Math 131AH – Honors Real Analysis I

University of California, Los Angeles

Duc Vu

Winter 2021

This is math 131AH – Honors Real Analysis I taught by Professor Visan, and our TA is Thierry Laurens. We meet weekly on MWF from 10:00am – 10:50am for lectures. There are two textbooks used for the class, *Principles of Mathematical Analysis* by *Rudin* and *Metric Spaces* by *Copson*. You can find other lecture notes at my github site. Please let me know through my email if you spot any mathematical errors/typos.

Contents

List of Theorems

List of Definitions

§1 Lec 1: Jan 4, 2021

§1.1 Logical Statments & Basic Set Theory

Let A and B be two statements. We write

- A if A is true.
- not A if A is false.
- A and B if both A and B are true.
- A or B if A is true or B is true or both A and B are true (inclusive "or" – it is not either A or B).
- $\underbrace{A \implies B}$: if ($A$ and B) or (not A) – We read this "A implies B" or "If A then B".

  In this case, B is at least as true as A. In particular, a false statement can imply anything.

Example 1.1

Consider the following statement: If x is a natural number (i.e., $x \in \mathbb{N} = \{1, 2, 3, \ldots\}$, then $x \geq 1$. In this case, $A =$ "x is a natural number", $B =$ "$x \geq 1$". Taking $x = 3$, we get a $T \implies T$. Taking $x = \pi$ we get $F \implies T$. If $x = 0$, we get $F \implies F$.

Example 1.2

Consider the statement: $\underbrace{\text{If a number is less than 10}}_{A}$, $\underbrace{\text{then it's less than 20}}_{B}$.

Taking

$$\begin{aligned} \text{number } &= 5, \qquad T \implies T \\ &= 15, \qquad F \implies T \\ &= 25, \qquad F \implies F \end{aligned}$$

We write $\underbrace{A \iff B}$ if A and B are true together or false together. We read this as "A is equivalent to B" or "A if and only if B". Compare these notions to similar ones from set theory. Let X is an ambient space. Let A and B be subsets of X. Then

$$\begin{aligned} A^c &= \{x \in X; x \notin A\} \\ A \cap B &= \{x \in X; x \in A \text{ and } x \in B\} \\ A \cup B &= \{x \in X; x \in A \text{ or } x \in B \text{ or } x \in A \cap B\} \\ A \subseteq B &\text{ corresponds to } A \implies B \\ A = B &\qquad A \iff B \end{aligned}$$

Truth table:

A	B	not A	A and B	A or B	A $\implies$ B	A $\iff$ B
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Example 1.3

Using the truth table show that $A \implies B$ is logically equivalent to (not A) or B.

A	B	A $\implies$ B	not A	(not A) or B
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Homework 1.1. Using the truth table prove De Morgan's laws:

$$\text{not (A and B)} = \text{(not A) or (not B)}$$
$$\text{not (A or B)} = \text{(not A) and (not B)}$$

Compare this to

$$(A \cap B)^c = A^c \cup B^c$$
$$(A \cup B)^c = A^c \cap B^c$$

Exercise 1.1. Negate the following statement: If A then B.
Solution:

$$\begin{aligned} \text{not}(A \implies B) &= \text{not}\left(\text{(not A) or B}\right) \\ &= [\text{not(not A) and (not B)}] \\ &= A \text{ and (not B)} \end{aligned}$$

The negation is "A is true and B is false".

Example 1.4

Negate the following sentence: If I speak in front of the class, I am nervous.
I speak in front of the class and I am not nervous.

Quantifiers:

- $\forall$ reads "for all" or "for any"
- $\exists$ reads "there is" or "there exists"

The negation of $\forall A, B$ is true is $\exists A$ s.t. B is false.
The negation of $\exists A, B$ is true is $\forall A, B$ is false.

Example 1.5

Negate the following: Every student had coffee or is late for class.
$\forall$ student (had coffee) or (is late for class)
$\exists$ student s.t. not[(had coffee) or (is late for class)]
$\exists$ student s.t. not (had coffee) and not (is late for class)
<u>Ans</u>: There is a student that did not have coffee and is not late for class.

§2 Lec 2: Jan 6, 2021

§2.1 Mathematical Induction

The natural numbers – $\mathbb{N} = \{1, 2, 3, \ldots\}$; they satisfy the Peano axioms:

N1 $1 \in \mathbb{N}$

N2 If $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$

N3 1 is not the successor of any natural number.

N4 If $n, m \in \mathbb{N}$ such that $n + 1 = m + 1$ then $n = m$

N5 Let $S \subseteq \mathbb{N}$. Assume that S satisfies the following two conditions:

(i) $1 \in S$

(ii) If $n \in S$ then $n + 1 \in S$

Then $S = \mathbb{N}$.

Axiom N5 forms the basis for mathematical induction. Assume we want to prove that a property $P(n)$ holds for all $n \in \mathbb{N}$. Then it suffices to verify two steps:
Step 1 (base step): $P(1)$ holds.
Step 2 (inductive step): If $P(n)$ is true for some $n \geq 1$, then $P(n+1)$ is also true, i.e., $P(n) \implies P(n+1) \forall n \geq 1$.
Indeed, if we let

$$S = \{n \in \mathbb{N} : P(n) \text{ holds}\}$$

then Step 1 implies $1 \in S$ and Step 2 implies if $n \in S$ then $n + 1 \in S$. By Axiom N5 we deduce $S = \mathbb{N}$.

Example 2.1

Prove that

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad \forall n \in \mathbb{N}$$

Solution: We argue by mathematical induction. For $n \in \mathbb{N}$ let $P(n)$ denote the statement

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Step 1 (Base step): $P(1)$ is the statement

$$1^2 = \frac{1 \cdot 2 \cdot 3}{6}$$

which is true, so $P(1)$ holds.
Step 2 (Inductive step): Assume that $P(n)$ holds for some $n \in \mathbb{N}$. We want to know $P(n+1)$ holds. We know

$$1^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Let's add $(n+1)^2$ to both sides of $P(n)$

$$\begin{aligned} 1^2 + \ldots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= (n+1)\left[\frac{n(2n+1)}{6} + n + 1\right] \\ &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

So $P(n+1)$ holds.
Collecting the two steps, we conclude $P(n)$ holds $\forall n \in \mathbb{N}$. $\square$

Example 2.2

Prove that $2^n > n^2$ for all $n \geq 5$.
Solution: We argue by mathematical induction. For $n \geq 5$ let $P(n)$ denote the statement $2^n > n^2$.
Step 1 (base step): $P(5)$ is the statement

$$32 = 2^5 > 5^2 = 25$$

which is true. So $P(5)$ holds.
Step 2 (Inductive step): Assume $P(n)$ is true for some $n \geq 5$ and we want to prove $P(n+1)$. We know

$$2^n > n^2$$

Let us manipulate the above inequality to get $P(n+1)$

$$\begin{gathered} 2^n > n^2 \\ 2^{n+1} > 2n^2 = (n+1)^2 + n^2 - 2n - 1 \\ 2^{n+1} > (n+1)^2 + (n-1)^2 - 2 \end{gathered}$$

As $n \geq 5$ we have $(n-1)^2 - 2 \geq 4^2 - 2 = 14 \geq 0$. So

$$2^{n+1} > (n+1)^2$$

So $P(n+1)$ holds.
Collecting the two steps, we conclude that $P(n)$ holds $\forall n \geq 5$. □

Remark 2.3. Each of the two steps are essential when arguing by induction. Note that $P(1)$ is true. However, our proof of the second step fails if $n = 1 : (1-1)^2 - 2 = -2 < 0$.
Note that our proof of the second step is valid as soon as

$$(n-1)^2 - 2 \geq 0 \iff (n-1)^2 \geq 2 \iff n - 1 \geq 2 \iff n \geq 3$$

However, $P(3)$ fails.

