MATH 135: Introduction to the Theory of Sets

Jad Damaj

Fall 2022

Contents

Chapter 1

Introduction

1.1 August 25

1.1.1 Introduction

Foundations of Mathematics: language, axioms, formal proofs

- We focus on the axioms in set theory
- We use ZFC (Zermelo-Fraenkel + Choice)
- There is only one primitive notion : $\in$
- Within the ZFC universe, everything is a set

Course Outline:

- Basic axioms
- Operations, relations, functions
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$
- carindals
- AC
- ordinals

1.1.2 Basics

Principle of Extensionality: Two sets A, B are the same $\leftrightarrow$ they have the same elements $\forall x(x \in A \leftrightarrow x \in B)$
Example 1.1.1. $2, 3, 5 = \{5, 2, 4\} = \{2, 5, 2, 3, 3, 2\}$

Definition 1.1.2. There is a set with no elements, denoted $\varnothing$

- $\varnothing \neq \{\varnothing\}$
- $A \subseteq B$: A is a subset of $B \leftrightarrow$ each element of A is in B (use $\subsetneq$ to denote proper subset)

- $\{2\} \subseteq \{2,3,5\}$ but $\{2\} \notin \{2,3,5\}$
- Power set opertaion: $\mathcal{P}(A) = \{B \mid B \subseteq A\}$

We can define a hierarchy:
$V_0 = \varnothing$, $V_1 = \mathcal{P}(\varnothing) = \{\varnothing\}$, $V_2 = \mathcal{P}\mathcal{P}(\varnothing) = \{\varnothing, \{\varnothing\}\}$
$V_3 = \mathcal{P}(V_2) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$, $V_4, \ldots$
$V_\omega = \bigcup_{n\in\mathbb{N}} V_n$, $\mathcal{P}(V_\omega)$, $\mathcal{P}\mathcal{P}(V_\omega), \ldots, V_{\omega+\omega}, \ldots, V_{\omega+\omega+\cdots}, \ldots, V_{\omega\times\omega}, \ldots, V_{\omega^\omega}$

Chapter 2

Axioms and Operations

2.1 August 30

2.1.1 Zermelo Fraenkel Axioms of Set Theory

Setting: in ZFC all objects are sets
Language: contains vocabulary ($\in$), logical symbols ($=, \wedge, \vee\ \exists, \forall, \neg$), variables ($x, y, A, B$, etc.)

Axiom 2.1.1 (Extensionality Axiom)**.** Two sets are the same if they have the same elements
$\forall A, B(\forall x(x \in A \leftrightarrow x \in B) \to A = B)$

Axiom 2.1.2 (Empty Set Axiom)**.** There is a set with no members, denoted $\varnothing$
$\exists A \forall x(x \notin A)$

Axiom 2.1.3 (Pairing Axiom)**.** For any sets u, v there is a est whose elements are u and v, denoted $\{u, v\}$
$\forall u, v \exists A \forall x(x \in A \leftrightarrow x = u \vee x = v)$

Axiom 2.1.4 (Union Axiom (Preliminary Form))**.** For any sets a, b there is a set whose elements are elements of a and elements of b, denoted $a \cup b$
$\forall a, b \exists A \forall x(x \in Ax \in u \vee x \in v)$

Axiom 2.1.5 (Powerset Axiom)**.** Each set A, has a power set $\mathcal{P}(A)$.
$\forall A \exists B \forall x(x \in B \iff x \subseteq A)$ where $x \subseteq A$ stands for $\forall y(y \in x \to y \in A)$

Axiom 2.1.6 (Union Axiom)**.** For any set A, there is a set $\bigcup A$ whose members are members of the members of A.
$\forall A \exists B \forall x(x \in B \leftrightarrow \exists y \in A(x \in y))$

Idea for the subset axiom: For any set A, there is a set B whose memebrs are members of A satisfying some property.

eg. $B = \{x \in A \mid x \text{ satisfies property } P\} \subseteq A$

Example 2.1.7. $B = \{n \in \mathbb{N} \mid n\text{cannot be described in less that 20 words}\}$

- let b be the smallest element in B, then b is the smallest element that cannot be described in 20 words.
- Paradox : need to use formal language to express property P.

Example 2.1.8. Let $B = \{x \mid x \notin x\}$
Question: $B \in B$? $B \in B \leftrightarrow B \notin B$: need to have property be contained in some larger set.

We can now restate the axiom more formally:

Axiom 2.1.9 (Subset Axiom (Scheme))**.** For each formula $\phi(x)$, there is an axiom:
$\forall A \exists B \forall x (x \in B \leftrightarrow x \in A \wedge \phi(x))$

Example 2.1.10. Suppose there is a set of all sets A. Consider $B = \{x \in A \mid x \notin x\}$. Then $B \in B \leftrightarrow B \notin B$, contradiction. So there can be no such set A.

