Lecture 1

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

and \( \mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \).

It is easy to represent these on a line:

---

\[ \begin{array}{c}
\text{0} & \text{A}_1 & \text{A}_2 & \text{A}_3 & \ldots \\
\text{1} & \text{2} & \text{3} & \ldots \\
\end{array} \]

---

Place 0 somewhere on the line, and take \( OA_1, A_1A_2, A_2A_3, \ldots \) 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, \ldots w.r.t. 0.

---

\[ \begin{array}{c}
\text{-3} & \text{-2} & \text{-1} & \text{0} & \text{1} & \text{2} & \text{3} & \ldots \\
\end{array} \]
Let us now define the rational numbers:
\[ \mathbb{Q} := \{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \} \]

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 \( OB_1, B_1B_2, B_2B_3, \ldots, B_{n-1}B_n \) (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 \( B_1, B_2, \ldots, B_{n-1} \). These lines intersect \( OA_1 \) at points \( C_1, C_2, \ldots, C_{n-1} \). By similarity of the triangles \( OB_1C_1, OB_2C_2, OB_3C_3, \ldots, OB_nC_n \), and since \( OB_1=OB_2=\ldots=OB_{n-1} \), it follows that
$OC_1 = GC_2 = C_2 C_3 = \ldots = C_{n-1} A_1$; we have thus split $OA_1$ into $n$ equal line segments. Each of these has length \( \frac{OA_1}{n} = \frac{1}{n} \), so we can therefore represent $\frac{1}{n}$ by the point $C_1$.

Now, to represent $\frac{m}{n}$ on the line, we take $\frac{1}{n}$ consecutive copies of $OC_1$, starting from $O$:

![Diagram of line segment divided into n equal parts]

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

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. $O$.

![Diagram of reflection]

⚠️ 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,
create a triangle $ABC$, with $\overline{BAE}$ 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, there exists $m, n \in \mathbb{N}$, with greatest common divisor 1, s.t. $\sqrt{2} = \frac{m}{n}$.

Then, $2n^2 = m^2 \Rightarrow m^2 = 2n^2 \quad \Box$

By $\Box$, $m^2$ even, thus $m$ even.

(Indeed, the square of an odd number is always odd: $4k+1^2 = 4k^2 + 4k + 1 = 2(2k^2 + k) + 1$, odd. So, $m^2$ even $\Rightarrow m$ even.)
So, \( \exists k \in \mathbb{Z} \) s.t. \( m = 2k \). Then, by \( \star \):

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

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

Therefore, \( \square \).

So, there are certainly elements on the line that are not in \( \mathbb{R} \). 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 \( * : S \times S \to S \)

\[
(a, b) \to a * b
\]

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

**ex:** \( \ast S = \{ f : \mathbb{R} \to \mathbb{R}, 1-1 \text{ and onto} \} \).

Then, the composition of functions \( o : S \times S \to S \)

\[
(\circ, g) \to \circ g
\]
\[ S = \{0, 1\}, \quad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \quad \begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \]

Both \( \times \) and \( \vee \) are operations on \( S \).

* Usual addition and multiplication are operations on \( \mathbb{N}, \mathbb{Z}, \mathbb{Q} \).

\[ \text{A} \quad \text{From the examples above it is clear that, in general, the order in the pair matters when it comes to operations.} \]

+ 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).

\[ \text{Def:} \quad \text{Let} \quad \mathbb{F} \neq \emptyset, \text{a set. Let} \quad (+, \cdot) \text{ be two operations on } \mathbb{F}. \]

\[ \text{We say that the triple} \quad (\mathbb{F}, +, \cdot) \]

\[ \text{(or, the set } \mathbb{F} \text{ equipped with the operations } +, \cdot) \]

\[ \text{is a field if} \quad + \text{ and } \cdot \text{ satisfy the following:} \]
(I) Axioms for $+$:

I.1) $a + b = b + a, \forall a, b \in F$ (commutativity)