Example 2.4

Prove by mathematical induction that the number $4^n + 15n - 1$ is divisible by 9 for all $n \geq 1$.

Solution: We'll argue by induction. For $n \geq 1$, let $P(n)$ denote the statement that "$4^n + 15n - 1$ is divisible by 9". We write this $9/(4^n + 15n - 1)$.

Step 1: $4^1 + 15 \cdot 1 - 1 = 18 = 9 \cdot 2$. This is divisible by 9, so $P(1)$ holds.

Step 2: Assume $P(n)$ is true for some $n \geq 1$. We want to show $P(n+1)$ holds.

$$\begin{aligned} 4^{n+1} + 15(n+1) - 1 &= 4(4^n + 15n - 1) - 60n + 4 + 15n + 14 \\ &= 4(4^n + 15n - 1) - 45n + 18 \\ &= 4(4^n + 15n - 1) - 9(5n - 2) \end{aligned}$$

By the inductive hypothesis, $9/(4^n + 15n - 1) \implies 9/4(4^n + 15n - 1)$. Also $9/9\underbrace{(5n-2)}_{\in \mathbb{N}}$.

So

$$9/\left[4(4^n + 15n - 1) - 9(5n - 2)\right]$$

So $P(n+1)$ holds. Collecting the two steps, we conclude $P(n)$ holds $\forall n \in \mathbb{N}$. $\square$

Example 2.5

Compute the following sum and then use mathematical induction to prove your answer: for $n \geq 1$
$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\frac{1}{5\cdot 7}+\ldots+\frac{1}{(2n-1)(2n+1)}$$

Solution: Note that $\frac{1}{(2n-1)(2n+1)} = \frac{1}{2}\left[\frac{1}{2n-1}-\frac{1}{2n+1}\right] \forall n \geq 1$. So

$$\begin{aligned}\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{(2n-1)(2n+1)} &= \frac{1}{2}\left\{\frac{1}{1}-\frac{1}{3}+\frac{1}{3}\ldots+\frac{1}{2n-1}-\frac{1}{2n+1}\right\}\\ &= \frac{1}{2}\frac{2n}{2n+1}=\frac{n}{2n+1}\end{aligned}$$

For $n \geq 1$, let $P(n)$ denote the statement

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\ldots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}$$

Step 1: $P(1)$ becomes $\frac{1}{1\cdot 3}=\frac{1}{3}$, which is true. So $P(1)$ holds.
Step 2: Assume $P(n)$ holds for some $n \geq 1$. We want to show $P(n+1)$. We know

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

Let's add $\frac{1}{(2n+1)(2n+3)}$ to both sides

$$\begin{aligned}\frac{1}{1\cdot 3}+\ldots+\frac{1}{(2n+1)(2n+3)} &= \frac{n}{2n+1}+\frac{1}{(2n+1)(2n+3)}\\ &= \frac{2n^2+3n+1}{(2n+1)(2n+3)}\\ &= \frac{(n+1)(2n+1)}{(2n+1)(2n+3)}\\ &= \frac{n+1}{2n+3}\end{aligned}$$

So $P(n+1)$ holds.
Collecting the two steps, we conclude $P(n)$ holds for $\forall n \geq 1$. $\square$

§3 Lec 3: Jan 8, 2021

§3.1 Equivalence Relation

The set of integers is $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$.

Definition 3.1 (Equivalence Relation) — An equivalence relation $\sim$ on a non-empty set A satisfies the following three properties:

- Reflexivity: $a \sim a, \forall a \in A$
- Symmetry: If $a, b \in A$ are such that $a \sim b$, then $b \sim a$
- Transitivity: If $a, b, c \in A$ are such that $a \sim b$ and $b \sim c$, then $a \sim c$.

Example 3.2

$=$ is an equivalence relation on $\mathbb{Z}$.

Example 3.3

Let $q \in \mathbb{N}, q > 1$. For $a, b \in \mathbb{Z}$ we write $a \sim b$ if $q/(a-b)$. This is an equivalence relation on $\mathbb{Z}$. Indeed, it suffices to check 3 properties:

- Reflexivity: If $a \in \mathbb{Z}$ then $a - a = 0$, which is divisible by q. So $q/(a-a) \iff a \sim a$.
- Symmetry: Let $a, b \in \mathbb{Z}$ such that $a \sim b \iff q/(a-b)$ which means there exists $k \in \mathbb{Z}$ s.t. $a - b = kq \implies b - a = \underbrace{-k}_{\in \mathbb{Z}} \cdot q$. So $q/(b-a) \iff b \sim a$.
- Transitivity: Let $a, b, c \in \mathbb{Z}$ such that $a \sim b$ and $b \sim c$, $a \sim b \iff q/(a-b) \implies \exists n \in \mathbb{Z}$ s.t. $a - b = q \cdot n$. And $b \sim c \iff q/(b-c) \implies \exists m \in \mathbb{Z}$ s.t. $b - c = q \cdot m$. So, we must have $a - c = q\underbrace{(n+m)}_{\in \mathbb{Z}}$. So $q/(a-c) \iff a \sim c$.

§3.2 Equivalence Class

Definition 3.4 (Equivalence Class) — Let $\sim$ denote an equivalence relation on a non-empty set A. The equivalence class of an element $a \in A$ is given by

$$C(a) = \{b \in A : a \sim b\}$$

Proposition 3.5 (Properties of Equivalence Classes)

Let $\sim$ denote an equivalence relation on a non-empty set A. Then

1. $a \in C(a) \quad \forall a \in A$.
2. If $a, b \in A$ are such that $a \sim b$, then $C(a) = C(b)$.
3. If $a, b \in A$ are such that $a \not\sim b$, then $C(a) \cap C(b) = \emptyset$.
4. $A = \bigcup_{a \in A} C(a)$

Proof. 1. By reflexivity, $a \sim a \quad \forall a \in A \implies a \in C(a) \quad \forall a \in A$.

2. Assume $a, b \in A$ with $a \sim b$. Let's show $C(a) \subseteq C(b)$. Let $c \in C(a)$ be arbitrary. Then $a \sim c$ (by definition). As $a \sim b$ (by hypothesis), which implies $b \sim a$ (by symmetry). By transitivity, we obtain $b \sim c \implies c \in C(b)$. This proves that $C(a) \subseteq C(b)$.

   A similar argument shows that $C(b) \subseteq C(a)$. Putting the two together, we obtain $C(a) = C(b)$.

3. We argue by contradiction. Assume that $a, b \in A$ are such that $a \not\sim b$, but $C(a) \cap C(b) \neq \emptyset$. Let $c \in C(a) \cap C(b)$.

$$c \in C(a) \implies a \sim c$$
$$c \in C(b) \implies b \sim c \implies c \sim b \quad \text{(by symmetry)}$$

   By transitivity, $a \sim b$. This contradicts the hypothesis $a \not\sim b$. This proves that if $a \not\sim$ then $C(a) \cap C(b) = \emptyset$.

4. Clearly, $C(a) \subseteq A \quad \forall a \in A$, we get

$$\bigcup_{a \in A} C(a) \subseteq A$$

   Conversely, $A = \bigcup_{a \in A} \{a\} \subseteq \bigcup_{a \in A} C(a)$. Putting everything together, we obtain $A = \bigcup_{a \in A} C(a)$. □

Example 3.6

Take $q = 2$ in our previous example: for $a, b \in \mathbb{Z}$ we write $a \sim b$ if $2/(a-b)$. The equivalence classes are

$$\begin{aligned} C(0) &= \{a \in \mathbb{Z} : 2/(a-0)\} = \{2n : n \in \mathbb{Z}\} \\ C(1) &= \{a \in \mathbb{Z} : 2/(a-1)\} = \{2n+1 : n \in \mathbb{Z}\} \\ \mathbb{Z} &= C(0) \cup C(1) \end{aligned}$$

Let $F = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b \neq 0\}$. If $(a, b), (c, d) \in F$ we write $(a, b) \sim (c, d)$ if $ad = bc$.

