

# Math 131A Lecture Notes

Kyle Chui

2021-09-24

# 1 Lecture 1

## 1.1 Goals of This Class

The end goal of this class is to go over the Fundamental Theorem of Calculus, and to do that we must first cover:

- What is a real number and what makes them special?
- How do we define the convergence of a sequence of real numbers?
- What is a limit?
- What is continuity?
- What is a derivative?
- What is an integral?

## 1.2 Mathematical Arguments and Logic

We have the following components to reasoning about solutions to a mathematical problem:

- Assumptions
- Logical steps
- Conclusions

## 1.3 Logical Connections

We usually use the letters  $P$  and  $Q$  to denote logical statements (either true or false). We can also use conjunctions to connect logical statements to one another.

1. Conjunctions: “ $P$  and  $Q$ ”,  $P \wedge Q$
2. Disjunctions: “ $P$  or  $Q$ ”,  $P \vee Q$
3. Implications: “If  $P$ , then  $Q$ ”,  $P \implies Q$ 
  - (a) If the proposition is false (i.e. if  $P$  is false) then the whole statement is true.

**Definition.**

We say that the statement is *vacuously true*.

4. Negations: “Not  $P$ ”,  $\neg P$

### 1.3.1 Truth Tables

| $P$ | $Q$ | $P \implies Q$ |
|-----|-----|----------------|
| $T$ | $T$ | $T$            |
| $T$ | $F$ | $F$            |
| $F$ | $T$ | $T$            |
| $F$ | $F$ | $T$            |

**Example.** Prove that if  $n$  is an integer, then  $n(n+1)$  is even.

*Proof.* Suppose that  $n$  is an integer. Then we have two cases, where either  $n$  is even or  $n$  is odd. Let  $n$  be an even integer such that  $n = 2k$  where  $k \in \mathbb{Z}$ . Then we have

$$\begin{aligned}n(n+1) &= 2k(2k+1) \\ &= 2(2k^2 + k).\end{aligned}$$

Thus we see that  $n(n+1)$  is even when  $n$  is even. Now let  $n$  be odd such that  $n = 2m+1$  where  $m \in \mathbb{Z}$ . Then we have

$$\begin{aligned}n(n+1) &= (2m+1)(2m+1+1) \\ &= (2m+1)(2m+2) \\ &= 2(m+1)(2m+1).\end{aligned}$$

Thus  $n(n+1)$  is also even when  $n$  is odd, and so is even for all integers  $n$ . □

## 2 Lecture 2

### 2.1 Continuation of Logic

#### 2.1.1 De Morgan's Laws

$$\neg(P \vee Q) = \neg P \wedge \neg Q$$

$$\neg(P \wedge Q) = \neg P \vee \neg Q$$

**Note.** Negations turn “and” into “or” and vice versa.

**Example.** Suppose we have the following statement:

$$P: x \text{ is even and } x > 0.$$

Then the negation of  $P$  would be:

$$\neg P: x \text{ is odd or } x \leq 0.$$

#### 2.1.2 Converse

**Definition.** *Converse*

The *converse* of a statement  $P \implies Q$  is the statement  $Q \implies P$ . In general, the converse of a statement says nothing about the original statement.

**Example.** Consider the statement

$$\text{If } x > 0, \text{ then } x^3 \neq 0.$$

The converse is then

$$\text{If } x^3 \neq 0, \text{ then } x > 0.$$

Note that the converse is false even though the original statement is true.

If we know both the original statement and the converse are true, then we may write  $P \iff Q$  instead of  $(P \implies Q) \wedge (Q \implies P)$ . In this case, we call  $P$  and  $Q$  *logically equivalent*. In writing, we say “ $P$  if and only if  $Q$ ”.

#### 2.1.3 Proof by Contrapositive

We can show that

$$(\neg Q) \implies (\neg P) \iff P \implies Q.$$

This gives us another way of proving the original statement, since the contrapositive has the same truth values.

**Lemma 1.** Let  $a$  be an integer. If  $a^2$  is even, then  $a$  is even.

*Proof.* Suppose  $a$  is odd, so  $a = 2k + 1$  for some integer  $k$ . Then

$$\begin{aligned} a^2 &= (2k + 1)^2 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Thus  $a^2$  is odd and this completes the proof.  $\square$

### 2.1.4 Variables and Quantifiers

We have a value  $x$  that varies over some values, so we use  $P(x)$  to denote a statement that depends on the value of  $x$ .

**Example.** Consider the statement

$$P(x) : x + 2 = 3.$$

The statement is true if and only if  $x = 1$ .

We have two quantifiers— $\forall$  = “for all”, and  $\exists$  = “there exists”.

- $\forall x : P(x)$  is true if  $P(x)$  is true for all  $x$ .
- $\exists x : P(x)$  is true if there exists at least one  $x$  such that  $P(x)$  is true.

We can also have nested quantifiers,

$$\forall m \in \mathbb{N}, \exists n \in \mathbb{N} : m < n.$$

**Note.** The order of quantifiers matters. In the above example, the quantifiers tell us that our choice of  $n$  depends on  $m$ .

### 2.1.5 Proof by Counterexample

After “simplifying” the statement  $\neg(\forall x : P(x))$ , we get  $\exists x : \neg P(x)$ . We simply need to find a single counterexample to show that a statement is false for all  $x$ .