I.2) $a + (b + c) = (a + b) + c, \forall a, b, c \in F$ (associativity)

I.3) There exists an element of $F$, which we denote by $0$, s.t. $a + 0 = a, \forall a \in F$ (existence of additive identity)

I.4) $\exists a \in F, \text{ there exists } a' \in F \text{ s.t. } a + a' = 0$ (existence of additive inverse)

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

(II) Axioms for $\cdot$:

II.1) $a \cdot b = b \cdot a, \forall a, b \in F$ (commutativity)

II.2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in F$ (associativity)

II.3) 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)

II.4) $\exists a' \neq 0, \text{ there exists } a'' \in F \text{ s.t. } a \cdot a'' = 1$ (existence of multiplicative inverse)

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

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

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

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

- $(\mathbb{N}, +, \cdot)$ is not 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 not a field: there exists no multiplicative inverse for any $k \in \mathbb{Z}$, apart from $k=1$.
- $F = \{0, 1\}$, with the operations

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

is a field. $(F, +, \cdot)$ 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."
Some properties of fields:

Let \((F,+,\cdot)\) be a field. Then:

The axioms for the addition \(+\) imply:

For all \(a, b \in F\):

\[ a + b = a + c \Rightarrow b = c. \]  
\[ a + b = a \Rightarrow b = 0. \]  
\[ a + b = 0 \Rightarrow b = -a. \]  
\[ -(a) = a. \]

The axioms for the multiplication \(\cdot\) imply:

For all \(b, c \in F\), and all \([a \neq 0]\) in \(F\):

\[ ab = a \cdot c \Rightarrow b = c. \]  
\[ a \cdot b = a \Rightarrow b = 1. \]  
\[ a \cdot b = 1 \Rightarrow b = a^{-1}. \]  
\[ (a^{-1})^{-1} = a. \]

Also:

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

A (i) – (iv) really demonstrate the difference between + and \(\cdot\); one cannot expect,
for instance, that
1 \cdot a = 1 \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 \((\mathbb{R}, +, \cdot)\) 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 \(\mathbb{R}\). Indeed, \((\mathbb{R}, +, \cdot)\) is what we call an ordered field:

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

P1) \(\forall a \in F\), exactly one of the following
holds:
\[ a \in P \text{ or } a=0 \text{ or } -a \in P. \]
\[ \forall a, b \in P, \ a+b \in P \text{ and } a \cdot b \in P. \]

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 \( \leq \) on \( \mathbb{F} \), defined as:

\[ \text{for } a, b \in \mathbb{F}, \ a \leq b \text{ iff } b + (-a) \in P. \]

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

- \( b - a := b + (-a), \forall a, b \in \mathbb{F}. \)
\( a \leq b \) means \( a < b \) or \( a = b \).

\[ (\exists \delta \text{ s.t. } a - b \leq \delta) \]

\( a > b \) means \( b \leq a \).

\[ (\exists \delta \text{ s.t. } a - b > \delta) \]

**Observation:** \( a > 0 \) means \( a \in P \).

**Proof:** \( a > 0 \) means \( a + (-c) \in P \), i.e., \( a \in P \).

\[ \frac{a + 0}{a} \]

**ex:** \((\mathbb{R}, +, \cdot)\) is an ordered field, because the set \( P = \left\{ \frac{m}{n} : m \in \mathbb{N}, n \in \mathbb{N} \right\} \)

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

**ex:** The field \((\mathbb{Z}, +, \cdot)\) defined earlier is not an ordered field (exercise!)
Properties of ordered fields:

Let \((F, +, \cdot, \leq)\) be an ordered field, with order \(\leq\). Then:

(i) If \(a, b \in F\), 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 \(c \in F\), 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 \(b - a \in F\). Then, exactly one of the following holds:
\[ b - a > 0 \quad \text{or} \quad b - a = 0 \quad \text{or} \quad -(b - a) > 0, \]
i.e. \(b > a\) or \(b = a\) or \(a > b\).