Example 3.7

$(1,2) \sim (2,4) \sim (3,6) \sim (-4,-8)$.

Lemma 3.8

$\sim$ is an equivalence relation on F.

Proof. We have to check 3 properties:

- Reflexivity: Fix $(a,b) \in F$. As $ab = ba$ we have $(a,b) \sim (a,b)$
- Symmetry: Let $(a,b),(c,d) \in F$ such that

$$(a,b) \sim (c,d) \iff ad = bc \iff cb = da \iff (c,d) \sim (a,b)$$

- Transitivity: Let $(a,b),(c,d),(e,f) \in F$ such that $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$.

$$(a,b) \sim (c,d) \iff ad = bc \implies adf = bcf$$
$$(c,d) \sim (e,f) \iff cf = de \implies cfb = deb$$

$$\implies adf = deb \implies \underbrace{d}_{\neq 0}(af - be) = 0, \text{ so } af = be \iff (a,b) \sim (e,f).$$

□

For $(a,b) \in F$, we denote its equivalence class by $\frac{a}{b}$. We define addition and multiplication of equivalence classes as follows:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}; \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

We have to check that these operations are well-defined. Specifically, if $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$ then

$$(ad+bc, bd) \sim (a'd' + b'c', b'd') \tag{1}$$
$$(ac, bd) \sim (a'c', b'd') \tag{2}$$

Let's check (1). We want to show

$$(ad+bc)b'd' = bd(a'd' + b'c')$$

We know

$$(a,b) \sim (a',b') \iff ab' = ba' \quad | \cdot dd'$$
$$(c,d) \sim (c',d') \iff cd' = dc' \quad | \cdot bb'$$

Adding the two (after multiplying the two terms) together, we have

$$ab'dd' + cd'bb' = ba'dd' + dc'bb'$$
$$(ad+bc)b'd' = bd(a'd' + b'c')$$

This proves addition is well defined.

Hw: Check (2)

The set of rational numbers is

$$\mathbb{Q} = \left\{ \frac{a}{b} : (a,b) \in F \right\}$$

§4 Lec 4: Jan 11, 2021

§4.1 Field & Ordered Field

Definition 4.1 (Field) — A field is a set F with at least two elements with two operators: addition (denoted $+$) and multiplication (denoted $\cdot$) that satisfy the following

A1) Closure: if $a, b \in F$ then $a + b \in F$

A2) Commutativity: if $a, b \in F$ then $a + b = b + a$

A3) Associativity: if $a, b, c \in F$ then $(a + b) + c = a + (b + c)$

A4) Identity: $\exists 0 \in F$ s.t. $a + 0 = 0 + a = a \; \forall a \in F$

A5) Inverse: $\forall a \in F \exists (-a) \in F$ s.t. $a + (-a) = -a + a = 0$

M1) Closure: if $a, b \in F$ then $a \cdot b \in F$

M2) Commutativity: if $a, b \in F$ then $a \cdot b = b \cdot a$

M3) Associativity: if $a, b, c \in F$ then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

M4) Identity: $\exists 1 \in F$ s.t. $a \cdot 1 = 1 \cdot a = a \; \forall a \in F$

M5) Inverse: $\forall a \in F \setminus \{0\} \, \exists a^{-1} \in F$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$

D) Distributivity: if $a, b, c \in F$ then $(a + b) \cdot c = a \cdot c + b \cdot c$

Example 4.2

$(\mathbb{N}, +, \cdot)$ is not a field. A4 fails.

Example 4.3

$(\mathbb{Z}, +, \cdot)$ is not a field. M5 fails.

Example 4.4

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

Hw

Recall:

$$\mathbb{Q} = \left\{ \frac{a}{b} : (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \right\}$$

where $\frac{a}{b}$ denotes the equivalence class of $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ with respect to the equivalence relation

$$(a, b) \sim (c, d) \iff a \cdot d = b \cdot c$$

Note $\frac{1}{2} = \frac{2}{4}$ because $(1,2) \sim (2,4)$. We defined

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Additive identity $\frac{0}{1}$ equivalence class $(0,1)$.
Multiplicative identity $\frac{1}{1}$ equivalence class of $(1,1)$.
Additive inverse: $\frac{a}{b} \in \mathbb{Q}$ has inverse $-\frac{a}{b}$
Multiplicative inverse: $\frac{a}{b} \in \mathbb{Q} \setminus \left\{\frac{0}{1}\right\}$ has inverse $\frac{b}{a}$.

Proposition 4.5

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

1. The additive and multiplicative identities are unique.
2. The additive and multiplicative inverses are unique.
3. If $a, b, c \in F$ s.t. $a + b = a + c$ then $b = c$. In particular, if $a + b = a$ then $b = 0$.

3'. If $a, b, c \in F$ s.t. $a \neq 0$ and $a \cdot b = a \cdot c$ then $b = c$. In particular, $a \neq 0$ and $a \cdot b = a$ then $b = 1$.

4. $a \cdot 0 = 0 \cdot a = 0 \ \forall a \in F$.
5. If $a, b \in F$ then $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
6. If $a, b \in F$ then $(-a) \cdot (-b) = a \cdot b$
7. If $a \cdot b = 0$ then $a = 0$ or $b = 0$.

Proof. 1. We'll show the additive identity is unique. Assume

$$\exists 0, 0' \in F \text{ s.t. } \forall a \in F, \begin{cases} a + 0 = 0 + a = a & (i) \\ a + 0' = 0' + a = a & (ii) \end{cases}$$

Take $a = 0'$ in (i) and $a = 0$ in (ii) to get

$$\begin{cases} 0' + 0 = 0' \\ 0' + 0 = 0 \end{cases} \implies 0 = 0'$$

2. We'll show that the additive inverse is unique. Let $a \in F$. Assume $\exists (-a), a' \in F$ s.t.

$$\begin{cases} -a + a = a + (-a) = 0 \\ a' + a = a + a' = 0 \end{cases}$$

We have

$$a' + a = 0 \qquad | + (-a)$$

$$(a' + a) + (-a) = 0 + (-a) \overset{A3, A4}{\implies} a' + (a + (-a)) = -a$$
$$\overset{A5}{\implies} a' + 0 = -a \overset{A4}{\implies} a' = -a$$

3. Assume $a + b = a + c \quad | + (-a)$ to the left

$$
\begin{aligned}
-a + (a+b) &= -a + (a+c) \\
\xrightarrow{A3} (-a+a) + b &= (-a+a) + c \\
\xrightarrow{A5} 0 + b &= 0 + c \xrightarrow{A4} b = c
\end{aligned}
$$

   So if $a + b = a = a + 0$, then $b = 0$.

4.

$$
\begin{aligned}
a \cdot 0 &\overset{A4}{=} a \cdot (0+0) \overset{D}{=} a \cdot 0 + a \cdot 0 \xrightarrow{(3)} a \cdot 0 = 0 \\
0 \cdot a &\overset{A4}{=} (0+0) \cdot a = 0 \cdot a + 0 \cdot a \xrightarrow{(3)} 0 \cdot a = 0
\end{aligned}
$$

5. $(-a) \cdot b + a \cdot b \overset{D}{=} (-a + a) \cdot \overset{A5}{=} 0 \cdot b \overset{(4)}{=} 0 \implies (-a) \cdot b = -(a \cdot b)$. Similarly, $a \cdot (-b) = -(a \cdot b)$.

