E$

ii) $M \geq e \quad \forall\, e \in E$ $m \leq e \quad \forall e \in E$

Proposition: Every maximum is a supremum

" minimum is an infimum

Proof:

Example: 1 is the maximum of $\left\{\frac{1}{n}, n \in \mathbb{N}\right\}$

0 is infimum but not a minimum, because $0 \notin \left\{\frac{1}{n}, n \in \mathbb{N}\right\}$

In these examples the infimum and the supremum exist.

(**Exercise**: Show that infimum and supremum are unique)

on $\mathbb{Q}$ two operation Sum and product

$+$ { is associative $(q_1+q_2)+q_3 = q_1+(q_2+q_3)$

is commutative: $q_1+q_2 = q_2+q_1$

$\exists$ "zero" neutral $q_1+0=q_1$

Existance of the "inverse" $\forall q \ \exists$ element $p \in \mathbb{Q}$ $q+p=0$, and we write $p=-q$

$\cdot$ { associative ---

commutative ---

$\exists$ neutral "1" ---

$\forall q \in \mathbb{Q}\setminus\{0\} \ \exists$ inverse p i.e $p\cdot q = 1$ and we write $p=\frac{1}{q}$

$q=\frac{m}{n}$ $\frac{1}{q}=\frac{n}{m}=q^{-1}$

- $(q_1+q_2)\cdot q_3 = q_1\cdot q_3 + q_1 q_2$
- if $q_1 \le q_2$ $\forall q \in \mathbb{Q}$ $q_1+q \le q_2+q$

if $0 \le q_1 \le q_2$ $q \ge 0$ $q_1 \cdot q \le q_2 q$

Property C If E is (lower) upper bounded (i.e. there exists a upper bound) then there exists $\sup E$ ($\inf E$)

$$E = \{ q \in \mathbb{Q} \quad q^2 \leq 2 \}$$

We claim that $\sup E = \sqrt{2}$

Indeed: (Use the proof by contradiction that is: deny the thesis and find contradiction with hypothesis)

If, by contradiction $p \neq \sqrt{2}$, which means $p^2 \neq 2$ we have two possibilities: either $p > \sqrt{2}$ or $p < \sqrt{2}$. Let us see that in both cases we reach a contradiction

If $p > \sqrt{2}$. If I find n such that $p > p - \frac{1}{n} > \sqrt{2}$ we should find $q \in E$ such that

$$p \geq q \geq p - \frac{1}{n} > \sqrt{2} \quad (*)$$

$$\Rightarrow q^2 \geq \left(p - \frac{1}{n}\right)^2 > 2 \Rightarrow q \notin E$$

contradiction

So it is sufficient to find n which verifies $p - \frac{1}{n} > \sqrt{2}$. If n is suff. large $p - \frac{1}{n} > 0$. So, taking the square:

$$\left(p - \frac{1}{n}\right)^2 > 2$$

$$\Leftrightarrow$$

$$p + \frac{1}{n^2} - \frac{2p}{n} > 2 \quad (**)$$

Observe: if we find n such that $(***)$ $p - \frac{2}{n} > 2$, then $(**)$ is true as well, because $\frac{1}{n^2} > 0$

Now

$$(***) \Leftrightarrow p\left(1 - \frac{2}{n}\right) > 2 \Leftrightarrow 1 - \frac{2}{n} > \frac{2}{p}$$

$$\Leftrightarrow \frac{2}{n} < 1 - \frac{2}{p} = \frac{p-2}{p}$$

$$\Leftrightarrow n > \frac{2p}{p-2}$$

So for such a n $(***)$ is verified i.e. $(*)$ is verified.

If instead $p \in \mathbb{Q}$, $\boxed{p < \sqrt{2}}$ $(\star)$

Clearly $p > 0$, so $(\star)$ is equivalent

to $p^2 < 2$. If we can find $n \in \mathbb{N}$ such that $\left(p + \frac{1}{n}\right)^2 < 2$ (★★) we have concluded, because $p + \frac{1}{n} \in E$ so that p is NOT an upper bound. So, let us find n such that (★★) holds true.

(★★) $\iff$ $p^2 + \frac{1}{n^2} - \frac{2p}{n} < 2$

It is clearly sufficient to find n such that

$p^2 + \frac{1}{n^2} < 2$ (★★★)

(Now ★★★ $\iff$ $\frac{1}{n^2} < \overbrace{2 - p^2}^{>0} \iff$ $n^2 > \frac{1}{(2-p^2)}$

yes, for n sufficiently large

$\Rightarrow p^2 + \frac{1}{n^2} - \frac{2p}{n} < 2$)

So also in this case we have obtained a contradiction.

q.e.d

The previous example tells us that there are subsets $E \subset \mathbb{Q}$ which are upper bounded (i.e there exist upper bound) but do not have a supremum

(best upper bound = the minimum of upper bounds)

So $\mathbb{Q}$ lacks the property, called completeness.