**Example.** Consider the statement  $\forall x \in \mathbb{R} : x + 2 = 3$ . All we need to do is show that there exists some  $x \in \mathbb{R}$  such that  $x + 2 \neq 3$ . This occurs when  $x = 0$ , so the statement is false.

### 2.1.6 Proof by Contradiction

**Key Idea.** We want to show that  $P \implies Q$  indirectly.

**Lemma 2.** We can show that

$$P \implies Q = (\neg P) \vee Q.$$

Then  $P \implies Q$  is true if and only if  $\neg(P \implies Q)$  is false, and so by Lemma 2 and De Morgan’s Laws,  $P \wedge \neg Q$  is false.

For proof by contradiction, we assume  $P$  is true and  $\neg Q$  is true, and try to show that  $P \wedge \neg Q$  is false (a contradiction).

## 3 Lecture 3

### 3.1 More Logic

#### 3.1.1 Proof by Contradiction

To do a proof by contradiction for a statement  $P \implies Q$ , we assume  $P \wedge \neg Q$ . We aim to show that  $P \wedge \neg Q$  is false (a contradiction).

**Theorem** — *Irrationality of  $\sqrt{2}$*

There is no rational number  $x$  such that  $x^2 = 2$ . In other words, if  $x \in \mathbb{Q}$ , then  $x^2 \neq 2$ .

*Proof.* Suppose towards a contradiction that there exists some  $x \in \mathbb{Q}$  such that  $x^2 = 2$ . Since  $x$  is rational, there exist integers  $p, q$  such that  $q \neq 0$ ,  $\frac{p}{q} = x$ , and  $p$  and  $q$  have no common divisors (other than 1). Then

$$\begin{aligned}x^2 &= 2 \\ \frac{p^2}{q^2} &= 2 \\ p^2 &= 2q^2.\end{aligned}$$

Since  $p^2$  is even, there exists some integer  $k$  such that  $p = 2k$ . Thus

$$\begin{aligned}(2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2.\end{aligned}$$

By the same logic as before, we know that  $q$  must also be even (they share a common factor of 2). However, this contradicts our original assumption that  $p$  and  $q$  share no common factors, and this completes the proof.  $\square$

### 3.2 Set Theory

We write  $x \in A$  when we want to say that “ $x$  is an element of  $A$ ”, and  $x \notin A$  when we want to say that “ $x$  is not an element of  $A$ ”.

#### 3.2.1 Set Combinations

- Union:  $A \cup B = \{x \mid x \in A \vee x \in B\}$ .
- Intersection:  $A \cap B = \{x \mid x \in A \wedge x \in B\}$ .
- Difference:  $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$ .
- Subset (Inclusion):  $A \subseteq B$  if and only if  $x \in A \implies x \in B$ .

**Definition.** *Proper Subset*

A set  $A$  is a *proper subset* of a set  $B$  if  $A \subseteq B$  and there exists some  $x \in B$  such that  $x \notin A$ . We denote this as  $A \subset B$ .

- Equality:  $A = B$  if and only if  $A \subseteq B$  and  $B \subseteq A$ .

**Note (Showing Equality of Sets).** If you want to show  $A = B$ , you need to show both  $A \subseteq B$  and  $B \subseteq A$ . In other words, you must show that for all  $x \in A$ , we have  $x \in B$ , and vice versa.

**Example.** We have  $\mathbb{N} = \{1, 2, 3, \dots\}$ .

- Let  $E$  be the set of even natural numbers. Note that  $E \subseteq \mathbb{N}$ .
- Let  $S = \{p \in \mathbb{Q} \mid p^2 < 2\} \subseteq \mathbb{Q}$ .

Then we have:

- $\mathbb{N} \cup E = \mathbb{N}$ .
- $\mathbb{N} \cap E = E$ .
- $\mathbb{N} \cap S = \{n \in \mathbb{N} \mid n^2 < 2\} = \{1\}$ .
- $E \cap S = \emptyset$ .

**Definition.** *Disjoint Sets*

If  $A \cap B = \emptyset$ , we call  $A$  and  $B$  *disjoint* sets.

*Proof.* Suppose towards a contradiction that there exists some  $x \in E \cap S$ , which is to say  $x \in E$  and  $x \in S$ . Since  $x \in E$ , we know that  $x$  is even, and so there exists some integer  $k$  such that  $x = 2k$ . Then

$$x^2 = (2k)^2 = 4k^2,$$

so  $4 \mid x^2$ . Therefore  $x \geq 4$ , which contradicts the condition for  $x \in S$ , namely  $x^2 < 2$ .  $\square$

- Given some  $n \in \mathbb{N}$ , we define  $A_n = \mathbb{N} \setminus \{1, \dots, n-1\}$ .
  - $\bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}$ .
  - $\bigcap_{n \in \mathbb{N}} A_n = \emptyset$ .

**Definition.** *Set Complement*

If  $A \subseteq B$ , then we define the *complement* of  $A$  in  $B$  to be  $A^c = B \setminus A$ .