6. $(-a) \cdot (-b) + [-(a \cdot b)] \overset{(5)}{=} (-a) \cdot (-b) + (-a) \cdot b \overset{D}{=} (-a)(-b+b) \overset{A5}{=} (-a) \cdot 0 \overset{(4)}{=} 0$. So $(-a) \cdot (-b) = a \cdot b$.

7. Assume $a \cdot b = 0$. Assume $a \neq 0$. Want to show $b = 0$. As $a \neq 0$ then $\exists a^{-1} \in F$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

$$
a \cdot b = 0 \quad | \cdot a^{-1} \text{ to the left}
$$

$$
a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \xrightarrow{M3,(4)} (a^{-1} \cdot a) \cdot b = 0 \xrightarrow{M5} 1 \cdot b = 0 \xrightarrow{M4} b = 0 \qquad \square
$$

Definition 4.6 (Order Relation) — An order relation $<$ on a non-empty set A satisfies the following properties:

- Trichotomy: if $a, b \in A$ then one and only one of the following statement holds: $a < b$ or $a = b$ or $b < a$.
- Transitivity: if $a, b, c \in A$ such that $a < b$ and $b < c$, then $a < c$.

Example 4.7

For $a, b \in \mathbb{Z}$ we write $a < b$ if $b - a \in \mathbb{N}$. This is an order relation.

Notation: We write

$$
\begin{aligned}
&a > b \text{ if } b < a \\
&a \leq b \text{ if } [a < b \text{ or } a = b] \\
&a \geq b \text{ if } b \leq a
\end{aligned}
$$

Definition 4.8 (Ordered Field) — Let $(F, +, \cdot)$ be a field. We say $(F, +, \cdot)$ is an <u>ordered field</u> if it is equipped with an order relation $<$ that satisfies the following

01) if $a, b, c \in F$ such that $a < b$ then $a + c < b + c$.

02) if $a, b, c \in F$ such that $a < b$ and $0 < c$ then $a \cdot c < b \cdot c$.

Note:

To check something is an ordered field, we have to check that it satisfies the properties of order relation and ordered field.

§5 Lec 5: Jan 13, 2021

§5.1 Ordered Field (Cont'd)

Proposition 5.1

Let $(F, +, \cdot, <)$ be an ordered field. Then,

1. $a > 0 \iff -a < 0$.
2. If $a, b, c \in F$ are such that $a < b$ and $c < 0$, then $ac > bc$.
3. If $a \in F \setminus \{0\}$ then $a^2 = a \cdot a > 0$. In particular, $1 > 0$.
4. If $a, b \in F$ are such that $0 < a < b$ then $0 < b^{-1} < a^{-1}$.

Proof. 1. Let's prove " $\implies$ ". Assume $a > 0$.

$$\overset{01}{\implies} a + (-a) > 0 + (-a) \overset{A5,A4}{\implies} 0 > -a$$

Let's prove " $\impliedby$ ". Assume $-a < 0$

$$\overset{01}{\implies} -a + a < 0 + a \overset{A5,A4}{\implies} 0 < a$$

2. Assume $a < b$ and $c < 0$

$$\begin{cases} a < b \\ c < 0 \overset{01}{\implies} -c > 0 \end{cases} \begin{aligned} &\overset{02}{\implies} a \cdot (-c) < b \cdot (-c) \\ &\overset{01}{\implies} -ac + (ac + bc) < -bc + (ac + bc) \\ &\overset{A3,A2}{\implies} (-ac + ac) + bc < -bc + (bc + ac) \\ &\overset{A5,A3}{\implies} 0 + bc < (-bc + bc) + ac \\ &\overset{A4,A5}{\implies} bc < 0 + ac \\ &\overset{A4}{\implies} bc < ac \end{aligned}$$

3. By trichotomy, exactly one of the following hold:

$$a > 0 \overset{02}{\implies} a \cdot a > 0 \cdot a \implies a^2 > 0$$

or

$$a < 0 \overset{2)}{\implies} a \cdot a > 0 \cdot a \implies a^2 > 0$$

4. First we show that if $a > 0$ then $a^{-1} > 0$. Let's argue by contradiction. Assume $\exists a \in F$ s.t. $a > 0$ but $a^{-1} < 0$. Then

$$\begin{cases} a > 0 \\ a^{-1} < 0 \end{cases} \overset{(2)}{\implies} a \cdot a^{-1} < 0 \overset{M5}{\implies} 1 < 0$$

This contradicts (3). So if $a > 0$ then $a^{-1} > 0$.

Say

$$
\begin{aligned}
0 < a < b \quad | \cdot a^{-1} \cdot b^{-1} \\
&\overset{02}{\Longrightarrow} 0 \cdot (a^{-1} \cdot b^{-1}) < a \cdot (a^{-1} \cdot b^{-1}) < b \cdot (a^{-1} \cdot b^{-1}) \\
&\overset{M3,M2}{\Longrightarrow} 0 < (a \cdot a^{-1}) \cdot b^{-1} < b \cdot (b^{-1} \cdot a^{-1}) \\
&\overset{M5,M3}{\Longrightarrow} 0 < 1 \cdot b^{-1} < (b \cdot b^{-1}) \cdot a^{-1} \\
&\overset{M4,M5}{\Longrightarrow} 0 < b^{-1} < 1 \cdot a^{-1} \\
&\overset{M4}{\Longrightarrow} 0 < b^{-1} < a^{-1}
\end{aligned}
$$

□

Theorem 5.2

Let $(F, +, \cdot)$ be a field. The following are equivalent

1) F is an ordered field.

2) There exists $P \subseteq F$ that satisfies the following properties

   01') For every $a \in F$ one and only one of the following statements holds: $a \in P$ or $a = 0$ or $-a \in P$.

   02') If $a, b \in P$ then $a + b \in P$ and $a \cdot b \in P$.

Proof. Let's show 1) $\implies$ 2). Define $P = \{a \in F : a > 0\}$. Let's check (01'). Fix $a \in F$. By trichotomy for the order relation on F we get that exactly one of the following statements is true:

- $a > 0 \implies a \in P$.
- $a = 0$.
- $a < 0 \implies -a > 0 \implies -a \in P$.

Let's check (02'). Fix $a, b \in P$.

$$
\begin{cases} a \in P \implies a > 0 \\ b \in P \implies b > 0 \end{cases} \overset{01}{\Longrightarrow} a + b > 0 + b \overset{A4}{=} b > 0 \implies a + b \in P
$$

And

$$
\begin{cases} a \in P \implies a > 0 \quad | \cdot b \\ b \in P \implies b > 0 \end{cases} \overset{02}{\Longrightarrow} a \cdot b > 0 \cdot b = 0 \implies a \cdot b \in P
$$

Let's check that 2) $\implies$ 1).

For $a, b \in F$ we write $a < b$ if $b - a \in P$. Let's check this is an order relation.

- <u>Trichotomy</u>: Fix $a, b \in F$. By 01') exactly one of the following hold:

$$\begin{aligned} b-a \in P &\implies a<b \\ b-a=0 &\implies a=b \\ -(b-a) \in P &\implies a-b \in P \implies b<a \end{aligned}$$

- <u>Transitivity</u> Assume $a, b, c \in F$ s.t. $a<b$ and $b<c$

$$\begin{cases} a<b \implies b-a \in P \\ b<c \implies c-b \in P \end{cases} \overset{02'}{\implies} (b-a)+(c-b) \in P \implies c-a \in P \implies a<c$$

Now let's check that with this order relation, F is an ordered field. We have to check 01 and 02.

01) Fix $a, b, c \in F$ s.t. $a<b \implies b-a \in P \implies b-a \in P \implies (b+c)-(a+c) \in P \implies a+c<b+c$.

