Math 131AH – Honors Real Analysis I

University of California, Los Angeles

Duc Vu

Fall 2020

This is math 131AH – Honors Real Analysis I taught by Professor Greene, and our TA is Haiyu Huang. We meet weekly on MWF from 1:00pm – 2:00pm 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 blog site ductuanvu.wordpress.com/notes/. Please let me know through my email if you spot any mathematical errors/typos.

Contents

1	Lec 1: Oct 2, 2020 1.1 Introduction	2
2	Lec 2: Oct 5, 2020 2.1 Mathematical Induction and More on Real Numbers	3
3	Lec 3: Oct 7, 20203.1 Cauchy Sequence	5 5 7
4	Lec 4: Oct 9, 2020 4.1 Bolzano – Weierstrass Theorem	7 7
5	Lec 5: Oct 12, 2020 5.1 Equivalence Relation	10
6	Dis 1: Oct 1, 2020 6.1 Induction	12 12
7	Dis 2: Oct 8, 2020 7.1 Number System	
8	Dis 3: Oct 13, 2020 8.1 Equivalence Relation (Cont'd)	

$\S1$ Lec 1: Oct 2, 2020

Overview:

 \bullet Hmwrk: 30 %

 \bullet Midterm 1: 20 %

• Midterm 2: 20 %

 \bullet Final: 30 %

§1.1 Introduction

 $\underline{\text{functions}} \to 1, 2, 3, 4, 5, 6, 7 \dots$

functions defined on \mathbb{Q} with value in \mathbb{Q}

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

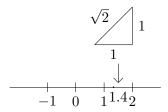
 $a_i \in \mathbb{Q}$ $f(x) \in \mathbb{Q}$ if $x \in \mathbb{Q}$. Continuity makes sense.

$$x_0, x$$
 xclose to $x_0 \implies f(x) \operatorname{close} f(x_0)$

polynomials are continuous.

Somthing wrong: $\sqrt{2}$ is missing. What are these numbers that are not $\in \mathbb{Q}$? Choice:

- 1. Assume everything works and isolate what you need about "real numbers" (most of Rudin chap 1).
- 2. Construct the real numbers from rational numbers.



Classical argument:

$$x^2 \neq 2$$
 if $x = \frac{p}{q} \in \mathbb{Q}$

Proof. Suppose $\left(\frac{p}{q}\right)^2 = 2$

<u>Note</u>: wolog(without loss of generality)

 $\operatorname{can take} \frac{p}{q} > 0 \quad p > 0 \quad q > 0$

$$\left(\frac{p}{q}\right)^2 = 2$$

$$\frac{p^2}{q^2} = 2$$

$$p^2 = 2q^2$$

Now also wolog, can assume p and q are not <u>both</u> even numbers. But $p^2 = 2q^2$ means p has to be even $(p^2 \text{ odd if } p \text{ is odd})$.

$$p = 2n$$
$$p^2 = 2q^2$$
$$4n^2 = 2q^2$$

So $q^2=2n^2,\,q$ is even. But it contradicts the initial assumption, p and q not both even $\ \square$

Related to: Why functions $\mathbb Q$ to $\mathbb Q$ not ideal for analysis? – INFINITE DECIMAL

$\S 2$ Lec 2: Oct 5, 2020

§2.1 Mathematical Induction and More on Real Numbers

 $P(n) \to 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$, where n is positive numbers. Math induction: Proof by two steps:

- 1. Check P(1) is true \checkmark
- 2. Assume P(n) is true for all $n \leq N$. Check that

$$P(N+1)$$
 is true

Assume $1 + \ldots + N = \frac{N(N+1)}{2}$. Check

$$1 + \ldots + N + (N+1) = \frac{(N+1)(N+1+1)}{2}$$

Induction on k:

$$1^k + 2^k + \ldots + n^k$$

2nd illustration:

$$1 + r + r^2 + \ldots + r^n = \frac{1 - r^{n+1}}{1 - r} \quad r \neq 1$$

 $r=1 \implies 1+r=\frac{1-r^2}{1-r}$

$$1 + r + r^{2} + \dots + r^{n} + r^{n+1} = \frac{1 - r^{n+1}}{1 - r} + r^{n+1}$$

$$= \frac{1 - r^{n+1} + r^{n+1} - r^{n+2}}{1 - r}$$

$$= \frac{1 - r^{n+2}}{1 - r}$$

$$(1-r)(1+r+\ldots+r^n) = 1-r^{n+1}$$
 Inspection
$$1+r+r^2+\ldots+r^n = \frac{1-r^{n+1}}{1-r}, \quad r \neq 1$$

|r| < 1 get inifite sum $\frac{1}{1-r}$

Example 2.1

Prime factors, prime = positive integers (> 1) with no factors except itself and 1, p = ab, a > 1, b > 1

