

Introduction to Analysis - Math 104.

Lecture 1

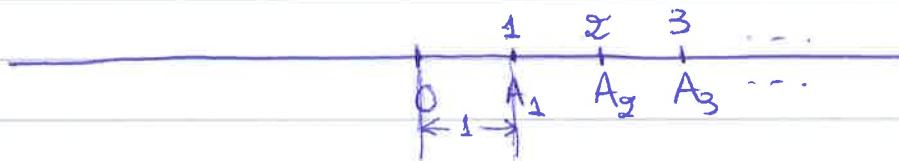
24 Aug 2016.

Our aim is to define the real numbers, so that they are in 1-1 correspondence with a line; something we are always using.

Here is some discussion first:

We define $\mathbb{N} := \{1, 2, 3, \dots\}$ (note that we exclude 0 for technical reasons)
and $\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

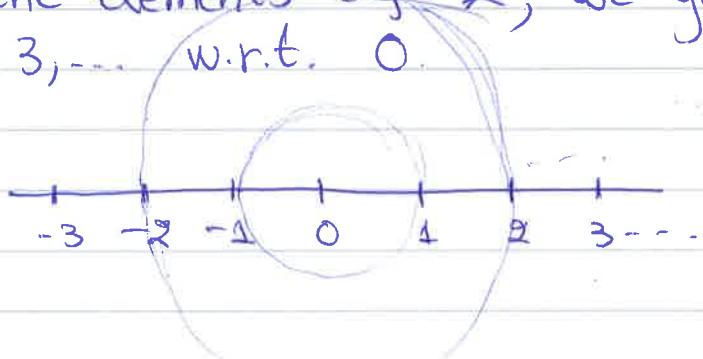
It is easy to represent these on a line:



Place 0 somewhere on the line, and take $OA_1, A_1A_2, A_2A_3, \dots$ to be equal line segments on the line. We place 1 at A_1 , 2 at A_2 , 3 at A_3 , etc. (Note that, this way, we are accepting that the length of OA_1 is 1).

This way \mathbb{N} is represented on the line.

As for the elements of \mathbb{Z} , we get the reflections of $1, 2, 3, \dots$ w.r.t. 0.



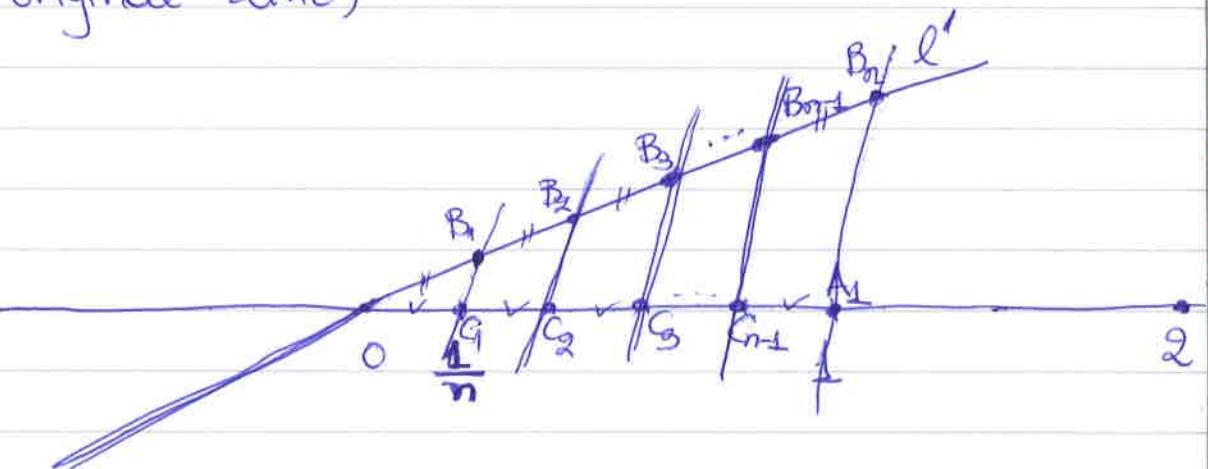
(2)

Let us now define the rational numbers:

$$\mathbb{Q} := \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

To represent $\frac{m}{n}$ on the line above,

first we take line l' through 0 intersecting our original line,



and on l' we take equal line segments $OB_1, B_1B_2, B_2B_3, \dots, B_{n-1}B_n$ (it doesn't matter

how long they are, as long as they all have equal lengths).

We connect B_n with A_1 ,

and draw parallel lines to $B_n A_1$ through

B_1, B_2, \dots, B_{n-1} . These lines intersect OA_1

at points C_1, C_2, \dots, C_{n-1} . By similarity

of the triangles $OB_1C_1, OB_2C_2, OB_3C_3, \dots, OB_nA_1$,

and since $OB_1 = B_1B_2 = \dots = B_{n-1}B_n$, it follows that

(3)

$OG_1 = G_1G_2 = G_2G_3 = \dots = G_{n-1}A_1$; we have

thus split OA_1 in n equal line segments.

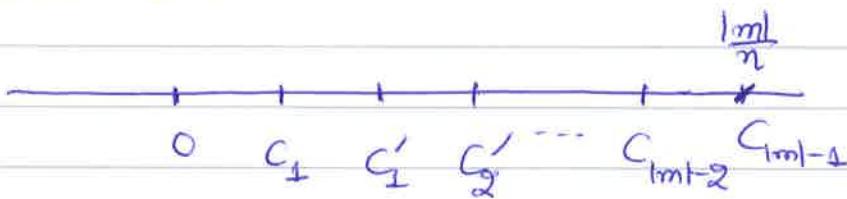
Each of these has length $\frac{|OA_1|}{n} = \frac{1}{n}$, we

can therefore represent $\frac{1}{n}$ by the point G_1 .