02) Fix $a, b, c \in F$ s.t. $a<b$ and $0<c$

$$\begin{cases} a<b \implies b-a \in P \\ 0<c \implies c-0=c \in P \end{cases} \overset{02'}{\implies} (b-a) \cdot c \in P \overset{D}{\implies} b \cdot c-a \cdot c \in P \implies a \cdot c<b \cdot c$$

$\square$

We extend the order relation $<$ from $\mathbb{Z}$ to the field $(\mathbb{Q},+,\cdot)$ by writing $\frac{a}{b}>0$ if $a \cdot b>0$. Let's see this is well defined. Specifically, we need to show that if $\frac{a}{b}=\frac{c}{d}$, i.e., $(a, b) \sim (c, d)$ and $a \cdot b>0$ then $c \cdot d>0$.

$$\begin{aligned} (a, b) \sim (c, d) &\implies a \cdot d=b \cdot c \quad \mid \cdot (ad) \\ &\implies 0<(ad)^2=(ab) \cdot (cd) \text{ where } a \cdot d \neq 0 \end{aligned}$$

So

$$\begin{cases} 0<(ab) \cdot (cd) \\ 0<ab \end{cases} \implies cd>0 \implies \frac{c}{d}>0$$

Let $P=\left\{\frac{a}{b} \in \mathbb{Q} : \frac{a}{b}>0\right\}$. By the theorem, to prove that $\mathbb{Q}$ is an ordered field, it suffices to show that P satisfies (01') and (02').

Hw: check (01') and (02')

§6 Lec 6: Jan 15, 2021

§6.1 Least Upper Bound & Greatest Lower Bound

Definition 6.1 (Boundedness – Maximum and Minimum) — Let $(F, +, \cdot, <)$ be an ordered field. Let $\emptyset \neq A \subseteq F$. We say that A is bounded above if $\exists M \in F$ s.t. $a \leq M \forall a \in A$. Then M is called an upper bound for A. If moreover, $M \in A$ then we say that M is the maximum of A.
We say that A is bounded below if $\exists m \in F$ s.t. $m \leq a \forall a \in A$. Then m is called a lower bound for A. If moreover, $m \in A$ then we say that m is the minimum of A.
We say that A is bounded if A is bounded both above and below.

Example 6.2
$A = \left\{1 + \frac{(-1)^n}{n} : n \in \mathbb{N}\right\}$.

- 3 is an upper bound for A.
- $\frac{3}{2}$ is the maximum of A.
- 0 is a lower bound for A ; 0 is the minimum of A.

Example 6.3
$A = \left\{x \in \mathbb{Q} : 0 < x^4 \leq 16\right\}$ bounded.

- 2 is the maximum of A.
- -2 is the minimum of A.

Example 6.4

$A = \left\{x \in \mathbb{Q} : x^2 < 2\right\}$ bounded.

- 2 is an upper bound for A.
- -2 is lower bound for A.
- A does not have a maximum. Indeed, let $x \in A$. We'll construct $y \in A$ s.t. $y > x$. Define $y = x + \frac{2-x^2}{2+x}$.

$$x \in A \implies x \in \mathbb{Q} \implies 2 - x^2, 2 + x \in \mathbb{Q}$$
$$x \in A \implies 2 + x > 0 \implies \frac{1}{2+x} \in \mathbb{Q}$$

$\implies \frac{2-x^2}{2+x} \in \mathbb{Q} \implies y \in \mathbb{Q}$ (i). Also note

$$\begin{cases} 2 - x^2 > 0 (\text{as } x \in A) \\ 2 + x > 0 \implies \frac{1}{2+x} > 0 \end{cases} \implies \frac{2-x^2}{2+x} > 0$$

So $y = x + \frac{2-x^2}{2+x} > x$ (ii). Let's compute $y^2 = \left(\frac{2x+x^2+2-x^2}{2+x}\right)^2 = \frac{2(x^2+4x+4)+2x^2-4}{x^2+4x+4} = 2 + \underbrace{\frac{2(x^2-2)}{(x+2)^2}}_{<0}$. So $y^2 < 2$. (iii)

So collecting (i) – (iii) we get $y \in A$ and $y > x$.

Homework 6.1. Show that the maximum and minimum of a set are unique, if they exist.

Definition 6.5 (Least Upper Bound) — Let $(F, +, \cdot, <)$ be an ordered field. Let $\emptyset \neq A \subseteq F$ and assume A is bounded above. We say that L is the least upper bound of A if it satisfies:

1. L is an upper bound of A.
2. If M is an upper bound of A then $L \leq M$.

We write $L = \sup A$ and we say L is the supremum of A.

Lemma 6.6

The least upper bound of a set is unique, if it exists.

Proof. Say that a set $\emptyset \neq A \subseteq F$, A bounded above, admits two least upper bounds L, M.
L is a least upper bound $\overset{(1)}{\implies}$ L is an upper bound for A.
M is a least upper bound $\overset{(2)}{\implies}$ $M \leq L$.

M is a least upper bound for $A \overset{(1)}{\Longrightarrow} M$ is an upper bound for $A \Longrightarrow L$ is a least upper bound for $A \overset{(2)}{\Longrightarrow} L \leq m$. So $L = M$. □

Definition 6.7 (Greatest Lower Bound) — Let $(F, +, \cdot, <)$ be an ordered field. Let $\emptyset \neq A \subseteq F$ and assume A is bounded below. We say that l is the greatest lower bound of Aif it satisfies

1. l is a lower bound of A.
2. If m is a lower bound of A then $m \leq l$.

We write $l = \inf A$ and we say l is the infimum of A.

Homework 6.2. Show that the greatest lower bound of a set is unique if it exists.

Definition 6.8 (Bound Property) — Let $(F, +, \cdot, <)$ be an ordered field. Let $\emptyset \neq S \subseteq F$. We say that S has the the least upper bound property if it satisfies the following: For any non-empty subset A of S is bounded above, there exists a least upper bound of A and $\sup A \in S$.
We say that S has the greatest lower bound property if it satisfies the following: $\forall \emptyset \neq A \subseteq S$ with A bounded below, $\exists \inf A \in S$.

Example 6.9
$(\mathbb{Q}, +, \cdot, <)$ is an ordered field.
$\emptyset \neq \mathbb{N} \subseteq \mathbb{Q}$, $\mathbb{N}$ has the least upper bound property. Indeed if $\emptyset \neq A \subseteq \mathbb{N}$, A bounded above, then the largest elements in A is the least upper bound of A and $\sup A \in \mathbb{N}$. $\mathbb{N}$ also has the greatest lower bound property.

Example 6.10
$(\mathbb{Q}, +, \cdot, <)$ is an ordered field.
$\emptyset \neq \mathbb{Q} \subseteq \mathbb{Q}$, $\mathbb{Q}$ does not have the least upper bound property.
Indeed, $\emptyset \neq A = \left\{x \in \mathbb{Q} : x \geq 0 \text{ and } x^2 < 2\right\} \subseteq \mathbb{Q}$. A is bounded above by 2. However, $\sup A = \sqrt{2} \notin \mathbb{Q}$.

Proposition 6.11
Let $(F, +, \cdot, <)$ be an ordered field. Then F has the least upper bound property if and only if it has the greatest lower bound property.

Proof. ($\Longrightarrow$) Assume F has the least upper bound property. Let $\emptyset \neq A \subseteq F$ bounded below. WTS $\exists \inf A \in F$. A is bounded below $\Longrightarrow \exists m \in F$ s.t. $m \leq a \forall a \in A$. Let

$B = \{b \in F : b \text{ is a lower bound for } A\}$. Note $B \neq \emptyset$ (as $m \in B$), $B \subseteq F$, B is bounded above (every element in A is an upper bound for B) and F has the least upper bound property $\implies \sup B \in F$.