### 3.2.2 De Morgan's Laws

If  $I$  is an index set and  $\{A_j\}_{j \in I}$  are subsets of  $B$ , then

$$\left( \bigcup_{j \in I} A_j \right)^c = \bigcap_{j \in I} A_j^c, \quad \text{and} \quad \left( \bigcap_{j \in I} A_j \right)^c = \bigcup_{j \in I} A_j^c$$

## 4 Lecture 4

### 4.1 Cartesian Product

If I have two sets  $A$  and  $B$ , then we may form their *Cartesian Product*, which is

$$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}.$$

**Definition.** *Binary Relation*

A *binary relation* is a subset  $R \subseteq A \times B$ . We say  $x \in A$  is in relation to  $y \in B$  if  $(x, y) \in R$ . We denote this by

$$xRy \iff (x, y) \in R.$$

**Example.** Consider the relation

$$\mathbb{R} \times \mathbb{R} \supseteq R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}.$$

Then the relation is *reflexive*, because  $xRx$ . It is also *antisymmetric*, because  $xRy \wedge yRx \implies x = y$ . Finally, this relation is *transitive*, because  $xRy \wedge yRz \implies xRz$ .

These properties only make sense if  $A = B$ , i.e.  $R \subseteq A \times A$ , and we say that “ $R$  is a relation on  $A$ ”.

**Definition.** *Partial Order*

If a relation is reflexive, antisymmetric, and transitive on  $A$ , then it is a *partial order* on  $A$ .

The notion of “less than or equal to” is a partial order for  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ , and  $\mathbb{R}$ , but there exists no partial order for  $\mathbb{C}$ .

**Definition.** *Power Set*

For a set  $A$ , we may define its *power set* by

$$\mathcal{P}(A) = \{C \mid C \subseteq A\}.$$

Note that set inclusion is a partial order on  $\mathcal{P}(A)$ .

**Definition.** *Equivalence Relation*

An *equivalence relation*  $R$  over  $A$  is a relation that is reflexive, symmetric, and transitive.

**Note.** Just like a partial order behaves much like  $\leq$ , an equivalence relation behaves much like  $=$ .

**Definition.** *Equivalence Class*

Given an equivalence relation on  $A$ , we define a new set

$$[x] := \{y \in A \mid x \sim y\}.$$

We call  $[x]$  the *equivalence class* of  $x$ . Any  $z \in [x]$  is called a *representative* of the equivalence class  $[x]$ . In particular,  $x$  is a representative of its own equivalence class.

Let  $A$  be a set with equivalence relation  $\sim$ . Then for any  $x, y \in A$ ,

$$[x] = [y] \quad \text{or} \quad [x] \cap [y] = \emptyset.$$



*Proof.* Let  $x, y \in A$ . We know that  $x$  is either equivalent to  $y$  or it is not. Suppose the former is true and let  $z \in [x]$ . Thus we know that  $z \sim x$  and  $x \sim y$ , and by transitivity we have  $z \sim y$ . Thus  $z \in [y]$  and  $[x] \subseteq [y]$ . The reverse argument is the same.

If  $x$  is not equivalent to  $y$ , then suppose towards a contradiction that  $[x] \cap [y] \neq \emptyset$ . Let  $x \in [x] \cap [y]$ . Then  $z \sim x$  and  $z \sim y$ . By symmetry we know that  $x \sim z$  and by transitivity we have  $x \sim y$ . We have arrived at the contradiction that  $x$  is both equivalent and not equivalent to  $y$ .  $\square$

**Definition.** *Function*

A relation  $R \subseteq A \times B$  is a *function* if for all  $x \in A$  and all  $y, z \in B$ , we have the following:

- $xRy \wedge xRz \implies y = z$ .

In other words, every input  $x$  has only one output.

**Definition.** *Injective Functions*

A function  $f$  is *injective* if  $f(x_1) = f(x_2) \implies x_1 = x_2$ .

**Definition.** *Surjective Functions*

A function  $f$  is *surjective* if for every  $y \in B$ , there exists some  $x \in A$  such that  $f(x) = y$ .

## 5 Lecture 5

### 5.1 The Natural Numbers

We know that the natural numbers are defined via:

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

#### 5.1.1 Properties of the Natural Numbers

- (P1)  $1 \in \mathbb{N}$
- (P2) If  $n \in \mathbb{N}$ , then it has a *successor*,  $n + 1 \in \mathbb{N}$
- (P3) 1 is *not* the successor of any element of  $\mathbb{N}$
- (P4) If  $m, n$  have the same successor, then  $m = n$

**Note.** The properties above can be abstracted to become:

- (P1)  $1 \in \mathbb{N}$
- (P2) There exists some  $S: \mathbb{N} \rightarrow \mathbb{N}$  where  $S(n)$  is the successor  $n$
- (P3)  $1 \notin \text{range } S$
- (P4)  $S$  is injective
- (P5) Suppose  $A \subseteq \mathbb{N}$  with the properties:
  - (i)  $1 \in A$
  - (ii) If  $n \in A$ , then  $S(n) \in A$
 Then  $A = \mathbb{N}$ .

#### Theorem — 1.1 (Induction)

Let  $\{P(n) \mid n \in \mathbb{N}\}$  be a set of logical propositions. Suppose that

- (i)  $P(1)$  is true.
- (ii) If  $P(n)$  is true, then  $P(n + 1)$  is true.