Thin out as go along

Theorem 2.2

Every positive integer > 1 is a product of primes.

Proof. Induction: P(n) n = 2, 3, ...

$$P(2) = 2\sqrt{}$$

Assume $P(n) \dots n \le N$ (N > 2). Every integer greater than 1 but smaller than or equal to N as a product of primes. We try to prove: N + 1 is a product of primes.

- 1. N + 1 is prime: Done N + 1 = N + 1
- 2. N+1 is not a prime

$$N+1=a\cdot b$$
 $a>1$ $b>1$

Induction assumption (a < N + 1 since b > 1), a is a product of primes $a > 1 \implies b < N + 1$, b also a product of primes. So, N + 1 = ab is a product of primes.

N+1=ab is a product of prime.

Why does induction work? If P(n) not always true, P(n) look at smallest n where P(n) is false.

n=1 not there P(1) is supposed true (checked already). N_0 smallest one where $P(N_0)$ false $N_0 > 1$. Induction step says that P(n) is true for all $n \le \underbrace{N_0 - 1}_{>0} \implies P(N_0)$ true (×

).

Let's go back to real numbers.

Last time: talked about $\sqrt{2}$ is irrational but $\sqrt{2}$ exists, so we need to enlarge our number system: $\mathbb Q$ rational numbers.

$$\frac{p}{q} > \frac{r}{s} \qquad ps > rq \qquad (p, q, r, s > 0)$$

$$-1 \qquad -\frac{1}{2} \qquad \qquad \frac{1}{2} \qquad 1$$

$$0$$

x, y rational x, y > 0, x + y > 0, xy > 0

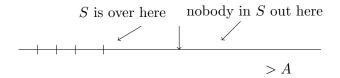
 $x^2 = 2$ no answer in \mathbb{Q} . Enlarge number system, $\mathbb{Q} \subset \mathbb{R}$. What should \mathbb{R} be like?

1. \mathbb{R} ought of have arithmetic like \mathbb{Q}

$$x+y$$
 xy $\frac{x}{y}$ 0 1

- 2. $\mathbb{Q} \subset \mathbb{R}$, arithmetic in \mathbb{R} restricted to \mathbb{Q} , $\frac{1}{2} + \frac{1}{3}$ in \mathbb{Q} ought to be $\frac{5}{6}$ in \mathbb{R} .
- 3. Order should positive in $\mathbb{Q} \implies$ in \mathbb{R} . \mathbb{R} should have an order of its own too, x y positive then x + y pos and xy pos.
- 4. want to fill in the holes in Q. Want to have Least Upper Bound Property

 $S \subset \mathbb{R}$: An upper bound for S is a number A with property $A \geq x$ if $x \in S$



 $1, 2, 3, 4, \ldots$ have no upper bound.

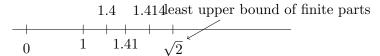
S is <u>bounded above</u> means that some upper bound A exists.

§2.2 Least Upper Bound Property

If S is bounded above $(S \neq \emptyset)$ then it has a "least upper bound" where a number A_0 is called the least upper bound of S if A_0 is an upper bound for S & if A is an upper bound for S then $A_0 \leq A$.



Motivation: Think about $\sqrt{2}$



Denote: l.u.b(or supremum)(sequence) = $\sqrt{2}$

Means can define an infinite decimals: least upper bound of successive truncations

$$0.99999... \rightarrow 1.0$$

$\S3$ Lec 3: Oct 7, 2020

§3.1 Cauchy Sequence

$$\{x_n\}$$
 x_1, x_2, x_3, \dots values $x_j \in \mathbb{Q}$ $x_j \in \mathbb{R}$
 S $x_1, x_i \dots x_j \in S$

Definition 3.1 — A sequence with values in a set S is a function from positive integers $\{1, 2, 3...\}$ into S.