Now, to represent $\frac{m}{n}$ on the line,

we take $|ml|$ consecutive copies of OG_1 ,

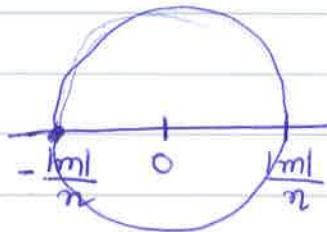
starting from O :



We can place $\frac{1}{n}$ at the point C_{lm1-1} .

That is $\frac{m}{n}$ for $m \geq 0$; for $m < 0$,

we take the reflection of $\frac{1}{n}$ on the line,
w.r.t. O .



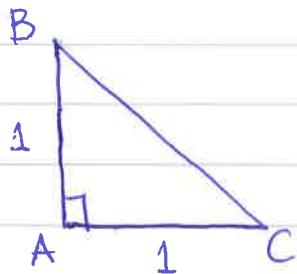
We have placed all elements of \mathbb{Q} on the line merely by ruler-and-

compass construction. We can create more

such "natural lengths" this way. For instance,

(4)

create a triangle ABC , with \hat{BAC} a right angle, and



AB, AC with length 1 each
(where the length 1 is the length of OA_1 described earlier).

Note that this can also be done by ruler-and-compass construction!

And, the hypotenuse of this triangle has length $\sqrt{1^2 + 1^2} = \sqrt{2}$.

So, $\sqrt{2}$ is a "naturally occurring" length;

it can be found by ruler and compass only, and put on the line as well, together

with all the elements of \mathbb{Q} . However:

Proposition: $\sqrt{2} \notin \mathbb{Q}$

Proof: Suppose $\sqrt{2} \in \mathbb{Q}$. Then, $\exists m \in \mathbb{Z}, n \in \mathbb{N}$,

with greatest common divisor 1, st. $\sqrt{2} = \frac{m}{n}$

$$\text{Then, } \sqrt{2}^2 = \frac{m^2}{n^2} \implies m^2 = 2n^2 \quad \textcircled{*}$$

By $\textcircled{*}$, m^2 even, thus m even.

$\left(\begin{array}{l} \text{Indeed, the square of an odd number is} \\ \text{always odd: } \forall k \in \mathbb{Z}, (2k+1)^2 = 4k^2 + 4k + 1 = \\ = 2(\cancel{2k^2} + 1) + 1, \text{ odd. So, } m^2 \text{ even} \rightarrow m \text{ even.} \end{array} \right)$

(5)

So, $\exists k \in \mathbb{Z}$ s.t. $m = 2k$. Then, by $\textcircled{*}$:

$$(2k)^2 = 2n^2 \Rightarrow 4k^2 = 2n^2 \Rightarrow n^2 = 2k^2 \Rightarrow n \text{ even.}$$

So, both m and n are even, so 2 divides both m, n . This is a contradiction, as $\gcd(m, n) = 1$.

Therefore, $\sqrt{2} \notin \mathbb{Q}$. ■

So, there are certainly elements on the line that are not in \mathbb{Q} . What exactly are the elements of the line? We are used to believing that they are the real numbers; but what are the real numbers? We will try to understand this, as well as their properties.

To that end, we first need to understand \mathbb{Q} , and see what properties it is missing.

Def: Let $S \neq \emptyset$, a set. An operation *

on S is a map $*: S \times S \rightarrow S$
 $(a, b) \rightarrow a * b$

I.e., it is a map that sends each pair (a, b) in $S \times S$ to an element $a * b$ in S.

ex: • $S = \{f: \mathbb{R} \rightarrow \mathbb{R}, 1-1 \text{ and onto}\}$.

Then, the composition of functions $\circ: S \times S \rightarrow S$
 $(f \circ g) \rightarrow f \circ g$

(6)

- $S = \{0, 1\}$, \star | 0 | 1
 0 | 1 | 0
 1 | 1 | 1

	0	1
0	1	0
1	1	1

	0	1
0	0	1
1	1	0

Both \star , \dagger are operations on S .

- Usual addition and multiplication are operations on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$.



From the examples above it is clear that, in general, the order in the pair matters when it comes to operations.

$+$ and \cdot on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are special cases exactly because order doesn't matter (i.e. $+$ and \cdot happen to be commutative in these settings)

Def: Let $F \neq \emptyset$, a set. Let $(+, \cdot)$ be two operations on F .

for now, just symbols!

We say that the triple $(F, +, \cdot)$ (or, the set F equipped with the operations $+, \cdot$)

is a field if $+$ and \cdot satisfy the following:

(7)

(I) Axioms for $+$:

I1) $a+b=b+a, \forall a, b \in F$ (commutativity)

I2) $a+(b+c)=(a+b)+c, \forall a, b, c \in F$ (associativity)

I3) There exists an element of F , which we denote by 0 , s.t. $a+0=a, \forall a \in F$

(existence of additive identity)

I4) ~~$\exists a \in F$~~ , there exists $a' \in F$ s.t.

$a+a'=0$ (existence of additive inverse).

We call a' the opposite of a , and we denote it by $-a$.

(II) Axioms for \cdot :

II1) $a \cdot b = b \cdot a, \forall a, b \in F$ (commutativity)

II2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in F$ (associativity)

II3) There exists an element of F , different to 0 , which we denote by 1 , s.t.