(ii) \(a > b \Rightarrow a - b > 0 \Rightarrow (a - b) + (b - c) > 0\), i.e. \(a - c > 0\).
(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 \(\ast\) holds. So, we have a contradiction.

Therefore, \(1 > 0\).

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

(i) \(R\) is in a 1-1 correspondence with the number line, and
(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. $(\mathbb{R}, +, \cdot, <)$ 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 $\mathbb{A} \subseteq \mathbb{F}$.

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

\[
\forall a \leq b, \forall a \in \mathbb{A} \quad a \leq b
\]

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

\[
\begin{array}{c}
A \\
\hline
a \leq b, \forall a \in \mathbb{A} \\
\hline
A \quad b \\
\hline
\end{array}
\]

I.e.: $\mathbb{A}$ can have many upper bounds.
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.

\[ \text{ex. } \quad \text{in } (\mathbb{Q}, +, \cdot, \leq) : \]

- $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{N}$, $\{x \in \mathbb{Q} : x > 0\}$, $\{x \in \mathbb{Z}^*: x \in \mathbb{N}\}$ are not bounded from above (in $\mathbb{Q}$).

- $\mathbb{Q}$ is bounded from above (by any $q \in \mathbb{Q}$ with $q > 1$).

- $\{x \in \mathbb{Q} : x < 0\}$ is bounded from above (by any $q \in \mathbb{Q}$ with $q \geq 0$).

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

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

**Obs:** Note that $b$ doesn't have to be in $A$. 


in order to be a least upper bound of $A$.

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

**Def.:** Let $(F, +, \cdot, \leq)$ be an ordered field. We say that $(F, +, \cdot, \leq)$ is complete if every (non-empty) subset of $F$ that is bounded from above has a least upper bound (in $F$).

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

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

\[
\exists x \in \mathbb{Q} : x < \sqrt{2}
\]
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 \( \mathbb{Q} \).

However, we are not even allowed to write \( \sqrt{2} \) yet; we haven't defined anything beyond \( \mathbb{Q} \), and we know that \( g \in \mathbb{Q} \) s.t.

\( q^2 = 2 \) ... 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:

- \( A \neq \emptyset : 1 \in A (1 \in \mathbb{Q}, 1 > 0, 1^2 < 2) \)

- \( A \) is bounded from above (in \( \mathbb{Q} \)): for instance,
4 is an upper bound of $A$, because, $\forall x \in A$, $4^2 \geq x^2 \Rightarrow 4x^2 \geq x^2 \Rightarrow 4 \geq x$. 

(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 $b$. Then, exactly one of the following holds (as $\mathbb{Q}$ is an ordered field):

- $b^2 < 2$
- $b^2 = 2$
- $b^2 > 2$

Idea: in the picture below, which we have explained we cannot officially use yet (but which we know 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
upper bound of $A$, contradiction.

- If $b=\emptyset \rightarrow \exists \emptyset \in A$, contradiction

So, $A$ cannot have a least upper bound.

- Suppose that $b^2=2$. Then there exists a rational that squares to $2$, contradiction.

- Suppose that $b^2<2$. We will find $\varepsilon>0$ st. $b+\varepsilon \in A$, in which case $b(b+\varepsilon)>b$, where $b$ is the least upper bound of $A$, contradiction.

**Details:** Indeed, we want $\varepsilon \in A$, $\varepsilon>0$, $(b+\varepsilon)^2<2$.

Now, $(b+\varepsilon)^2<2 \iff b^2 + 2b\varepsilon + \varepsilon^2 < 2 \iff 2b\varepsilon + \varepsilon^2 < 2 - b^2$. \(\square\)

So, if we look for $\varepsilon<1$ with the above properties, we will be able to use properties of ordered field. That $\varepsilon^2<\varepsilon$, which implies that $2b\varepsilon + \varepsilon^2 < 2b\varepsilon + \varepsilon = (2b+1)\cdot \varepsilon$. So, if we find
\( \epsilon \in \mathbb{Q} \) with \( 0 < \epsilon < 1 \) s.t. \( (2b+1) \cdot \epsilon \leq 2 - b^2 \),

we automatically have \( \Phi \) as well.

