MATH 131H Notes

Jiantong Liu

October 5, 2022

Preliminaries

This document is the notes based on Professor Monica Visan's teaching in the MATH 131AH and 131BH course in winter and spring 2021. The corresponding textbook is Baby Rudin.

1 Lecture 1: Statements

In Rubin's notation, natural numbers start with 1, i.e. $\mathbb{N} = \{1, 2, \cdots\}$.

Let A and B be two statements. We use the following notations:

- We write "A" if A is true.
- We write "not A" if A is false.
- We write "A and B" if both A and B are true.
- We write "A or[1] B" if A is true or B is true or both A and B are true.
- We write "$A \Rightarrow B$ if "A and B" or "not A". We read this as "A implies B" or "if A then B". In this case, B is at least as true as A. In particular, A, a false statement A can imply anything.

We usually write shorthand notation "T" and "F" to represent "true" and "false".

Example 1.1. Consider the following statement:

$$\text{If } x \text{ is a natural number, i.e. } x \in \mathbb{N} = \{1, 2, 3, \cdots\}, \text{ then } x \geq 1.$$

In this case, A is the statement "x is a natural number" and B is the statement "$x \geq 1$".

- Taking $x = 3$, we get $T \Rightarrow T$.
- Taking $x = \pi$, we get $F \Rightarrow T$.
- Taking $x = 0$, we get $F \Rightarrow F$.

[1] The notation "or" in mathematics is inclusive. We distinguish it from the exclusive or, usually called "xor", which means "either A or B"

Example 1.2. Consider the statement:

If a number is less than 10, then it is less than 20.

The statement is of the form "if... then...", where A is the statement "a number is less than 10", and B is the statement "it is less than 20".

- Taking a number 5, we get $T \Rightarrow T$.
- Taking a number 15, we get $F \Rightarrow T$.
- Taking a number 25, we get $F \Rightarrow F$.

We also write "$A \iff B$" 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".

We can now compare these notions in logic to similar ones from set theory. Let X be an ambient space. Let A and B be subsets of X. Then

- ${}^cA = \{x \in X : x \notin A\}$.
- $A \cap B = \{x \in X : x \in A \text{ and } x \in B\}$.
- $A \cup B = \{x \in X : x \in A \text{ or } x \in B \text{ or } x \in A \cap B\}$.
- $A \subseteq B$ corresponds to $A \Rightarrow B$.
- $A = B$ corresponds to $A \iff B$.

We now can use truth tables to check the statements.

A	B	not A	A and B	A or B	$A \Rightarrow B$	$A \iff B$
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. We can use the truth table to show that $A \Rightarrow B$ is logically equivalent to (not A) or B. Indeed, by considering the following truth table,

A	B	$A \Rightarrow B$	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

we realize that the column of $A \Rightarrow B$ and (not A) or B are the same.

Exercise 1.4. Use the truth table to prove De Morgan's laws:

not (A and B) = (not A) or (not B)
not (A or B) = (not A) and (not B)

One can compare these statements to

$$^c(A \cap B) = {}^cA \cup {}^cB$$
$$^c(A \cup B) = {}^cA \cap {}^cB$$

Example 1.5. Negative the following statement:

If A then B.

Note that the negation is "not $(A \Rightarrow B)$", then it is equivalent to not ((not A) or B), which is equivalent to [not(not A)] and (not B), and that is just A and (not B).

Therefore, the negation is "A is true and B is false".

Example 1.6. Negate the following statement:

If I speak in front of the class, I am nervous.

That would be I speak in front of the class and I am not nervous.

We now introduce quantifiers.

- $\forall$ reads "for all " or "for any".
- $\exists$ reads "there is" or "there exists".
- The negation of "$\forall A$, B is true" is "$\exists A$ such that B is false".
- The negation of "$\exists A$ such that B is true" is "$\forall A$, B is false".

Example 1.7. Negate the following:

Every student had coffee or is late for class.

This statement is represented as

$\forall$ student (had coffee) or (is late for this)

and so the negation would be

$\exists$ student such that not (had coffee) and not (is late for class)

Writing this out, we get "there is a student that did not have coffee and is not late for class".

2 Lecture 2: Peano Axiom and Mathematical Induction

Definition 2.1 (Peano Axiom)**.** The natural numbers $\mathbb{N} = \{1, 2, 3, \cdots\}$ satisfy the Peano axioms:

1. $1 \in \mathbb{N}$.
2. If a number $n \in \mathbb{N}$, then its successor $n + 1 \in \mathbb{N}$.
3. 1 is not the successor of any natural number.
4. If two numbers $n, m \in \mathbb{N}$ are such that they have the same successor, i.e. $n+1 = m+1$, then they are the same, i.e. $n = m$.
5. Let $S \subseteq \mathbb{N}$. Assume that S satisfies the following two conditions:

   (i) $1 \in S$,

   (ii) and if $n \in S$ then $n + 1 \in S$,

   then $S = \mathbb{N}$.

Axiom number 5 forms the basis for mathematical induction.

Definition 2.2 (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 true, i.e. $P(n) \Rightarrow P(n + 1)$ $\forall n \geq 1$.

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 5, we deduce that $S = \mathbb{N}$.

Example 2.3. Prove that

$$1^2 + 2^2 + \cdots + n^2 = \tfrac{n(n+1)(2n+1)}{6} \quad \forall n \in \mathbb{N}.$$

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

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

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 show that $P(n + 1)$ holds. We know

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

then we have

$$\begin{aligned}
1^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= (n+1)[\frac{n(2n+1}{6} + n + 1] \\
&= (n+1) \cdot \frac{2n^2 + 7n + 6}{6} \\
&= \frac{(n+1) \cdot [2n(n+2) + 3n + 6]}{6} \\
&= \frac{(n+1)(n+2)(2n+3}{6}
\end{aligned}$$

So $P(n+1)$ holds.

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

Example 2.4. Prove that $2^n > n^2$ for all $n \geq 5$.

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 $2^n > n^2$, then

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

For $n \geq 5$, we have $(n-1)^2 - 2 \geq 4^2 - 2 = 14 \geq 0$, so we know $2^{n+1} > (n+1)^2$. Therefore, $P(n+1)$ holds.

Collecting the two steps, we conclude $P(n)$ holds $\forall n \geq 5$.

Remark 2.5. 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 $n = 1$: $(1-1)^2 - 2 = -2 < 0$. Also 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 2.6. Prove by mathematical induction that the number $4^n + 15n - 1$ is divisible by 9 for all $n \geq 1$.

We will 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 as $9 \mid (4^n + 15n - 1)$.

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.

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

By the inductive hypothesis, $9 \mid (4^n + 15n - 1)$ implies $9 \mid 4 \cdot (4^n + 15n - 1)$. Also we know $9 \mid 9 \cdot (5n - 2)$ since $5n - 2 \in \mathbb{N}$. Therefore, we know $9 \mid [4 \cdot (4^n + 15n - 1) - 9 \cdot (5n - 2)]$. Hence, $9 \mid [4 \cdot (4^n + 15n - 1) - 9 \cdot (5n - 2)]$, so $P(n+1)$ holds.

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

Example 2.7. Compute the following sum and then use mathematical induction to prove your answer: for $n \geq 1$,

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)}.$$

Note that $\frac{1}{(2n-1)(2n+1)} = \frac{1}{2}[\frac{1}{2n-1} - \frac{1}{2n+1}]$ for all $n \geq 1$. So

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

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

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

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

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

and so

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

So $P(n+1)$ holds.

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

3 Lecture 3: Equivalence Relation

We now extend $\mathbb{N}$ and construct the set of integers $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n : n \in \mathbb{N}\}$.

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

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

Example 3.2. The equal relation $=$ is an equivalence relation on $\mathbb{Z}$.

Example 3.3. Let $q \in \mathbb{N}$ and $q > 1$. For $a, b \in \mathbb{Z}$ we write $a \sim b$ if $q \mid (a - b)$. This is an equivalence relation on $\mathbb{Z}$. Indeed, it suffices to check the three properties:

- Reflexivity: If $a \in \mathbb{Z}$, then $a - a = 0$, which is divisible by q. So $q \mid (a - a)$, by definition we know $a \sim a$.
- Symmetry: Let $a, b \in \mathbb{Z}$ such that $a \sim b$, then by definition we know $q \mid (a - b)$. Therefore, there exists some $k \in \mathbb{Z}$ such that $a - b = kq$, so $b - a = (-k) \cdot q$. Note that $-k \in \mathbb{Z}$, so $q \mid (b - a)$, and by definition we know $b \sim a$.
- Transivitity: Let $a, b, c \in \mathbb{Z}$ such that $a \sim b$ and $b \sim c$. Now $a \sim b$ indicates $q \mid (a - b)$, so there exists $n \in \mathbb{Z}$ such that $a - b = qn$. Similarly there exists $m \in \mathbb{Z}$ such that $b - c = qm$. Therefore, $a - c = q(n + m)$, where $n + m \in \mathbb{Z}$. Therefore, $q \mid (a - c)$, so by definition $a \sim c$.

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. $a \in C(a)$ for all $a \in A$.
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 $C(a) \cap C(b) = \varnothing$.
4. $A = \bigcup_{a \in A} C(a)$.

Proof. 1. By reflexivity, $a \sim a$ for all $a \in A$, then $a \in C(a)$ for all $a \in A$.

2. Assume $a, b \in A$ with $a \sim b$. Let us show $C(a) \subseteq C(b)$. Let $c \in C(a)$ be arbitrary, then $a \sim c$. Because $a \sim b$, by symmetry we have $b \sim a$, then by transitivity we know $b \sim c$, and so $c \in C(b)$. This proves that $C(a) \subseteq C(b)$. A similar argument shows that $C(b) \subseteq C(a)$, and so $C(a) = C(b)$.

3. We argue by contradiction. Assume that $a, b \in A$ are such that $a \not\sim b$, but $C(a) \cap C(b) \neq \varnothing$. Let $c \in C(a) \cap C(b)$, then $c \in C(a)$ and $c \in C(b)$. The first property implies $a \in c$, and the second property implies $b \sim c$, so $c \sim b$, and therefore by transitivity we have $a \sim b$. This contradicts the hypothesis $a \not\sim b$. Therefore, if $a \not\sim b$, then $C(a) \cap C(b) = \varnothing$.

4. Clearly, as $C(a) \subseteq A$ for all $a \in A$, we get $\bigcup_{a \in A} C(a) \subseteq A$. Then conversely, $A = \bigcup_{a \in A} \{a\} \subseteq \bigcup_{a \in A} C(a)$, and therefore $A = \bigcup_{a \in A} C(a)$.

□

Example 3.6. Take $q = 2$ in our previous example: for $a, b \in \mathbb{Z}$, we write $a \sim b$ if $2 \mid (a - b)$. The equivalence classes are

$$C(0) = \{a \in \mathbb{Z} : 2 \mid (a - 0)\} = \{2n : n \in \mathbb{Z}\}$$
$$C(1) = \{a \in \mathbb{Z} : 2 \mid (a - 1)\} = \{2n + 1 : n \in \mathbb{Z}\}$$

and $\mathbb{Z} = C(0) \cup C(1)$.

Example 3.7. 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 $ad = bc$. Then for example, we have $(1, 2) \sim (2, 4) \sim (3, 6) \sim (-4, -8)$.

Lemma 3.8. $\sim$ is an equivalence relation on F.

Proof. We have to check the three properties.

Reflexivity: Fix $(a, b) \in F$. As $ab = ba$, we have $(a, b) \sim (b, a)$.

Symmetry: Let $(a, b), (c, d) \in F$ such that $(a, b) \sim (c, d)$, then by definition we know $ad = bc$, and so $cb = da$, and by definition $(c, d) \sim (a, b)$.

Transitivity: Let $(a, b), (c, d), (e, f) \in F$ such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Now $(a, b) \sim (c, d)$ implies $ad = bc$, then $adf = bcf$. Similarly, $cfb = deb$. Therefore, $adf = deb$. Now $d(af - be) = 0$, and because $d \neq 0$ by definition, we know $af = be$, and by definition we have $(a, b) \sim (e, f)$ as desired. □

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 we should have

$$\begin{cases} (ad + bc, bd) \sim (a'd' + b'c', b'd') \\ (ac, bd) \sim (a'c', b'd') \end{cases}$$

We now check the first property and left the second property as an exercise to the readers. We want to show $(ad + bc)b'd' = bd(a'd' + b'c')$. We know that $(a, b) \sim (a'b')$, so $ab' = ba'$,

and therefore $ab'dd' = badd'$. Similarly we know $(c,d) \sim c'd'$, so $cd' = dc'$, and therefore $cd'bb' = dc'bb'$. Now we get

$$ab'dd' + cd'bb' = ba'dd' + dc'bb',$$

and so

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

This proves addition is well-defined.

Now the set of rational numbers is exactly the set of equivalence classes on F, i.e.

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

4 Lecture 4: Field

Definition 4.1 (Field)**.** A field is a set F with at least two elements equipped with two operations: addition (denoted $+$) and multiplication (denoted $\cdot$) that satisfies the following:

1. $(A1)$ Closure: if $a, b \in F$, then $a + b \in F$.
2. $(A2)$ Commutativity: if $a, b \in F$, then $a + b = b + a$.
3. $(A3)$ Associativity: if $a, b, c \in F$, then $(a + b) + c = a + (b + c)$.
4. $(A4)$ Identity: $\exists 0 \in F$ such that $a + 0 = 0 + a = a\ \forall a \in F$.
5. $(A5)$ Inverse: $\forall a \in F$, $\exists(-a) \in F$ such that $a + (-a) = -a + a = 0$.
6. $(M1)$ Closure: if $a, b \in F$, then $a \cdot b \in F$.
7. $(M2)$ Commutativity: if $a, b \in F$, then $a \cdot b = b \cdot a$.
8. $(M3)$ Associativity: if $a, b, c \in F$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
9. $(M4)$ Identity: $\exists 1 \in F$ such that $a \cdot 1 = 1 \cdot a = a\ \forall a \in F$.
10. $(M5)$ Inverse: $\forall a \in F \backslash \{0\}$, $\exists a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
11. (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 because (A_4) fails.

Example 4.3. $(\mathbb{Z}, +, \cdot)$ is not a field because (M_5) fails.

Example 4.4. $(\mathbb{Q}, +, \cdot)$ is a field.

Recall $\mathbb{Q} = \{\frac{a}{b} : (a,b) \in \mathbb{Z} \times (\mathbb{Z}\backslash\{0\}\}$ where $\frac{a}{b}$ denotes the equivalence class of $(a,b) \in \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ with respect to the equivalence relation $\sim$, where $(a,b) \sim (c,d)$ if and only if $a \cdot d = b \cdot c$. We defined two operations

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

Then the additive identity $\frac{0}{1}$ is the equivalence class of $(0,1)$, and the multiplicative identity $\frac{1}{1}$ is the equivalence class of $(1,1)$.

The additive inverse of $\frac{a}{b} \in \mathbb{Q}$ is given by $\frac{-a}{b}$, and for $\frac{a}{b} \in \mathbb{Q}\backslash\{\frac{0}{1}\}$, the multiplicative inverse is given by $\frac{b}{a}$.

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 $a, b, c \in F$ such that $a + b = a + c$, then $b = c$. In particular, if $a + b = a$, then $b = 0$.
4. If $a, b, c \in F$ such that $a \neq 0$ and $a \cdot b = a \cdot c$, then $b = c$. In particular, if $a \neq 0$ and $a \cdot b = a$, then $b = 1$.
5. $a \cdot 0 = 0 \cdot a = 0 \ \forall a \in F$.
6. If $a, b \in F$, then $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.
7. If $a, b \in F$, then $(-a) \cdot (-b) = a \cdot b$.
8. If $a \cdot b = 0$, then $a = 0$ or $b = 0$.

Proof.

1. We will show the additive identity is unique. Assume $\exists 0, 0' \in F$ such that $a + 0 = 0 + a = a$ and $a + 0' = 0' + a = a$ for all $a \in F$. Take $a = 0'$ in the first equation and $a = 0$ in the second equation yields $0' + 0 = 0'$ and $0' + 0 = 0$, so $0 = 0'$.
2. We will show that the additive inverse is unique. Let $a \in F$. Assume there exists $-a, a' \in F$ such that $-a + a = a + (-a) = 0$ and $a' + a = a + a' == 0$. Because $a' + a = 0$, then $(a' + a) + (-a) = 0 + (-a)$, so $a' + (a + (-a)) = -a$, but that means $a' + 0 = -a$, so $a' = -a$.
3. Assume $a + b = a + c$. Then $-a + (a + b) = -a + (a + c)$. Therefore, $(-a + a) + b = (-a + a) + c$, so $0 + b = 0 + c$, which means $b = c$. So if $a + b = a = a + 0$, then $b = 0$.
4. We have a proof similar as above.
5. $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, so $a \cdot 0 = 0$. Similarly, $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$, we have $0 \cdot a = 0$.
6. $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$, and so $(-a) \cdot b = -(a \cdot b)$. Similarly, we have $a \cdot (-b) = -(a \cdot b)$.
7. $(-a) \cdot (-b) + [-(a \cdot b)] = (-a) \cdot (-b) + (-a) \cdot b = (-a)(-b + b) = (-a) \cdot 0 = 0$. Therefore, $(-a) \cdot (-b) = a \cdot b$.
8. Assume $a \cdot b = 0$. Assume $a \neq 0$, then $\exists a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Now because $a \cdot b = 0$, then $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$, and so $(a^{-1} \cdot a) \cdot b = 0$, then $1 \cdot b = 0$, so $b = 0$.

