LECTURE 2: RATIONAL AND REAL NUMBERS

Let's get real and talk about real numbers! Just like we did for $\mathbb{N}$, we can again define $\mathbb{R}$ in terms of axioms. In other words, what properties make $\mathbb{R}$ so special?

1. What is a field?

Video: What is a field?

First of all, what distinguishes $\mathbb{R}$ from $\mathbb{N}$ (or $\mathbb{Z}$) is that $\mathbb{R}$ is a **field:**

Definition:

A field $\mathbb{F}$ is a set equipped with two operations[a] addition $+$ and multiplication $\cdot$ such that the following properties are true.

Addition Axioms:

(A0) $a, b \in \mathbb{F} \Rightarrow a + b \in \mathbb{F}$ (closed under $+$)

(A1) $(a + b) + c = a + (b + c)$ (associativity)

(A2) $a + b = b + a$ (commutativity)

[a] That is, functions from $\mathbb{F} \times \mathbb{F}$ to $\mathbb{F}$

Date: Thursday, September 2, 2021.

(A3) There is an element $0 \in \mathbb{F}$ such that $a + 0 = 0 + a = a$ for all $a \in \mathbb{F}$ (zero-element)

(A4) For all $a \in \mathbb{F}$ there is an element $-a \in \mathbb{F}$ such that $a + (-a) = (-a) + a = 0$ (additive inverse)

Multiplication Axioms:

(M0) $a, b \in \mathbb{F} \Rightarrow ab \in \mathbb{F}$ (closed under $\cdot$)

(M1) $(ab)c = a(bc)$ (associativity)

(M2) $ab = ba$ (commutativity)

(M3) There is an element $1 \in \mathbb{F}$ such that $a1 = 1a = a$ for all $a \in \mathbb{F}$ (1-element)

(M4) For all $a \neq 0$ there exists an element $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = a^{-1}a = 1$

Distributive law:

(DL) $a(b + c) = ab + ac$, $(a + b)c = ac + bc$

Examples: $\mathbb{R}$ (of course), but also $\mathbb{Q}$ (rational numbers), $\mathbb{C}$ (complex numbers) and even $\{0, 1\}$ (with addition defined as $1 + 1 = 0$).

Non-Examples: $\mathbb{N}$ (if $n \in \mathbb{N}$ then $-n \notin \mathbb{N}$), $\mathbb{Z}$ (if $m \in \mathbb{Z}$, then $m^{-1} \notin \mathbb{Z}$), so already this distinguishes $\mathbb{R}$ from $\mathbb{N}$ and $\mathbb{Z}$

Hopefully those axioms are "obvious" to you; they are meant to be a good model of $\mathbb{R}$, and in fact a lot of properties of $\mathbb{R}$ are true for general fields. Here are some natural consequences of our axioms:

Theorem:

The following properties are true in any field $\mathbb{F}$.

(1) $a + c = b + c \Rightarrow a = b$ (cancellation law)

(2) If $a \neq 0$, then $ab = ac \Rightarrow b = c$ (another cancellation law)

(3) $a0 = 0$

(4) $(-a)b = -ab$

(5) $(-a)(-b) = ab$

(6) $ab = 0 \Rightarrow a = 0$ or $b = 0$ ($\mathbb{F}$ is an *integral domain*)

Proof:

(1)

$$\begin{aligned} a + c =& b + c \\ \Rightarrow (a + c) + (-c) =& (b + c) + (-c) \\ \Rightarrow a + (c + (-c)) =& b + (c + (-c)) \quad \text{(Associativity)} \\ \Rightarrow a + 0 =& b + 0 \quad \text{(Definition of } -c\text{)} \\ \Rightarrow a =& b \quad \text{(Definition of 0)} \end{aligned}$$

(2) Similar (Multiply by a^{-1})

(3) First of all, by definition of 0, we have $0 + 0 = 0$ (you're adding nothing to 0). Now consider $0 + a0$:

$$\begin{aligned} & 0 + a0 \\ =& a0 \text{ (Definition of 0)} \\ =& a(0 + 0) \\ =& a0 + a0 \text{ (Distributivity)} \end{aligned}$$