Then  $P(n)$  is true for all  $n \in \mathbb{N}$ .

*Proof.* Let  $A = \{n \mid P(n) \text{ is true}\} \subseteq \mathbb{N}$ . By our first assumption,  $1 \in A$ . By (ii), if  $n \in A$ , then  $n + 1 \in A$ . So by (P5) of the natural numbers, we know that  $A = \mathbb{N}$ .  $\square$

#### Definition. 1.2 (Peano Axioms)

A triplet  $(\mathbb{N}, 1, S)$  is said to be a *system of the naturals* if it satisfies:

- 1)  $\mathbb{N}$  is a set and  $1 \in \mathbb{N}$
- 2)  $S: \mathbb{N} \rightarrow \mathbb{N}$  is a function
- 3)  $1 \notin \text{range } S$
- 4)  $S$  is injective
- 5)  $\forall A \subseteq \mathbb{N}$  such that  $1 \in A$  and  $S(A) \subseteq A$ , then  $A = \mathbb{N}$

**Definition.** *Addition*

We define the binary relation  $+$  over  $\mathbb{N}$ :

- (i)  $\forall n \in \mathbb{N}, n + 1 := S(n)$
- (ii)  $\forall m, n \in \mathbb{N}, \text{ we have } m + S(n) = S(m + n)$

The following properties can be proven from the above definition of addition:

- (a) Associativity:  $\forall x, y, z \in \mathbb{N}, \text{ we have } (x + y) + z = x + (y + z)$
- (b) Commutativity:  $\forall x, y \in \mathbb{N}, \text{ we have } x + y = y + x$
- (c) Cancellative Law:  $\forall x, y, z \in \mathbb{N}, \text{ we have } x + y = y + z \implies x = z$

**Theorem — 1.3** (*Existence of the Naturals*)

There exists a unique system of the naturals. In other words, there is a bijection between different systems of the naturals and so we may write:

$$(\mathbb{N}, 1, S) \iff (\mathbb{N}', 1', S').$$

## 5.2 Fields

**Definition.** *Field*

A *field* is a set with two binary operations,

- $+$ , or ‘addition’
- $\cdot$ , or ‘multiplication’

### 5.2.1 Axioms for Addition

- (A1)  $x \in \mathbb{F} \wedge y \in \mathbb{F} \implies x + y \in \mathbb{F}$
- (A2)  $\forall x, y \in \mathbb{F}, \text{ we have } x + y = y + x$
- (A3)  $\forall x, y, z \in \mathbb{F}, \text{ we have } (x + y) + z = x + (y + z)$
- (A4) There exists some  $0 \in \mathbb{F}$  such that  $0 + x = x$  for all  $x \in \mathbb{F}$
- (A5)  $\forall x \in \mathbb{F}, \text{ there exists } -x \in \mathbb{F} \text{ such that } x + (-x) = 0$

### 5.2.2 Axioms for Multiplication

- (M1)  $x \in \mathbb{F} \wedge y \in \mathbb{F} \implies x \cdot y \in \mathbb{F}$
- (M2)  $\forall x, y \in \mathbb{F}, \text{ we have } x \cdot y = y \cdot x$
- (M3)  $\forall x, y, z \in \mathbb{F}, \text{ we have } (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- (M4) There exists some  $1 \in \mathbb{F}$  such that  $1 \neq 0$  and  $1 \cdot x = x$  for all  $x \in \mathbb{F}$
- (M5)  $\forall x \in \mathbb{F}, \text{ there exists some } \frac{1}{x} \in \mathbb{F} \text{ such that } x \cdot \frac{1}{x} = 1$

### 5.2.3 Distributive Law

- (D1)  $\forall x, y, z \in \mathbb{F}, \text{ we have } x \cdot (y + z) = x \cdot y + x \cdot z$

## 6 Lecture 6

### 6.1 The Rationals

On the natural numbers, we have a notion of addition, multiplication, and comparison ( $\leq$ ). We constructed the integers and so we now have:

- A notion of an additive identity,  $0 \in \mathbb{Z}$
- Additive inverses

However, we *don't* have:

- Multiplicative inverses

When we think of the rationals, we consider the set

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

**Note.** When dealing with  $\mathbb{Q}$ , we now have multiplicative inverses.

In particular,  $(\mathbb{Q}, +, \cdot, \leq)$  is an *ordered field*.

**Definition.** *Ordered Field*

An *ordered field* is a field  $\mathbb{F}$  which is also an ordered set ( $\leq$ ) such that:

- (i) If  $x, y, z \in \mathbb{F}$  and  $y < z$ , then  $x + y < x + z$
- (ii) If  $x, y \in \mathbb{F}$ ,  $x > 0$  and  $y > 0$ , then  $x \cdot y > 0$

Unfortunately, the rational numbers still don't allow us to solve polynomial equations (i.e.  $x^2 = 2$ ).

**Definition.** *Algebraic Numbers*

A number is called *algebraic* if it solves

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0,$$

where  $c_0, \dots, c_n \in \mathbb{Z}$ ,  $c_n \neq 0$ ,  $n \in \mathbb{N}$ .