Definition 3.2 — A <u>Cauchy sequence</u> is (\mathbb{Q} valued or \mathbb{R} valued) $\{x_i\}$ is sequence s.t. for every $\epsilon > 0$ there is a positive integer N_{ϵ} s.t.

$$|x_i - x_j| < \epsilon$$
 if $i, j > N_{\epsilon}$

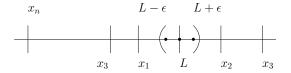


 ϵ rational or real (same idea).

Lemma 3.3

If $\{x_j\}$ has a finite limit then it's a Cauchy sequence.

 $\{x_i\}$ has L as a limit $\lim x_j = L$ means for every $\epsilon > 0$ then there is an N_{ϵ} such that $j \geq N_{\epsilon}$, $|x_j - L| < \epsilon$



Everybody in $(L - \epsilon, L + \epsilon)$ except a finite number

Proof. Given $\epsilon > 0$, want to find N so that $i, j \geq N \implies |x_i - x_j| < \epsilon |x_i - L| \text{ small}, |x_j - L| \text{ small and } \lim x_j = L.$

$$|x_{i} - x_{j}| \leq |x_{i} - L| + |x_{j} - L|$$

$$|x_{i} - x_{j}| = |L - x_{i}| + |L - x_{j}|$$

$$\xrightarrow{x_{i}} L x_{j}$$

 $i,j \geq N_{\frac{\epsilon}{2}}$:

$$|x_i - x_j| \le \underbrace{|x_i - L|}_{< \frac{\epsilon}{2}} + \underbrace{|x_j - L|}_{< \frac{\epsilon}{2}}$$

Because $\lim x_n = L$, there is an $N_{\frac{\epsilon}{2}}$ s.t. $|L - x_n| < \frac{\epsilon}{2}$ if $n \ge N_{\frac{\epsilon}{2}}$ Get $|x_i - x_j| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$ if $i, j \ge N$. Cauchy sequence: there exists number N s.t.

$$|x_i - x_j| < \epsilon$$
 if $i, j \ge N$

Cauchy sequence \implies the existence of limit? Yes, for $\mathbb R$ valued sequences but NO for $\mathbb Q$ valued things.

 $\{x_n\}$ can be Cauchy seq without there being a rational number L such that $\lim x_j = L$

But allow real L then $\exists L$ s.t. $\lim x_j = L$ if $\{x_j\}$ is Cauchy sequence(no rational limit – since $\sqrt{2}$ is irrational). Because \mathbb{Q} has holes in it! (intuitive idea).

Example 3.4

 $1, 1.4, 1.41, 1.414, 1.4142\dots$ (decimal approx of $\sqrt{2}$) – Cauchy sequence. No – since $\sqrt{2}$ is irrational.

$\S 3.2$ Cauchy Completeness of \mathbb{R}

If $\{x_i\}, x_i \in \mathbb{R}$ is Cauchy sequence, then $\exists L \in \mathbb{R}$ s.t. $\lim x_i = L$.

" \mathbb{Q} is not Cauchy complete" but \mathbb{R} is. Why does this work?

Need: Least upper bound property. Assume L.U.B Property proof.

 ${\it Proof.} \ ({\rm Cauchy\ completeness\ from\ L.U.B\ Property})$

Hypothesis: $\{x_i\}$ Cauchy seq

1. Prove that $\{x_i\}$ bounded $\iff \exists M > 0 \text{ s.t. } |x_i| \leq M \text{ all } i.$

Clear if take $\epsilon = 1$ in def. of Cauchy seq $\exists N \text{ s.t. } |x_i - x_j| < 1 \text{ if } i, j \geq N \implies$

 $|x_N - x_j| < 1 \text{ if } j \ge N \implies |x_j| \le |x_N| + 1 \quad j \ge N$

So, $M = \max(|x_N| + 1, |x_1|, \dots, |x_{N-1}| \text{ then } |x_j| \le M \text{ all } j !$

Next stage is to show that a bounded sequence always has a subsequence (tricky!) with a limit. Then if a Cauchy seq has a subseq with limit L, then L is limit of whole seq. (Bolzano – Weierstrass Theorem)

 $\S4$ Lec 4: Oct 9, 2020

§4.1 Bolzano – Weierstrass Theorem

- implied by Least Upper Bound Property

Theorem 4.1

If $\{x_n\}$ sequence $(x_1, x_2, x_3...)$ that is bounded (means: $\exists M > 0 \ni |x_n| \le M \forall n$, then $\exists L$ and a subsequence $\{x_{n_i}\}$ s.t. $\lim x_{n_i} = L$.