$a \cdot 1 = a, \forall a \in F$ (existence of multiplicative identity)

II4) ~~$\nexists a \in F$~~ , there exists $a'' \in F$ s.t.

$a \cdot a'' = 1$ (existence of multiplicative inverse).

We call a' the inverse of a , and we denote it by a^{-1} .

(III) Axiom connecting $+$ and \cdot :

~~\oplus~~ $a \cdot (b+c) = a \cdot b + a \cdot c, \forall a, b, c \in F$

(distributivity)

(8)

A

Due to the fact that the usual addition and multiplication in \mathbb{Q} satisfy the above axioms, $+$ and \cdot are referred to as addition and multiplication.

ex: • $(\mathbb{Q}, +, \cdot)$ is a field.

the usual
operations

• $(\mathbb{N}, +, \cdot)$ is not a field: there is no additive identity, nor multiplicative or additive inverse for any $n \in \mathbb{N}$.

Each of these reasons would suffice.

• $(\mathbb{Z}, +, \cdot)$ is not a field: there exists no multiplicative inverse for any $k \in \mathbb{Z}$, apart from $k=1$.

• $\mathbb{F} = \{0, 1\}$, with the operations

$+$	0	1
0	0	1
1	1	0

\cdot	0	1
0	0	0
1	0	1

is a field. $(\mathbb{F}, +, \cdot)$ is usually denoted by \mathbb{Z}_2 in this case

(the 2 stands for the length of a cycle starting from 0 and adding 1 consecutively).

(9)

Some properties of fields:

Let $(\mathbb{F}, +, \cdot)$ be a field, Then:

The axioms for the addition + imply:

For all $a, b \in \mathbb{F}$:

$$(a_1) \quad a+b = a+c \Rightarrow b=c.$$

$$(a_2) \quad a+b = a \Rightarrow b=0.$$

$$(a_3) \quad a+b = 0 \Rightarrow b=-a.$$

$$(a_4) \quad -(-a) = a.$$

The axioms for the multiplication \cdot imply:

for all $b, c \in \mathbb{F}$, and all $\boxed{a \neq 0}$ in \mathbb{F} :

$$(m_1) \quad ab = a \cdot c \Rightarrow b=c.$$

$$(m_2) \quad a \cdot b = a \Rightarrow b=1.$$

$$(m_3) \quad a \cdot b = 1 \Rightarrow b = a^{-1}.$$

$$(m_4) \quad (a^{-1})^{-1} = a$$

Also:

$$(i) \quad 0 \cdot a = 0, \forall a \in \mathbb{F}.$$

$$(ii) \quad \text{If } a \neq 0, b \neq 0 \text{ in } \mathbb{F}, \text{ then } a \cdot b \neq 0$$

$$(iii) \quad (-a) \cdot b = a \cdot (-b) = -(a \cdot b), \forall a, b \in \mathbb{F}.$$

$$(iv) \quad (-a) \cdot (-b) = a \cdot b, \forall a, b \in \mathbb{F}.$$

⚠ (i) - (iv) really demonstrate the difference between $+$ and \cdot ; one cannot expect,

(10)

for instance, that
 $1 \cdot a = a$ $\forall a \in F$, or that
 $(a^{-1}) \cdot (b^{-1}) = a \cdot b$ $\forall a, b \in F$!)

- (v) There is a unique additive identity.
- (vi) There is a unique multiplicative identity.
- (vii) $\forall a \in F$, the additive inverse of a is unique.
- (viii) $\forall a \in F, a \neq 0$, the multiplicative inverse of a is unique.

Proof: Try the proof yourselves.

$(a_1) - (a_4)$, $(m_1) - (m_4)$, (i) - (iv) are in Rudin's book, but try by yourselves first. ■

So, this far we know that $(\mathbb{Q}, +, \cdot)$ is a field. However, we know that, eventually, we will be able to order its elements on the number line (see start of these notes). So, there is an order in \mathbb{Q} . Indeed, $(\mathbb{Q}, +, \cdot)$ is what we call an ordered field.

Def: Let $(F, +, \cdot)$ be a field. We say that it is ordered if $\exists P \subseteq F$, s.t.

P1) $\forall a \in F$, exactly one of the following

(11)

holds:

$$\alpha \in P \quad \text{or} \quad \alpha = 0 \quad \text{or} \quad -\alpha \in P.$$

P2) $\forall \alpha, b \in P, \alpha + b \in P \text{ and } \alpha \cdot b \in P.$

→ If such a set P exists, we can refer to it as the set of positive elements of $(\mathbb{F}, +, \cdot)$.

The existence of such a set P induces an order in $(\mathbb{F}, +, \cdot)$ (whence the term "ordered" field).

In particular, the order is defined as such:

Def: Let $(\mathbb{F}, +, \cdot)$ be an ordered field, with $P \subseteq \mathbb{F}$ as the chosen subset of positive elements. Then, we have an order $<$ on \mathbb{F} , defined as:

for $a, b \in \mathbb{F}, a < b \text{ iff } b + (-a) \in P.$

Notation: Let $(\mathbb{F}, +, \cdot)$ be an ordered field, with $P \subseteq \mathbb{F}$ as the chosen subset of positive elements, and $<$ the induced order. Then:

- $b - a := b + (-a), \forall a, b \in \mathbb{F}.$

(12.)

- $a \leq b$ means $a < b$ or $a = b$.

$\left(\begin{array}{l} \\ \text{i.e., } b-a \in P \end{array} \right)$

- $a > b$ means $b < a$.

$\left(\begin{array}{l} \\ \text{i.e., } a-b \in P \end{array} \right)$

Observation: $a > 0$ means $a \in P$.

Proof: $a > 0$ means $\underbrace{a + (-0)}_{=a} \in P$, i.e. $a \in P$.

$\begin{array}{c} a+0 \\ =a \end{array}$



ex.: • $(\mathbb{Q}, +, \cdot)$ is an ordered field,
because the set $P = \left\{ \frac{m}{n} : m \in \mathbb{N} \cup \{0\}, n \in \mathbb{N} \right\}$

satisfies the conditions in the definition
of an ordered field. For this choice
of P , the induced order on \mathbb{Q}
is the usual one on \mathbb{Q} . It is this
order that allows us to put the
elements of \mathbb{Q} on the number line in
the way we did.

- The field $(\mathbb{Z}_2, +, \cdot)$ defined earlier

is not an ordered field (exercise!).

(13.)

Properties of ordered fields:

Let $(\mathbb{F}, +, \cdot)$ be an ordered field, with order $<$.
Then :

(i) If $a, b \in \mathbb{F}$, then exactly one of the following hold:

$$a < b \quad \text{or} \quad a = b \quad \text{or} \quad a > b.$$

(ii) If $a > b$ and $b > c$, then $a > c$.

(iii) If $a > b$ and $c \in \mathbb{F}$, then $a+c > b+c$.

(iv) If $a > b$ and $c > 0$, then $a \cdot c > b \cdot c$.

(v) If $a > b$ and $c > d$, then $a+c > b+d$.

(vi) $1 > 0$ (i.e. the multiplicative identity is larger than the additive identity)

Proof: (i) Consider $b-a \in \mathbb{F}$. Then, exactly one of the following holds:

$$b-a > 0 \quad \text{or} \quad b-a=0 \quad \text{or} \quad b-a < 0,$$

$$\text{i.e. } b > a \quad \text{or} \quad b = a \quad \text{or} \quad a > b$$

(ii) $a > b \Rightarrow a-b > 0$ $b > c \Rightarrow b-c > 0$ $\left. \begin{array}{l} \\ \end{array} \right\} \rightarrow (a-b)+(b-c) > 0$, i.e.
 \downarrow def. of field $a-c > 0$.

(1)

Lecture 2

26 Aug 2016.

(vi) By the definition of an ordered field, exactly one of the following holds:

(*)

$$1 > 0 \quad \text{or} \quad 1 = 0 \quad \text{or} \quad -1 > 0.$$

- Suppose that $1 = 0$. This is a contradiction, as it violates the definition of a field.
- Suppose that $-1 > 0$.
Then, $(-1) \cdot (-1) > 0$ (by definition of an ordered field).

But $(-1) \cdot (-1) = 1$ (by properties of a field).

So, $1 > 0$. At the same time, $-1 > 0$, so two of the conditions (*) holds.

So, we have a contradiction.

Therefore, $1 > 0$. ■

→ Problem: How to define an extension \mathbb{R} of \mathbb{Q} , s.t.

(i) \mathbb{R} is in a 1-1 correspondence with the number line, and

(2)

(ii) The operations $+$ and \cdot that we know on \mathbb{Q} , as well as the order $<$ on \mathbb{Q} , are extended on \mathbb{R} , s.t. $(\mathbb{R}, +, \cdot, \leq)$

↓
 the extension
of $+$, \cdot
 ↓
 the extension
of \leq

is an ordered field.

To do this, we need to understand what properties \mathbb{Q} is missing, that prevent it from covering the whole number line.

→ Def.: Let $(\mathbb{F}, +, \cdot)$ be an ordered field, and $A \subseteq \mathbb{F}$.

→ We say that A is bounded from above if there exists $b \in \mathbb{F}$ s.t.

$$a \leq b, \forall a \in A \quad \begin{array}{c} \text{---} \\ | \\ A \end{array} \quad b \quad \begin{array}{c} \text{---} \\ | \\ \mathbb{F} \end{array}$$

Obs: • Suppose that A is bounded from above, with $b \in \mathbb{F}$ an upper bound of A . If $c \in \mathbb{F}$ and $b \leq c$, then c is also an upper bound of A .

$$\begin{array}{c} \text{---} \\ | \\ A \end{array} \quad b \quad c \quad \begin{array}{c} \text{---} \\ | \\ \mathbb{F} \end{array}$$

I.e.: A can have many upper bounds;

(3)

A doesn't have to have an upper bound; and if it does, that upper bound doesn't have to be in A - it just belongs to the ambient field, \mathbb{F} . If we look for upper bounds of A inside larger ordered fields that contain \mathbb{F} , then we will probably have more options for upper bounds.

Ex: In $(\mathbb{Q}, +, \cdot, \leq)$:

- $\mathbb{Q}, \mathbb{Z}, \mathbb{N}, \{x \in \mathbb{Q} : x > 0\}, \{2^n : n \in \mathbb{N}\}$ are not bounded from above (in \mathbb{Q}).
- $\{1\}$ is bounded from above (by any $q \in \mathbb{Q}$ with $q \geq 1$).
- $\{x \in \mathbb{Q} : x < 0\}$ is bounded from above (by any $q \in \mathbb{Q}$ with $q \geq 0$).