**Example.** Every rational number is algebraic, because it solves the equation

$$qx - p = 0.$$

**Definition.** *Dividing*

We say  $k \in \mathbb{Z}$  *divides*  $m \in \mathbb{Z}$  if  $\frac{m}{k} \in \mathbb{Z}$ .

**Theorem — Rational Zeros Theorem**

Suppose  $c_0, \dots, c_n \in \mathbb{Z}$ ,  $c_n \neq 0$  and  $r \in \mathbb{Q}$  satisfies

$$c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r + c_0 = 0.$$

Then writing  $r = \frac{c}{d}$  with  $c, d$  having no common factors,  $d \neq 0$ , we have:

$$\begin{aligned} c &\text{ divides } c_0 \\ d &\text{ divides } c_n \end{aligned}$$

*Proof.* Since  $r$  solves the equation, we have

$$c_n \left(\frac{c}{d}\right)^n + c_{n-1} \left(\frac{c}{d}\right)^{n-1} + \cdots + c_1 \left(\frac{c}{d}\right) + c_0 = 0.$$

Multiplying both sides by  $d^n$ , we get

$$c_n c^n + c_{n-1} c^{n-1} d + \cdots + c_1 c d^{n-1} + c_0 d^n = 0.$$

Rearranging, we have

$$c_n c^n = -d(c_{n-1} c^{n-1} + \cdots + c_1 c d^{n-2} + c_0 d^{n-1}).$$

We know that  $d \mid c_n c^n$ . Since  $c$  and  $d$  have no common factors, we know  $d \mid c_n$ . Rearranging terms again,

$$-c(c_n c^{n-1} + c_{n-1} c^{n-2} d + \cdots + c_1 d^{n-1}) = c_0 d^n.$$

By the same reasoning as before, we have that  $c \mid c_0$ . □

**Corollary.** Suppose  $r \in \mathbb{Q}$  solves

$$r^n + c_{n-1} r^{n-1} + \cdots + c_1 r + c_0 = 0.$$

Then  $r \in \mathbb{Z}$  and  $r \mid c_0$ .

*Proof.* Since  $r \in \mathbb{Q}$ , we may express  $r = \frac{c}{d}$ ,  $c \mid c_0$  and  $d \mid 1$ . From this we know that  $d = 1$ , so  $r = c$  and  $c \mid c_0$ . Therefore  $r \in \mathbb{Z}$  and  $r \mid c_0$ . □

We have some deficiencies for  $\mathbb{Q}$ :

- There seem to be some “gaps” in  $\mathbb{Q}$ .

**Proposition.** We consider the sets  $A = \{p \in \mathbb{Q} \mid p \geq 0 \text{ and } p^2 < 2\}$  and  $B = \{p \in \mathbb{Q} \mid p \geq 0 \text{ and } p^2 > 2\}$ . Notice that  $A$  has no largest element and  $B$  has no smallest element.

*Proof.* Given  $p \in \mathbb{Q}$ , let

$$q = p - \frac{p^2 - 2}{p^2 + 2} = \frac{2(p+1)}{p+2}.$$

We also have  $q^2 - 2 = \frac{2(p^2 - 2)}{(p+2)^2}$ . If  $p \in A$ ,  $p^2 - 2 < 0$  so  $q > p$  and  $q^2 - 2 > 0$ . If  $p \in B$ ,  $p^2 - 2 > 0$  so  $q < p$  and  $q^2 - 2 < 0$ . □

## 7 Lecture 7

### Definition. 2.11—Upper and Lower Bounds

Let  $E$  be an ordered set and  $A \subset E$ .

- (a) If there exists  $x \in E$  such that for all  $a \in A$ ,  $a \leq x$ , we say  $A$  is *bounded above* by  $x$  and call  $x$  an *upper bound* for  $A$ .
- (b) Suppose  $A \subset E$  is non-empty and bounded above and there exists some  $x^* \in E$  such that
  - i)  $x^*$  is an upper bound for  $A$
  - ii) If  $y$  is any upper bound for  $A^*$ , then  $x^* \leq y$

Then we call  $x^*$  the *least upper bound* for  $A$ , and we write

$$x^* = \sup A. \quad (\text{sup meaning supremum})$$

The *greatest lower bound* or *infimum* of a set  $B$ , which is bounded below and non-empty, satisfies

- i)  $\inf B$  is a lower bound for  $B$
- ii) If  $y$  is any lower bound for  $B$ , then  $y \leq \inf B$

**Example.** Suppose

$$A = \{p \in \mathbb{Q} \mid p \geq 0, p^2 < 2\},$$

$$B = \{p \in \mathbb{Q} \mid p \geq 0, p^2 > 2\}.$$

Then  $A$  is bounded above (say by 2) and  $B$  is bounded below (say by 0). In the last lecture we proved that neither  $\sup A$  nor  $\inf B$  exist in  $\mathbb{Q}$  (because the values would have been  $\sqrt{2}$ ).

**Example.** Let

$$C = \{p \in \mathbb{Q} \mid p < 0\},$$

$$D = \{p \in \mathbb{Q} \mid p \leq 0\}.$$

Then

$$\sup C = \sup D = 0.$$

However, notice that  $\sup C \notin C$  and  $\sup D \in D$ .