Slogan: Every bounded sequence has a convergent subsequence.

Example 4.2

$$1, 2, 1, 2, 1, 2, \dots$$

The subsequence of the above sequence has either 1 or 2 as the limit.

$$1, 1, 2, 1, 2, 3, 1, 2, 3, 4, 1, 2, 3, 4, 5, \dots$$

Unbounded sequence – subsequence (limit 1, limit 2, limit 3...)

No claim of uniqueness of anything.

Proof - Summer 2008 Analysis Lec 4

Proof. So either [-M,0] or [0,M] (maybe both) contains x_n for infinitely many n values. If each contained x_n for only finitely many n values X.

$$-M \qquad 0 \qquad M$$

$$\vdash \qquad \vdash \qquad \vdash$$
Every x_n is in $[-M, M] - \{x_n\}$ is bounded
$$[-M, M] = [-M, 0] \cup [0, M]$$

$$I_1 = [-M, 0] \quad \text{or} \quad [0, M]$$

where chosen intervalhas x_n for infinitely many n values. Do this again!

$$I_1 = [a_1, b_1]$$
 $|b_1 - a_1| = M$

$$I_1 \leftarrow \text{length}$$

left half of I_1 , right half of I. Let $I_2 =$ one of halves that contains x_n for infinitely many n values.

$$I_2 = [a_2, b_2]$$
 $a_2 < b_2, b_2 - a_2 = \frac{M}{2}$

Continue

$$I_3 = [a_3, b_3]$$
 $a_3 < b_3, b_3 - a_3 = \frac{M}{4}$

:

$$I_k = [a_k, b_k]$$
 $b_k - a_k = \frac{M}{2^{k-1}}$

Each I_k contains x_n for infinitely many n values.

Claim $\bigcap_{k=1}^{\infty} I_k \neq \emptyset$

Reason: $\sup a_k \in \bigcap_{k=1}^{\infty} I_k$ where $\sup = \sup$ of left hand endpoint(=greatest lower bound of bs). l.u.b of a's $\leq b_k$, b_k bigger than or \geq all a's.

$$\alpha = \text{lub a's}$$
 $\alpha \ge a_k \quad \forall k$
 $\alpha \le b_k \quad \forall k$
 $\alpha \in [a_k, b_k]$

Goal: $\alpha \in \bigcap_{k=1}^{\infty}$. Find a subsequence of $\{x_n\}$ converges to α .

Choose $x_k = x_n$ that belongs to I_k . Can also arrange successively:

$$n_1 < n_2 < n_3 < n_4$$

 $x_{n_1} \in I_1$ $x_{n_2} \in I_2$ can make $n_2 > n_1$ because infinitely possible $x'_n s$ in I_2 n value. Continue to get subsequence, $\{x_{n_k}\}$ subsequence. Claim:

$$\lim_{k \to \infty} x_{n_k} = \infty$$

Reason:

$$\operatorname{dis}(x_{n_k}, \alpha) \leq \operatorname{length} \text{ of } I_k \quad \alpha \in I_k, \quad x_{n_k} \in I_k$$

which is equivalent to

$$|x_{n_k} - \alpha| \le \frac{M}{2^{k-1}}$$
 given $\epsilon > 0$

When k is large,

$$\frac{M}{2^{k-1}} < \epsilon$$

So $|x_{n_k} - \alpha| < \epsilon$

This argument (or a variant) shows something else:

If $\{x_n\}$ sequence in [0,1] then there's an $\alpha \in [0,1]$ with it never happening that

$$x_n = \alpha$$

"The real numbers in [0, 1] are uncountable." (come from the least upper bound property)

$$\begin{array}{c|c} x_1 & \checkmark \\ \hline & + & + & I_1 \end{array}$$

 I_1 one of $[0, \frac{1}{3}]$ $[\frac{1}{3}, \frac{2}{3}]$ $[\frac{2}{3}, 1]$ such that $x_1 \notin I_1$,

$$[0,\frac{1}{3}]\cap [\frac{1}{3},\frac{2}{3}]\cap [\frac{2}{3},1]=\emptyset$$

 $x_1 \notin I_2$ $I_2 \subset I_1$, & $x_1 \notin I_1$. Continue. Get

$$I_1 \supset I_2 \supset I_3 \supset \dots$$

length $I_k = \frac{1}{3^k}$ and I_k is such that $x_1, x_2, x_3 \dots x_k$ are none of the ?n? in I_k . Same as before

$$\exists \alpha \in \bigcap_{\infty}^{k=1} I_k$$

 $\alpha = \sup$ of set of left hand endpoints of I_k . Claim α cannot be an x_N value. Clear: $x_N \notin I_N$ but $\alpha \in I_n$ $\alpha \in \bigcap_{n=1}^{\infty} I_n$. But contrast:

There is a list of rational numbers in [0, 1]

$\S 5$ Lec 5: Oct 12, 2020

§5.1 Equivalence Relation

(p.10, Copson – Metric Space) R set, relation of A and B $(A \times B)$ $(a,b) \in R$ aRb Functions: one b given a – exact one. $(A \to B)$

Example 5.1

$$A = B = Q$$

 aRb or $(a, b) \in R$ if $a > b$
(mother,child)

- (Sara, Sebastian) $\in R$
- (Sara, Alita) $\in R$

Equivalence is a special kind of relation: (on a set A; B = A = B) Properties:

- 1. aRa A = Q
- $2. \ aRb \implies bRa$
- 3. aRb & bRc then aRc

Example: \mathbb{Z} $a \sim b$ means a - b is divisible by 5

$$1 \sim 6 \quad 0 \sim 5 \dots$$

$$a \sim a$$
 $a - b$ div $\implies b - a$ div. by 5.

If a-b div. by 5, and b-c div by 5, then is a-c div. by 5 true? Sure, a-b=5k, $b-c=5l \implies a-c=5(k+l)$ "Equivalence classes": set $[a]=\{$ all b such that $aRb\}$ In the example above, $[a] = \{ \text{ all b such that } a - b \text{ div. by 5} \}$

$$[2] = \{2, 7, -3, 12, -8, \ldots\}$$

 \mathbb{Z}_5 : integer mod 5.

- 1. [a] [p] either equal or have nothing in common.
- 2. $a \in [a]$ so is in some equivalence class.

A equivalence relation \sim on $A \leftrightarrow$ a partition of A into subsets which are pairwise disjoint. Q Cauchy seq. of rational numbers

$$\{x_n\} \sim \{y_n\}$$

means $\lim_{n\to\infty} |x_n - y_n| = 0$. Equivalence relation:

- 1. $\{x_n\} \sim \{x_n\} (\lim (x_n x_n) = 0)$
- 2. $\{x_n\} \sim \{y_n\} \implies \{y_n\} \sim \{x_n\}$
- 3. $\{x_n\} \sim \{y_n\} \& \{y_n\} \sim \{z_n\} \implies \{x_n\} \sim \{z_n\}$

Idea: Define a real number to be a (Cauchy seq. of rationals) equivalence class. Homework: want to check that arithmetic extends to "real numbers"

$$[\{x_n\}] + [\{z_n\}] = [\{x_n + z_n\}]$$

Check that

- 1. $\{x_n + z_n\}$ is a Cauchy seq.
- 2. Only depends on equivalence classes.

Want

$$\{x_n\} \sim \{y_n\} \qquad \{z_n\} \sim \{w_n\}$$

then $\{x_n + z_n\} \sim \{y_n + w_n\}$. So,

$$[\{x_n + z_n\}] = [\{y_n + w_n\}]$$

Example 5.2

 \mathbb{Z}_5

$$[2] + [11] = [2 + 11] = [13]$$

So, $[2+1] \sim [13]([11] = [1])$. Arithmetic (addition) in \mathbb{Z}_5 thus makes sense. How about multiplication?

$$\frac{[1]}{[a]} \leftarrow \text{exists } [a] \neq 0$$

$$\frac{[1]}{[2]} = [3]$$
 $[2][3] = [6] = [1]$

Thus, \mathbb{Z}_5 is a field.

 $\frac{p}{q} \sim \frac{r}{s}$, $q, s \neq 0$ means ps = rq (when talking about fractions – associate it with equivalence relation). Q = set of equivalences classes. $(\frac{p}{q})$: equivalence classes).

Last time, we proved that Cauchy seq. of real numbers have limits (lub property). Also, no sequence $\{x_n\}$ such that it hits all real numbers in [0,1] – this is important. Contrast with $Q \cap [0,1]$, then there is a sequence that hits them all. Refer to the last figure in Lec 4 or math.ucla.edu/~greene – Summer 2008.

§6 Dis 1: Oct 1, 2020

Notation:

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$$

$$\mathbb{Q} = \left\{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\right\}$$

$$\mathbb{R} = \text{real numbers}$$

$$\mathbb{C} = \{a + bi, a, b \in \mathbb{R}\}$$

Set theory:

- $A \subset B$ (or $A \subseteq B$) means $x \in A \implies x \in B$
- $x \in A \cap B$ means $x \in A$ and $x \in B$
- $x \in A \cup B$ means $x \in A$ or $x \in B$
- $x \in A \setminus B \iff x \in A \text{ and } x \notin B$
- $A = B \iff A \subset B \text{ and } B \subset A$

§6.1 Induction

Given a sequence of mathematical statement P(n) indexed by \mathbb{N} . If P(1) is true and $P(k) \implies P(k+1)$ is true $\forall k \in \mathbb{N}$, then P(n) is true $\forall n \in \mathbb{N}$.

Example 6.1

Prove $\sum_{k=1}^{n} (2k-1) = n^2$ (*) using induction.

Base case $n = 1: 1 = 1^2$

Induction step: assume as induction hypothesis that (*) holds

$$\sum_{k=1}^{n+1} (2k-1) = \sum_{k=1}^{n} (2k-1) + 2(n+1) - 1$$
$$= n^2 + 2n + 1$$
$$= (n+1)^2$$

Or we can prove it the following way

$$S = 1 + 3 + 5 + \dots + (2n - 1)$$

$$S = (2n - 1) + (2n - 3) + \dots + 3 + 1$$

$$2S = 2n \cdot n$$

$$S = n^{2}$$

Example 6.2

 $a_{n+1} = \sqrt{2 + a_n}$, $a_1 = 1$. Prove $a_n > 0$ and a_n increasing. $a_1 > 0$ assume $a_n > 0$, $a_{n+1} = \sqrt{2 + a_n} > 0$

$$a_2 = \sqrt{3} \approx 1.732 > 1 = a_1$$

Assume $a_n \le a_{n+1}$, want to show $a_{n+1} \le a_{n+2} \iff \sqrt{a_n+2} \le \sqrt{a_{n+1}+2} \iff a_n \le a_{n+1}$

Example 6.3

 $(1+x)^n \ge 1 + nx$: Bernoulli Inequality

 $x \ge -1, \quad n \ge 0$

base case $1 \ge 1$

Assume $(1+x)^n \ge 1 + nx$

$$(1+x)^{n+1} = (1+x)^n (1+x) \ge (1+nx)(1+x) = 1 + (n+1)x + nx^2$$
$$= 1 + (n+1)x$$

Strong Induction:

If P(1) true and $P(1), P(2), \dots P(k) \implies P(k+1)$ true $\forall k \in \mathbb{N}$ then P(n) holds for all $n \in \mathbb{N}$

Remark 6.4. Induction \iff strong induction

Example 6.5

Every integer greater than 1 is a product of primes.

Assume 2, 3, ..., n is a product of primes. n+1 is either a prime or a composite, in which case n+1=ab, 1 < a, b < n+1.

By strong induction hypothesis, both a and b are product of primes, hence so is n+1=ab.

Exercise 6.1. Every integer greater than 1 has a prime divisior.

