Introduction to Analysis - Math 104.

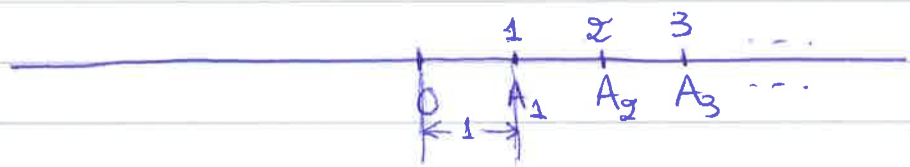
Lecture 1 — 24 Aug 2016.

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:

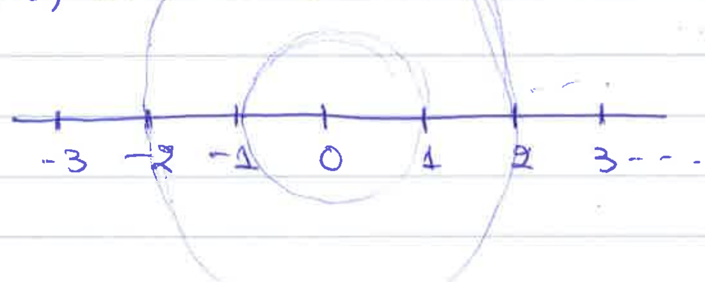
We define $\mathbb{N} := \{1, 2, 3, \dots\}$ (note that we exclude 0 for technical reasons)

and $\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

It is easy to represent these on a line:



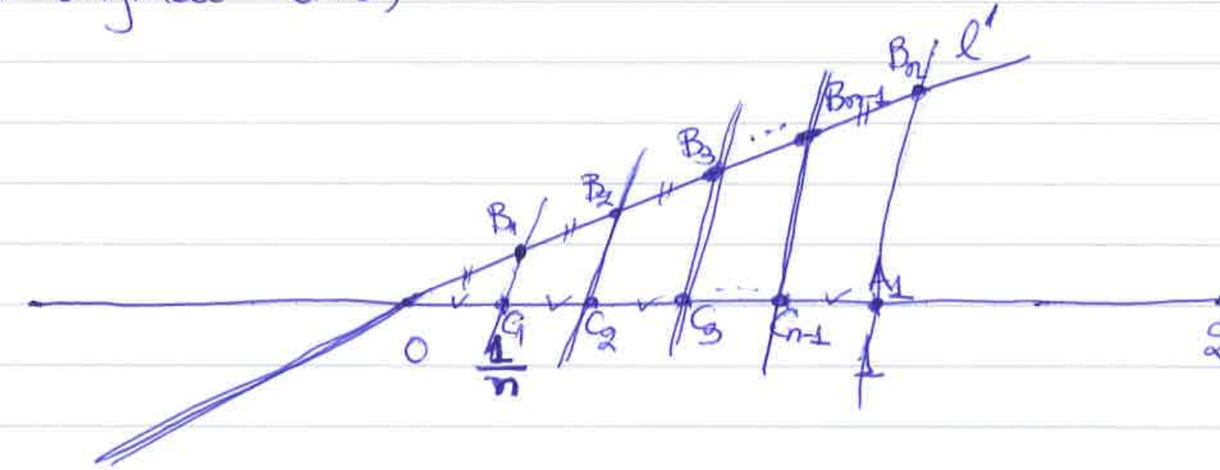
Place O somewhere on the line, and take $OA_1, A_1A_2, A_2A_3, \dots$ to be equal line segments on the line. We place 1 at A_1, 2 at A_2, 3 at A_3, etc. (Note that, this way, we are accepting that the length of OA_1 is 1)
This way $\mathbb{N}$ is represented on the line.
As for the elements of $\mathbb{Z}$, we get the reflections of $1, 2, 3, \dots$ w.r.t. O.



Let us now define the rational numbers:

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

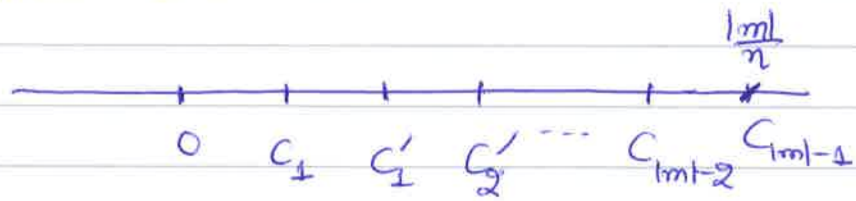
To represent $\frac{m}{n}$ on the line above, first we take line l' through O intersecting our original line,



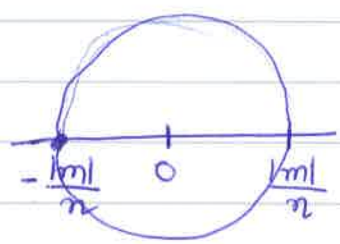
and on l' we take equal line segments $OB_1, B_1B_2, B_2B_3, \dots, B_{n-1}B_n$ (it doesn't matter how long they are, as long as they all have equal lengths). We connect B_n with A_1, and draw parallel lines to B_nA_1 through $B_1, B_2, \dots, B_{n-1}$. These lines intersect OA_1 at points $C_1, C_2, \dots, C_{n-1}$. 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

$OC_1 = C_1C_2 = C_2C_3 = \dots = C_{n-1}A_1$; 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 C_1.

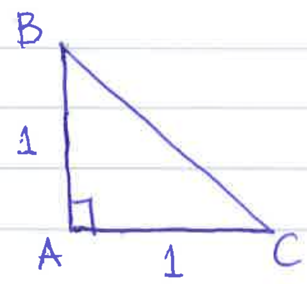
Now, to represent $\frac{m}{n}$ on the line, we take $|m|$ consecutive copies of OC_1, starting from O:



We can place $\frac{|m|}{n}$ at the point $C_{|m|-1}$. That is $\frac{m}{n}$ for $m \geq 0$; for $m < 0$, we take the reflection of $\frac{|m|}{n}$ on the line, w.r.t. O.



⚠ We have placed all elements of $\mathbb{Q}$ on the line <u>merely</u> by ruler-and-compass construction. We can create more such "natural lengths" this way. For instance, create a triangle ABC, with $B\hat{A}C$ a <u>right angle</u>, 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 occuring" length;

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

with all the elements of $\mathbb{Q}$. <u>However</u>:

<u>Proposition:</u> $\sqrt{2} \notin \mathbb{Q}$.

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

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

Then, $\sqrt{2}^2 = \frac{m^2}{n^2} \Longrightarrow \boxed{m^2 = 2n^2}$ (*)

By (*), m^2 even, thus m even.

(Indeed, the square of an odd number is always odd: $\forall k \in \mathbb{Z}, (2k+1)^2 = 4k^2+4k+1 =$
$= 2\underbrace{(2k^2+1)}_{\in\mathbb{Z}}+1$, odd. So, m^2 even $\Rightarrow m$ even.)

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

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

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

$$\begin{aligned} * : S \times S &\longrightarrow S \\ (a,b) &\longmapsto a*b \end{aligned}$$

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

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

Then, the composition of functions

$$\begin{aligned} \circ : S \times S &\to S \\ (f,g) &\to f \circ g \end{aligned}$$

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

$*$	0	1
0	1	0
1	1	1

∇	0	1
0	0	1
1	1	0

Both $*$, ∇ 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 <u>order</u> in the pair <u>matters</u> 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)

<u>Def:</u> Let $\mathbb{F} \neq \emptyset$, a set. Let $+, \cdot$ be two operations on $\mathbb{F}$.

for now, just symbols!

We say that the triple $(\mathbb{F}, +, \cdot)$ (or, the set $\mathbb{F}$ equipped with the operations $+, \cdot$) is a <u>field</u> if $+$ and $\cdot$ satisfy the following:

I) Axioms for $+$:

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

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

I3) There exists an element of $\mathbb{F}$, which we denote by 0, s.t. $a+0=a$, $\forall a\in\mathbb{F}$
(existence of additive identity)

I4) $\forall a\in\mathbb{F}$, there exists $a'\in\mathbb{F}$ s.t.
$a+a'=0$ (existence of additive inverse).
We call a' the <u>opposite</u> of a, and we denote it by $-a$.

II) Axioms for $\cdot$:

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

II2) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$, $\forall a,b,c\in\mathbb{F}$ (associativity).

II3) There exists an element of $\mathbb{F}$, different to 0, which we denote by 1, s.t.
$a\cdot 1=a$, $\forall a\in\mathbb{F}$ (existence of multiplicative identity)

II4) $\forall a\in\mathbb{F}$, $a\neq 0$, there exists $a''\in\mathbb{F}$ s.t.
$a\cdot a'=1$ (existence of multiplicative inverse).
We call a' the <u>inverse</u> of a, and we denote it by a^{-1}.

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

$a\cdot(b+c)=a\cdot b+a\cdot c$, $\forall a,b,c\in\mathbb{F}$
(distributivity).

⚠ 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.

<u>ex:</u>
- $(\mathbb{Q}, +, \cdot)$ is a field.
  the usual operations
- $(\mathbb{N}, +, \cdot)$ is <u>not</u> a field: there is no additive identity, not multiplicative or additive inverse for any $n \in \mathbb{N}$. Each of these reasons would suffice.
- $(\mathbb{Z}, +, \cdot)$ is <u>not</u> 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

·	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 that we get starting from 0 and adding 1 consecutively).

Some properties of fields:

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

The axioms for the addition $+$ imply:
For all $a, b, c \in \mathbb{F}$:

(a_1) $a+b = a+c \Rightarrow b=c$.
(a_2) $a+b = a \Rightarrow b=0$.
(a_3) $a+b = 0 \Rightarrow b=-a$.
(a_4) $-(-a) = a$.

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) $ab = a\cdot c \Rightarrow b=c$.
(m_2) $a\cdot b = a \Rightarrow b=1$.
(m_3) $a\cdot b = 1 \Rightarrow b=a^{-1}$.
(m_4) $(a^{-1})^{-1} = a$

Also:

(i) $0\cdot a = 0$, $\forall a \in \mathbb{F}$.
(ii) If $a \neq 0$, $b \neq 0$ in $\mathbb{F}$, then $a\cdot b \neq 0$
(iii) $(-a)\cdot b = a\cdot(-b) = -(a\cdot b)$, $\forall a, b \in \mathbb{F}$.
(iv) $(-a)\cdot(-b) = a\cdot b$, $\forall a, b \in \mathbb{F}$.

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

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

(v) There is a unique additive identity.
(vi) There is a unique multiplicative identity.
(vii) $\forall a \in \mathbb{F}$, the additive inverse of a is unique.
(viii) $\forall a \in \mathbb{F}$, $a \neq 0$, 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 $(\mathbb{F}, +, \cdot)$ be a field. We say that it is ordered if $\exists P \subseteq \mathbb{F}$, s.t.

P1) $\forall a \in \mathbb{F}$, exactly one of the following holds:

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

P2) $\forall\, a, b \in P$, $a+b \in P$ and $a \cdot b \in P$.

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

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

In particular, the order is defined as such:

<u>Def:</u> 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:

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

<u>Notation:</u> 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:

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

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

  (i.e., $b - a \in P$)

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

  (i.e., $a - b \in P$)

<u>Observation:</u> $a > 0$ means $a \in P$.

<u>Proof:</u> $a > 0$ means $\underbrace{a + (-0)}_{\substack{\| \\ a+0 \\ \| \\ a}} \in P$, i.e. $a \in P$. $\blacksquare$

<u>ex:</u>

- $(\mathbb{Q}, +, \cdot)$ is an ordered field, because the set $P = \left\{ \frac{m}{n} : \begin{array}{l} m \in \mathbb{N} \cup \{0\}, \\ n \in \mathbb{N} \end{array} \right\}$ 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 <u>not</u> an ordered field (exercise!).

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:

$$b-a>0 \quad \text{or} \quad b-a=0 \quad \text{or} \quad \overbrace{-(b-a)}^{=a-b}>0,$$

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

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