Completeness: If M is a space with an order "$\leq$" (like $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$) we say that it is COMPLETE if

- every upper bounded subset $E \subset M$ has a supremum
- every lower bounded subset $E \subset M$ has an infimum

The previous example $E = \{q \in \mathbb{Q} \;\; q^2 \leq 2\}$ shows that $\mathbb{Q}$ is NOT COMPLETE

This is the main reason to enlarge $\mathbb{Q}$. The enlargement is represented by

$\mathbb{R}$ the set of real numbers

This can be done constructively, but that would go beyond the aims of this course. So we give $\mathbb{R}$ axiomately, that is

Theorem: There exists a set $\mathbb{R}$ such that, $\mathbb{R} \supset \mathbb{Q}$, and on it there are two operations, the "sum" and the "product", with the usual properties: associativity, commutativity, existence of a neutral element (0 for the sum, 1 for the product), existence of a inverse of each $x \in \mathbb{R}$ ($-x$ for the sum, $\frac{1}{x}$ for the product, (with $x \neq 0$)), distributivity of sum on product,

AND

Completeness

(See a more rigorous version on

the printed notes)

So completeness distinguish $\mathbb{Q}$ from $\mathbb{R}$.

And the example above tells us that $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$

Similarly one shows that $\mathbb{R}$ contains the square root $\sqrt{x}$ of every $x \geq 0$.

So we have

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

the last inclusion being the most tricky:

why $\mathbb{Z}$ and $\mathbb{Q}$ are countable (i.e. they can be put in one-to-one correspondence with their subset $\mathbb{N}$)

$\mathbb{R}$ is not countable

(hence $\mathbb{R}$ is much bigger than $\mathbb{Q}$)

We will come back on this issue.

Consider the following question.

Question 1

Suppose that a set E has n elements. How many are the subsets of E?

ANSWER: They are 2^n.

To prove this theorem we will utilize the so-called "proof by induction".

PROOF BY INDUCTION: Suppose you want to prove that $\forall n \in \mathbb{N}$ some sentence S_n is true. Proving it "by induction means"

1) Prove that S_1 is true
2) Prove that "if S_n is true then also S_{n+1} is true"

(It works.... why it does work would need.... a proof! But we skip it here)

Let us apply the proof by induction to show that

Theorem 1: A set E with n elements has 2^n subsets, $\forall n \in \mathbb{N}$

NOTATION: The set of subsets of E is called "the set of parts of E" and is denoted by $\mathcal{P}(E)$

So Theorem 1 can be rephrased as:

"If E has n elements, then $\mathcal{P}(E)$ has 2^n elements"

Proof (by induction)

Our $\mathcal{S}_n$ now is "if E has n elements $\mathcal{P}(E)$ has 2^n elements"

So $\mathcal{S}_1$ is: A set E with 1 elements has $2^1 = 2$ subsets.

This is true, since if $E = \{a\}$ then then E has 2 subsets: E and $\emptyset$.

So we have verified the first step of induction

Let us prove that $\mathcal{S}_n \Rightarrow \mathcal{S}_{n+1}$ $\forall n \in \mathbb{N}$

Let E have n elements, and for $x \notin E$ consider the set $F = E \cup \{x\}$, so F has $n+1$ elements. Clearly

$$\mathcal{P}(F) = \underbrace{\{\text{subsets of } F \text{ that contain } x \text{ as an element}\}}_{A} \cup \underbrace{\{\text{subsets of } F \text{ that do not contain } x \text{ as an element}\}}_{B}$$

Notice that $B = \mathcal{P}(E)$, so by inductive hypothesis B contains 2^n elements.

But A has the same number of elements as B, because each element (= subset of F) of A is obtained by an element (= subset of F) of B united with $\{y\}$. So also A has 2^n elements.

Therefore

number of subsets of F = number of elements of A + number of elements of B =

$$2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$$

The proof is concluded

q.e.d.

Exercise: Prove that, $\forall n \in \mathbb{N}$,

$$1+2+3+4 \ldots\ldots + n = \frac{n(n+1)}{2}$$

:

Historians say that the six years old Gauss answered correctly in a few seconds ....

But we are humans, so let us prove it by induction: