Math 131AH lecture notes

Nakul Khambhati

May 24, 2023

Contents

1 Introduction

1.1 Propositional logic

We can define the following operations on propositions: $\neg, \wedge, \vee, \implies, \iff$ via truth tables. They correspond to `NOT, AND, OR, IMPLIES, EQUIVALENCE` respectively. Now I will be using some shortcuts like

Example 1.1.1. $P \implies Q$

P	Q	P $\implies$ Q
0	0	1
0	1	1
1	0	0
1	1	1

$P \implies Q$ is only false when P is true and Q is false. In other words, $P \implies Q$ is true when P is false or Q is true. Therefore, we can write $P \implies Q = \neg P \vee Q$.

De Morgan's laws tell us how to distribute negation over an expression.

1. $\neg(P \wedge Q) = \neg P \vee \neg Q$
2. $\neg(P \vee Q) = \neg P \wedge \neg Q$

Remark. As a corollary, we can write $\wedge$ using only $\neg$ and $\vee$: $P \wedge Q = \neg(\neg P \vee \neg Q)$.

Proposition 1.1.1. *Implications are not associative.*

Proof. Let P, Q, R be propositions. Consider $(P \implies Q) \implies R$ and $P \implies (Q \implies R)$. For $(P, Q, R) = (0, 1, 0)$, the former is 0 while the latter is 1. □

Definition 1.1.1. A predicate is a proposition that depends on a parameter. For example, $P(x)$ where the truth value is dependent on x.

We introduce the universal quantifier $\forall x : P(x)$ and the existential quantifier $\exists x : P(x)$. The former is true if $P(x)$ is true over the entire domain X whereas the latter is true if there exists some $x_0 \in X$ such that $P(x_0)$ is true.

Example 1.1.2. 1. $\neg(\forall x : P(x)) = \exists x : \neg P(x)$

2. $\neg(\exists x : P(x)) = \forall x : \neg P(x)$

The two examples above are very important while proving implications. Some concrete examples are:

1. $\neg(\forall n \in \mathbb{N} : 2|n^2 \implies 2|n) = \exists n \in \mathbb{N} : 2|n^2 \wedge 2 \nmid n$
2. $\neg(\forall \epsilon > 0\ \exists N \in \mathbb{N}\ \forall n \geq N : |a_n - a) < \epsilon = \exists \epsilon > 0\ \forall N \in \mathbb{N}\ \exists n \geq N : |a_n - a| \geq \epsilon$

Lemma 1.1. $\forall x \forall y : P(x, y) = \forall y \forall x : P(x, y)$

Lemma 1.2 (proof by contraposition)**.** $P \implies Q = \neg Q \implies \neg P$

Lemma 1.3 (proof by contradiction)**.** $P \implies Q = \neg(\neg Q \wedge P)$

1.2 Set theory

Definition 1.2.1 (naive set theory)**.** Formally, we define all objects to be sets. We use capital letters $A, B, C \ldots$ to denote sets. $A \in B := A$ is an element of B. The negation is $A \notin B := \neg(A \in B)$.

We now need a tool to buid more sets out of existing sets.

Axiom 1.2.1 (comprehension principle)**.** *For every logical proposition $P(X)$, $\{X : P(X)\}$ is a set. It is the set of all X such that $P(X) =$ `TRUE`.*

We can then construct the following sets:

1. $\emptyset := \{X : \texttt{FALSE}\}$ is the empty set
2. $A^c := \{X : X \notin A\}$ complement of A
3. $A \cup B := \{X : X \in A \vee X \in B\}$ union
4. $A \cap B := \{X : X \in A \wedge X \in B\}$ intersection
5. $A \setminus B := \{X : X \in A \wedge X \notin B\}$ set difference
6. $A \Delta B := (A \setminus B) \cup (B \setminus A)$ symmetric difference

Moreover, we can define the following:

1. singleton: $\{A\} := \{X : X = A\} \quad A = B := \forall X : X \in A \iff X \in B$
2. pairset: $\{A, B\} := \{X : X = A \vee X = B\}$
3. general union: $\bigcup A := \{X : (\exists B \in A : X \in B)\}$
4. power set: $\mathcal{P}(A) := \{X : X \subset A\}$, $A \subset B := \forall X : X \in A \implies X \in B$
5. infinite set: $I := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \cdots\}$

Theorem 1.4 (Russel, 1902)**.** *Assuming the comprehension principle, $\{X : X \notin X\}$ is not a set i.e. the comprehension principle fails.*

Proof. Assume $A = \{X : X \notin X\}$ is a set. Then $A \in A \implies A \notin A$ and $A \notin A \implies A \in A$ so A cannot be a set $\Rightarrow\!\Leftarrow$ □

Corollary 1.4.1. *The comprehension principle is inconsistent.*

To get around this, we replace the comprehension principle with Zermelo's separation axiom.

Axiom 1.2.2. *(separation axiom) For every set B and logical proposition $P(X)$, $\{X : X \in B \wedge P(X)\}$ is a set. For brevity, we will write it as $\{X \in B : P(X)\}$.*

Remark. It is then easy to verify that Russel's paradox disappears. If we define $A := \{X \in B : X \notin X\}$ then $B \notin A$.

1.3 Zermelo's axioms

1. **Axiom of Extensionality**: $\forall A, B : A = B \iff \forall x : x \in A \iff x \in B$
2. **Axiom of Separation**: $\forall A \forall P(x) : \{X \in A : P(X)\}$ is a set.
3. **Emptyset Axiom**: $\exists \emptyset : \forall X : X \notin \emptyset$
4. **Pairset Axiom**: $\forall X, Y \exists A \forall Z : Z \in A \iff (Z = X \vee Z = Y)$. It follows from (1) that A is unique and we denote it as $\{X, Y\}$
5. **Axiom of Union**: $\forall A \exists B \forall X : X \in B \iff (\exists C \in B : X \in C)$. Again, by uniqueness, we will denote it as $\bigcup A$.
6. **Powerset Axiom**: $\forall A \exists B \forall C : C \subset A \iff C \in B$, denoted $\mathcal{P}(X)$.
7. **Axiom of Infinity**: $\exists I : \emptyset \in I \wedge (\forall X : X \in I \Rightarrow \{X\} \in I)$. We cannot claim that this set is unique since the elements of I are not explicitly listed. In fact, it is not.

We will also see the **Axiom of Replacement** and the **Axiom of Choice** appear later.

Remark. Using the **Axiom of Union** we can also define the intersection $\bigcap A = \{x \in \bigcup A : (\forall B \in A : X \in B)\}$.

Definition 1.3.1 (caretesian product)**.** Given sets A, B define $A \times B = \{(x, y) \in \mathcal{P}(\mathcal{P}(A \cup B)) : x \in A \wedge y \in B\}$ where we have used the notation $(x, y) := \{\{x\}, \{x, y\}\}$

Lemma 1.5. $\forall A, B \; \forall x, x' \in A \; \forall y, y' \in B : (x, y) = (x', y') \Rightarrow (x = x' \wedge y = y')$

Remark. If we have to iterate this process over multiple sets, there is an arbitrary choice involved. For example, we can take the caretesian product of A, B, C as $(A \times B) \times C$ or $A \times (B \times C)$. Upon expanding, we get different expressions. It would be nice if, in some sense, these would be equal. This motivates us to introduce the concept of and functions and relations.

2 Functions and relations

We start with relations and then construct functions using the concept of a relation.

2.1 Relations

Definition 2.1.1 (relation)**.** A relation on A, B is a set $R \subset A \times B$. We introduce the notation $xRy := (x, y) \in R$. When $B = A$ we call it a relation on A.

Example 2.1.1.

1. Subset $\subset$ on $\mathcal{P}(A) : R = \{(A, B) \in \mathcal{P}(C) \times \mathcal{P}(C) : A \subset B\}$
2. Equality $=$ on $A : R = \{(x, x) \in A : \texttt{TRUE}\}$

Definition 2.1.2 (partial order)**.** We say that $R \subset A \times A$ is:

1. Reflexive if $\forall x \in A : xRx$
2. Antisymmetric if $\forall x, y \in A : (xRy \wedge yRx) \Rightarrow x = y$
3. Transitive if $\forall x, y, z \in A : (xRy \wedge yRz) \Rightarrow xRz$

If (1), (2) and (3) are true, then we call R a partial order (for reasons that will be clear later).

Definition 2.1.3 (equivalence)**.** we say $R \subset A \times A$ is (4) symmetric if $\forall x, y \in A : xRy \iff yRx$. If (1), (4) and (3) are true then we call R an equivalence and denote xRy as $x \sim y$.

Definition 2.1.4 (equivalence class)**.** We define the equivalence class of $x \in A$ as $[x] := \{y \in A : y \sim x\}$

Lemma 2.1. $\forall x, y \in A : [x] \cap [y] = \emptyset \vee [x] = [y]$

2.2 Functions

Definition 2.2.1. (domain, range, composition, inverse) Given $R \subset A \times B$:

1. $\mathrm{Dom}(R) = \{x \in A : (\exists y \in B : xRy)\}$
2. $\mathrm{Ran}(R) = \{y \in B : (\exists x \in A : xRy)\}$
3. Given $R \subset A \times B, S \subset B \times C$, we define $RS = \{(x, z) \in A \times C : (\exists y \in B : xRy \wedge yRz)\}$ and $R^{-1} := \{(y, x) \in B \times A : xRy\}$

Definition 2.2.2 (function)**.** A relation $R \subset A \times B$ is a function if $\forall x \in A \forall y, z \in B : (xRy \wedge xRz) \Rightarrow y = z$

We have defined a function in such a way that we can introduce the notation $f(x)$ for the unique (if it exists) $y \in B$ such that xRy.

Definition 2.2.3 (image, preimage)**.** Let $f : A \to B$ be a function.

1. Let $C \subset A$. We define the image of C as $f(C) := \{y \in B : (\exists x \in C : f(x) = y)\}$
2. Let $D \subset B$. We define the preimage of D as $f^{-1}(D) := \{x \in A : (\exists y \in D : f(x) = y)\}$

Remark. The inverse of a function always exists as a relation but, in general, it will not be a function because of the asymmetry of the definition of a function.

Definition 2.2.4 (bijection)**.** A function $f : A \to B$ is called:

1. Injective if $Dom(f) = A \wedge \forall x, y \in A : f(x) = f(y) \Rightarrow x = y$.
2. Surjective if $Ran(f) = B$.
3. Bijective if it is both injective and surjective.

Definition 2.2.5. Sets A, B are said to be equinumerous if $\exists f : A \to B$ a bijection.

Definition 2.2.6. A set A is said to be Dedekind infinite if $\exists f : A \to A$ injective such that $Ran(f) \neq A$. This is equivalent to there being a bijection from A onto a proper subset of itself.

2.3 General cartesian product

Definition 2.3.1. Let A, I be sets. A collection $\{A_\alpha : \alpha \in I\}$ of subsets A indexed by I is $Ran(\phi)$ for a function $\phi : I \to \mathcal{P}(A)$ with $Dom(\phi) = I$. Then, we define $A_\alpha := \phi(\alpha)$.

Definition 2.3.2. Given a collection $\{A_\alpha : \alpha \in I\}$ we define the general caretesian product over the collection as a set of functions

$$\bigtimes A_\alpha := \left\{ f \in \mathcal{P}(I \times \bigcup_{\alpha \in I} A_\alpha) : f \text{ a function} \wedge Dom(f) = I \wedge (\forall \alpha \in I : f(\alpha) \in A_\alpha) \right\}$$

In other words, something is an element of the Cartesian product of a family of sets, indexed by I, if and only if it is a family, also indexed by I, whose i-th term, a_i is an element of the i-th set, A_i for every index point $i \in I$.

Consider the special case where $\forall \alpha \in I : A_\alpha = A$
$A^I := \{f \in \mathcal{P}(I \times A) : f \text{ a function} \wedge Dom(f) = I\}$ called the cartesian power of A to the I.

Example 2.3.1. $\mathbb{R}^\mathbb{N}$ = set of real-valued sequences. $\mathbb{R}^\mathbb{R}$ = set of functions $\mathbb{R} \to \mathbb{R}$ with full domain.

Remark. It's clear that for non-empty sets A, B, the cartesian product $A \times B$ is non-empty. But this argument cannot be generalized to the generalized cartesian product. This is why we introduce the next axiom.

Axiom of Choice: Let I be a nonempty set and $\{A_\alpha : \alpha \in I\}$ be a collection such that $\forall \alpha \in I : A_\alpha \neq \emptyset$. Then $\exists f \in \mathcal{P}(I \times \bigcup_{\alpha \in I} A_\alpha) : f$ a function $\wedge$ $Dom(f) = I \wedge (\forall \alpha \in I : f(\alpha) \in A_\alpha)$. In other words, if each set in the collection is nonempty, then the generalized cartesian product is nonempty.

Remark. The Axiom of Choice (AC) is called such because $f(\alpha)$ is a choice of a representation for A_α.

If each A_α is a singleton, then can we demonstrate that $\bigtimes_{\alpha \in I} A_\alpha$ is nonempty without using the axiom of choice?

Lemma 2.2. *Let $A_\alpha : \alpha \in I$ be a colletion such that $\forall \alpha \in I\ \exists x_\alpha : A_\alpha = \{x_\alpha\}$. Then $\exists f : I \to A$ such that $Dom(f) = I \wedge \forall \alpha \in I : f(\alpha) \in A_\alpha$ (without using AC).*

Proof. Consider $\mathcal{F} = \{F \subset I \times A : \forall \alpha \in Dom(F) \forall x \in A : \alpha F x \Rightarrow x \in A_\alpha\}$. Note that each $F \in \mathcal{F}$ is just the graph of a function $f : \forall \alpha \in Dom(f) : f(\alpha) \in A_\alpha$.

Every F in this family satisfies all but one of the desired properties of our function. We need to construct a function with full domain $Dom(f) = I$. We can fulfil this by setting $F = \bigcup \mathcal{F}$. Then, $F \in \mathcal{F}$ since all $f, g \in \bigcup \mathcal{F}$ must coincide on common $\alpha \in I$. From here, it is easy to argue that $Dom(F) = I$. Let $\alpha \in I$. Then $\{(\alpha, x) : x \in A_\alpha\} \in \mathcal{F}$ so $\{(\alpha, x) : x \in A_\alpha\} \in F$ so $\alpha \in Dom(F)$. Therefore, $I \subset Dom(F)$ and $Dom(F) = I$. □

Remark. A similar arguement can be used to show that AC is equivalent to $\exists \phi : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ such that $\forall B \in \mathcal{P}(A) \setminus \{\emptyset\} : \phi(B) \in B$.

3 Naturals

3.1 Definitions

Definition 3.1.1. A system of natruals is a triplet $(\mathbb{N}, 0, S)$ that satisfy the Peano Axioms:

(P1) N is a set, $0 \in \mathbb{N}$

(P2) $S : \mathbb{N} \to \mathbb{N}$ is a function with $Dom(S) = \mathbb{N}$

(P3) $\forall n \in \mathbb{N} : S(n) \neq 0$ i.e. $0 \notin Ran(S)$

(P4) S is injective

(P5) $\forall A \subset \mathbb{N} : S(A) \subset A \Rightarrow A = \mathbb{N}$

3.2 Principle of induction

Let's discuss some consequences of (P5).

Lemma 3.1. *Let $(N, 0, S)$ be a system of naturals. Then $Ran(S) = \mathbb{N} \setminus \{0\}$.*

Proof. Let $A = \{0\} \cup S(\mathbb{N})$. Then $0 \in A$ by construction and $S(A) \subset S(\mathbb{N}) \subset A$ so $A = \mathbb{N}$. Since $0 \notin Ran(S)$, $S(\mathbb{N}) = \mathbb{N} \setminus \{0\}$ □

Lemma 3.2 (proof by induction)**.** *Let $\{P_n : n \in \mathbb{N}\}$ be a collection of logication propositions such that P_0 is `TRUE` and $P_n \Rightarrow P_{S(n)}$.*

Proof. Let $A := \{n \in \mathbb{N} : P_n \ \texttt{TRUE}\}$. Then (1) $\Rightarrow 0 \in A$ and (2) $\Rightarrow (\forall n \in \mathbb{N} : n \in A \Rightarrow S(n) \in A)$. So $S(A) \subset A$. Then, by (P5) $A = \mathbb{N}$. □

3.3 Existence of naturals

Theorem 3.3. *Assuming Zermelo's axioms, there is at least one system of naturals i.e. a triple $\mathbb{N}, 0, S$ satisfying (P1)-(P5).*

Proof. By the Axiom of Infinity, $\exists I : \emptyset \in I \wedge (X \in I \Rightarrow \{X\} \in I)$. Intuitively, it contains a unique "minimal" element and is closed under a certain map. If we define $0 = \emptyset, S : X \to \{X\}$ then S is injective by the Axiom of Extensionality and $\emptyset \notin Ran(S)$ as there is no set contained within the emptyset. So, I satisfies (P1)-(P4). However, we run into some difficulty trying to prove (P5). Informally, I is too large to satisfy the principle of induction. Instead, consider $K = \{J \subset I : \emptyset \in J \wedge (\forall X \in J : \{X\} \in J)\}$. Clearly, $\emptyset \in K$ so it's non-empty. Define $\mathbb{N} := \bigcap K$. It can be verified that (P1)-(P4) still hold. Want to show that (P5) also holds. Let $A \subset \mathbb{N} : \emptyset \in A \wedge S(A) \subset A$ i.e. $\forall X \in A : \{X\} \in A$. In particular, $A \in K$ so $\mathbb{N} = \bigcap K \subset A$. So, $\mathbb{N} = A$. Therefore, (P5) is satisfied. □

Remark. Informally, $\mathbb{N} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \cdots\}$. $\mathbb{N}$ is Dedekind infinite (via $S : \mathbb{N} \to \mathbb{N}$).

3.4 Uniqueness of naturals

Now that we have exhibited that there exists a system satisfying the conditions we desire, we want to determine the uniqueness of such a configuration. First, we must define uniquenss.

Definition 3.4.1. We say that two systems of naturals $\mathbb{N}, 0, S$ and $\mathbb{N}', 0', S'$ are unique if there exists a function $\phi : \mathbb{N} \to \mathbb{N}'$ such that:

1. ϕ is a bijection
2. $\phi(0) = 0'$
3. ϕ commutes with S: $\phi(S(n)) = S'(\phi(n)) \; \forall n \in \mathbb{N}$

Theorem 3.4 (recursive construction)**.** *Let $(\mathbb{N}, 0, S)$ be a system of naturals, E a set and $h : E \to E$ a function. Then $\forall a \in E \; \exists \{x_n : n \in \mathbb{N}\} \subset E : x_0 = a \wedge \forall n \in \mathbb{N} : x_{S(n)} = h(x_n)$.*

Proof. Let $a \in E$. Consider the family of functions $\mathcal{F}$ where
$\mathcal{F} = \{f \subset \mathbb{N} \times E : 0 \in Dom(f) \wedge f(0) = a \wedge f(S(n)) = h(f(n))\}$
The motivation here is that this family consists of all functions that satisfy our desired properties except for the fact that $Dom(f) = \mathbb{N}$. To do this, let's take the union of these functions, verify that it is still a function and then verify that it has full domain.

1. $\{(0, a) \in \mathcal{F}\}$ so $\mathcal{F}$ is nonempty.
2. We need to show that $\forall f, g \in \mathcal{F}, \forall n \in Dom(f) \cap Dom(g) : f(n) = g(n)$. Fix $f, g \in \mathcal{F}$. We will first consider the subset $A \subset \mathbb{N}$ where $f(n) = g(n)$. Clearly $0 \in A$. Assume $n \in A$. Then, $f(n) = g(n)$. If $S(n) \notin Dom(f) \cap Dom(g)$ then $S(n) \in A$ vaccuously. If $S(n) \in Dom(f) \cap Dom(g)$ then, $f(S(n) = h(f(n)) = h(g(n)) = g(S(n)))$. Therefore, $S(n) \in A$. By (P5) $A = \mathbb{N}$.

3. Now we can take the union $\tilde{f} = \bigcup \mathcal{F}$ and be sure that it is a function. Furthermore, $\tilde{f} \in \mathcal{F}$ which can be easily verified using arguments of the form: $\exists f$ such that … and $\tilde{f}(n) = f(n)$.
4. Lastly, we show $Dom(\tilde{f}) = \mathbb{N}$. Let $A = Dom(\tilde{f})$. Then $0 \in A$. Let $n \in A$. Assume, by contradiction, that $S(n) \notin A$. Let $f \in \mathcal{F}$ such that $n \in Dom(f)$. Also, $S(n) \notin Dom(f)$. So, we can extend f to g in a way that it still lives in the family $\mathcal{F}$. Let $g(m) = f(m)$ if $m \in Dom(f)$ and $= h(f(n))$ if $m = S(n)$. But then, $g \in \mathcal{F}$ so $S(n) \in Dom(g) \subset Dom(\tilde{f}) = A$. This results in a contradiction so $S(n) \in A$. Again, by (P5), $A = \mathbb{N}$. $S_{\mathbb{Z}} = a + 1$.

By setting $x_n = \tilde{f}(n)$, this obeys the required relation. □

Lemma 3.5. *Any two collections* $\{x_n : n \in \mathbb{N}\}$ *and* $\{x'_n : n \in \mathbb{N}\}$ *satisfying the above are equal.*

Proof. Let $B = \{n \in \mathbb{N} : x_n = x'_n\}$. Clearly $0 \in B$. Assume $n \in B$. Then, $x_{S(n)} = h(x_n) = h(x'_n) = x'_{S(n)}$. So, $S(n) \in B$. By (P5), $B = \mathbb{N}$. □

Theorem 3.6. *Any two systems of naturals* $(\mathbb{N}, 0, S)$ *and* $(\mathbb{N}', 0', S')$ *are unique.*

Proof. We need to construct $\phi : \mathbb{N} \to \mathbb{N}'$ as defined earlier and show that it satisfies the required properties. We will do this by applying recursive construction with the set $E = \mathbb{N}', a = 0', \phi = S'$. Immediately, $0' = \phi(0)$ and $\phi \circ S = S' \circ \phi$. Let us show that the map is bijective. Define $A = Ran(\phi)$. Then $0' \in \mathbb{N}'$ by construction. $S'(A) = S' \circ \phi(\mathbb{N}) = \phi \circ S(\mathbb{N}) \subset \phi(\mathbb{N}) = A$. By (P5), $A = \mathbb{N}'$. So the map is surjective. Now set $A = \{n \in \mathbb{N} : (\forall m \in \mathbb{N} : \phi(m) = \phi(n) \Rightarrow m = n)\}$. In a similar way, we can show that $0 \in A$ and $n \in A \Rightarrow S(n) \in A$. By (P5) $A = \mathbb{N}$ so ϕ is injective. □

3.5 Addition of naturals

Define $m+n$ recursively by $m+0 = m$ and $\forall n \in \mathbb{N} : m + S(n) = S(m+n)$. We wish to check whether $m+n = n+m$ and whether $m+(n+k) = (m+n)+k$ i.e. whether additional of naturals is commutative and associative.

We will define addition using the theorem of recursive construction. For this, let's set $E = \mathbb{N}, a = m \in \mathbb{N}$ and $h = S$. By the theorem, $\exists \{x_n : n \in \mathbb{N}\}$ such that $x_n = m$ and $\forall n \in \mathbb{N} : x_{S(n)} = S(x_n)$. Now we introduce the notation $m + n := x_n$. So, $m + 0 = m \wedge S(n) = S(m+n)$.

Lemma 3.7. $\forall m \in \mathbb{N} : 0 + m = m$.

Proof. The base case P_0 is trivial. Assume P_m is true. Then, $0 + S(m) = S(0+m) = S(m)$ so P_{m+1} is true. By induction, P_m is true for all $m \in \mathbb{N}$. □

Lemma 3.8. $\forall m, n \in \mathbb{N} : m + S(n) = S(m) + n$.

Proof. Fix $m \in \mathbb{N}$ and induct on n. P_0 is true as $m+S(0) = S(m+0) = S(m)+0$. Assume that P_n is true. Consider $m+S(S(n)) = S(m+S(n)) = S(S(m)+n) = S(m) + S(n)$. So, P_{n+1} is true. By induction, this is true for $n \in \mathbb{N}$. □

Theorem 3.9. *Addition of naturals $\mathbb{N}$ is commutative.*

Proof. We need to prove that $\forall m, n \in \mathbb{N} : m + n = n + m$. Fix $m \in \mathbb{N}$ and induct on n. For $n = 0$, we have $m + 0 = 0 + m$ by Lemma 3.7. Now, assume P_n. Then, $m + S(n) = S(m) + n = S(m + n) = S(n + m) = S(n) + m$. This proves P_{n+1}. By induction, this is true for all $n \in \mathbb{N}$.

□

Theorem 3.10. *Addition of naturals N is associative.*

Proof. In HW2. □

Proposition 3.5.1. *Addition by $k \in \mathbb{N}$ is injective as a function. $\forall m, n \in \mathbb{N} : k + m = k + n \Rightarrow m = n$.*

Proof. The statement is trivial for $k = 0$. Assume $P(k)$. Let $S(k) + m = S(k) + n$. Then, $S(k + m) = S(k + n) \Rightarrow S(m) = S(n)$. By injectivity of S, we get $m = n$. By induction, this proves the statement for all $k \in \mathbb{N}$. □

3.6 Ordering of naturals

Definition 3.6.1. We say $m \leq n$ if $\exists k \in \mathbb{N} : n = m + k$.

Lemma 3.11. *The relation $\leq$ is reflexive, antisymmetric and transitive. Therefore, it is a partial order.*

Proof.
1. Clearly $m \leq m$ since $m = m + 0$.
2. Assume $m \leq n$ and $n \leq m$. Then $\exists l, k \in \mathbb{N} : m = n + k, n = m + l$. Therefore, by associativity, $m = m + l + k$. By injectivity, $0 = k + l$ so $k = l = 0$ and $m = n$.
3. Assume $m \leq n$ and $n \leq k$. Therefore $n = m + a, k = n + b$. Then, $k = m + (a + b)$ so $m \leq k$.

□

Now we will show that the naturals are totally ordered. This lets us visualize it as a discrete number line.

Lemma 3.12. *$\leq$ is a total order i.e. $\forall m, n \in \mathbb{N} : m \leq n \vee n \leq m$.*

Proof. We prove this by induction on m. $P_m : \forall n \in \mathbb{N} : m \leq n \vee n \leq m$. P_0 is true. We use cases to prove $P_m \Rightarrow P_{m+1}$. □

In the next class we will define multiplication recursively. We can prove the following propositions, some of them will come in the exams.

1. $\forall m, n \in \mathbb{N} : mn = nm$
2. $\forall m, n, k \in \mathbb{N} : m(nk) = (mn)k$
3. $\forall m, n, k \in \mathbb{N} : (m + n)k = mk + nk$
4. Define $1 = S(0)$. Then $\forall m \in \mathbb{N} : 0m = 0 \wedge 1m = m$.
5. $\forall m, n, k \in \mathbb{N} : k \neq 0 \wedge km = kn \Rightarrow m = n$.

3.7 Multiplication of naturals

Definition 3.7.1. We also define multiplication on naturals as $0m = 0$ and $S(n)m = nm + m$.

Definition 3.7.2. We define $1 = S(0)$ therefore $S(n) = S(n+0) = n + S(0) = n + 1$.

Definition 3.7.3. $\forall m.n \in \mathbb{N}$ we define m^n recursively as: $m^0 = 1$ and $m^{n+1} = m \cdot m^n$. We call m^n the n^{th} power of m.

Lemma 3.13. $\forall m \in \mathbb{N} \setminus \{0\}$ $\forall r, s \in \mathbb{N} : m^{r+s} = m^r m^s$ *and* $m^r s = (m^r)^s$.

Definition 3.7.4. $0! = 1$ and $\forall n \in \mathbb{N} : S(n)! = S(n)n!$ called n factorial.

4 Integers

4.1 Construction of integers

Recall that the function "add k" is injective i.e. $\forall m, n, k \in \mathbb{N} : m+k = n+k \Rightarrow m = n$. However, it is not surjective.

We will achieve this by *extending* the set $\mathbb{N}$ to a set $\mathbb{Z}$. Intuitively, we think of Z as the set of difference of naturals. Define $\overset{+}{\sim}$ on $\mathbb{N} \times \mathbb{N}$ as $(m, n) \overset{+}{\sim} (m', n') := m + n' = m' + n$.

Lemma 4.1. *The relation* $\overset{+}{\sim}$ *is an equivalence relation on* $\mathbb{N} \times \mathbb{N}$.

Proof. Trivially, $m + n = m + n$ so $(m, n) \overset{+}{\sim} (m, n)$. Assume $(m, n) \overset{+}{\sim} (m', n')$ so $m + n' = m' + n$. So, $(m', n') \overset{+}{\sim} (m, n)$. Assume $(m, n) \overset{+}{\sim} (m', n')$ and $(m', n') \overset{+}{\sim} (m'', n'')$. Then, $m + n' = m' + n$ and $m' + n'' = m'' + n'$. Then, $m + n' + n'' = m' + n + n'' = m'' + n + n'$. By injectivity of "add n'": $m + n'' = n + m''$. □

As a result, we can look at the set of equivalence clases of $\overset{+}{\sim}$ over $\mathbb{N} \times \mathbb{N}$. $\mathbb{Z} = \{[(m, n)] : m, n \in \mathbb{N}\}$. We check that this set inherits $+, \cdot$ from $\mathbb{N}$ in a way that it is well-defined. It turns out that $+$ is as expected but $[(m, n)] \cdot [(m', n')] =$

$[(mm' + nn', mn' + nm')]$.

We will also define $-[(m,n)] = [(n,m)]$. Further, we define the operation $a - b = a + (-b)$.

Lemma 4.2. *$\forall m, n, m', n' \in \mathbb{N} : (m', n') \overset{+}{\sim} (m, n) \wedge m \leq m' \iff \exists k \in \mathbb{N} : m' = m + k \wedge n' = n + k$.*

Remark.

1. $[(0,0)]$ is zero under $+$
2. $-[(m,n)]$ is the additive inverse $[(m,n)]$ under $+$
3. $[(1,0)]$ is the unit under $\cdot$
4. $0 \cdot [(m,n)] = 0$
5. $N \cong \{[(n,0)] : n \in \mathbb{N}\}$ preserved by $+, \cdot$

Lemma 4.3. *$\mathbb{Z}$ is a ring. Also, $+$ is injective and $\cdot$ is injective for nonzero c. In other words, $c \cdot a = c \cdot b \Rightarrow a = b$ for $c \neq 0$.*

Remark. Given $\mathbb{Z}$, we can reconstruct N as follows. $\mathbb{N}_{\mathbb{Z}} = \bigcap \{A \subset \mathbb{Z} : 0 \in A \wedge (\forall a \in A : a + 1 \in A)\}$

4.2 Ordering of integers

$[(m,n)] \leq [(m', n')] := m + n' \leq m' + n$

Proposition 4.2.1. *This definition is independent of representation.*

Proposition 4.2.2. *$\leq$ is a total ordering.*

Proposition 4.2.3. *It is preserved by addition and multiplication by non-negative element.*

5 Rationals

For integers, for integers we have an injection $ca = cb \Rightarrow a = b$ for $c \neq 0$. However, this is not a surjection. Again, we extend our system such that this is a surjection.

5.1 Construction

Our goal is to solve $ax = b$ for any x, for all $a \neq 0$ and for all b.

Definition 5.1.1. We define $\dot{\sim}$ on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ as $(p,q) \dot{\sim} (p', q') : pq' = p'q$

Lemma 5.1. *$\dot{\sim}$ is an equivalence relation.*

Definition 5.1.2. We define $\mathbb{Q}$ as the set of equivalence classes under this relation.

This time, multiplication is defined in the standard way. We define addition as follows: $[(p,q)] + [(p',q')] := [(pq' + p'q, qq')]$

Remark. The set $\mathbb{Z}_{\mathbb{Q}} := \{[p,1] : p \in \mathbb{Z}\}$ identifies $\mathbb{Z} \subset \mathbb{Q}$.

5.2 Fields

Definition 5.2.1. A field is a set F with two operations $+, \cdot$ such that:

(F1) $+, \cdot$ obey commutativity, associativity and distributivity.

(F2) $\exists 0 \in F : \forall a \in F : a + 0 = a$. It can be seen that this element is unique so it's given a special name.

(F3) $\exists 1 \in F : 0 \neq 1 \wedge (\forall a \in F : 1a = 1)$.

(F4) $\forall a \in F : \exists b \in F : a + b = 0$. It can be seen this b is unique so we call it $-a$.

(F5) $\forall a \in F \setminus \{0\} : \exists b \in F : ab = 1$. Again, this b is unique so we call it a^{-1}.

Theorem 5.2. $(\mathbb{Q}, +, [(0,0)], \cdot, [(1,0)])$ *is a field.*

Example 5.2.1. $F = \{0,1\}$ is a field with $1 + 1 = 0$. The other operations follow from the axioms.

Proposition 5.2.1. *1.* $0, 1, -a, a^{-1}$ *are unique.*

2. $(-a)b = -(ab)$.

Definition 5.2.2. A field $(F, +, 0, \cdot, 1)$ is ordered if $\exists$ a binary relation $\leq$ on F such that:

(O1) $\leq$ is a total order on F

(O2) $\forall a, b, c \in F : a \leq b \Rightarrow a + c \leq b + c$

(O3) $\forall a, b, c \in F : a \leq b \wedge 0 \leq c \Rightarrow ca \leq cb$

Definition 5.2.3. On rationals, we define an ordering in the following way:

$$[(p,q)] \leq [(p',q')] := \left\{ \begin{array}{ll} pq' \leq p'q, & \text{if } qq' \geq 0 \\ p'q \leq pq', & \text{if } qq' \leq 0 \end{array} \right\} \tag{1}$$

Lemma 5.3. $0 < 1$ *in any ordered field* F.

Proof. Assume not i.e. $1 \leq 0$. Then, $1 - 1 \leq 0 - 1 \iff 0 \leq -1$. Then, -1 is positive so multiplying by it preserves the ordering relation. In particular, $0(-1) \leq (-1)(-1) \Rightarrow 0 \leq 1$. Then, $0 = 1$ which contradicts (F3). Therefore, $0 < 1$. □

Now that we have defined a field and exhibited that $\mathbb{Q}$ is an example of an ordered field, is there a way to identify $\mathbb{N}$ as a subset of any ordered field?

Lemma 5.4. *Let $(F, +, 0, \cdot, 1)$ be an ordered field. Define $\mathbb{N}_F = \bigcap\{A \subset F : 0 \in A \wedge (\forall x \in A : x + 1 \in A)\}$ and $S_F(x) = x + 1$. Then $(\mathbb{N}_F, 0, S_F)$ is a system of naturals.*

Proof. (P1) Every set in the intersection contains 0 so $0 \in \mathbb{N}_F$.

(P2) S_F maps $\mathbb{N}_F$ to $\mathbb{N}_F$ and $Dom(S_F) = \mathbb{N}_F$.

(P3) The set $\{x \in F : 0 \leq x\}$ belongs to this family so $Ran(S_F) \subset \{x \in F : 1 \leq x\}$ which does not contain 0.

(P4) S_F is injective by the injectivity of + on F.

(P5) Consider $A \in \mathbb{N}_F$ such that $0 \in A$ and $S_F(A) \subset A$. By definition, A belongs to the family being intersected. Therefore $\mathbb{N}_F \subset A$. So, $A = \mathbb{N}_F$.

□

Definition 5.2.4. A system of rationals is an ordered field $(F, +, 0, \cdot, 1)$ such that $\forall x \in F : \exists r, m, n \in \mathbb{N}_F : r \neq 0 \wedge x = r^{-1}(m - n)$. This definition makes sense because we just showed that every ordered field comes with a system of naturals. Also, it can be seen that $\mathbb{Q}$ that was constructed from some $\mathbb{N}$ also satisfies these properties.

Theorem 5.5 (uniqueness of rationals)**.** *Consider two systems of rationals $F, \tilde{F}$ as defined above. Then $\exists$ a bijection $\phi : F \to \tilde{F}$ such that*

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$
3. $\phi(0) = 0, \phi(1) = 1$
4. $a \leq b \Rightarrow \phi(a) \leq \phi(b)$

Proof sketch. We prove this by the uniqueness of naturals and hope that the properties extend in a nice way.
We know that $\exists\phi : \mathbb{N}_F \to \mathbb{N}_{\tilde{F}}$ such that $\phi(0) = 0$ and $S_{\tilde{F}} \circ \phi = \phi \circ S_F$. We have proved that zero is mapped to zero and the succession property allows us to show that $\phi(1) = \phi(S_F(0)) = S_{\tilde{F}}(\phi(0)) = S_{\tilde{F}}(0) = 1$. Then, by induction it follows that $\forall m, n : \phi(m + n) = \phi(m) + \phi(n)$ and $\phi(mn) = \phi(m)\phi(n)$.
Next, we extend ϕ from $\mathbb{N}_F$ to F via: $x = r^{-1}(m-n) \Rightarrow \phi(x) = \phi(r)^{-1}(\phi(m) - \phi(n))$. Then, it suffices to check that this definition is independent of representation (we did not specificy uniqueness only existence), preserves the operations and ordering and ϕ stays a bijection. □

5.3 Deficiency of rationals

Definition 5.3.1 (integer powers in a field)**.** Let F be a field with $\mathbb{N}_F$ a set of naturals in the field. $\forall b \in F$ we can define b^n as $b^0 = 1$ and $\forall n \in \mathbb{N}_F : b^{n+1} = bb^n$. If $b \neq 0$ we can also define $b^{-n} = (b^{-1})^n$.

A natural question that now arises is "Does every polynomial $a_nx^n + \cdots + a_1x + a_0 = 0$ have a solution in F if all $a_i \in F$?". In general, the answer is no. A counterexample is provided by Euclid in the next lemma.

Lemma 5.6. $\forall x \in \mathbb{Q} : x^2 \neq 2$

Proof. Assume that $\exists x \in \mathbb{Q} : x^2 = 2$. We can write $x = \dfrac{\tilde{p}}{\tilde{q}}$ for $\tilde{p}, \tilde{q} \in \mathbb{Z}$. Now we let q be the smallest element in the set $\left\{ \tilde{q} \in \mathbb{N} : (\exists \tilde{p} \in \mathbb{Z} : x = \dfrac{\tilde{p}}{\tilde{q}}) \right\}$. By HW, every subset of $\mathbb{N}$ has a smallest element so q is well defined. Let p be the corresponding $\tilde{p}$ in the set above. We can then write $p^2 = 2q^2$. As a result, p^2 is even so p is even. Write $p = 2k$. Then, $4k^2 = 2q^2$ so q^2 is even and q is even. This contradicts the minimality of the representation $\dfrac{p}{q}$ as we can cancel out a 2. Therefore, no such $x \in \mathbb{Q}$ exists. □

Definition 5.3.2. We define $p \in \mathbb{N}$ as prime if $p \neq 0, 1$ and $\forall q \in \mathbb{N} \setminus \{0\} : q | p \Rightarrow q = p$.

Remark. The above proof can be extended to show that no rational number solves $x^2 = p$ where p is a prime.

Since rational numbers cannot solve all polynomial equations, the ancient solution was to append to $\mathbb{Q}$ all radicals that solve some polynomial.

Example 5.3.1. $\sqrt{2}$ is the solution to $x^2 = 2$. We can iterate this process, then $\sqrt{2 + \sqrt{2}}$ is a solution to $(x^2 - 2)^2 = 2$.

However, some polynomial solutions clearly exist as rational numbers. We are interested in knowing whether a given polynomial equation defines a new number.

Theorem 5.7 (rational root theorem)**.** *Suppose $x \in \mathbb{Q}$ solves $a^nx^2 + \cdots + a_1x + a_o = 0$. Then $\exists p, q \in \mathbb{Z} \setminus \{0\} : x = \dfrac{p}{q} \wedge \gcd(p, q) = 1 \wedge p | a_0 \wedge q | a_n$.*

Proof. The proof follows easily by replacing x with $\dfrac{p}{q}$. We then rearrange to get $a_np^n = -q[a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + \cdots + a_0q^{n-1}]$. Since $\gcd(p, q) = 1$, we must have that $a_n | q$. The other side also follows similarly to show $p | a_0$. □

Example 5.3.2. $x^4 - 4x^2 + 2 = 0$ using the theorem, $q = \pm 1, p = \pm 1, \pm 2 \Rightarrow x = \pm 1, \pm 2$. By substituting we see that this polynomial has no rational roots.

Remark. Not all radical expressions are irrational. $\sqrt{7 + 2\sqrt{3}} = \sqrt{(2 + \sqrt{3})^2} - \sqrt{3} = 2 + \sqrt{3} - \sqrt{3} = 2$.

We now need a systematic way of including rationals in our number system. Let $F = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$. We can define addition component wise and multiplication in the expected way: $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. Similarly, the inverse is what we would expect after "rationalizing" the denominator: $(a + b\sqrt{2})^{-1} = \dfrac{a}{a^2 - 2b^2} - \dfrac{b}{a^2 - 2b^2}\sqrt{2}$. By Euclid's lemma, we never have $a^2 - 2b^2 = 0$ so the inverse always exists. It can be checked that this is a field.