→ Suppose the non-empty $A \subseteq \mathbb{F}$ is bounded from above. ~~Suppose that~~ Suppose that $b \in \mathbb{F}$ is an upper bound of A . We say that b is a least upper bound of A if

$b \leq c$, for all c upper bounds of A (in \mathbb{F})

Obs: • Note that b doesn't have to be in A

(4)

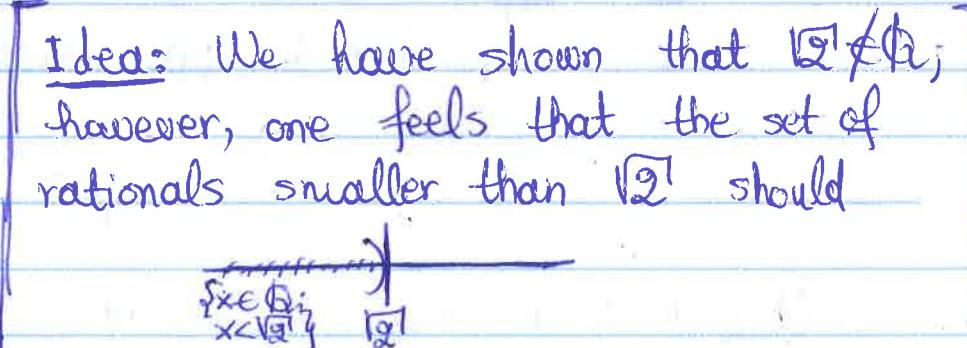
in order to be a least upper bound of A.

- A cannot have more than one least upper bounds. I.e., if A has a least upper bound (in \mathbb{F}), then that least upper bound is unique (exercise)
- A bounded from above $A \subseteq \mathbb{F}$ doesn't necessarily have a least upper bound (in \mathbb{F}). So, existence of least upper bounds is a special property; it is known as completeness.

 Def.: Let $(\mathbb{F}, +, \cdot, <)$ be an ordered field. We say that $(\mathbb{F}, +, \cdot, <)$ is complete if every (non-empty) subset

of \mathbb{F} that is bounded from above has a least upper bound (in \mathbb{F}).

→ Prop: The ordered field $(\mathbb{Q}, +, \cdot, <)$ is not complete.

Proof: 
 Idea: We have shown that $\sqrt{2} \notin \mathbb{Q}$, however, one feels that the set of rationals smaller than $\sqrt{2}$ should

$$\overbrace{\dots}^{\{x \in \mathbb{Q} : x < \sqrt{2}\}} \quad \boxed{\sqrt{2}}$$

(5)

have $\sqrt{2}$ as a least upper bound. So:
 We will use essentially $\{x \in \mathbb{Q} : x < \sqrt{2}\}$
 as an example of a non-empty subset
 of \mathbb{Q} without a least upper bound in \mathbb{R} .
However, we are not even allowed to
 write $\sqrt{2}$ yet; we haven't defined anything
 beyond \mathbb{Q} , and we know that $\nexists q \in \mathbb{Q}$ s.t.
 $q^2 = 2 \dots$ And, even if I could write $\sqrt{2}$,
 I have not defined any order relation
 involving $\sqrt{2}$ (as my order is so far
 only defined in \mathbb{Q}); so writing $x < \sqrt{2}$
 doesn't make sense.

So, we will write $\{x \in \mathbb{Q} : x < \sqrt{2}\}$
 as $\{x \in \mathbb{Q} : x \leq 0 \text{ or } x^2 < 2\}$; this set
 makes sense with respect to everything we
 have defined so far. In fact, we will
 take a smaller subset of it, that
 only contains positive elements (for technical
 reasons).

The set $A = \{x \in \mathbb{Q} : x > 0 \text{ and } x^2 < 2\}$ is
 non-empty, bounded from above, and doesn't
 have a least upper bound (in \mathbb{Q}). Indeed:

- $A \neq \emptyset : \exists a \in A (a \in \mathbb{Q}, a > 0, a^2 < 2)$
- A is bounded from above (in \mathbb{Q}): for instance,

(6)

4 is an upper bound of A, because,

$$\forall x \in A, 4^2 > 2 > x^2 \Rightarrow 4^2 > x^2 \Rightarrow 4 > x \quad (4, x > 0)$$

$$(\text{indeed, } x < y \Leftrightarrow x^2 < y^2)$$

for $x > 0, y > 0$ in an

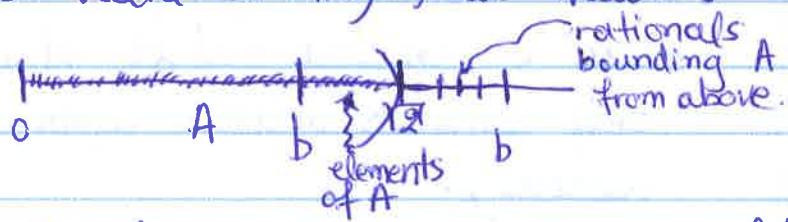
ordered field; exercise).

Suppose that A has a least upper bound, say $b \in \mathbb{Q}$. Then, exactly one of the following holds (as \mathbb{Q} is an ordered field):

(4)

$$b^2 < 2 \quad \text{or} \quad b^2 = 2 \quad \text{or} \quad b^2 > 2$$

Idea: in the picture below, which we have explained we cannot officially use yet (but which we know ~~isn't~~ will eventually be valid in \mathbb{R}), we have:



- If $b < \sqrt{2}$, then there would exist elements of A larger than b, contradiction, as b is the least upper bound of A.
- If $b > \sqrt{2}$, then there would exist rationals in $(\sqrt{2}, b)$, bounding A from above, thus smaller than the least

(7)

upper bound of A , contradiction.

- If $b = \sqrt{2} \rightarrow \sqrt{2} \notin \mathbb{Q}$, contradiction

So, A cannot have a least upper bound.

- Suppose that $\underline{b^2 < 2}$. Then there exists a rational that squares to 2 ; contradiction.
- Suppose that $\underline{b^2 > 2}$. We will find

~~$\epsilon > 0$~~ $\epsilon > 0$ st. $b + \epsilon \in A$, in which case $b + \epsilon \geq b$, where b is the least upper bound of A ; contradiction.

Details: Indeed, we want $\epsilon \in \mathbb{Q}$, $\epsilon > 0$, $(b + \epsilon)^2 < 2$.

$$\text{Now, } (b + \epsilon)^2 < 2 \Leftrightarrow b^2 + 2b\epsilon + \epsilon^2 < 2 \Leftrightarrow \\ \Leftrightarrow 2b\epsilon + \epsilon^2 < 2 - b^2. \quad \text{(*)}$$

So, if we look for $\epsilon < 1$ with the above properties, we will be able to use that $\epsilon^2 < \epsilon$, which implies that $2b\epsilon + \epsilon^2 < 2b\epsilon + \epsilon = (2b+1) \cdot \epsilon$. So, if we find

~~so that $2b+1 > \frac{1}{\epsilon}$~~

(8)

$\varepsilon \in \mathbb{Q}$ with $0 < \varepsilon < 1$ s.t. $(2b+1) \cdot \varepsilon < 2 - b^2$,

we automatically have ④ as well.

Therefore, it suffices to find

$\varepsilon \in \mathbb{Q}$ s.t. $\varepsilon > 0$, $\varepsilon \leq 1$, and

$$(2b+1) \cdot \varepsilon < 2 - b^2 \iff \begin{cases} \varepsilon < \frac{2-b^2}{2b+1} \\ 2b+1 > 0 \end{cases} \quad (\text{check!})$$

Notice that $\varepsilon = \frac{1}{2} \cdot \min \left\{ 1, \frac{2-b^2}{2b+1} \right\}$

satisfies all these conditions; thus, for this ε , $b+\varepsilon \notin A$, and $b+\varepsilon > b$, the least upper bound of A , a contradiction.

- Suppose $b^2 > 2$. We will find $\varepsilon > 0$ (in \mathbb{Q}), s.t. $b-\varepsilon$ is an upper bound of A (in \mathbb{Q}). In this case $b-\varepsilon$ is ~~an~~ an upper bound smaller than the least upper bound, a contradiction.

Details: for $b-\varepsilon$ to be an upper bound of A for some $\varepsilon \in \mathbb{Q}$, it suffices to have $(b-\varepsilon)^2 > 2$ and $b-\varepsilon > 0$ (prove this!).

$$b^2 - 2b\varepsilon + \varepsilon^2$$

(9)

So, it suffices to have :

$$\varepsilon \in \mathbb{Q}, \varepsilon > 0, \varepsilon < b \text{ and } b^2 - 2b\varepsilon + \varepsilon^2 > 2.$$

Notice that, if I find $\varepsilon \in \mathbb{Q}$ s.t. $\varepsilon > 0, \varepsilon < b$ and $b^2 - 2b\varepsilon > 2$, then I automatically also have $b^2 - 2b\varepsilon + \varepsilon^2 > 2$ (as $\varepsilon^2 > 0$ in the ordered field \mathbb{Q})

so I am done.

So, it suffices to find $\varepsilon \in \mathbb{Q}$ s.t. $\varepsilon > 0, \varepsilon < b$

$$\text{and } b^2 - 2b\varepsilon > 2 \iff 2b\varepsilon < b^2 - 2 \iff \varepsilon < \frac{b^2 - 2}{2b}.$$

(check!)

Notice that $\varepsilon = \frac{1}{2} \cdot \min\left\{b, \frac{b^2 - 2}{2b}\right\}$ satisfies all

these conditions; thus, for this ε , $b - \varepsilon$ is an upper bound of A (in \mathbb{Q}). And $b - \varepsilon < b$, the least upper bound of A , a contradiction.

Eventually, we have shown that $\textcircled{*}$

is false. This is a contradiction, so our initial assumption that A has a least upper bound is false. ■

(10)

So, we have shown that \mathbb{Q} is missing the completeness property! \mathbb{R} will be the unique extension of $(\mathbb{Q}, +, \cdot, <)$ to an ordered field that is complete (this essentially covers the gaps on the number line).

→ Theorem (the real numbers):

① There exists an extension of $(\mathbb{Q}, +, \cdot, <)$ to a complete ordered field $(\mathbb{R}, +, \cdot, <)$

i.e. : $\mathbb{Q} \subseteq \mathbb{R}$.

- The operations $+$ and \cdot on \mathbb{R} , when restricted on \mathbb{Q} , are the original operations $+$ and \cdot on \mathbb{Q} .
- The order $<$ on \mathbb{R} , restricted on \mathbb{Q} , is the same as the order $<$ on \mathbb{Q} .
- Every $A \subseteq \mathbb{R}$, $A \neq \emptyset$, that is bounded from above has a least upper bound (in \mathbb{R}).

② There exists a unique complete ordered field (up to isomorphism).

(11)

→ Corollary: The extension of $(\mathbb{Q}, +, \cdot, \leq)$ to a complete ordered field is unique. We call this unique extension the field of real numbers.

We will not worry about the proof of the existence and uniqueness of the real field. If you are interested, you can find all the details in Spivak's book. It is actually not a hard proof, just a very long one.

Lecture 3

29 Aug 2016.

①

the supremum of A

→ Def: If $A \subseteq \mathbb{R}$, let $\sup A :=$ the least upper bound of A in \mathbb{R} .

↪ We have shown that $\nexists q \in \mathbb{Q}$ with $q^2 = 2$.
However:

→ Prop: There exists a unique $x \in \mathbb{R}$, $x > 0$
with $x^2 = 2$.

Proof: Exercise. ■

We denote by $\sqrt{2}$ this unique positive real.
Moreover, the following holds:

→ Prop: For any $r > 0$ in \mathbb{R} and any $n \in \mathbb{N}$,
there exists a unique $x \in \mathbb{R}$, $x > 0$
with $x^n = r$.

Proof: See Theorem 1.21 in p. 10 of Rudin's book. ■

We denote by $r^{\frac{1}{n}}$ this unique positive real.

We will now see how the extra property
of completeness gives \mathbb{R} the amazing
properties that make it so useful.

(2)

Some basic consequences of completeness of $(\mathbb{R}, +, \cdot, <)$

① The real numbers have the Archimedean property:

The Archimedean property can be expressed in the following 3 ways:

→ Prop. 1: \mathbb{N} is not bounded from above in \mathbb{R} .

Proof: Suppose that \mathbb{N} is bounded from above in \mathbb{R} . Since \mathbb{R} is complete, \mathbb{N} has a least upper bound $\alpha \in \mathbb{R}$.

Then:

for all $n \in \mathbb{N}$, $n \leq \alpha$ (α an upper bound)

so, for all $n \in \mathbb{N}$, $\underbrace{n+1}_{\in \mathbb{N}} \leq \alpha$

i.e., for all $n \in \mathbb{N}$, $n \leq \alpha - 1$.

So, $\alpha - 1$ is an upper bound of \mathbb{N} in \mathbb{R} .

However, $\alpha - 1 < \alpha$, the least upper bound of \mathbb{N} . This is a contradiction. So,

\mathbb{N} is not bounded from above.

(3)

Δ Prop. 1 tells us that we can find as large natural numbers as we wish. The next one gives us another way to quantify this information.

→ Prop. 2: Let $a, \varepsilon \in \mathbb{R}$, with $\varepsilon > 0$. Then, there exists $n \in \mathbb{N}$ with $n \cdot \varepsilon > a$

Δ We tend to always think of ε as very small. This proposition tells us that, no matter how small ε is, we can always make it as large as we want by multiplying it with an appropriately large natural number. (Note: Prop. 1 is Prop. 2 for $\varepsilon = 1$.)

Proof: Consider the element $\frac{a}{\varepsilon} \in \mathbb{R}$. We know that \mathbb{N} is not bounded from above in \mathbb{R} , so $\frac{a}{\varepsilon}$ is not an upper bound of \mathbb{N} .

Thus, there exists some $n \in \mathbb{N}$ with $n > \frac{a}{\varepsilon}$

$$0 \quad \varepsilon \qquad \qquad a \quad n \cdot \varepsilon$$

$$\text{ex. } n \cdot \varepsilon > a.$$



(4)

→ Prop. 3: Let $\varepsilon > 0$. Then, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \varepsilon$.

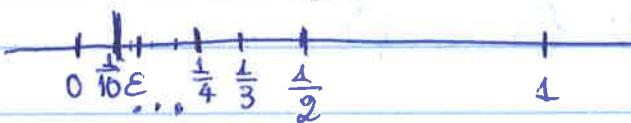
! This tells us that, no matter how small ε is, we can always divide 1 in so many equal line segments that each will be smaller than ε .

Proof: Consider the element $\frac{1}{\varepsilon} \in \mathbb{R}$.

Since \mathbb{N} is not bounded from above, there exists $n \in \mathbb{N}$ such that

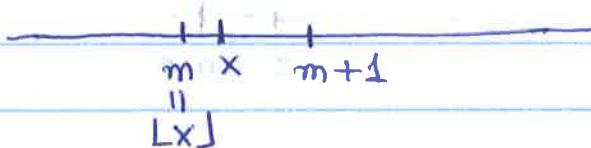
$$n > \frac{1}{\varepsilon} \implies \frac{1}{n} < \varepsilon.$$

$\varepsilon > 0,$
 $n > 0$



(2) Existence of integer part of every real:

→ Prop.: Let $x \in \mathbb{R}$. There exists a unique integer $m \in \mathbb{Z}$, such that $m \leq x < m+1$.



We say that this m is the integer part of x ,

(5)

and we denote it by $[x]$.

NOT required.

"Proof": The above may seem obvious (in fact,

in the proof of 1.20(b) in p. 9 of Rudin's book this fact seems to be derived from the fact that we can find $m_1, m_2 \in \mathbb{N}$ st.

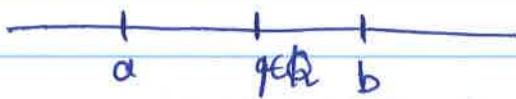
$-m_1 < x < m_2$. However, one also needs to use that every subset of \mathbb{N} has a minimal element (eventually, $m+1$ will be the

minimal element of $\{k \in \mathbb{Z} : k > x\}$, practically a copy of \mathbb{N} which will imply that $m \leq x$). This

property of \mathbb{N} is called the well-ordering principle, and is equivalent to the induction axiom, which is in the axiomatic definition of the natural numbers. You don't need to know these for the exam, but you should investigate further if you are curious.

③ Denseness of \mathbb{Q} in \mathbb{R} :

→ Prop. for any $a, b \in \mathbb{R}$ with $a < b$, there exists $q \in \mathbb{Q}$ with $a < q < b$.

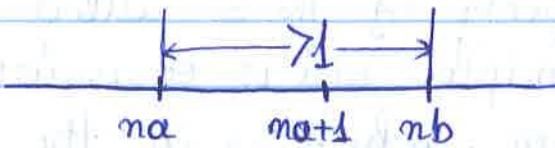


(6)

Proof:

Idea: If two real numbers differ by more than 1, then there should exist an integer between them, which is of course rational! Since we don't know if a and b differ by more than 1, we'll multiply their difference with an $n \in \mathbb{N}$ large enough to make the difference larger than 1, and see what happens...

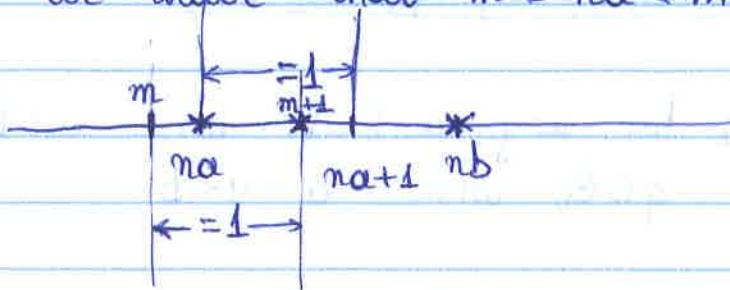
$b-a > 0$. So, by the Archimedean property of the reals, there exists $n \in \mathbb{N}$ such that $n(b-a) > 1$, i.e. $nb - na > 1$.



$$\text{So, } na < m+1 < nb$$

(check both inequalities formally!)

Let $m = \lfloor na \rfloor$; by the definition of integer part, we have that $m \leq na < m+1$. So:



$$m \leq na < m+1 \leq m+1 < nb \quad (\text{check formally}).$$

(7)

What we will use from this is that

$$na < m+1 < nb$$

$$\downarrow n > 0$$

$$a < \frac{m+1}{n} < b$$

$\in \mathbb{Q}$

■

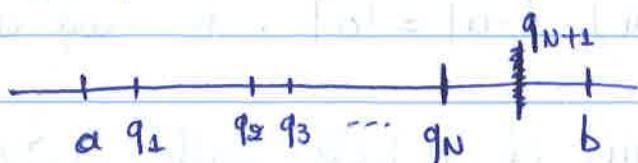
→ Corollary: for any $a, b \in \mathbb{R}$ with $a < b$, there exist infinitely many rationals q with $a < q < b$.

Proof: We know that there exists at least one $q \in \mathbb{Q}$ such that $a < q < b$. So, the set $\{q \in \mathbb{Q} : a < q < b\}$ is non-empty.

Suppose that $\{q \in \mathbb{Q} : a < q < b\}$ is finite; let

$$\{q_1, q_2, \dots, q_N\} = \{q \in \mathbb{Q} : a < q < b\}$$

with $q_1 < q_2 < \dots < q_N$.



Since $q_N, b \in \mathbb{R}$ with $q_N < b$, it follows by the last proposition that $\exists q_{N+1} \in \mathbb{Q}$ with $q_N < q_{N+1} < b$.

(8)

So, $q_{n+1} \in \mathbb{Q}$ is larger than the largest rational between a and b , contradiction.

So, $\{q \in \mathbb{Q} : a < q < b\}$ is not finite. Since it is non-empty, it has to be infinite.

(4) Dense ness of $\mathbb{R} \setminus \mathbb{Q}$ in \mathbb{R} :

We know that $\mathbb{Q} \subsetneq \mathbb{R}$: indeed, we have seen that $\nexists q \in \mathbb{Q}$ with $q^2 = 2$, while $\exists x \in \mathbb{R}$ with $x^2 = 2$.

→ Def: We define the set of irrational numbers to be $\mathbb{R} \setminus \mathbb{Q}$.

→ Prop: for any $a, b \in \mathbb{R}$ with $a < b$, there exists

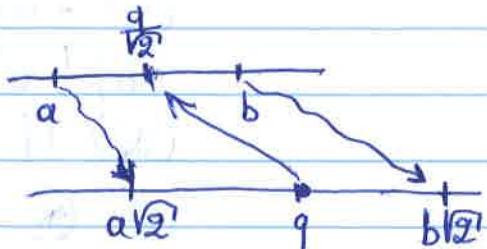
$x \in \mathbb{R} \setminus \mathbb{Q}$ with $a < x < b$.



Proof: Since $a < b$ and $\sqrt{2} > 0$, we have

$$a\sqrt{2} < b\sqrt{2}$$

By dense ness of \mathbb{Q} in \mathbb{R} ,
there exists $q \in \mathbb{Q}$, $q \neq 0$,



s.t. $a\sqrt{2} < q < b\sqrt{2}$.

(9)

(it is the Corollary earlier, rather than the Proposition, that ensures that we can find such q that is non-zero).

Since $\sqrt{2} > 0$, we have $a < \frac{q}{\sqrt{2}} < b$.

And $\frac{q}{\sqrt{2}} \in \mathbb{R} \setminus \mathbb{Q}$ (indeed, if $\frac{q}{\sqrt{2}} = q' \in \mathbb{Q}$,
then $q \neq 0 \Rightarrow q' \neq 0$, so
 $\sqrt{2} = \frac{q}{q'} \in \mathbb{Q}$, a contradiction). ■

→ Corollary: for any $a, b \in \mathbb{R}$ with $a < b$,
there exist infinitely many irrationals x with $a < x < b$.

Proof: Exercise.