### Definition. Maximum

We define  $\max A$  to be the largest element of  $A$ , which satisfies:

- i)  $\max A \in A$
- ii) For all  $a \in A$ ,  $a \leq \max A$

The definition for minimum is similar.

### Definition. 2.12—Least Upper Bound Property (LUBP)

An ordered set  $E$  has the *least upper bound property* if the following is true:

- i) If  $A \subseteq E$ ,  $A \neq \emptyset$ ,  $A$  is bounded above, then  $\sup A$  exists and  $\sup A \in E$ .

**Note.**  $\mathbb{Q}$  does not have the least upper bound property.

**Theorem — 2.13 (Existence of  $\mathbb{R}$ )**

There exists an ordered field  $\mathbb{R}$  which has

- i)  $\mathbb{Q}$  as a sub-field
- ii) The least upper bound property

## 7.1 Fundamental Properties of the Real Numbers (because of LUBP)

**Theorem — 2.14 (Archimedean Property of  $\mathbb{R}$ )**

If  $x, y \in \mathbb{R}$ , and  $x > 0$ , then  $\exists n \in \mathbb{N}$  such that  $n \cdot x > y$ .

*Proof.* Let  $A = \{nx \mid n \in \mathbb{N}\} \subseteq \mathbb{R}$ . Suppose towards a contradiction that there is no such  $n$  that satisfies the statement above. In other words, for all  $n \in \mathbb{N}$ ,  $nx \leq y$ . Thus  $A$  is bounded above by  $y$ . Since  $A$  is nonempty and is a subset of  $\mathbb{R}$ , we know that  $\sup A$  exists. Consider the value given by  $\sup A - x$ , which is not an upper bound for  $A$ . Then we know there exists some  $z \in A$  such that  $\sup A - x < z$ . Since  $z = mx$  (because  $z \in A$ ), we have

$$\begin{aligned}\sup A - x &< z \\ \sup A - x &< mx \\ \sup A &< (m+1)x.\end{aligned}$$

We know that  $(m+1)x \in A$ , which contradicts the definition of  $\sup A$ . □

Some remarks:

1. Let  $x = 1$ . Then  $\forall y \in \mathbb{R}, \exists n \in \mathbb{N}$  such that  $n > y$ .
2. Let  $y = 1$ . Then  $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}$  such that  $x > \frac{1}{n} > 0$ .

**Theorem — 2.15 (Density of  $\mathbb{Q}$  in  $\mathbb{R}$ )**

For all  $x, y \in \mathbb{R}$ ,  $x < y$ , there exists some  $p \in \mathbb{Q}$  such that  $x < p < y$ .

*Proof.* Fix  $x < y$ . Then by the Archimedean property we have some  $n \in \mathbb{N}$  such that  $n(y - x) > 1$ , or  $y - x > \frac{1}{n}$ . We may suppose  $x > 0$ , because otherwise we either have  $x < 0 < y$  or  $x < y < 0$  (multiply all sides by  $-1$ ).

We want to show that

$$nx < m < ny.$$

Since  $nx + 1 < ny$ , we have  $nx < m < nx + 1$ , or  $m - 1 < nx < m$ . If  $nx \in \mathbb{Z}$ , we can take  $m = nx + 1$ . Thus

$$x < x + \frac{1}{n} = \frac{nx + 1}{n} = \frac{m}{n} < \frac{ny}{n} < y.$$

Otherwise we have  $nx \notin \mathbb{Z}$ . We then apply the following lemma:

**Lemma.** If  $x \in \mathbb{R}$ , there exists a  $k \in \mathbb{Z}$  such that  $k - 1 \leq x \leq k$ .

Then  $m - 1 < nx < m$ , as desired. □

## 8 Lecture 8

### 8.1 A Construction of the Real Numbers

We want to show that there exists some field  $\mathbb{R}$  such that  $\mathbb{Q}$  is a sub-field and  $\mathbb{R}$  has the least upper bound property. This construction will be via Dedekind cuts.

**Definition.** 2.17—*Cut*

A *cut* in  $\mathbb{Q}$  is a pair of subsets  $A, B \subset \mathbb{Q}$  such that:

- (i)  $A \cap B = \emptyset$ ,  $A \cup B = \mathbb{Q}$ ,  $A, B \neq \emptyset$  (They partition  $\mathbb{Q}$ )
- (ii) If  $a \in A$  and  $b \in B$ , then  $a < b$
- (iii)  $A$  contains no largest element

**Example.** An example of such a cut could be  $A = \{p \in \mathbb{Q} \mid p < 1\}$  and  $B = \{p \in \mathbb{Q} \mid p \geq 1\}$ . We say that  $A \mid B$  is a cut. Another such example is  $A = \{p \in \mathbb{Q} \mid p \leq 0 \text{ or } p^2 < 2\}$  and  $B = \{p \in \mathbb{Q} \mid p > 0 \text{ and } p^2 \geq 2\}$

**Definition.** 2.18—*The Reals*

We may define

$$\mathbb{R} = \{X \mid X \text{ is a cut in } \mathbb{Q}\}.$$

In order to show that the above is a valid definition for  $\mathbb{R}$ , we must show:

- (i)  $\mathbb{Q}$  is contained in  $\mathbb{R}$  in some “natural way”
- (ii)  $\mathbb{R}$  is an ordered field
- (iii)  $\mathbb{R}$  has the least upper bound property

**Definition.** 2.19—*Partial Order for the Reals*

We define a *partial order* on  $\mathbb{R}$  as follows: If  $X = A \mid B$  and  $Y = C \mid D$ , then we say  $X < Y$  if and only if  $A \subset C$  and  $X \leq Y$  if and only if  $A \subseteq C$ .