Proof of infinitude of primes by Euclid:

Proof. Assume on the contrary there are finitely many primes $\{p_1, p_2, \ldots, p_k\}$. Define $N = p_1 \ldots p_k + 1 > 1$ and (by above exercise) let p be a prime divisior of N but $p \neq p_j$ for any $1 \leq j \leq k$ otherwise if $p = p_j$ then $p|p_2 \ldots p_k$ also $p|N \implies p|N - p_1 \ldots p_k \implies p|1$, a contradiction. (no primes divide 1)

$\S7$ Dis 2: Oct 8, 2020

§7.1 Number System

- $(\mathbb{N}, +, \cdot, <) : + : \mathbb{N} \times \mathbb{N} = \mathbb{N}^2 \to \mathbb{N}$ satisfies commutativity and associativity. Note that 0 is the identity with respect to addition, but \mathbb{N} has no additive inverse.
- $(\mathbb{Z}, +, \cdot, <) : (\mathbb{Z}, +)$ is a commutative group (associativity, identity, inverse). (\mathbb{Z}, \cdot) satisfies commutativity, associativity with 1 as mult identity but 2 has no mult inverse.
- $(\mathbb{Q}, +, \cdot, <) : (\mathbb{Q}, +)$ and (\mathbb{Q}, \cdot) are commutative group(i). + and \cdot are compatible with distributive law: a(b+c) = ab + ac (ii). Both (i) and (ii) mean $(\mathbb{Q}, +, \cdot)$ is a FIELD. (Q, <) is an ordered set with < satisfying trichotomy and transitivity. $+, \cdot$ are compatible: $y < z \implies x + y < x + z \forall x, x > 0, y > 0 \implies xy > 0$. With the above compatibility, $(\mathbb{Q}, +, \cdot, <)$ is an ordered field. Even though \mathbb{Q} is additivity adn multiplicatively complete, \mathbb{Q} is not satisfying in that
 - 1. \mathbb{Q} is not algebraically closed, x^2-2 is a polynomial with no root in \mathbb{Q} .
 - 2. \mathbb{Q} is not complete in a metric space: there exists subsets of \mathbb{Q} bounded above but with no least upper bound (supremum), e.g. $A := \{p \in \mathbb{Q} : p < 0 \text{ or } p^2 < 2\}$ and $B = \mathbb{Q} \setminus A$. A contains no largest number and B contains no smallest.

$$\forall p \in A \exists q \in A \quad q > p$$

Let $p \in A$. Define $q := p - \frac{p^2 - 2}{p + 2} > p$

$$q^{2} - 2 = \left(\frac{2p+2}{p+2}\right)^{2} - 2 = \frac{2(p^{2}-2)}{(p+2)^{2}} < 0 \implies q^{2} < 2$$

If A has an upper bound α , $\alpha \notin A$: then $\alpha \in B$. It follows that B is the set of all upper bounds for A. Since B contains no smallest number, A has no least upper bound in \mathbb{Q} .

Definition 7.1 — S has the least-upper-bound property if $\forall E \subset S$ nonempty, bounded above $\sup E \in S$.

Remark 7.2. Q does not satisfy the least-upper-bound property.

 $(\mathbb{R}, +, \cdot, <)$ there exists an ordered field with the l.u.b property that contains an isomorphic copy of \mathbb{Q} .

§7.2 Equivalence Relation

An equivalence relation given \sim on $A \times A$ satisfies

- $x \sim x$ reflexity
- $x \sim y \iff y \sim x \text{ symmetry}$
- $x \sim y \cdot y \sim z \implies x \sim z$ transitivy

Example 7.3

 \mathbb{Q} Define \sim on $\{(a,b): a,b\in\mathbb{Z},b\neq0\}$ by $(a,b)\sim(c,d)$ if ad=bc

$$A = \mathbb{Z}^2 \setminus \{(a,0) : a \in \mathbb{Z}\}\$$

 $\mathbb{Q}=\ \text{the set of all equivalence classes of A write}\ \sim$

$$=A/\sim=\{[x]:x\in A\}$$

In this construction, $\mathbb{Z} \to \mathbb{Q}$, $n \to [(n,1)]$

 $+ \setminus : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$: note that + and \cdot need to be well-defined on \mathbb{Q}^2 . (need to show $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ if $\frac{a}{b} \sim \frac{a'}{b'}$ and $\frac{c}{d} \sim \frac{c'}{d'}$.