□

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 statements 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.

We write $a > b$ if $b < a$, we write $a \leq b$ if $[a < b$ or $a = b]$, and we write $a \geq b$ if $b \leq a$.

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

- $(O1)$: If $a, b, c \in F$ such that $a < b$, then $a + c < b + c$.
- $(O2)$: If $a, b, c \in F$ such that $a < b$ and $0 < c$, then $a \cdot c < b \cdot c$.

5 Lecture 5: Ordered Field

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 $a \cdot c > b \cdot c$.
3. if $a \in F \backslash \{0\}$, 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. ($\Rightarrow$): assume $a > 0$, then $a + (-a) > 0 + (-a)$, so $0 > -a$.

($\Leftarrow$): assume $-a < 0$, then $-a + a < 0 + a$, then $0 < a$.

2. Assume $a < b$ and $c < 0$, then $-c > 0$, so $a \cdot (-c) < b \cdot (-c)$, which means $-a \cdot c < -b \cdot c$. Therefore, $-ac + (ac + bc) < -bc + (ac + bc)$. We then see $(-ac + ac) + bc < -bc + (bc + ac)$, so $0 + bc < (-bc + bc) + ac$, and so $bc < 0 + ac$, which means $bc < ac$.

3. By trichotomy, exactly one of the following holds:
   - if $a > 0$, then $a \cdot a > 0 \cdot a$, so $a^2 > 0$.
   - if $a < 0$, then $a \cdot a > 0 \cdot a$, so $a^2 > 0$.

4. First we show that if $a > 0$ then $a^{-1} > 0$. Let us argue by contradiction. Assume $\exists a \in F$ such that $a > 0$ but $a^{-1} \leq 0$. Note $a^{-1} \neq 0$ since a^{-1} has a multiplicative inverse a. Since $a > 0$ and $a^{-1} < 0$, then $a \cdot a^{-1} < 0$, so $1 < 0$. This contradicts the previous part. So if $a > 0$, then $a^{-1} > 0$. Because $0 < a < b$, then $0 \cdot (a^{-1} \cdot b^{-1}) < a \cdot (a^{-1} \cdot b^{-1}) < b \cdot (a^{-1} \cdot b^{-1})$, and so $0 < (a \cdot a^{-1}) \cdot b^{-1} < b \cdot (b^{-1} \cdot a^{-1})$, therefore $0 < 1 \cdot b^{-1} < (b \cdot b^{-1}) \cdot a^{-1}$. Then we have $0 < b^{-1} < 1 \cdot a^{-1}$, therefore $0 < b^{-1} < a^{-1}$.

□

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:
   - $(O1')$: For every $a \in F$, one and only one of the following statements holds: $a \in P$, or $a = 0$, or $-a \in P$.
   - $(O2')$: If $a, b \in P$, then $a + b \in P$, and $a \cdot b \in P$.

Proof. Let us show that (1) $\Rightarrow$ (2). Define $P = \{a \in F : a > 0\}$. Let us check $(O1')$. Fix $a \in F$. By trichotomy for the order relation on F, we get that exactly one of the following statements is true: $a > 0$, which implies $a \in P$, or $a = 0$, or $a < 0$, which implies $-a > 0$, so $-a \in P$. We can now check $(O2')$. Fix $a, b \in P$. Because $a \in P$, then $a > 0$, and similarly $b > 0$. Therefore, $a + b > 0 + b = b > 0$, so $a + b \in P$. Also, we know $a \cdot b > 0 \cdot b = 0$, so $a \cdot b \in P$.

We now show that (2) $\Rightarrow$ (1). For $a, b \in F$, we write $a < b$ if $b - a \in P$. Let us check that this is an order relation.

Trichotomy: fix $a, b \in F$. By $(O1')$, exactly one of the following hold: $b - a \in P$, which means $a < b$, or $b - a = 0$, which means $a = b$, or $-(b - a) \in P$, which means $a - b \in P$ and so $b < a$.

Transitivity: assume $a, b, c \in F$ such that $a < b$ and $b < c$. Therefore, $b - a \in P$ and $c - b \in P$, so $(b - a) + (c - b) = c - a \in P$, and so $a < c$.

We now check that with this order relation, F is an ordered field. We have to check $(O1)$ and $(O2)$.

$(O1)$: fix $a, b, c \in F$ such that $a < b$, then $b - a \in P$, so $(b + c) - (a + c) \in P$, which means $a + c < b + c$.

$(O2)$: fix $a, b, c \in F$ such that $a < b$ and $0 < c$. Because $a < b$, then $b - a \in P$, and because $0 < c$, then $c - 0 = c \in P$. Therefore, $(b - a) \cdot c \in P$, and so $b \cdot c - a \cdot c \in P$, therefore $a \cdot c < b \cdot c$. □

We extend the order relation $<$ from $\mathbb{Z}$ to the field $(\mathbb{Q}, +, \cdot)$ br writing $\frac{a}{b} > 0$ ikf $a \cdot b > 0$.

Let us show that 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 $c \cdot d > 0$. Now if $(a, b) \sim (c, d)$, then $a \cdot d = b \cdot c$, so $0 < (ad)^2 = (a \cdot b) \cdot (c \cdot d)$.[2] Therefore, $0 < (ab) \cdot (cd)$ and because $0 < ab$, so $cd > 0$, and therefore $\frac{c}{d} > 0$.

Let $P = \{\frac{a}{b} \in \mathbb{Q} : \frac{a}{b} > 0\}$. By the theorem, to prove that $\mathbb{Q}$ is an ordered field, it suffices to show that P satisfies $(O1')$ and $(O2')$, which is left as an exercise to the readers.

6 Lecture 6: Bounds

Definition 6.1. Let $(F, +, \cdot, <)$ be an ordered field. Let $\varnothing \neq A \subseteq F$.

[2] Note that $a \cdot d \neq 0$ since $d \neq 0$ and $a \cdot b > 0$, and so $a \neq 0$.

- We say that A is bounded above if $\exists M \in F$ such that $a \leq M \ \forall a \in A$. 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 $\exists m \in F$ such that $m \leq a \ \forall a \in A$. 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.
- $A = \{1 + \frac{(-1)^n}{n} : n \in \mathbb{N}\}$ is a bounded set. 3 is an upper bound for A, $\frac{3}{2}$ is the maximum of A, 0 is a lower bound for A, and 0 is the minimum of A.
- $A = \{x \in \mathbb{Q} : 0 < x^4 \leq 16\}$ is a bounded set. 2 is the maximum of A, and -2 is the minimum of A.
- $A = \{x \in \mathbb{Q} : x^2 < 2\}$ is a bounded set. 2 is an upper bound for A, and -2 is a lower bound for A. But A does not have a maximum. Indeed, let $x \in A$. We will construct $y \in A$ such that $y > x$.

  Define $y = x + \frac{2-x^2}{2+x}$. Because $x \in A$, then $x \in \mathbb{Q}$, so $2 - x^2, 2 + x \in \mathbb{Q}$. Moreover, because $x \in A$, then $2 + x > 0$, and so $\frac{1}{2+x} \in \mathbb{Q}$. Therefore, $\frac{2-x^2}{2+x} \in \mathbb{Q}$. Hence, we know $y \in \mathbb{Q}$.

  Also note that $2 - x^2 > 0$ since $x \in A$, and $2 + x > 0$ indicates $\frac{1}{2+x} > 0$, so $\frac{2-x^2}{2+x} > 0$. Therefore, $y = x + \frac{2-x^2}{2+x} > x$.

  Let us compute y^2. Note that

$$\begin{aligned} y^2 &= \frac{2x + x^2 + 2 - x^2{}^2}{2 + x} \\ &= \frac{4(x+1)^2}{(2+x)^2} \\ &= \frac{4x^2 + 8x + 4}{x^2 + 4x + 4} \\ &= \frac{2(x^2 + 4x + 4) + 2x^2 - 4}{x^2 + 4x + 4} \\ &= 2 + \frac{2 \cdot (x^- 2)}{(x+2)^2} \\ &< 2. \end{aligned}$$

  Collecting the properties above, we constructed $y \in A$ and $y > x$ as desired.

Exercise 6.3. Show that the maximum and minimum of a set are unique, if they exist.

Definition 6.4. Let $(F, +, \cdot, <)$ be an ordered field. Let $\varnothing \neq A \subseteq F$ 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 6.5. The least upper bound of a set is unique, if it exists.

Proof. Say that a set A, satisfies $\varnothing A \subseteq F$ and is bounded above, admits two least upper bounds L and M. Because L is a least upper bound, then L is an upper bound for A. But because M is a least upper bound for A, we have $M \leq L$. Similarly we conclude that $L \leq M$, and so $L = M$. □

Definition 6.6. Let $(F, +, \cdot, <)$ be an ordered field. Let $\varnothing \neq A \subseteq F$ and assume A is bounded below. We say that l is the greatest lower bound of A if 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.

Exercise 6.7. Show that the greatest lower bound of a set is unique, if it exists.

Definition 6.8. Let $(F, +, \cdot, <)$ be an ordered field. Let $\varnothing \neq S \subseteq F$.

We say that S has the least upper bound property if its satisfies the following: for any non-empty subset A of S that 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: $\forall \varnothing \neq A \subseteq S$ with A bounded below, $\exists \inf(A) \in S$.

Example 6.9. $(\mathbb{Q}, +, \cdot, <)$ is an ordered field. Note that

1. Consider $\varnothing \neq \subseteq \mathbb{Q}$, $\mathbb{N}$ has the least upper bound property. Indeed, if $\varnothing \neq A \subseteq N$, A bounded above, then the largest element in A is the least upper bound of A and $\sup(A) \in \mathbb{N}$. $\mathbb{N}$ also has the greatest lower bound property.

2. Consider $\varnothing \neq \mathbb{Q} \subseteq \mathbb{Q}$, but $\mathbb{Q}$ does not have the least upper bound property. Indeed, $\varnothing \neq A = \{x \in \mathbb{Q} : x \geq 0, x^2 < 2\} \subseteq \mathbb{Q}$. Note that A is bounded above by 2. However, $\sup(A) = \sqrt{2} \notin \mathbb{Q}$.

Proposition 6.10. 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. We will only prove the $(\Rightarrow)$ direction: the opposite direction has a similar proof.

Assume F has the least upper bound property. Let $\varnothing \neq A \subseteq F$ bounded below. We want to show that $\exists \inf(A) \in F$. Because A is bounded below, then $\exists m \in F$ such that $m \leq a$ $\forall a \in A$. Let $B = \{b \in F : b \text{ is a lower bound for } A\}$. Note $B \neq \varnothing$ because $m \in B$, and we know $B \subseteq F$, and B is bounded above (in fact, every element in A is an upper bound for B), and F has the least upper bound property. Therefore, $\exists \sup(B) \in F$.

Claim 6.11. $\sup(B)$ is a lower bound for A.

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

Claim 6.12. If l is a lower bound for A, then $l \leq \sup(B)$.

Subproof. Because l is a lower bound for A, then $l \in B$. Also, because $\sup(B)$ is an upper bound for B, we know $l \leq \sup(B)$. ■

Using the two claims above, we find that $\inf(A) = \sup(B)$. □

7 Lecture 7: Archimedean Property

We present an alternative proof of the previous proposition.

Remark 7.1 (Alternative Proof)**.** Let $\varnothing \neq A \subseteq F$ be such that A is bounded below. Let $B = \{-a : a \in A\}$. Note $B \subseteq F$ by (A5), and $B \neq \varnothing$ because $A \neq \varnothing$, and B Is bounded above: indeed, if m is a lower bound for A, then $-m$ is an upper bound for B.[3] Also note that F has the least upper bound property. Collecting these properties above, we know $\exists \sup(B) \in F$. The reader can easily show that $-\sup(B) = \inf(A) \in F$.

Theorem 7.2. 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. (We will prove this statement in Theorem 8.4.) 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 exist a bijection $\varphi : \mathbb{R} \to F$ such that

(i) $\varphi(x + y) = \varphi(x) + \varphi(y)$.

(ii) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

(iii) if $x < y$, then $\varphi(x) < \varphi(y)$.

Theorem 7.3. $\mathbb{R}$ has the Archimedean property, that is, $\forall x \in \mathbb{R}$, $\exists n \in \mathbb{N}$ such that $x < n$.

Proof. We argue by contradiction. Assume $\exists x_0 \in \mathbb{R}$ such that $x_0 \geq n \ \forall n \in \mathbb{N}$. Then we know $\varnothing \neq \mathbb{N} \subseteq \mathbb{R}$, $\mathbb{N}$ is bounded above by x_0, and $\mathbb{R}$ has the least upper bound property. Therefore, $\exists L = \sup(\mathbb{N}) \in \mathbb{R}$.

Now we know $L = \sup(\mathbb{N})$ and $L - 1 < L$, so $L - 1$ is not an upper bound for $\mathbb{N}$. That means $\exists n_0 \in \mathbb{N}$ such that $n_0 > L - 1$, so $\sup(\mathbb{N}) = L < n_) + 1 \in \mathbb{N}$. We therefore have a contradiction. □

Remark 7.4. $\mathbb{Q}$ has the Archimedean property. If $r \in \mathbb{Q}$ is such that $r \leq 0$, then choose $n = 1$. If $r \in \mathbb{Q}$ is such that $r > 0$, then write $r = \frac{p}{q}$ for $p, q \in \mathbb{N}$, and we can choose $n = p+1$ since $\frac{p}{q} < p + 1$.