Definition 5.3.3. A polynomial equation $a_n x^n + \cdots + a_1 x + a_0 = 0$ admits a solution in radicals if $\exists m \in \mathbb{N}, \exists F_0, F_1, \ldots, F_m$ fields such that:

1. $F_0 = \mathbb{Q}$
2. $\forall i = 0, \ldots, m-1 : F_{i+1} = \{a + bz : a, b \in F_i\}$ where z solves, for example, $z^k = x$ for some $x \in F$
3. $\exists x \in F_m$ such that x solves the above equation. In other words, F_m is a vector space over F_{m-1} not just over F

Remark. While there exists formulas (involving radical expressions) to solve quadratic, cubic and quartic polynomials, it was shown that $x^5 - x - 1 = 0$ has no solution in radicals.

As a result, the algebraic approach to reals fails.

6 Real numbers

6.1 Supremum and infimum in posets

Definition 6.1.1. Let $(E, \leq)$ be a poset. Let $A \subset E$. We say that $x \in E$ is an upper bound on A if $\forall y \in A : y \leq x$. Note that this is actually two coniditions. Each y in A must be comparable with x and x must compare favorably. We similarly define the lower bound on A as $z \in E$ such that $\forall y \in A : z \leq y$.

Remark. We do not require that the upper bound of the set A lies in A.

Example 6.1.1.

1. Let F be a set and consider $E = \mathcal{P}(F)$ ordered via inclusion. It is clear that F is an upper bound and $\emptyset$ is a lower bound for any subset.
2. Let $E = \mathbb{N} \setminus \{0\}$ and define $m|n := (\exists k \in E : n = k \cdot m)$. Then, 1 is an upper bound for any subset.
3. Let $E = \mathbb{Q} \times \mathbb{Q} : (x, y) \leq (\tilde{x}, \tilde{y}) := x < \tilde{x} \vee (x = \tilde{x} \wedge y < \tilde{y})$. This set is not bounded. For example, $A = \{(x, y) : x + y = 0\}$ has no upper bound or lower bound.

At this point it is evident that bounds are not unique. We are interested in finding the *tightest* bounds possible. In particular, we want to find the lowest upper bound and the greatest lower bound of a set.

Definition 6.1.2. Let E be a poset and $A \subset E$. Then $x \in A$ is said to be:

1. The supremum of A if x is an upper bound and is smaller than any other upper bound.
2. The infimum of A if x is a lower bound and is greater than any other lower bound.

Remark. In this definition, we use the article *the* to define supremum and infimum. It seems like we took uniqueness for granted. This usage is justified by the next lemma.

Lemma 6.1. *If* $\sup(A)$ *or* $\inf(A)$ *exists, then it is unique.*

Proof. Let $x, \tilde{x}$ be suprema. It then follows that $x \leq \tilde{x}$ and $\tilde{x} \leq x$. By antisymmetry $x = \tilde{x}$. □

Lemma 6.2. *Let F be a set. Then,* $\forall A \in \mathcal{P}(F) : A \neq \emptyset \Rightarrow \sup(A) = \bigcup A \wedge \inf(A) = \bigcap A$.

Proof. Check HW 4. □

Lemma 6.3. *Let $(E, \leq)$ be a poset. Let $A \subset E$ such that* $\inf(A), \sup(A)$ *exist. Then,* $A \neq \emptyset \Rightarrow \inf(A) \leq \sup(A)$.

Proof. Since $A \neq \emptyset$, we can pick $a \in A$. Then $\inf(A) \leq a$ and $a \leq \sup(A)$. By transitivity, $\inf(A) \leq \sup(A)$. □

Lemma 6.4. $(E, \leq)$ *be posets. $A, B \subset E$ nonempty such that* $\sup(A), \inf(B)$ *exist. Then* $\forall a, b : a \leq b \iff \sup(A) \leq \inf(B)$.

Proof. $\Leftarrow$ Assume $\sup(A) \leq \inf(B)$. Then $\forall a : a \leq \sup(A)$ and $\forall b : \inf(B) \leq b$. Therefore, $\forall a, b : a \leq b$.
$\Rightarrow$ Assume that $\forall a, b : a \leq b$. We are given that $\sup(A)$ exists. Let $b \in B$. Then b is an upper bound on A. Therefore, $\sup(A) \leq b$. But this is true $\forall b \in B$. So, $\sup(A)$ is a lower bound on B. Therefore, $\sup(A) \leq \inf(B)$ □

Corollary 6.4.1. $\sup(A) = \inf \{x \in A : x \textit{ is an upper bound on } A\}$

Lemma 6.5. *Let* $(\mathbb{N}, \leq)$ *be a system of naturals. Then* $\forall A \in \mathbb{N} : A \neq \emptyset \Rightarrow (\inf(A) \textit{ exists } \wedge \inf(A) \in A)$ *i.e. each subset of the naturals has a minimal element.*

Proof. Check notes. □

6.2 Completeness

Definition 6.2.1. An ordered field F is said to be complete if every set A with an upper bound admits $\sup(A)$.

Corollary 6.5.1. *If F is a complete field, every set B with a lower bound has an infimum.*

Proof. Let B have a lower bound l i.e. $\forall b \in B : l \leq b$. Now consider the set $-B = \{-b : b \in B\}$. Then, $\forall(-b) \in -B : -b \leq -l$. Therefore, $-l$ is an upper bound on this set. By the completeness of F, $\sup(-B)$ exists. This means that for any upper bound u of $-B$, $\sup(-B) \leq u$. Therefore, for any lower bound l of B, $l \leq -\sup(-B)$. Therefore, $\inf(B) = -\sup(-B)$. □

Lemma 6.6. *The ordered field $\mathbb{Q}$ is not complete.*

To prove this lemma, we need to find a set with an upper bound that doesn't have a supremum. We will use the set $A = \big\{x : x \leq 0 \vee x^2 \leq 2\big\}$ which is clearly nonempty since $1 \in A$ and has a upper bound of $x = 2$.

Lemma 6.7 (archimedian property of rationals)**.** *$\forall a \in \mathbb{Q} : (a > 0 \Rightarrow \exists n \in \mathbb{N} : na > 1)$.*

Proof. From our construction of rationals, this follows almost immediately. Let $a \in \mathbb{Q}$. Then, we can write $a = \dfrac{p}{q}$ for $p, q \geq 1$. Then, $(q+1)a > p > 1$. □

Proof of earlier lemma. Assume that A has a supremum, call it c. Since $c \in \mathbb{Q}, c^2 \neq 2$. First we show that $c^2 \geq 2$. Consider $\left(c + \dfrac{1}{n}\right)^2 = c^2 + \dfrac{2c}{n} + \dfrac{1}{n^2} \leq c^2 + \dfrac{5}{n}$. Since c was defined as $\sup(A)$, $c + \dfrac{1}{n} \notin A$ so $c^2 + \dfrac{5}{n} \geq 2$ which is saying that $2 - c^2 \leq \dfrac{5}{n}$ $\forall n \in \mathbb{N}$. Now, if $c^2 < 2$ this is a contradiction of the Archimedian principle as we have found a positive number that is $\leq \dfrac{1}{n}$ for all $n \in \mathbb{N}$. As a result, we must have that $c^2 < 2$. We will now show that this is false. Consider $\left(c - \dfrac{1}{n}\right)^2 = c^2 - \dfrac{2c}{n} + \dfrac{1}{n^2} \geq c^2 - \dfrac{4}{n}$. Again, since $c = \sup(A)$, $\left(c - \dfrac{1}{n}\right)^2 \leq 2$. This gives us $c^2 - 2 \leq \dfrac{4}{n}$ for all $n \in \mathbb{N}$ which again is a contradiction. Therefore, $\sup(A)$ does not exist. □

6.3 Construction of reals

Definition 6.3.1. A system of reals is a complete ordered field.

Theorem 6.8 (Dedekind 1872)**.** *There exists a system of reals.*

We will devote this section to constucting that system of reals by taking subsets of $\mathbb{Q}$.

Definition 6.3.2. A Dedekind cut is a set $A \subset \mathbb{Q}$ such that:

(C1) $A \neq 0 \wedge A \neq \mathbb{Q}$

(C2) $\forall a \in A, \forall q \in Q : q \leq a \Rightarrow q \in A$

(C3) $\forall a \in A, \exists b \in A : a < b$

Note that (C1) says A is a nonempty, proper subset of $\mathbb{Q}$, (C2) says that if an element belongs to A then every smaller element belongs to A. Finally, by (C3), for every element in A we can find another element in A that is strictly bigger i.e. there is no maximal element in A.

Definition 6.3.3. $\mathbb{R} = \{A \subset Q : \text{ A is a cut }\}$

Remark. This gives us the intuition that every cut is a partition of Q into two halves.

Example 6.3.1. $\forall a \in \mathbb{Q} : \{b \in \mathbb{Q} : b < a\}$ is a cut. Also, $\big\{b \in \mathbb{Q} : b < 0 \wedge b^2 < 2\big\}$ is a cut.

Remark. In the first example, it seems like $a \in \mathbb{Q}$ represents the cut. In the second one, $\sqrt{2} \notin \mathbb{Q}$ represents the cut. This already gives us the hope that each cut can be represented by some element in a set ($\mathbb{R}$) which also contains a $\sqrt{2}$. We will look at this set more carefully and see whether it gives us the complete ordered field for which we are looking.

First, we verify our intuition that all cuts look like partitions "bounded" by some element not in the set.

Lemma 6.9. $\forall A \in \mathbb{R}$:

1. $\forall b \notin A, \forall q \in \mathbb{Q} : b \leq q \Rightarrow q \notin A$ *(if an element is not in A, then every bigger element is not in A)*
2. $\forall a \in A, \forall b \notin A : a < b$ *(every element in A is smaller than every element not in A)*
3. $\{b - a : a \in A \wedge b \notin A\} = \{c \in \mathbb{Q} : c > 0\}$ *(the partition allows elements on both sides to get arbitrarily close)*

Proof.