Claim 6.1. $\sup B = \inf A$.

(Cont'd – Lec 7) $\square$

§7 Lec 7: Jan 20, 2021

§7.1 Lec 6 (Cont'd)

Proof. (Cont'd of proposition 6.11)

Claim 7.1. $\sup B = \inf A$.

Method 1:

- $\sup B$ is a lower bound for A. Indeed, let $a \in A$. We know that $a \geq b \quad \forall b \in B$. $\sup B$ is the least upper bound for $B \implies a \geq \sup B$. As $a \in A$ was arbitrary, we conclude that $\sup B \leq a \quad \forall a \in A$ and so $\sup B$ is a lower bound for A.

- If l is a lower bound for A then $l \leq \sup B$. Well, l is a lower bound for $A \implies l \in B$ and $\sup B$ is an upper bound for B. So $l \leq \sup B$.

Collecting the two bullet points above, we find that $\inf A = \sup B$.
Method 2: Let $\emptyset \neq A \subseteq F$ s.t. A is bounded below. Let $B = \{-a : a \in A\}$. Note $B \subseteq F$ by A5. $B \neq \emptyset$ because $A \neq \emptyset$. B is bounded above: indeed if m is a lower bound for A then $-m$ is an upper bound for B.

$$m \leq a \quad \forall a \in A \implies -m \geq -a \quad \forall a \in A$$

F has the least upper bound property. Altogether, it implies that $\sup B \in F$. In Hw3, you show $-\sup B = \inf A \in F$ (by A5). □

Homework 7.1. Prove the " $\Longleftarrow$ " direction.

Theorem 7.1 (Existence of $\mathbb{R}$)

There exists an ordered field with the least upper bound property. We denote it $\mathbb{R}$ and we call it the set of real numbers. $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield. Moreover, we have the following uniqueness property: If $(F, +, \cdot, <)$ is an ordered field with the least upper bound property, then F is order isomorphic with $\mathbb{R}$, that is, there exists a bijection $\phi : \mathbb{R} \to F$ such that

i) $\phi(x \underbrace{+}_{\mathbb{R}} y) = \phi(x) \underbrace{+}_{F} \phi(y)$

ii) $\phi(x \underbrace{\cdot}_{\mathbb{R}} y) = \phi(x) \underbrace{\cdot}_{F} \phi(y)$

iii) If $x \underbrace{<}_{\mathbb{R}} y$ then $\phi(x) \underbrace{<}_{F} \phi(y)$

Theorem 7.2 (Archimedean Property)

$\mathbb{R}$ has the Archimedean property, that is, $\forall x \in \mathbb{R} \quad \exists n \in \mathbb{N}$ s.t. $x < n$.

Proof. We argue by contradiction. Assume

$$\exists x_0 \in \mathbb{R} \text{ s.t. } x_0 \geq n \quad \forall n \in \mathbb{N}$$

Then $\emptyset \neq \mathbb{N} \subseteq \mathbb{R}$. $\mathbb{N}$ is bounded above by x_0. $\mathbb{R}$ has the least upper bound property $\implies \exists L = \sup \mathbb{N} \in \mathbb{R}$.

$$\begin{cases} L = \sup \mathbb{N} \\ L - 1 < L \end{cases} \implies L - 1 \text{ is not an upper bound for } \mathbb{N}$$

$\implies \exists n_0 \in \mathbb{N}$ s.t. $n_0 > L - 1$. So $\sup \mathbb{N} = L < n_0 + 1 \in \mathbb{N}$, which is a contradiction. □

Remark 7.3. $\mathbb{Q}$ has the Archimedean property.

If $r \in \mathbb{Q}$ is s.t. then choose $n = 1$. For $r \in \mathbb{Q}$ is s.t. $r > 0$, then write $r = \frac{p}{q}$ with $p, q \in \mathbb{N}$. Choose $n = p + 1$ since $\frac{p}{q} < p + 1$.

Corollary 7.4

If $a, b \in \mathbb{R}$ such that $a > 0, b > 0$ then there exists $n \in \mathbb{N}$ s.t. $n \cdot a > b$.

Proof. Apply the Archimedean Property to $x = \frac{b}{a}$. □

Corollary 7.5

If $\epsilon > 0$ there exists $n \in \mathbb{N}$ s.t. $\frac{1}{n} < \epsilon$.

Proof. Apply the Archimedean property to $x = \frac{1}{\epsilon}$. □

Lemma 7.6

For any $a \in \mathbb{R}$ there exists $N \in \mathbb{Z}$ s.t. $N \leq a \leq N + 1$.

Proof. Case 1: $a = 0$. Take $N = 0$.
Case 2: $a > 0$. Consider $A = \{n \in \mathbb{Z} : n \leq a\} \subseteq \mathbb{R}$, $A \neq \emptyset (0 \in A)$. A is bounded above by a. $\mathbb{R}$ has the least upper bound property. So $\exists L = \sup A \in \mathbb{R}$.

$$L - 1 < L = \sup A \implies L - 1 \text{ is not an upper bound for } A$$

$\implies \exists N \in A$ s.t. $L - 1 < N \implies L < N + 1$ but $L = \sup A$, so $N + 1 \notin A$. So

$$\begin{cases} N \in A \implies N \leq a \\ N + 1 \notin A \implies N + 1 > a \end{cases} \implies N \leq a < N + 1$$

Case 3: $a < 0 \implies -a > 0$. By case 2, $\exists n \in \mathbb{Z}$ s.t. $n \leq -a < n + 1$. So $-n - 1 < a \leq -n$. If $a = -n$, let $N = -n$ and so $N \leq a < N + 1$. If $a < -n$ let $N = -n - 1$ and so $N \leq a < N + 1$. □

Definition 7.7 (Dense Set) — We say that a subset A of $\mathbb{R}$ is dense in $\mathbb{R}$ if for every $x, y \in \mathbb{R}$ such that $x < y$ there exists $a \in A$ such that $x < a < y$.

Lemma 7.8

$\mathbb{Q}$ is dense in $\mathbb{R}$.

Proof. Let $x, y \in \mathbb{R}$ such that $x < y$. Since $y - x > 0$ by corollary 7.5, $\exists n \in \mathbb{N}$ s.t. $\frac{1}{n} < y - x \implies \frac{1}{n} + x < y$.
Consider $nx \in \mathbb{R}$. By the lemma 7.6, $\exists m \in \mathbb{Z}$ s.t.

$$m \le nx < m + 1 \implies \frac{m}{n} \le x < \frac{m+1}{n}$$

Then

$$x < \frac{m+1}{n} = \frac{m}{n} + \frac{1}{n} \le x + \frac{1}{n} < y$$

w where $\frac{m+1}{n} \in \mathbb{Q}$. $\square$

Lemma 7.9

$\mathbb{R} \setminus \mathbb{Q}$ is dense in $\mathbb{R}$.

§8 Dis 1: Jan 7, 2021

§8.1 Logical Statements

Example 8.1

Negate the following statements:

a) If there is a job worth doing, then it is worth doing well.

not(If a then B) = A and (not B)

"There is a job worth doing, and it is not worth doing well."

b) Every cloud has a silver lining.

not ($\forall$ A,B is true) = $\exists$ A s.t. B is false

"There is a cloud without a silver lining."

Example 8.2

Let P, Q, R be statements about elements $x \in X$. Negate the following:

a) For every $x \in X$, $P(x)$ is true or $(Q(x) \implies R(x))$.

not $(\forall x \in X, (P(x) \text{ or } (Q(x) \implies R(x))))$ which is equivalent to $\exists x \in X$ s.t. (not $P(x)$) and $(Q(x))$ and (not $R(x)$).