Hence $0 + a0 = a0 + a0$, and canceling out $a0$ (by (1)) we get $0 = a0$, so $a0 = 0$

(4) Consider

$$\begin{aligned} & ab + (-a)b \\ =& (a + (-a))b \quad \text{(Distributivity)} \\ =& 0b \quad \text{(Definition of } -a\text{)} \\ =& 0 \quad \text{(By (3))} \end{aligned}$$

Hence $ab + (-a)b = 0$, so $(-a)b$ is the additive inverse of ab, that is, $(-a)b = -ab$ (by definition of $-ab$)

(5) Skip (basically apply (4) twice)

(6) Suppose $ab = 0$ but $a \neq 0$, then

$$\begin{aligned} ab =& 0 \\ a^{-1}(ab) =& a^{-1}(0) \\ \left(a^{-1}a\right) b =& 0 \quad \text{(Associativity and (1))} \\ 1b =& 0 \quad \text{(Definition of } a^{-1}\text{)} \\ b =& 0 \quad \text{(Definition of 1)} \end{aligned}$$

□

Note: If you're interested in learning more about fields, make sure to take a course in Abstract Algebra.

2. Ordered Fields

Video: Ordered Fields

That said, there is more to $\mathbb{R}$ than just being a field. In particular, notice that in $\mathbb{R}$ we can compare elements, like saying $2 \leq 3$. This distinguishes $\mathbb{R}$ from its parent $\mathbb{C}$, because we cannot compare complex numbers, see this optional video as to why:

Optional Video: Can we compare complex numbers?

Definition:

A field $\mathbb{F}$ is called an **ordered field** if it has a structure[a] $\leq$ that satisfies the following.

(O1) Either $a \leq b$ or $b \leq a$ (Trichotomy)

(O2) $a \leq b$ and $b \leq a \Rightarrow a = b$ (also Trichotomy)

(O3) $a \leq b$ and $b \leq c \Rightarrow a \leq c$ (Transitivity)

(O4) $a \leq b \Rightarrow a + c \leq b + c$ (Addition preserves order)

(O5) $a \leq b$ and $0 \leq c \Rightarrow ac \leq bc$ (Nonnegative multiplication preserves order)

[a] That is, a function from $\mathbb{F} \times \mathbb{F}$ to { True , False }

Note: $a \geq b$ is defined to be $b \leq a$ and $a < b$ means "$a \leq b$ and $a \neq b$" (Similar for $a > b$)

Examples: $\mathbb{R}$ and $\mathbb{Q}$

Non-Examples: $\mathbb{Z}$ (not a field), $\mathbb{C}$ (cannot order elements)

And of course, from those axioms one can prove other neat facts:

Theorem:

The following properties are true in any ordered field $\mathbb{F}$. Here a, b, c are arbitrary elements in $\mathbb{F}$:

(1) $a \leq b \Rightarrow -a \geq -b$

(2) $a \leq b$ and $c \leq 0 \Rightarrow ac \geq bc$

(3) $b \geq 0$ and $c \geq 0 \Rightarrow bc \geq 0$

(4) $a^2 \geq 0$

(5) $0 < 1$

(6) $a > 0 \Rightarrow a^{-1} > 0$

(7) $a > b > 0 \Rightarrow a^{-1} < b^{-1}$

Proof:

(1)

$$
\begin{aligned}
a &\leq b \\
\Rightarrow a + ((-a) + (-b)) &\leq b + ((-a) + (-b)) \qquad \text{(Since + preserves order)} \\
-b &\leq -a \\
-a &\geq -b \qquad \text{(By definition of } \geq\text{)}
\end{aligned}
$$

(2) First note that if $c \leq 0$, then $-c \geq 0$ (by (1)), but then, by $(O5)$,

$$
\begin{aligned}
a &\leq b \\
(-c)a &\leq (-c)b \\
-ac &\leq -bc \\
ac &\geq bc \text{ (By (1))}
\end{aligned}
$$

(3) This is just $(O5)$ with $a = 0$

(4) By trichotomy, we know either $a \geq 0$ or $a \leq 0$.