Corollary 7.5. If $a, b \in \mathbb{R}$ are such that $a > 0, b > 0$, then there exists $n \in \mathbb{N}$ such that $n \cdot a > b$.

[3] Note that $m \leq a \ \forall a \in A$ implies $-m \geq -a \ \forall a \in A$.

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

Corollary 7.6. If $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \varepsilon$.

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

Lemma 7.7. For any $a \in \mathbb{R}$ there exists $N \in \mathbb{Z}$ such that $N \leq a < N + 1$.

Proof. If $a = 0$, then we can just take $N = 0$.

If $a > 0$. Consider $A = \{n \in \mathbb{Z} : n \leq a\} \subseteq \mathbb{R}$. Obviously $A \neq \varnothing$, as $0 \in A$. We also know A is bounded above by a, and $\mathbb{R}$ has the least upper bound property. Therefore, there exists $L = \sup(A) \in \mathbb{R}$. Now consider $L - 1 < L = \sup(A)$, then $L - 1$ is not an upper bound for A, so there exists $N \in A$ such that $L - 1 < N$, and so $L < N + 1$. But $L = \sup(A)$, so $N + 1 \notin A$. Therefore, $N \in A$, so $N \leq a$, and as $N + 1 \notin A$, then $N + 1 > a$. Therefore, $N \leq a < N + 1$.

If $a < 0$, then $-a > 0$. Then by the case $a > 0$, $\exists n \in \mathbb{Z}$ such that $n \leq -a < n + 1$, 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 $N \leq a < N + 1$. Either way, we conclude the proof. □

Definition 7.8 (Dense)**.** 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 7.9. $\mathbb{Q}$ is dense in $\mathbb{R}$.

Proof. Let $x, y \in \mathbb{R}$ such that $x < y$. Since $y - x > 0$, by Corollary 7.6, $\exists n \in \mathbb{N}$ such that $\frac{1}{n} < y - x$, so $\frac{1}{n} + x < y$.

Consider $nx \in \mathbb{R}$. By Lemma 7.7, $\exists m \in \mathbb{Z}$ such that $m \leq nx < m + 1$, so $\frac{m}{n} \leq x < \frac{m+1}{n}$. Therefore,

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

□

8 Lecture 8: Construction of real numbers

Remark 8.1. For any two rational numbers $r_1, r_2 \in \mathbb{Q}$ such that $r_1 < r_2$, there exists $s \in \mathbb{Q}$ such that $r_1 < s < r_2$. Indeed, if $r_1 < 0 < r_2$, then we may take $s = 0 \in \mathbb{Q}$. Assume $0 < r_1 < r_2$, write $r_1 = \frac{a}{b}$ and $r_2 = \frac{c}{d}$ with $a, b, c, d \in \mathbb{N}$. Take $s = \frac{ad+bc}{2bd} \in \mathbb{Q}$. Note $r_1 < s < r_2$:

$$r_1 < s \iff \frac{a}{b} < \frac{ad+bc}{2bd} \iff 2ad < ad + bc \iff ad < bc \iff \frac{a}{b} < \frac{c}{d} \iff r_1 < r_2.$$

We leave the construction of s in the remaining cases as an exercise to the readers.

Lemma 8.2. $\mathbb{R}\backslash\mathbb{Q}$ is dense in $\mathbb{R}$.

Proof. Let $x, y \in \mathbb{R}$ such that $x < y$, then $x + \sqrt{2} < y + \sqrt{2}$. Because we know $\mathbb{Q}$ is dense in $\mathbb{R}$, we know $\exists q \in \mathbb{Q}$ such that $x + \sqrt{2} < q < y + \sqrt{2}$, so $x < q - \sqrt{2} < y$. It now suffices to prove the following claim.

Claim 8.3. $q - \sqrt{2} \in \mathbb{R} \backslash \mathbb{Q}$.

Subproof. Otherwise, $\exists r \in \mathbb{Q}$ such that $q - \sqrt{2} = r$, so $\sqrt{2} = q - r \in \mathbb{Q}$, contradiction. ■

□

Theorem 8.4. There exists an ordered field with the least upper bound property. We denote it $\mathbb{R}$ and call it the set of real numbers. $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield.

We will construct an ordered field with the least upper bound property using Dedekind cuts.