There exists $x \in X$ s.t. $P(x)$ is false, $Q(x)$ is true, and $R(x)$ is false.

b) There is $x \in X$ such that for every $y \in X$ not equal to $x, P(y), Q(y)$, and $R(y)$ are true. Use similar approach, we have

For every $x \in X$, there is $y \in X$ not equal to x such that $P(y), Q(y)$ or $R(y)$ is false.

Example 8.3

Suppose X, Y, Z are statements and we know X $\implies$ Y and X $\implies$ Z. Can we conclude the following: (X and (not Y)) $\implies$ Z.

X	Y	Z	X $\implies$ Y	X $\implies$ Z	X and not Y	the above
T	T	T	T	T	F	T
~~T~~	~~T~~	~~F~~	~~T~~	~~F~~		
~~T~~	~~F~~	~~T~~	~~F~~			
~~T~~	~~F~~	~~F~~	~~F~~			
F	T	T	T	T	F	T
F	T	F	T	T	F	T
F	F	T	T	T	F	T
F	F	F	T	T	F	T

So this statement is true.

§8.2 Induction

Example 8.4

Prove that $\forall n \in \mathbb{N}, n^3 + 2n$ is divisible by 3.

- Base case: $n = 1 - n^3 + 2n = 3$ which is divisible by 3.
- Inductive step: Assume $n^3 + 2n$ is divisible by 3. Want to show $(n+1)^3 + 2(n+1)$ is divisible by 3.

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 3n + 1 + 2n + 2 \\ &= \underbrace{(n^3 + 2n)}_{=3k \text{ for some } k} + 3n^2 + 3n + 3 \\ &= 3\underbrace{\left(k + n^2 + n + 1\right)}_{\text{an integer}}\end{aligned}$$

which is divisible by 3. By induction, statement is true $\forall n \in \mathbb{N}$. $\square$

§9 Dis 2: Jan 14, 2021

§9.1 Induction (Cont'd)

Example 9.1

Find and prove a formula for

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}+\sqrt{k+1}}$$

$$\begin{aligned}\frac{1}{\sqrt{k}+\sqrt{k+1}} &= \frac{\sqrt{k+1}-\sqrt{k}}{\left(\sqrt{k+1}+\sqrt{k}\right)\left(\sqrt{k+1}-\sqrt{k}\right)}\\ &= \sqrt{k+1}-\sqrt{k}\\ \sum_{k=1}^{n}\frac{1}{\sqrt{k}+\sqrt{k+1}} &= \sqrt{n+1}-\sqrt{1} \qquad (*)\end{aligned}$$

Claim 9.1. $\sum_{k=1}^{n} \frac{1}{\sqrt{k}+\sqrt{k+1}} = \sqrt{n+1}-\sqrt{1} \quad \forall n \geq 1 \ (P(n))$

Proof. We'll use induction

- Base case: $n = 1$

  $$\sum_{k=1}^{n} \frac{1}{\sqrt{k}+\sqrt{k+1}} = \frac{1}{\sqrt{1}+\sqrt{2}} \overset{(*)}{=} \sqrt{2}-\sqrt{1}$$

  So $P(1)$ is true.

- Inductive step: Assume $P(n)$ true. Want to show $P(n+1)$ is true

  $$\begin{aligned}\sum_{k=1}^{n+1} \frac{1}{\sqrt{k}+\sqrt{k+1}} &= \sum_{k=1}^{n} \frac{1}{\sqrt{k}+\sqrt{k+1}} + \underbrace{\frac{1}{\sqrt{n+1}+\sqrt{n+2}}}_{=\sqrt{n+2}-\sqrt{n+1}}\\ &= \sqrt{n+2}-\sqrt{n+1}+\sqrt{n+1}-\sqrt{1}\\ &= \sqrt{n+2}-\sqrt{1}\end{aligned}$$

  This is $P(n+1)$

Together, we conclude $P(n)$ is true $\forall n \geq 1$ by induction. □

Example 9.2

Define the sequence

$$a_1 = 3, a_2 = 5, \text{ and } a_n = 3a_{n-1} - 2a_{n-2} \text{ for } n \geq 3$$

Prove that $a_n = 2^n + 1$.

Proof. Let $P(n)$ be the statement $a_n = 2^n + 1$. We'll use induction

- Inductive step: Assume $P(n)$ and $P(n-1)$ are true. Want $P(n+1)$ true:

$$\begin{aligned} a_{n+1} &= 3a_n - 2a_{n-1} = 3(2^n + 1) - 2(2^{n-1} + 1) \\ &= 3 \cdot 2^n + 3 - 2^n - 2 = 2^{n+1} + 1 \end{aligned}$$

  This is $P(n+1)$.

- Base case:

$$\begin{aligned} n = 1 : a_1 = 3, 2^n + 1 = 3, &\quad P(1) \text{ true} \\ n = 2 : a_2 = 5, 2^n + 1 = 5, &\quad P(2) \text{ true} \end{aligned}$$

Together, we conclude $P(n)$ is true $\forall n \geq 1$ by induction. □

Remark 9.3. We can formulate this as regular induction for $Q(n) = (P(n) \text{ and } P(n-1))$.

§9.2 Fields

Example 9.4

Let $F = \{0, 1, \alpha\}$ with the operations

$+$	0	1	α
0	0	1	α
1	1	α	0
α	α	0	1

$\cdot$	0	1	α
0	0	0	0
1	0	1	α
α	0	α	1

a) Show that $(F, +, \cdot)$ is a field.

Addition:

- $a, b \in F \implies a + b \in F$: True, since entries of the $+$ table are elements of F.
- $a, b \in F \implies a + b = b + a$: True, since entries above diagonal are same as below the diagonal.
- $a, b, c \in F \implies (a + b) + c = a + (b + c)$: Check $3^3 = 27$ cases individually. For this example, they're all true.
- $a + 0 = a = 0 + a \forall a \in F$: True, since column and row for 0 are unaltered.
- $\forall a \in F \exists (-a) \in F$ s.t. $a + (-a) = 0 = (-a) + a$

Multiplication:

- $a, b \in F \implies a \cdot b \in F$: True, since entries of $\cdot$ table are elements of F.
- $a, b \in F \implies a \cdot b = b \cdot a$: True, since table is symmetric across the diagonal.
- $a, b, c \in F \implies (a \cdot b) \cdot c = a \cdot (b \cdot c)$: Check 27 cases. All true.
- $a \cdot 1 = a = 1 \cdot a \forall a \in F$: True, since column and row for 1 are unaltered.
- $\forall a \in F \setminus \{0\} \, \exists a^{-1}$ s.t. $a \cdot a^{-1} = 1 = a^{-1} \cdot a$: True, since every nonzero column and row contain a 1.

Distributivity: $a, b, c \in F \implies (a + b) \cdot c = a \cdot c + b \cdot c$. We'll check all cases. Let $a, b, c \in F$

1. Case $c = 0$. From table
$$(a + b) \cdot 0 = 0, \quad a \cdot 0 + b \cdot 0 = 0 + 0 = 0$$
2. Case $c = 1$
$$(a + b) \cdot 1 = a + b, \quad a \cdot 1 + b \cdot 1 = a + b$$

Example 9.5 (Cont'd (from above)) 3. Case $c = \alpha$ choices for $a, b \in F$:

a	b	$(a+b)\cdot\alpha$	$a\cdot\alpha + b\cdot\alpha$	Equal?
0	0	$0\cdot\alpha = 0$	$0+0=0$	✓
0	1	$1\cdot\alpha = \alpha$	$0+\alpha=\alpha$	✓
0	α	$\alpha\cdot\alpha = 1$	$0+1=1$	✓
1	0	$1\cdot\alpha = \alpha$	$\alpha+0=\alpha$	✓
1	1	$\alpha\cdot\alpha = 1$	$\alpha+\alpha=1$	✓
1	α	$0\cdot\alpha = 0$	$\alpha+1=0$	✓
α	0	$\alpha\cdot\alpha = 1$	1+0=1	✓
α	1	$0\cdot\alpha = 0$	$1+\alpha=0$	✓
α	α	$1\cdot\alpha = \alpha$	$1+1=\alpha$	✓

b) Show that there is not order relation on F that makes F an ordered field. Idea: $1+1+\ldots+1$ is eventually on the "other side" of 1.