Case 1: If $a \geq 0$, then by $(O5)$, we get $aa \geq a0$, so $a^2 \geq 0$ ✓

Case 2: If $a \leq 0$, then by (2), we get $aa \geq a0$, so $a^2 \geq 0$ ✓

So in any case $a^2 \geq 0$

(5) Follows from (4) because $1 = 1^2 \geq 0$, so to conclude, all that's left to show is that $1 \neq 0$ (skip)

(6) Suppose $a > 0$ but $a^{-1} \leq 0$. Since $a \geq 0$, we have $aa^{-1} \leq a0$, so $1 \leq 0$, but this contradicts (5) $\Rightarrow\Leftarrow$

(7) (Skip; Start with $a < b$ and multiply by b^{-1} and then by a^{-1})

Now you may have noticed that everything above is not just valid for $\mathbb{R}$, but also for $\mathbb{Q}$. In particular being an ordered field *isn't* what makes $\mathbb{R}$ so special.

But then *what* makes $\mathbb{R}$ so special? Unfortunately we won't be able to fully answer that question until section 4, but let me already tell you the answer.

Definition:

A **subfield** B is a subset $A \subseteq B$ that is also a field. (kind of like a subspace of a vector space in Linear Algebra)

Example: $\mathbb{Q}$ is a subfield of $\mathbb{R}$ since $\mathbb{Q} \subseteq \mathbb{R}$ and $\mathbb{Q}$ is a field

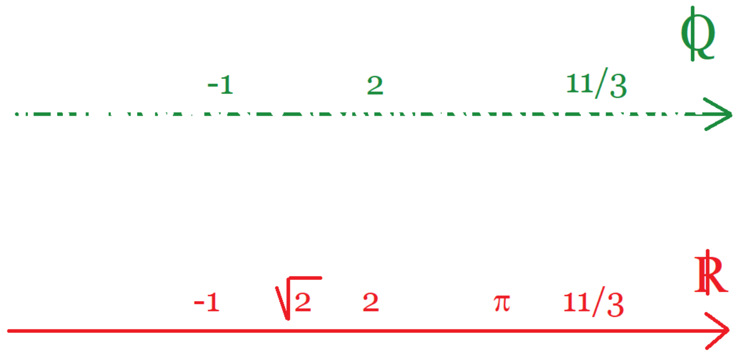
Here is what makes $\mathbb{R}$ so special:

Fact:

There exists an ordered field called $\mathbb{R}$ that contains $\mathbb{Q}$ as a subfield and which satisfies the least upper bound property (see section 4)

Note: In this course we'll take $\mathbb{R}$ as a given, but I'd like to point out that there is an explicit construction of $\mathbb{R}$ in section 6 (which we won't go over)

Again, the least upper bound property will be discussed in section 4, but intuitively it is saying that, unlike $\mathbb{Q}$, $\mathbb{R}$ has no holes, as in the following picture:



In some sense, $\mathbb{Q}$ has lots of gaps, but $\mathbb{R}$ fills those gaps, that's why $\mathbb{R}$ is so much nicer than $\mathbb{Q}$.