1. Let $b \notin A, q \in \mathbb{Q} : b \leq q$. Assume, by contradiction, that $q \in A$. Then by (C2) $b \leq q \Rightarrow b \in A$ which is a contradiction. So $q \notin A$.
2. Let $b \notin A$. Then by (1) $\forall a \in Q : b \leq a \Rightarrow a \notin A$. By contraposition, $a \in A \Rightarrow a < b$.
3. $\subset$ is easy. Let $a \in A, b \notin B$ then $a < b$. Therefore, $b - a > 0$. For $\supset$, assume by contradiction that $\exists c > 0$ such that it cannot be written in the form $b - a$ for $b \notin A, a \in A$. This means that $\forall a \in A : a + c \in A$. But

by induction, this means that $\forall n \in \mathbb{N} : a + nc \in A$. By (C3) $\exists b \in A$ such that $a + nc < b$ for all $n \in \mathbb{N}$ which contradicts the Archimedian property.

□

Definition 6.3.4 (ordering on cuts)**.** We define $A \leq B := A \subset B$.

Lemma 6.10. *$\leq$ is a total ordering on $\mathbb{R}$.*

Proof. It is a partial ordering since $\subset$ is always a partial order on sets. Assume that it isn't a total ordering so that $\exists A, B \in \mathbb{R}$ such that $\exists a \in A \setminus B, \exists b \in B \setminus A$. By the above lemma, $a \notin B, b \in B$ so $b < a$. Similarly, $b \notin A, a \in A$ so $a < b$ which is a contradiction. □

Lemma 6.11. *Every nonempty subset of cuts $C \subset \mathbb{R}$ that has an upper bound i.e. $\exists B \in \mathbb{R} : \forall A \in C : A \leq B$ has $\cup C \in \mathbb{R}$ i.e. it has a supremum. In other words, $\mathbb{R}$ is complete.*

Proof. We need to show that $\cup C$ is a cut.

(C1) It is nonempty as it is the union of cuts. C has an upper bound B. Since B is a cut, $\exists b \notin B$. But since each $A \subset B$, $b \notin A \Rightarrow b \notin \cup C$.

(C2) Let $a \in \cup C, q \in \mathbb{Q} : q \leq a$. Then there exists some cut A such that $c \in A$ so $q \in \cup C$

(C3) Let $a \in \cup C$, then $a \in A$ for some cut and so $\exists b \in A \subset \cup C$ such that $a < b$.

□

Next, we endow $\mathbb{R}$ with certain operations $\oplus, \odot$ such that it becomes a field. These are all defined in a natural (albeit not straightforward) way. Check end of Lec 13 notes for more details.

Lemma 6.12. *$(\mathbb{R}, \oplus, \underline{0}, \odot, \underline{1}, \leq)$ is an ordered field.*

Proof. Omitted. □

6.4 Uniqueness of reals

We now want to show that reals are in some sense unique (upto a certain isomorphism that we define). We have show that $\mathbb{R}$ the set of Dedekind cuts in $\mathbb{Q}$ is a complete ordered field. We want to show that for any other complete order field, there is an order-preserving bijection $\phi : \mathbb{R} \to F$. The idea here is that any ordered field "comes" with its own naturals and rationals. Therefore, we can construct a set of reals $\mathbb{R}_F$ by taking cuts of $\mathbb{Q}_F$ and get a bijection by simply extending the known bijection between $\mathbb{Q}$ and $\mathbb{Q}_F$. Now, we need to find a map to go back from $\mathbb{R}_F$ to F which is a *bijection.* The fact that such a map exists is at the core of the uniqueness of reals so it's reasonable to guess that we use completeness of reals to define a map $\sup : \mathbb{R}_F \to F$. It is unclear how to show that every Dedekind cut in $\mathbb{Q}$ has a supremum (so that the map is well-defined) and that we can write every Dedekind cut as $A = \{a \in \mathbb{Q}_F : a < \sup(A)\}$ which shows that the map is injective. However, it is clear that the map is surjective as $\{a \in \mathbb{Q}_F : a < b\}$ is a set $\forall b \in F$. This discussion shows us that we need to prove is the following lemma.

Lemma 6.13. $\forall A \in \mathbb{R}_F : \sup(A)$ *exists* $\wedge\, A = \{a \in \mathbb{Q}_F : a < \sup(A)\}$.

Proof. The wording of this statement automatically implies that there is a unique correspondence between every $A \in \mathbb{R}_F$ and $\sup(A) \in F$.
Let $A \in \mathbb{R}_F$ i.e. it is a cut of $\mathbb{Q}_F$. Since $\mathbb{Q}_F \setminus A$ is nonempty, $\exists b \notin A$. By the previous lemma, b is an upper bound for A. Since we have defined $\mathbb{Q}_F$ in way that $\mathbb{Q}_F \subset F$, we have that $A \subset F$ with an upper bound. By the completeness of F, $\sup(A)$ exists.

Now we show that $A = \{a \in \mathbb{Q}_F : a < \sup(A)\}$. Let $a \in A$. Then, since $\sup(A)$ is an upper bound on A, it is clear that $a < \sup(A)$. Now assume that $a < \sup(A)$. If $a \notin A$ then $\forall x \in A : x < a$ by the earlier lemma. But then, a is an upper bound on A so $\sup(A) \leq a$ which is a contradiction. So $a \in A$.

For all $f \in F$, the set $A = \{x \in \mathbb{Q}_F : x < f\}$ is a cut $\in \mathbb{R}_F$ and has $\sup(A) = f$. This is because f is an upper bound on A. Also, let $u \in F$ be another upper bound on A. Assume $u < f$, then $u \in A$. But this contradicts (C3) as there is no maximal element in A. Therefore, $f \leq u$. So $f = \sup(A)$. Therefore sup is surjective.

Let $A \neq B$ be cuts. WLOG, $\exists b \in B \setminus A$. Then, b is an upper bound on A. However, $b \in B$ so there exists $b' \in B : b < b'$. As a result, $\sup(A) \leq b < b' \leq \sup(B)$ so $\sup(A) \neq \sup(B)$. Therefore sup is injective. □

This proves the following theorem.

Theorem 6.14. *Let F be a complete ordered field. Let $\mathbb{R}$ be the field of Dedekind cuts over $\mathbb{Q}$. Then $\exists \phi : \mathbb{R} \to F$ which is an order-preserving bijection.*

Proof. We have an order preserving bijection $\psi : \mathbb{Q} \to \mathbb{Q}_F$ which can be extended to $\psi : \mathbb{R} \to \mathbb{R}_F$. By the above lemma, $\phi = \sup \circ \psi : \mathbb{R} \to F$ is a bijection. It is straightforward to check that sup preserves operations, which is stated in the next lemma. □

Lemma 6.15. $\forall A, B \in \mathbb{R}_F$

1. $\sup(A \oplus B) = \sup(A) + \sup(B)$
2. $\sup(A \odot B) = \sup(A) \cdot \sup(B)$
3. $\sup(\ominus A) = -\sup(A)$
4. $\sup(A^{-1}) = \sup(A)^{-1}$

5. $A \subset B \Rightarrow \sup(A) \leq \sup(B)$

Remark. The takeaway here is that there is only one Real Analysis.

6.5 Consequences of completeness

Lemma 6.16 (archimedian property of $\mathbb{R}$)**.** *For every* $x \in \mathbb{R} : x > 0 \Rightarrow (\exists n \in \mathbb{N} : nx > 1)$

Proof. Assume not. Let $x > 0$ such that $\forall n \in \mathbb{N} : nx \leq 1$. Then the set $X = \{nx : n \in \mathbb{N}\}$ is bounded by 1 i.e. $\mathbb{N}$ is bounded by $\frac{1}{x}$. By completeness, $\sup(\mathbb{N})$ exists. This means that $\sup(\mathbb{N}) - 1$ is not an upper bound on $\mathbb{N}$ so $\exists n : \sup(\mathbb{N}) - 1 < n$ i.e. $n + 1 > \sup(\mathbb{N})$ which contradicts $\sup(\mathbb{N})$ being an upper bound. □

Theorem 6.17 (denisty of rationals in $\mathbb{R}$)**.** $\forall x, y \in \mathbb{R} : x < y \Rightarrow (\exists a \in \mathbb{Q} : x < a \wedge a < y)$*. In other words, between any two real numbers, we can find a rational number.*

Proof. WLOG let $y > 0$. If not, we can flip signs, get an a and flip its sign.

$x < y \Rightarrow y - x > 0$. Therefore, $\exists n \in \mathbb{N} : n(y - x) > 1$. Therefore, $A = \{k \in \mathbb{N} : k \geq yn\}$ is nonempty so consider $m = \inf(A)$. Then, $yn \leq m \wedge m - 1 < yn$. As a result, $nx = ny + n(y-x) < ny - 1 \leq m - 1 < ny$. So, $nx < m - 1 < ny$ or $x < \frac{m-1}{n} < y$. □

Corollary 6.17.1 (density of irrationals in $\mathbb{R}$)**.** $\forall x, y \in \mathbb{R} : x < y \Rightarrow \exists a \in \mathbb{R} \setminus \mathbb{Q} : x < a \wedge a < y$.

Proof. Let $x < y$. Recall that $\sqrt{2}$ is irrational. Consider the reals $\frac{x}{\sqrt{2}} < \frac{y}{\sqrt{2}}$. By the density of rationals, there exists a rational $q \in \mathbb{Q}$ such that $\frac{x}{\sqrt{2}} < q < \frac{y}{\sqrt{2}}$. Therefore, $x < q\sqrt{2} < y$ where $q\sqrt{2}$ is irrational. □

Theorem 6.18 (general roots)**.** *For all positive reals* $a \geq 0$ *and* $\forall n \in \mathbb{N} : n \geq 1$ *there exists a unique* $x \in \mathbb{R} : x \geq 0$ *such that* $x^n = a$*.*

Proof. First we will show existence. The theorem is trivial for $a = 0$ so let $a > 0$. Consider the set $A = \{y \in \mathbb{R} : y \geq 0 \wedge y^n \leq a\}$. This set is nonempty since $0 \in A$ and $(1 + a)$ is an upper bound since $(1 + a)^n \geq 1 + a > a$. Assume that $\exists y \in A$ i.e. $y^n \leq a$ such that $(1 + a) < y$. Then, $(1 + a)^n < y^n \leq a$ which contradicts the above. Therefore, we can now consider $\sup(A)$ by completeness. We claim that the required $x = \sup(A)$.

We first verify a lemma which will be needed to complete this proof.