We will show that the reals contain the rationals.

*Proof.* We will begin by showing that  $\mathbb{Q} \subseteq \mathbb{R}$ . We say that  $A \mid B$  is a *rational cut* if for some  $c \in \mathbb{Q}$ , we have  $A = \{p \in \mathbb{Q} \mid p < c\}$  and  $B = \mathbb{Q} \setminus A$ . We will use  $c^*$  to denote the rational cut at  $c$ . Then we may associate every  $c \in \mathbb{Q}$  with a corresponding rational cut  $c^* \in \mathbb{R}$ .  $\square$

**Theorem — 2.20 (The Reals have the LUBP)**

With respect to the partial order  $\leq$  defined earlier, we may show that  $\mathbb{R}$  has the least upper bound property.

*Proof.* Let  $\mathcal{C}$  be any non-empty collection of cuts which are bounded above, say by the cut  $X$ . We want to show that  $\sup \mathcal{C}$  exists in  $\mathbb{R}$ , so  $\sup \mathcal{C}$  is itself a cut. A candidate for  $\sup \mathcal{C}$  is  $C \mid D$ , where

$$C = \{a \in \mathbb{Q} \mid \text{There exists a cut } A \mid B \in \mathcal{C} \text{ such that } a \in A\}.$$

Now,  $Z = C \mid D$  is a cut in  $\mathbb{Q}$ . We claim that  $C$  has no largest element. If  $a \in C$ , then there exists a cut  $A \mid B \in \mathcal{C}$  such that  $a \in A$ . Since  $A$  is a part of a cut, it has no largest element, so there exists some  $a' \in A$  such that  $a < a'$ . Thus  $a' \in C$  so  $C$  has no largest element.

We must now show that  $Z$  is the least upper bound of  $\mathcal{C}$ . For any  $A \mid B \in \mathcal{C}$ ,  $A \subseteq C$ . Therefore  $A \mid B \leq C \mid D = Z$  and  $Z$  is an upper bound for  $\mathcal{C}$ . We must now show that it is the *least* upper



bound. Let  $Z' = C' \mid D'$  be an upper bound for  $\mathcal{C}$ . Then  $A \mid B \leq C' \mid D'$  and  $A \subseteq C'$  for any  $A \mid B \in \mathcal{C}$ . Now by definition of  $C$ , we have  $C \subseteq C'$ . Therefore  $C \mid D \leq C' \mid D'$ , so  $Z \leq Z'$ . We have  $Z = \sup \mathcal{C} \in \mathbb{R}$ , so  $\mathbb{R}$  has the least upper bound property.  $\square$

We now show that  $\mathbb{R}$  is a field, namely an ordered field. We define the binary relations  $+$  and  $\cdot$  as follows: Given two cuts  $A \mid B$  and  $C \mid D$ , we may define

$$E = A + C = \{p \in \mathbb{Q} \mid p = a + c \text{ for some } a \in A, c \in C\}.$$

**Note.** This set summation is known as the Minkowski sum.

We must check that  $E \mid F$  is a cut. We must also show that the additive identity for  $\mathbb{R}$  is 0, i.e. we must show that  $0 + x = x + 0 = x$  for all  $x \in \mathbb{R}$ . To show the existence of additive inverses, show that for any cut  $A \mid B$ , there exists some  $C \mid D \in \mathbb{R}$  such that  $A \mid B + C \mid D = 0$ .

Similarly, we define multiplication by

$$E = \{p \in \mathbb{Q} \mid p = ac \text{ for some } a \in A, c \in C\}.$$

## 8.2 Interesting Questions

- (a) Can we cut  $\mathbb{R}$  to get something larger? No, because every possible cut in  $\mathbb{R}$  is an element of  $\mathbb{R}$ . This is because  $\mathbb{R}$  has the least upper bound property and every cut in  $\mathbb{R}$  would just be a “real cut” at  $\sup A$ .
- (b) Is  $\mathbb{R}$  unique in some natural way? Yes. If you take any other ordered field  $\mathbb{F}$  such that  $\mathbb{Q} \subseteq \mathbb{F}$  and  $\mathbb{F}$  has the least upper bound property, then there exists some bijection between  $\mathbb{F}$  and  $\mathbb{R}$ .
- (c) What about  $+\infty$  and  $-\infty$ ? We can’t treat these as real numbers using Dedekind cuts, as either  $A$  or  $B$  would have to be empty.

## 9 Lecture 9

### 9.1 Sequences

**Example.** *Approximating  $\pi$*

We know that the area of the unit circle should be  $\pi$ . We can approximate the area of a unit circle by inscribing various shapes in the circle and finding their areas (giving us a sequence of lower bounds). If we inscribe an equilateral triangle in the circle, we find that its side length is  $\sqrt{3}$ , so the area of the triangle is  $a_1 = \frac{3\sqrt{3}}{4} \approx 1.299$ .