Example 7.4

$$S' = \left[0, 1\right] / 0_m$$

Definition 7.5 (Convergent Sequences) — $\{a_n\}_{n\geq 1}\subseteq \mathbb{R}$ is said to be convergent to l if $\forall \epsilon>0$ $\exists N(\epsilon)>0$ s.t. $\forall n\geq N, \quad |a_n-l|<\epsilon$

§8 Dis 3: Oct 13, 2020

§8.1 Equivalence Relation (Cont'd)

Example 8.1

Define $\sim p$ on \mathbb{Z} by $a \sim pb$ if $a - b \in p\mathbb{Z}(p|a - b)$. $\forall a \exists ! b \in \mathbb{Z}, \quad 0 \le r$

$$F_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\sim p = \{[0]_p, [1]_p, [2]_p, \dots, [p-1]_p\}$$

$$[a]_p + [b]_p = [a+b]_p$$
 & $[a]_p[b]_p = [ab]_p$

Remark 8.2. $(F_p, +, \cdot)$ is a finite field. F_p cannot be ordered: $1 > 0, 1 + 1 > 0, \dots, p - 1 > 0$ but p - 1 = -1

Example 8.3

$$\begin{split} T &= \mathbb{R}/\mathbb{Z} \quad a \sim b \text{ if } ab \in \mathbb{Z} \\ &[0,1]/0 \sim 1 \\ \forall a \in \mathbb{R}, \quad \exists b = \underbrace{\{a\}}_{\text{fractional part of } a} \in [0,1) \text{ s.t. } a \sim b \end{split}$$

§8.2 Construction of R via Cauchy Sequences (Cantor)

S = set of rational Cauchy sequences.

 \sim on $S: \{x_n\} - \{y_n\}$ if $\lim(x_n - y_n) = 0$ (Q3 – Homework 2)

 $Q = S/\sim = \{[\{x_n\}] : \{x_n\} \in S\}$. First we need to define arithmetic on Q.

$$\begin{aligned} &[\{p_n\}] + [\{q_n\}] = [\{p_n + q_n\}] \\ &[\{p_n\}] - [\{q_n\}] = [\{p_n - q_n\}] \\ &[\{p_n\}] \cdot [\{q_n\}] = [\{p_n q_n\}] \\ &[\{p_n\}] / [\{p_n/q_n\}] = [\{p_n/q_n\}] \,, \quad [\{q_n\}] \neq 0, = [\{0, 0, 0, \ldots\}] \end{aligned}$$

 $+: Q \times Q \to Q$. Check well-defined

- $\{x_n\} \cdot \{y_n\}$ cauchy then so is $\{x_n + y_n\}(Q4)$
- $\{x_n\} \sim \{y_n\}$ & $\{z_n\} \sim \{w_n\}$ then $\{x_n + z_n\} \sim \{y_n + w_n\}$ (Q5) Commutativity, assoc, identity, $\{0 = [\{0, 0, 0, \dots\}], \text{ inverse.}$
- Well-defined: $\{x_n\}, \{y_n\}$ so is $\{x_ny_n\}$ (Q4).
- {x_n} ~ {y_n} & {z_n} ~ {w_n} (Q6, Q7) comm, assoc, iden, (1 = [{1,1,...,1}] mult. inverse (Q9,Q10).
 <: trichotomy (Q11), transitivity various compatibility (distributivity, etc) l.u.b property (Q12)

Note:All the Q used above is assumed to be Q^{hat}

Remark 8.4.

$$Q \to Q^{\text{hat}}$$

$$q \mapsto [q^*]$$

$$p < q \iff [p^*] < [q^*]$$

Sequences:

- Cauchy seq. are bounded.
- Convergent seq. is Cauchy.

Theorem: in \mathbb{R} , every Cauchy seq. is convergent.

Example 8.5

$$a_n = \frac{1}{n}$$

$$\forall \epsilon > 0 \exists N \text{ s.t. } \epsilon N > 1.$$

$$\forall n \ge N \quad \left| \frac{1}{n} - 0 \right| = \frac{1}{n} \le \frac{1}{N} < \epsilon.$$