Lemma 6.19. $\forall x, y \in \mathbb{R}, \forall m \in \mathbb{N} : x^{m+1} - y^{m+1} = (x-y)\sum\limits_{k=0}^{m} x^k y^{m-k}$

Proof of lemma. We will expand and distribute the RHS here.

$$\begin{aligned}
(x-y)\sum_{k=0}^{m} x^k y^{m-k} &= (x-y)(x^m + x^{m-1}y + \cdots + xy^{m-1} + y^m) \\
&= x^{m+1} + \cancel{x^m y} + \cdots + \cancel{xy^{m-1}} - (\cancel{yx^m} + \cdots + \cancel{y^m x} + y^{m+1}) \\
&= x^{m+1} - y^{m+1}
\end{aligned}$$

More formally we can write

$$\begin{aligned}
(x-y)\sum_{k=0}^{m} x^k y^{m-k} &= \sum_{k=0}^{m} x^{k+1} y^{m-k} - \sum_{k=0}^{m} x^k y^{m-k+1} \\
&= x^{m+1} + \sum_{k=0}^{m-1} x^{k+1} y^{m-k} - \sum_{k=1}^{m} x^k y^{m-k+1} - y^{m+1} \\
&= x^{m+1} + \cancel{\sum_{k=0}^{m-1} x^{k+1} y^{m-k}} - \cancel{\sum_{k=0}^{m-1} x^{k+1} y^{m-k}} - y^{m+1} \\
&= x^{m+1} - y^{m+1}
\end{aligned}$$

□

We now use this lemma to prove the following bound when $y \leq x : n(x-y)y^{n-1} \leq x^n - y^n \leq n(x-y)x^{n-1}$. We can prove both inequalities separately. In the above lemma, set $m = n-1$. Then, $n(x-y)y^{n-1} = (x-y)\sum\limits_{k=0}^{n-1} y^{n-1}$. Since $y \leq x$ we get that $y^{n-1} \leq x^k y^{n-k-1}$ for all $k : 0 \leq k \leq n-1$. Therefore, $(x-y)\sum\limits_{k=0}^{n-1} y^{n-1} \leq \sum\limits_{k=0}^{n-1} x^k y^{n-k-1} = x^n - y^n$. This gives us the first inequality. Similarly, since $x^k y^{n-k-1} \leq x^{n-1}$ for all $k : 0 \leq k \leq n-1$, we get $x^n - y^n = (x-y)\sum\limits_{k=0}^{n-1} x^k y^{n-k-1} \leq (x-y)\sum\limits_{k=0}^{n-1} x^{n-1} = n(x-y)x^{n-1}$ which is the second inequality.

We have now shown that $y \leq x \Rightarrow n(x-y)y^{n-1} \leq x^n - y^n \leq n(x-y)x^{n-1}$. We wish to show that $x^n = a$. The upper bound helps us show that $x^n \leq a$. Recall that $x = \sup(A)$ so $\forall y \in A, y \leq x$ and we cannot find a smaller upper bound. As a result, for every $m \in \mathbb{N}, \exists y \in A : y \leq x \leq y + \dfrac{1}{m+1}$. This is true because otherwise we would find a smaller upper bound on A. Now we use the lemma: $\forall y \in A : x^n - y^n \leq n(x-y)x^{n-1} \Rightarrow x^n \leq y^n + n(x-y)x^{n-1} \leq a + \frac{n}{m+1}x^{n-1}$. This is true for all $m \in \mathbb{N}$ so the Archimedian property rules out $x^n > a$. Therefore, $x^n \leq a$. To show equality, assume that $x^n < a$. Then $a - x^n > 0$ and we can use the Archimedian property to find an $l \in \mathbb{N}$ such that $(l+1)(a-x^n) > n(2+a)^{n-1}$ and set $y = x + \frac{1}{l+1}$. Recall that $1+a$ was an upper bound on A so $x \leq 1+a \Rightarrow y \leq 2+a$. Now, since $y > x$, $y^n \leq x^n + n(x-y)y^{n-1} \leq x^n + \frac{n(2+a)^{n-1}}{l+1} < x^n + (a - x^n) = a$. But then $y \in A$ which is a contradiction since $y > x$ and $x = \sup(A)$. Therefore, $x^n = a$. Uniqueness of this x easily follows from the fact that if there is another such $y \neq x$ then $y^n \neq x^n$. □

7 Cardinality

Definition 7.0.1. We call a set finite if $\exists n \in \mathbb{N} : \exists f : [0,n) \to A$ a bijection. We call a set infinite if it is not finite.

Example 7.0.1. $A = \emptyset$ is finite with $n = 0$, $A = \{x\}$ is finite with $n = 1$ and so on.

Lemma 7.1. $\forall m, n \in \mathbb{N} : \forall f : [0,n) \to [0,m)$*:*

1. *f is injective $\Rightarrow n \leq m$*
2. *f is surjective $\Rightarrow m \leq n$*
3. *f is bijective $\Rightarrow m = n$*

Proof. HW □

Remark. Therefore, the n mentioned in the definition must be unique. We can then call this the cardinality of A denoted $|A|$

Lemma 7.2. *For A, B finite:*

1. *$B \subset A \Rightarrow |B| \leq |A|$*
2. *$|A \cup B| \leq |A| + |B|$*
3. *$|A \times B| = |A| \cdot |B|$*

Definition 7.0.2 (Dedekind infinite)**.** A set A is called Dedekind infinite if $\exists f : A \to A$ that is injective but not surjective.

Lemma 7.3. *A is Dedekind infinite $\Rightarrow$ A is infinite.*

Proof. Assume, by contradiction, that A is finite. Then, we have a bijection $f : [0,n) \mapsto A$ for some $n \in \mathbb{N}$. But since A is Dedekind infinite, we also have an injection (and not surjection) $h : A \to A$. Then, we have an injection, not surjection, $f^{-1} \circ h \circ f : [0, n) \mapsto [0, n)$ which is a contradiction of the lemma. □

The converse is not true in general but it is true within $\mathbb{N}$.

Lemma 7.4. *$\forall A \subset \mathbb{N} : A$ Dedekind infinite $\iff A$ unbounded $\iff A$ infinite.*

Proof. First double implication in HW, second one omitted. □

Definition 7.0.3. An infinite set A is uncountable if $\exists f : \mathbb{N} \to A$ a bijection. If a set is not countable, we say it is uncountable.

Lemma 7.5. *Let A be countable. Then $\forall B \subset A : B$ infinite $\Rightarrow B$ countable.*

Proof. Let $h : \mathbb{N} \to A$ be a bijection. Therefore, we can identify $A = \mathbb{N}$ and prove the statement for $B \subset \mathbb{N}$. We can prove this using recursive construction. The intuition here is that if B is infinite then we can keep removing elements from it (in particular the unique infimum of the modified set) and we are left with an infinite set at every step (prove using induction). As a result, we get a chain of subsets B_n of B indexed by $\mathbb{N}$ where each is infinite and we also have a unique element $\inf(B_n)$ in each. Then, we can define the map $f : \mathbb{N} \to B$ with $f(n) = \inf(B_n)$. It injective since at each step we are removing the old infimum and replacing it with a new one. To prove that it is surjective, we note that every $b \in B$ is in every B_n uptil some B_k and then $b \notin B_{k+1}$. It must be that $b = \inf(B_k)$. The details can be filled in using a lot of elementary proofs by induction. (Check Lec 15 notes.) □

Definition 7.0.4. An A-valued sequence $\{x_n : n \in \mathbb{N}\}$ is a map $f : \mathbb{N} \to A$ with full domain. We write $\{x_n : n \in \mathbb{N}\}$ for $Ran(f)$.

Corollary 7.5.1. *Let A be an infinite countable set. Then $\forall B \subset A$ infinite, we can write $B = \{x_n : n \in \mathbb{N}\}$.*

Corollary 7.5.2. *$\forall B : B$ is finite or countable $\iff \exists f : B \to \mathbb{N}$ an injection.*

Lemma 7.6. *$\forall A, B$ countable, $A \times B$ is countable.*

Proof. We have bijections $f : A \to \mathbb{N}$ and $g : B \to N$. So we have a bijection $h : A \times B \to \mathbb{N} \times \mathbb{N}$ where $h(a, b) = (f(a), g(a))$. We need to show that there exists a bijection $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Check picture from Feb 13 lecture. □

Corollary 7.6.1. *$\mathbb{Q}$ is countable.*

Proof. It suffices to find an injection $\mathbb{Q} \to \mathbb{N} \times \mathbb{N}$. Let $a \in \mathbb{Q}$. We can write it in a relatively prime form $a = \frac{p}{q}$ chosen minimally we can define a function $h : \mathbb{Q} \to \mathbb{N} \times \mathbb{N}$ where $h(a) = (2p, q)$ if $p \geq 0$ and $h(a) = (1 - 2p, q)$ if $p < 0$. The parity is used to distinguish between the sign of the denominator here. It is easily checked that this is an injection. □

Corollary 7.6.2. *Let $\{A_n : n \in \mathbb{N}\}$ be a (countable) collection of sets such that each A_n is finite or countable. Then $\cup A_n$ is also finite or countable.*

Proof. Invoking the Axiom of Choice, we choose a collection of injections $f_i : A_i \to \mathbb{N}$. Let $a \in \cup A_n$ and define $n(a)$ as the smallest index of a set to which it belongs (well defined since a subset of naturals has a minimal element). Then, map $h(a) = (n(a), f_{n(a)}(a))$ which is an injection since $h(a) = h(b) \Rightarrow n(a) = n(b)$ so by injectivity of each f_n, $a = b$. □

Corollary 7.6.3 (Dedekind, Cantor)**.** *The set of algebraic reals is countable.*

Proof. Omitted. Check HW 6 for alternate proof. □

7.1 Uncountable sets

Theorem 7.7 (Cantor, 1891)**.** *The set $\{0,1\}^{\mathbb{N}}$ is uncountable.*

Proof. Assume it is countable so we have a surjection $f_n : \mathbb{N} \to \{0,1\}^{\mathbb{N}}$. Consider the function that sends a natural to the function it represents and then evaluates that function on that same natural, which we write as $f_n(n)$. Define $h(n) = 1 - f_n(n)$ which is another function $\mathbb{N} \to \{0,1\}$. By surjectivity, we can write $h(n) = f_m$ for some $m \in \mathbb{N}$. Then if we evaluate it on m we get a contradiction. □

Theorem 7.8. *The unit interval $[0,1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ is uncountable.*

Proof. Lec 16 □

Corollary 7.8.1. *The set $\mathbb{R}$ is uncountable.*

Corollary 7.8.2. *There are uncountably many non-algebraic reals.*

Remark. We define $A \cong B := (\exists f : A \to B)$ a bijection. This is an equivalence relation.

Definition 7.1.1. The cardinality of A is the equivalence class $[A]$. Therefore, $[\mathbb{N}]$ is the class of countable sets.