Proof. Suppose $(F, +, \cdot, <)$ is an ordered field. By trichotomy, either $0 < 1, 0 = 1, 0 > 1$.

- Case $0 = 1$: Impossible, since they are different elements of F.
- Case $0 < 1$: Apply $(a < b \implies a + c < b + c)$ with $c = 1$:

$$0 < 1 \overset{+1}{\implies} 1 < \alpha \overset{+1}{\implies} \alpha < 0$$

  By transitivity, $1 < \alpha$ and $\alpha < 0 \implies 1 < 0$. This contradicts $0 < 1$.

- Case $0 > 1$: Replace " $>$ " by " $<$ " above, get $1 > 0$ at the end. A contradiction.

All three cases are impossible, so no " $<$ " exists. □

§10 Dis 3: Jan 21, 2021

§10.1 Upper and Lower Bounds

Example 10.1

Suppose $A, B \subseteq \mathbb{R}$ are non-empty s.t. $x \leq y \quad \forall x \in A, \forall y \in B$.

a) Show that $\sup A \leq y \forall y \in B$.

Suppose not. $\exists b \in B$ s.t. $\sup A > b$.

Claim 10.1. If $A \subseteq \mathbb{R}$ nonempty and $b < \sup A$, then $\exists a \in A$ s.t. $b < a$.

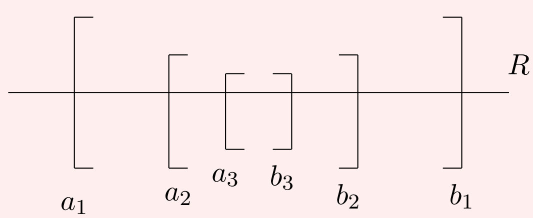
Suppose not. Then $\forall a \in A, b \geq a \implies b$ is an upper bound for $a \implies b \geq \sup A$, contradicting $b < \sup A$. □

By the claim, $\exists a \in A$ s.t. $b < a \leq \sup A$. But $a \leq b$ by given since $a \in A$, $b \in B$, which is a contradiction.

b) Show $\sup A \leq \inf B$.

Part a) $\implies \sup A$ is a lower bound for $B \implies \sup A \leq \inf B$ since $B \neq \emptyset$ and $\mathbb{R}$ has greatest lower bound property. □

Example 10.2 a) Suppose $I_n = [a_n, b_n] \neq \emptyset$ for $n \in \mathbb{N}$ s.t. $a_n \leq a_{n+1}$ and $b_{n+1} \leq b_n \forall n \in \mathbb{N}$. Prove $\exists x \in \mathbb{R}$ s.t. $x \in I_n \forall n \in \mathbb{N}$.



Let $x := \sup \{a_n : n \in \mathbb{N}\}$. We will show $x \in I_n \forall n \in \mathbb{N}$. Note that $a_n \leq x \forall n$ since x is an upper bound for the $a_n's$.

Claim 10.2. $x \leq b_n \forall n \in \mathbb{N}$.

Suppose not. Then $\exists n_1 \in \mathbb{N}$ s.t. $b_{n_1} < x$. Since x is the least upper bound, $\exists n_2 \in \mathbb{N}$ s.t. $b_{n_1} < a_{n_2} \leq x$ by claim 10.1.

Then $I_{n_1} \cap I_{n_2} \neq \emptyset$. But $n_1 \geq n_2$ or $n_1 \leq n_2$, so $I_{n_1} \subseteq I_{n_2}$ or $I_{n_2} \subseteq I_{n_1}$ and hence $\emptyset = I_{n_1} \cap I_{n_2} = I_{\max\{n_1, n_2\}}$ – a contradiction.

Altogether, $a_n \leq x \leq b_n \quad \forall n \in \mathbb{N}$, so $x \in I_n \quad \forall n \in \mathbb{N}$. □

b) Show that the conclusion is false if the I_n are open intervals.

Let $I_n = \left(0, \frac{1}{n}\right)$ for $n \in \mathbb{N}$. Suppose $\exists x \in I_n \forall n$. Then $x \in I_1$, so $x > 0$. By the Archimedean Property, $\exists N \in \mathbb{N}$ s.t. $\frac{1}{N} < x$. Then $x \notin I_n \forall n \geq N$. □

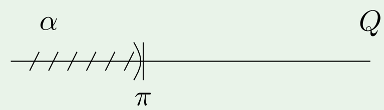
§10.2 Dedekind Cuts

Definition 10.3 (Dedekind Cuts) — $\alpha \subseteq \mathbb{Q}$ is a <u>cut</u> if

(I) $\alpha \neq \emptyset, \mathbb{Q}$

(II) $p \in \alpha, q \in Q, q < p \implies q \in \alpha$.

(III) $p \in \alpha \implies \exists r \in \alpha$ s.t. $p < r$.



Example 10.4

Let $R \coloneqq \{\alpha \subseteq \mathbb{Q} : \alpha \text{ is a cut}\}$ and for $\alpha, \beta \in R$ define

$$\alpha + \beta = \{r + s : r \in \alpha \text{ and } s \in \beta\}$$

Show that this satisfies A1-A5.

A1) $\alpha, \beta \in R \implies \alpha + \beta \in R$. Note $\alpha + \beta \subseteq \mathbb{Q}$ since $r + s \in \mathbb{Q}$ for $r, s \in \mathbb{Q}$.

(I) $\alpha + \beta \neq \emptyset$ since $\alpha, \beta \neq \emptyset$. Since $\alpha, \beta \neq \mathbb{Q}, \exists a \in \mathbb{Q} \setminus \alpha$ and $b \in \mathbb{Q} \setminus \beta$. For any $r \in \alpha, s \in \beta \implies r < a, s < b$ by (II) $\implies r + s < a + b \implies a + b \notin \alpha + \beta$ by (II). $\implies \alpha + \beta \neq \mathbb{Q}$.

(II) Let $r + s \in \alpha + \beta$ and $q \in \mathbb{Q}$ s.t. $q < r + S \implies q - s < r \implies q - s \in \alpha$ by (II) $\implies q = (q - s) + s \in \alpha + \beta$.

(III) Let $r + s \in \alpha + \beta \implies r \in \alpha \implies \exists t \in \alpha$ s.t. $r < t \implies t + s \in \alpha + \beta$ and $r + s < t + s$.

A2) $\alpha, \beta \in R \implies \alpha + \beta = \beta + \alpha$.

$\alpha + \beta = \{r + s : r \in \alpha \text{ and } s \in \beta\}$. Since $+$ is commutative on $\mathbb{Q}$, $r + s = s + r$. So

$$\alpha + \beta = \{s + r : s \in \beta \text{ and } r \in \alpha\} = \beta + \alpha$$

A3) $\alpha, \beta, \gamma \in R \implies (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

$$\begin{aligned}
(\alpha + \beta) + \gamma &= \{p + t : p \in \alpha + \beta \text{ and } t \in \gamma\} \\
&= \{(r + s) + t : r \in \alpha \text{ and } s \in \beta \text{ and } t \in \gamma\} \\
&= \{r + (s + t) : r \in \alpha \text{ and } s \in \beta \text{ and } t \in \gamma\} \\
&= \{r + q : r \in \alpha \text{ and } q \in \beta + \gamma\} = \alpha + (\beta + \gamma)
\end{aligned}$$