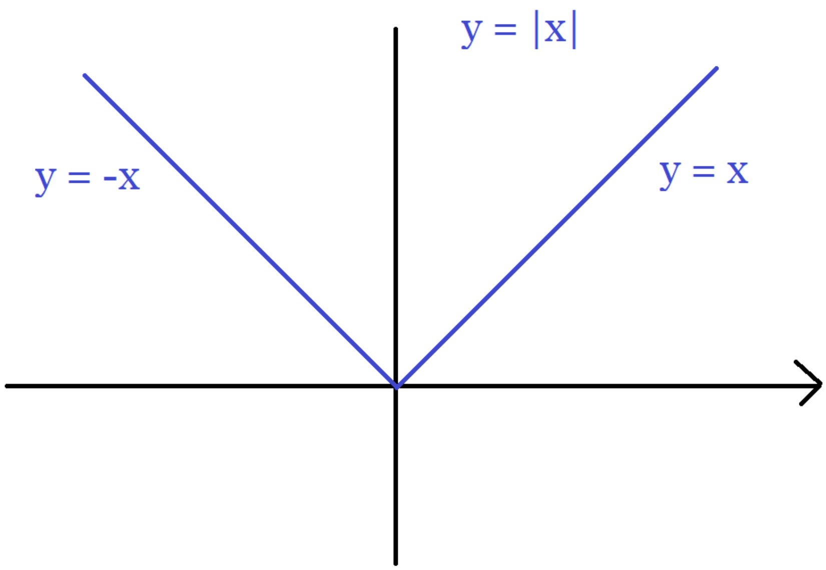
3. Triangle Inequality

Video: Triangle Inequality

Related to this, I would like to remind you of the most important inequality in this course: the triangle inequality. For this, let's recall the concept of absolute value from Calculus 1

Definition:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x \leq 0 \end{cases}$$



From this one can show things like $|x| \geq 0$ for all x (use the definition) and $|ab| = |a|\,|b|$ (do it by cases, for example $a \geq 0$ and $b \geq 0$, see book), and most importantly:

Triangle Inequality:

$$|a + b| \leq |a| + |b|$$

Proof:

STEP 1: We first need a small lemma:

Lemma:

$$-|x| \leq x \leq |x|$$

Proof of Lemma:

Case 1: $x \geq 0$, then $|x| = x$ so

$$- |x| \leq 0 \leq x = |x| \checkmark$$

Case 2: $x \leq 0$, then $|x| = -x$, so $x = - |x|$, so

$$- |x| = x \leq 0 \leq |x| \checkmark$$

STEP 2: By the Lemma, we have $a \leq |a|$ and $b \leq |b|$

Now, add b to both sides of $a \leq |a|$ to get $a + b \leq |a| + b \leq |a| + |b|$

Similarly, we have $a \geq - |a|$ and $b \geq - |b|$

So add b to both sides of $a \geq - |a|$ to get $a+b \geq - |a|+b \geq - |a| - |b| = - (|a| + |b|)$

Therefore we have:

$$- (|a| + |b|) \leq a + b \leq |a| + |b|$$

STEP 3: Finally, to prove $|a + b| \leq |a| + |b|$, we do it by cases:

Case 1: If $a + b \geq 0$, then $|a + b| = a + b \leq |a| + |b|$ (by STEP 2) ✓

Case 2: If $a + b \leq 0$, then $|a + b| = -(a + b) \leq - (- (|a| + |b|))$ (by STEP 2) $= |a| + |b|$. ✓

So in both cases we have the desired result □

Why is it called the triangle inequality? This will be clearer after the next result

Definition:

$$\text{dist}(a, b) = |a - b|$$

Note: This is sometimes written as $d(a, b)$

Corollary:

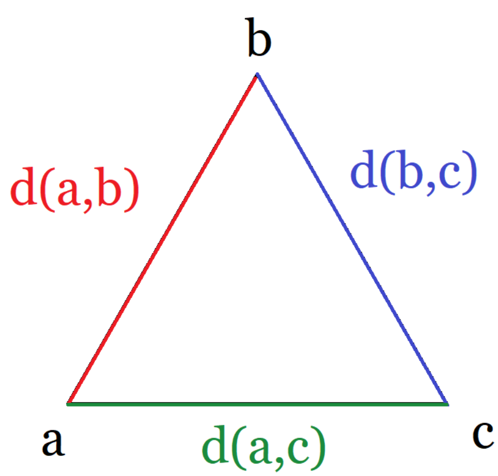
$$\text{dist}(a, c) \leq \text{dist}(a, b) + \text{dist}(b, c)$$

Proof:

$$\begin{aligned}\operatorname{dist}(a,c) &= |a-c| \\ &= |a-b+b-c| \\ &= |(a-b)+(b-c)| \\ &\leq |a-b|+|b-c| \\ &= \operatorname{dist}(a,b)+\operatorname{dist}(b,c)\end{aligned}$$

Important Note: This trick with adding/subtracting b is **SUPER** important and will be used many times over!!!