Theorem 7.9 (Cantor, 1891)**.** *$\forall A$ set, there is no surjection $A \to \mathcal{P}(A)$. In particular, $[A] \neq [\mathcal{P}(A)]$.*

Proof. Lec 16 □

Definition 7.1.2. We define $A \lesssim B$ as ($\exists f : A \to B$ injection). This is not a partial order as it is not antisymmetric.

Theorem 7.10 (Cantor/Schoder-Berstein)**.** *$\forall A, B$ sets $A \lesssim B \wedge B \lesssim A \Rightarrow A \cong B$. In words, $\lesssim$ is an equivalence relation upto isomorphism.*

Example 7.1.1.

1. $\{0,1\}^{\mathbb{N}} \leq [0,1] \leq \mathbb{R}$
2. $\mathcal{P}(\mathbb{N}) \cong \{0,1\}^{\mathbb{N}}$
3. $\mathcal{P}(\mathbb{Q}) \cong \mathcal{P}(\mathbb{N})$
4. $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Q})$ via Dedekind cuts.

Remark. It is not known (and in fact undecidable) whether there is an equivalence class in between $[\mathbb{N}]$ and $[\mathbb{R}]$. We assume that there is none, which we call the continuum hypothesis.

8 Convergence of sequences

We start with real-valued sequences.

Example 8.0.1. Define $\{a_n\}_{n\in\mathbb{N}}$ by $a_0 = 1 \wedge \forall n \in \mathbb{N} : a_{n+1} = 3 - \dfrac{1}{a_n}$.

Lemma 8.1. *$\forall n \in \mathbb{N} : 1 \leq a_n \leq 3$.*

Proof. By induction. Omitted. Check Lec 17. □

Definition 8.0.1. Cauchy and convergent sequences. Skipped.

Proposition 8.0.1. *The above sequence is Cauchy.*

Proof. Omitted. □

Proposition 8.0.2. *The above sequence has limit $L = \dfrac{1+\sqrt{5}}{2}$.*

Proof. Omitted. □

The stated definitions of convergence also generalize to an arbitrary metric space.

8.1 Metric spaces

Definition 8.1.1. We call (X, ρ) a metric space if $X \neq \emptyset$ and we $\rho : X \times X \to \mathbb{R}$ is a function (called metric) such that $\forall x, y, z \in X$:

1. $\rho(x,y) \geq 0 \wedge (\rho(x,y) = 0 \iff x = y)$
2. $\rho(x,y) = \rho(y,x)$
3. $\rho(x,y) \leq \rho(x,z) + \rho(z,y)$

Example 8.1.1. $X = \mathbb{R}$ has a metric $\rho(x,y) = |x-y|$.

More examples can be found in HW 6. An important class of metrics on $\mathbb{R}^d$ is Minkowski's p-metrics: $\rho_p(x,y) = (\sum\limits_{i=1}^{d} |x_i - y_i|^p)^{1/p}$ and we also define ρ_∞ to be the max of all segments.

Definition 8.1.2. Let V be a vector space over a field $F = \mathbb{C}$ or $\mathbb{R}$. We can define a norm $\|\cdot\| : V \to \mathbb{R}$ such that for al $x, y \in V$:

1. $\|x\| \geq 0 \wedge (\|x\| = 0 \iff x = 0)$
2. $\forall \lambda \in F : \|\lambda x\| = |\lambda| \|x\|$
3. $\|x + y\| \leq \|x\| + \|y\|$

Lemma 8.2. *Let $\|\cdot\|$ be a norm over a vector space V. Then $\rho : V \times V \to \mathbb{R}$ defined by $\rho(x,y) = \|x - y\|$ is a metric.*

Proof. Lec 18 □

Proposition 8.1.1. *$\forall p \geq 1, \forall d \in \mathbb{N} \setminus \{0\}$ we have that $\|x\|_p = (\sum\limits_{i=1}^{d} |x_i|^p)^{1/p}$ is a norm on $\mathbb{R}^d$.*

Proof. Omitted. □

Definition 8.1.3. Let X be a nonempty set, $\rho(x,y) = \delta_{xy}$ is called the discrete metric on X.

Definition 8.1.4. Modified definition of convergent and cauchy sequences on arbitrary metric space.

Lemma 8.3. *Any convergent sequence has a unique limit.*

Proof. Lec 18 □

Lemma 8.4. *Every convergent sequence is Cauchy.*

Proof. Omitted. □

Remark. The converse is not true.

Lemma 8.5. *When ρ is the discrete metric on X, all Cauchy sequences are convergent.*

Proof. Omitted. □

Definition 8.1.5. Given a sequence $\{x_n\}_{n\in\mathbb{N}}$, its subsequence is any sequence of the form $\{x_{n_k}\}_{n,k\in\mathbb{N}}$ where $\forall k, l \in \mathbb{N} : k < l \Rightarrow n_k < n_l$.

Lemma 8.6. *If $\{x_n\}$ is a Cauchy sequence and it admits a convergent subsequence, then it is convergent.*

Proof. Check HW 6 $\square$

9 Topology on metric spaces

Let (X, ρ) be a metric space.

Definition 9.0.1 (open ball)**.** $\forall x \in X : \forall r > 0 : B(x,r) := \{y \in X : \rho(x,y) < r\}$. Here, B is the open ball of radius r centered at x.

Example 9.0.1. On the discrete metric, $B(x,r) = \{x\}$ if $0 < r \leq 1$ and X if $r > 1$.

Example 9.0.2. Let $X = \mathbb{R}$ with $\rho(x,y) = |x-y|$ then $B(x,r) = (x-r, x+r)$.

Example 9.0.3. Let X $\mathbb{R}^d$ and $\rho = \rho_p$ where the corresponding open ball is denoted $B_i(x,r)$. Then $B_2(x,r)$ is the usual ball, $B_\infty(x,r) = \bigtimes_{i=1}^{d} (x_i - r, x_i + r)$. $B_1(x,r)$ looks like a diamond and for every other p, $B_p(x,r)$ lies somewhere in the middle.

9.1 Open sets

Definition 9.1.1. Let $A \subset X$. We say that A is open if $\forall x \in A, \exists r > 0 : B(x,r) \subset A$ i.e. A is open if every element of A can be surrounded by an open ball completely within A. Intuitively, A cannot have any boundary points. We say that A is closed if A^c is open.

Lemma 9.1. *Both X and $\emptyset$ are open and closed.*

Lemma 9.2. *$\forall x \in X, \{x\}$ is closed.*

Proof. We need to show that every $y \in X \setminus \{x\}$ can be surrounded by an open ball. But since $y \neq x$ we set $r = \rho(x,y) \neq 0$ and consider the ball $B(y,r)$. We need to show that this ball does not contain x. Let $z \in B(y,r)$ then $\rho(x,z) \geq \rho(x,y) - \rho(y,z) = r - \rho(y,z) > 0$ so $z \neq x$. $\square$

Lemma 9.3. *Every open ball $B(x,r)$ is open.*

Proof. We need to show that every $y \in B(x,r)$ is contained within some other ball which is contained within this ball. Let $y \in B(x,r)$, then by definition $\rho(x,y) < r$. So we can set $\epsilon = r - \rho(x,y) > 0$ and consider the ball $B(y,\epsilon)$. This is contained within $B(x,r)$ since if $z \in B(y,\epsilon)$ then $\rho(y,z) < \epsilon = r - \rho(x,y)$ so $\rho(x,z) < r$. $\square$

Lemma 9.4. *Let $\mathcal{T} = \{O \subset X : O$ is open $\}$. Then:*

1. $\emptyset, X \in \mathcal{T}$

2. $\mathcal{T}$ is closed under arbitrary union.

3. $\mathcal{T}$ is closed under finite intersection.

Proof. Trivial. Need finiteness to get minimal radius of ball. □

Definition 9.1.2. A set $\mathcal{T} \subset \mathcal{P}(X)$ satisfying (1-3) above is called a topology on the set X.

Remark. The concept of sets in which every element is contained within a smaller ball, defined over a metric space, defines a topology. We call this the metric toplogy on X with respect to ρ.

Example 9.1.1. For any nonempty set X we have two "extreme" topologies:

1. $\mathcal{T} = \{\emptyset, X\}$ is called the trivial or coarsest topology.
2. $\mathcal{T} = \mathcal{P}(X)$ is called the discrete (finest) topology.

Lemma 9.5. *With respect to the discrete metric on X, all subsets are open and closed.*

Proof. $B(x, \frac{1}{2}) = \{x\}$. □

Lemma 9.6. *Closed sets are closed under arbitrary intersection and finite unions.*

Proof. De Morgan's laws. □

Definition 9.1.3. Given a topology $\mathcal{T}$ on X and any subset $A \subset X$, we define:

1. $int(A)$ or the interior of A as the union of all open sets contained within A.
2. $\overline{A}$ or the closure of A as the intersection of all closed sets containing A.

Lemma 9.7. $int(A) \subset A \subset \overline{A}$

Lemma 9.8. *$int(A)$ is open, $\overline{A}$ is closed.*

Definition 9.1.4. $\partial A := \overline{A} \setminus int(A)$ is called the topological boundary of A.

Lemma 9.9. *For all $A \subset X$:*

1. A is open $\iff A = int(A)$

2. A is closed $\iff A = \overline{A}$

3. ∂A is closed.

Proof. (3) $\partial A = \overline{A} \cup (X \setminus int(A))$ □

Example 9.1.2. Let $X = \mathbb{R}$ with $\rho(x,y) = |x-y|$. Let $A = \mathbb{N}$. Then $int(\mathbb{N}) = \emptyset$ and $\overline{\mathbb{N}} = \mathbb{N}$ so $\partial\mathbb{N} = \mathbb{N}$. Similarly for $A = \mathbb{Q}$, we get $int(\mathbb{Q}) = \emptyset, \overline{\mathbb{Q}} = \mathbb{R}$ so $\partial\mathbb{Q} = \mathbb{R}$.

Example 9.1.3. For X with a discrete metric p, for all $A \subset X : \overline{A} = A, int(A) = A, \partial A = \emptyset$.

Remark. We call $B'(x,r) := \{y \in X : \rho(x,y) \leq r\}$ is called the closed ball. It is a closed set and contains the open ball. It is clear that the closure of the open ball is a subset of the closed ball but they are not necessarily equal.

Remark. Different metrics on a set can have the same topologies but still have distinct Cauchy sequencs. This is a deficiency in our approach.