Therefore, it suffices to find

\( \epsilon \in \mathbb{Q} \) s.t. \( \epsilon > 0 \), \( \epsilon < 1 \), and

\[
(2b+1) \cdot \epsilon \leq 2 - b^2 \iff \epsilon < \frac{2 - b^2}{2b+1}
\]

\( 2b+1 > 0 \) \quad \text{(check!)}

Notice that \( \epsilon = \frac{1}{2} \cdot \min \{1, \frac{2 - b^2}{2b+1} \} \) satisfies all these conditions; thus, for this \( \epsilon \), \( b+\epsilon \in A \), and \( b+\epsilon > b \), the least upper bound of \( A \), a contradiction.

- Suppose \( b^2 \geq 2 \). We will find \( \epsilon > 0 \) (in \( \Phi \)), s.t. \( b - \epsilon \) is an upper bound of \( A \) (in \( \Phi \)).

In this case \( b - \epsilon \) is an upper bound smaller than the least upper bound, a contradiction.

Details: for \( b - \epsilon \) to be an upper bound of \( A \)

for some \( \epsilon \in \mathbb{Q} \), it suffices to have

\[
\left( b - \epsilon \right)^2 > 2 \quad \text{and} \quad b - \epsilon > 0 \quad \text{(prove this!)}
\]

\[
\frac{b^2 - 2b\epsilon + \epsilon^2}{b^2 - 2\epsilon + \epsilon^2}
\]
So, it suffices to have:

e \in \mathbb{R}, \; e > 0, \; e < b \; \text{and} \; b^2 - 2be + e^2 > 2.

Notice that, if I find e \in \mathbb{R} \text{ s.t. } e > 0, \; e < 0

and \; b^2 - 2be > 2, \; \text{then I automatically}

also have \; b^2 - 2be + e^2 > 2 \; \text{(as } e > 0 \text{ in the ordered field } \mathbb{R})

so I am done.

So, it suffices to find e \in \mathbb{R} \text{ s.t. } e > 0, \; e < b

and \; b^2 - 2be > 2 \iff \; 2be < b^2 - 2 \iff \; e < \frac{b^2 - 2}{2b}.

\text{(check!)}

Notice that \; e = \frac{1}{2} \cdot \min \{b, \; \frac{b^2 - 2}{2b}\} \; \text{satisfies all}

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

Eventually, we have shown that \(\star\)

is false. This is a contradiction, so our initial assumption that \(A\) has a least upper bound is false.
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).
Corollary: The extension of \((\mathbb{Q}, +, \cdot, <)\) 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.
Def: If \( A \subseteq \mathbb{R} \), let \( \sup A \) := the least upper bound of \( A \) in \( \mathbb{R} \).

We have shown that \( \sqrt{2} \in \mathbb{Q} \) with \( \sqrt{2} = 2 \).

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 \( \sqrt[n]{r} \) 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.
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:
     
     \[
     \text{for all } n \in \mathbb{N}, \ n \leq \alpha \quad (\alpha \text{ an upper bound}),
     \]
     
     so, for all \(n \in \mathbb{N}\), \(\frac{n+1}{\in \mathbb{N}} \leq \alpha\),
     
     i.e., for all \(n \in \mathbb{N}\), \(n \leq \alpha - 1\).
     
     So, \(\alpha - 1\) is an upper bound of \(A\) in \(\mathbb{R}\). However, \(\alpha - 1 \leq \alpha\), the least upper bound of \(A\). This is a contradiction. So,
     
     \(\mathbb{N}\) is not bounded from above.
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 \( n \cdot \varepsilon > a \)

We tend to always think of \( \varepsilon \) as very small. This proposition tells us that, no matter how small \( \varepsilon \) 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 \( N \) is not bounded from above in \( \mathbb{R} \), so \( \frac{a}{\varepsilon} \) is not an upper bound of \( N \).