Note: This corollary explains why the triangle inequality is called as such. It says that the sum of the lengths of two legs of a triangle is always greater than or equal to the length of the third one. In this picture, the green segment is smaller than the sum of the red and blue ones:



A less useful inequality to note is the

Reverse Triangle Inequality:

$$|a-b| \geq ||a|-|b||$$

Example:

$$\underbrace{|3-(-5)|}_{8} \geq ||3|-|-5|| = |3-5| = 2$$

Proof: See the next HW

Note: The reverse triangle inequality *sounds* useful but is actually really useless, it rarely works.

4. Rational Roots Theorem (optional)

Video: Rational Roots Theorem

Let's now go back to rational numbers and explore some useful properties, although we won't really use them in this course. The next theorem explains why we care about algebraic numbers (= roots of polynomials):

Rational Roots Theorem:

Suppose that the polynomial

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

with integer coefficients has a rational root, that is a zero of the form $x = \frac{p}{q}$ where p and q are integers with $q \neq 0$ and no common factors

Then p divides a_0 (constant term) and q divides a_n (leading term)

This theorem is useful for finding roots of polynomials:

Example 1:

Find a root of $x^3 + 3x^2 - 14x + 8$

Here $a_0 = 8$ and $a_3 = 1$. The theorem says that if $x = \frac{p}{q}$ is a root, then p must divide 8 (so $p = \pm 1, \pm 2, \pm 4, \pm 8$), and q must divide 1 (so $q = \pm 1$), which gives the following choices for $x = \frac{p}{q}$

$$x = \pm 1, \pm 2, \pm 4, \pm 8$$

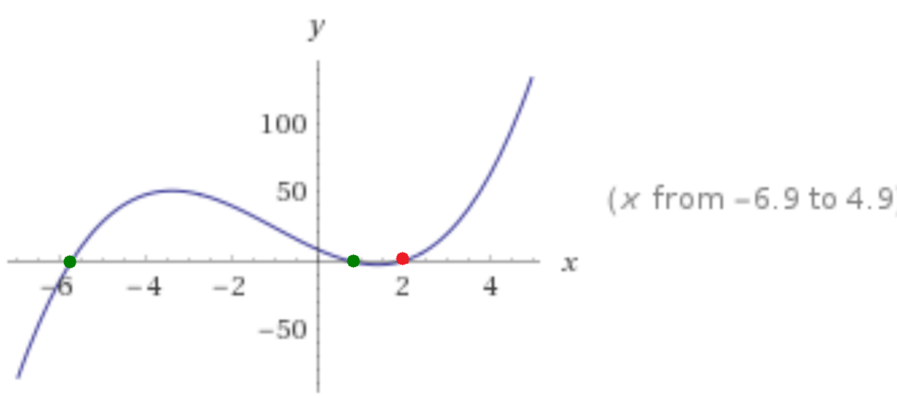
Let's plug in your choices one by one in $x^3 + 3x^2 - 14x + 8$ and see which one (if any) gives you zero.

$x = 1$	$1^3 + 3(1)^2 - 14(1) + 8 = -2 \neq 0$
$x = -1$	$-1 + 3 + 14 + 8 = 24 \neq 0$
$x = 2$	$8 + 3(4) - 28 + 8 = 0$ **BAZINGA!**

Hence $x = 2$ is a root!

Remarks:

(1) Once you have a root, you can then use long division to factor out the polynomial. Here for instance we get: $x^3+3x^2-14x+8 = (x-2)(x^2+5x-4)$. In case you're interested, here is a plot of our function (the rational root we found is in red and the other two roots are in green)



(2) If none of the guesses work, this means that the polynomial has no rational roots. It could still have irrational roots, though, as for instance $x^2 + x + 1 = 0$ for example.

(3) It's useful to have the polynomial $x^2 - 4$ in mind, which has roots $x = \pm 2$, in case you forget the order in which the rational roots theorem works.