If we use a square instead, its side length is  $\sqrt{2}$ , so we have a new lower bound of  $a_2 = 2 < \pi$ .

Using a regular pentagon, we have a new approximation as given by  $a_3 = \frac{5}{2} \sin\left(\frac{2\pi}{5}\right) < \pi$ .

Continuing this pattern, we get

$$a_n = \frac{n+2}{2} \sin\left(\frac{2\pi}{n+2}\right) < \pi.$$

Notice that for all  $n \in \mathbb{N}$ , we have  $a_n < a_{n+1} < \pi$ . Computing this value for larger  $n$ , we have

$$a_{100} \approx 3.1396$$

$$a_{1000} \approx 3.141572$$

$$a_{10000} \approx 3.14159245.$$

Similarly, we may obtain upper bounds for  $\pi$  by circumscribing regular polygons around the unit circle. By circumscribing a square, we know that  $\pi < 4$ , so we know that there is some upper bound for what  $\pi$  is equal to. Thus we know that there exists some  $a \in \mathbb{R}$  such that  $a_n \approx a$  for some sufficiently large  $n$ .

In other words, there exists some  $a \in \mathbb{R}$  such that  $a_n$  converges to  $a$  as  $n$  approaches  $\infty$ .

One issue to note is that we are using  $\pi$  in our formula for  $a_n$  to approximate the value of  $\pi$ . Using some trigonometric identities, we may circumvent this by evaluating

$$a_{2n} = \frac{n}{2} \left( n - \sqrt{n - 4a_n^2} \right).$$

**Definition.** *3.1—Sequences*

A *sequence* is a function  $f: \mathbb{N} \rightarrow \mathbb{R}$ . Instead of writing  $f(1), f(2), \dots, f(n)$ , we tend to write a sequence as  $f_1, f_2, \dots, f_n$ .

**Note (Notations for Sequences).** There are many different notations for expressing sequences, a few popular notations being used below:

$$\left(1, \frac{1}{2}, \frac{1}{3}, \dots\right) = \left(\frac{1}{n}\right)_{n=1}^{\infty} = \left(\frac{1}{n}\right)_{n \in \mathbb{N}} = \left\{\frac{1}{n} \mid n \in \mathbb{N}\right\}.$$

#### 9.1.1 Behaviors of Sequences

- (a) “Convergence”—Getting closer and closer to a given point.
- (b) “Divergence”—Getting closer and closer to  $\pm\infty$ .
- (c) “Oscillation”—The sequence does not approach any value in particular.

### 9.1.2 Facts From the Homework

We define the absolute value function

$$|\cdot| : \mathbb{R} \rightarrow [0, \infty) = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

We have the following properties of the absolute value function:

- (i)  $|xy| = |x| |y|$  for all  $x, y \in \mathbb{R}$ .
- (ii)  $|x - y| \leq \ell$  if and only if  $y - \ell \leq x \leq y + \ell$ , where  $\ell \geq 0$  and  $x, y \in \mathbb{R}$ .
- (iii) **Triangle Inequality:**  $|x + y| \leq |x| + |y|$ .

**Note.** One consequence of this is

$$\begin{aligned} |x - y| &= |x - z + z - y| \\ &\leq |x - z| + |z - y|. \end{aligned}$$

In other words, the distance between two points  $x$  and  $y$  is always less than or equal to the sum of the distances of  $x$  and  $y$  to a third point,  $z$ .

We say that  $a_n$  approaches  $a$  if “ $|a_n - a|$  gets arbitrarily small as  $n$  gets arbitrarily large”.

### 9.1.3 Convergence

**Definition.** 3.2—*Convergence*

A sequence  $(x_n)$  of real numbers is said to *converge* to an  $x \in \mathbb{R}$  if for all  $\varepsilon > 0$ , there exists  $N > 0$  such that

$$|x_n - x| < \varepsilon$$

for all  $n > N$ . If  $(x_n)$  converges to  $x$ , we also write:

$$x_n \rightarrow x \text{ as } n \rightarrow \infty \quad \text{or} \quad \lim_{n \rightarrow \infty} x_n = x.$$

We call  $x$  the *limit* of the sequence  $(x_n)$ . We say that a sequence *diverges* if it does not converge.

**Note.** By the Archimedean property, we can always take  $N \in \mathbb{N}$ . In general,  $N$  is a function of  $\varepsilon$ . We fix  $\varepsilon > 0$ , and use that to find some sufficient  $N$  so that the sequence converges.

**Example.** Consider the sequence  $x_n = \frac{1}{n^2}$ . We suspect that  $x_n \rightarrow 0 \in \mathbb{R}$  as  $n \rightarrow \infty$ . Fix  $\varepsilon > 0$ . If we let  $N = \left\lceil \frac{1}{\sqrt{\varepsilon}} \right\rceil$  and  $n > N$ , we have

$$\begin{aligned} |x_n - 0| &= \left| \frac{1}{n^2} \right| \\ &= \frac{1}{n^2} \\ &< \frac{1}{N^2} \\ &< \varepsilon. \end{aligned}$$

Thus,  $x_n \rightarrow 0$  as  $n \rightarrow \infty$ , so

$$\lim_{n \rightarrow \infty} x_n = 0.$$