Thus, there exists some \( n \in \mathbb{N} \) with \( n \cdot \varepsilon > a \).
Prop. 3: Let $\epsilon > 0$. Then, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$.

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

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

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

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

Since $n > \frac{1}{\epsilon}$,

$$\frac{1}{n} < \epsilon.$$  

(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 $x$. 

Diagram:

- $0 < \frac{1}{\epsilon}$, $\frac{1}{\epsilon} - \frac{1}{2}$, $\frac{1}{\epsilon} - \frac{1}{3}$, $\frac{1}{\epsilon}$, $1$

- $m$, $m+1$
and we denote it by \( L \times 1 \).

**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 \( m_1, m_2 \in \mathbb{N} \) s.t. \(-m_1 < x < m_2\). 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 \( \{ k \in \mathbb{Z} : k > x \} \), 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 \( a < q < b \).
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 some 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

\[ n(b - a) > 1, \text{ i.e. } nb - na > 1. \]

\[ \overbrace{\quad > 1}^{n(b-a)} \quad \overbrace{\quad \text{na} \quad \text{na+1} \quad \text{nb}}^{\text{nb}} \]

So,

\[ \text{na} < \text{na+1} < \text{nb} \]

(check both inequalities formally!)

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

\[ \overbrace{\quad m}^{\text{m}} \quad \overbrace{\quad \text{na} \quad \text{na+1} \quad \text{nb}}^{\text{nb}} \]

\[ \overbrace{\quad m+1}^{\text{m+1}} \quad \overbrace{\quad -1}^{\text{-1}} \quad \overbrace{\quad \text{m} \quad \text{m+1}}^{\text{m+1}} \quad \overbrace{\quad \text{na} \quad \text{na+1} \quad \text{nb}}^{\text{nb}} \]

\[ m \leq na < m+1 \leq na+1 < nb \quad (\text{check formally}). \]
What we will use from this is that
\[ \forall a < m+1 < n, b \]

\[ \exists m > 0 \]

\[ a < \left( \frac{m+1}{n} \right) < b \]

\[ \in \mathbb{Q} \]

\[ \rightarrow \text{Corollary: For any } a, b \in \mathbb{R} \text{ with } a < b, \text{ there exist infinitely many rationals } q \text{ with } a < q < b. \]

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

\[ \supseteq \text{Suppose that } \{ q \in \mathbb{Q} : a < q < b \} \text{ is finite, let} \]

\[ \{ q_1, q_2, \ldots, q_N \} = \{ q \in \mathbb{Q} : a < q < b \} \]

\[ \text{with } q_1 < q_2 < \ldots < q_N. \]

\[ \text{Since } q_N, b \in \mathbb{R} \text{ with } q_N < b, \text{ it follows by the last proposition that } \exists q_{N+1} \in \mathbb{Q} \text{ with } q_N < q_{N+1} < b. \]
So, quite $\mathbb{Q}$ is larger than the largest rational between $a$ and $b$; contradiction.

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

**4. Denseness of $\mathbb{R} \setminus \mathbb{Q}$ in $\mathbb{R}$**

We know that $\mathbb{Q} \subseteq \mathbb{R}$; indeed, we have seen that $\exists q \in \mathbb{Q}$ with $q^2 = 2$, while $\not \exists x \in \mathbb{R}$ 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 $a < x < b$.

![Diagram showing the denseness of $\mathbb{Q}$ in $\mathbb{R}$]

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

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

![Diagram showing the existence of such a $q$]
s.t. \( a^{\frac{1}{2}} < q < b^{\frac{1}{2}} \)

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

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

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

\[ \rightarrow \text{Corollary: For any } a, b \in \mathbb{R} \text{ with } a < b, \]
there exist infinitely many irrationals \( x \) with \( a < x < b \).

Proof: Exercise.