5. Rational or Irrational (optional)

Video: $\sqrt{2+\sqrt{2}}$ is irrational

Another application is showing that a given number is irrational.

Example 2:

Show $x = \sqrt{2+\sqrt{2}}$ is irrational

Note: It's much easier in my opinion just to prove this using contradiction, but the method below is meant to illustrate the rational roots theorem.

First, find a polynomial whose root is x:

$$
\begin{aligned}
x =& \sqrt{2+\sqrt{2}} \\
\Rightarrow& x^2 = 2 + \sqrt{2} \\
\Rightarrow& x^2 - 2 = \sqrt{2} \\
\Rightarrow& \left(x^2 - 2\right)^2 = 2
\end{aligned}
$$

$$\Rightarrow x^4 - 4x^2 + 4 = 2$$
$$\Rightarrow x^4 - 4x^2 + 2 = 0$$

Now **if** $x^4 - 4x^2 + 2$ has a rational root of the form $x = \frac{p}{q}$, then p divides 2 (so $p = \pm 2$) and q divides 1 (so $q = \pm 1$), which gives the choices

$$x = \pm 1, \pm 2$$

$x = 1$	$1^4 - 4(1)^2 + 2 = -1 \neq 0$
$x = -1$	$-1 \neq 0$
$x = 2$	$16 - 16 + 2 = 2 \neq 0$
$x = -2$	$2 \neq 0$

So none of the choices work $\Rightarrow\Leftarrow$

Therefore $x^4 - 4x^2 + 2$ has no rational roots. But since $x = \sqrt{2 + \sqrt{2}}$ is for sure a root, it follows that $\sqrt{2 + \sqrt{2}}$ must irrational $\square$

6. Proof of the Rational Roots Theorem (optional)

Video: Rational Roots Theorem Proof

Note: You might be tempted to skip over proofs of theorems in this course, but in this upper-division math you *have* to look at them. I could very well ask you on the exam to reprove theorems.

Before we prove the rational roots theorem, we need a small lemma from number theory:

Lemma:

If a divides bc, and a and b have no factors in common, then a must divide c

Example: 5 divides (12)(25), but 5 and 12 have no factors in common, so 5 divides 25

Proof of the Rational Roots Theorem:

STEP 1: Suppose $x = \frac{p}{q}$ is a root of $a_n x^n + \cdots + a_1 x + a_0$ where p and q have no factors in common.

Then:

$$\begin{aligned} a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} \cdots + a_1\left(\frac{p}{q}\right) + a_0 =& 0 \\ a_n \left(\frac{p^n}{q^n}\right) + a_{n-1}\left(\frac{p^{n-1}}{q^{n-1}}\right) \cdots + a_1\left(\frac{p}{q}\right) + a_0 =& 0 \\ \frac{a^n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n}{q^n} =& 0 \end{aligned}$$

$$(\star) \qquad a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

Goal: Show p divides a_0 and q divides a_n.

STEP 2: On the one hand, solving for $a_n p^n$ in $(\star)$, we get:

$$\begin{aligned} a_n p^n =& -a_{n-1}p^{n-1}q - \cdots - a_0 q^n \\ a_n p^n =& -q\left(a_{n-1}p^{n-1} + \cdots + a_0 q^{n-1}\right) \end{aligned}$$

Since q divides the term on the right-hand-side, it follows that q divides $a_n p^n$.

But since q and p^n also have no factors in common, it then follows from our lemma that $\boxed{q \text{ divides } a_n}$ ✓

STEP 3: On the other hand, solving for $a_0 q^n$ in $(\star)$, we get:

$$a_n p^n + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$
$$a_0 q^n = -a_n p^n - \cdots - a_1 p q^{n-1}$$
$$a_0 q^n = -p \left(a_n p^{n-1} + \cdots + a_1 q^{n-1} \right)$$

Since p divides the right-hand-side, we get that p divides $a_0 q^n$, and since p and q^n have no factors in common, we deduce that $\boxed{p \text{ divides } a_0}$ $\square$