The language of 1rst order logic for ZFC:
The following are formulas:

- $x = y$, $x \in y$ atomic formulas
- $(\varphi \wedge \psi), (\varphi \vee \psi), \neg\varphi$ where φ, ψ are formulas
- $\exists v \varphi, \forall x \varphi$

Example 2.1.11. $\varphi(v, w) := (\exists v (v \in x \wedge \neg v = w)) \rightarrow (\forall y (\neg y \in y))$ is a formula

Chapter 3

Relations and Functions

3.1 September 1

3.1.1 Relations and Functions

Ordered Pair: $\langle a, b\rangle = \langle c, d\rangle \leftrightarrow a = c, b = d$

Definition 3.1.1. $\langle a, b\rangle = \{\{a\}, \{a, b\}\}$

Cartesian product of A and B, denoted $A \times B = \{\langle x, y\rangle x \in A, y \in B\}$
Using the subset axiom $A \times B = \{z \in \mathcal{P}\mathcal{P}(A \cup B) \,|\, \exists x \in A \exists y \in B z = \langle x, y\rangle\}$
Observation: $\langle x, y\rangle \in \mathcal{P}\mathcal{P}(C)$ for $x, y \in C$
$\{x\}, \{x, y\} \in \mathcal{P}(C)$ so $\{\{x\}, \{x, y\}\} \subseteq \mathcal{P}(C)$ so $\{\{x\}, \{x, y\}\} \in \mathcal{P}\mathcal{P}(C)$

Definition 3.1.2. A binary relation is a set R whose elements are ordered pairs.

If $R \subset A \times B$ then R is a relation from $A \to B$.

Definition 3.1.3. Given a relation R, dom $R = \{x \in \bigcup\bigcup R \,|\, \exists y\langle x, y\rangle \in R\}$,
range $R = \{y \in \bigcup\bigcup R \,|\, \exists x\langle x, y\rangle \in R\}$, field (R) = dom$(R)\cup$range(R)

Example 3.1.4. $R = \{\langle a, b\rangle, \langle c, d\rangle, \langle e, f\rangle\} = \{\{\{a\}, \{a, b\}\}, \{\{c\}, \{c, d\}\}, \{\{e\}, \{e, f\}\}\}$
$\bigcup R = \{\{a\}, \{a, b\}, \{c\}, \{c, d\}, \{e\}, \{e, f\}\}$
$\bigcup\bigcup R = \{a, b, c, d, e, f\}$

n-ary relations: define n-tuple by $\langle a, b, c\rangle = \langle\langle a, b, \rangle, c\rangle$ etc.

Definition 3.1.5. A function is a relation F such that $\forall x, y, z \ \langle x, y\rangle \in F$ and $\langle x, z\rangle \in F \to y = z$

$\forall x \in$dom (F) there is y such that $\langle x, y\rangle \in F$. If $A =$ dom(F), $B \supseteq$ range(F) then F is said to a funtion from A to B, $f : A \to B$
We say that $f : A \to B$ is onto if $B =$ range(F)

Definition 3.1.6. F is injective if $\forall x, y, z \ \langle x, z\rangle \in F \wedge \langle y, z\rangle inF \to x = y$.

Definition 3.1.7. For a set A, relations F, G

(a) inverse $F^{-1} = \{\langle y, x\rangle \,|\, \langle x, y\rangle \in F\}$

(b) composition: $G \circ F = \{\langle x, z\rangle \,|\, \exists y \langle x, y\rangle \in F, \langle y, z\rangle \in G\}$

(c) restriction: $F \upharpoonright_A - \{\langle x, y\rangle \in F \,|\, x \in A\}$

(d) image of A under F, $F[\![A]\!] = \{y \,|\, \exists x \in A \langle x, y\rangle \in F\} = \text{range}(F \upharpoonright_A)$

Example 3.1.8. If F is a function, F^{-1} may not be a function. F^{-1} is a function $\leftrightarrow$ F is one to one.

Example 3.1.9. $F^{-1} \circ F = \{\langle x, x\rangle \,|\, x \in \text{dom}(F)\}$ if F is one to one
More generally, $F^{-1} \circ F = \{\langle x, z\rangle \,|\, \exists y \in \text{range } F \langle x, y\rangle, \langle z, y\rangle \in F\}$.

3.2 September 6

3.2.1 Functions and Relations

Theorem 3.2.1. Let $F : A \to B$ with $A \neq \varnothing$

(a) There is a function $G : B \to A$ such that $G \circ F = \text{id}_A \leftrightarrow F$ is one to one.

(b) There is a function $G : B \to A$ such that $F \circ F = \text{id}_B \leftrightarrow F$ is onto.

Proof. (a) Suppose there is such a G. Take a_1, a_2 such that $F(a_1) = F(a_2)$, then $a_1 = G \circ F(a_1) = G \circ F(a_2) = a_2$
Conversely, suppose F is one to one. We want to define $G : B \to A$ given $b \in B$, let $G(b)$=the unique $a \in A$ such that $F(a) = b$ if $b \in$range(F). If $b \notin \text{range}(F)$, let $G(b) = a_0$ with $a_0 \in A$ arbitrary (exists since A nonempty)

(b) Supppose that $G : B \to A$, with $F \circ G = \text{id}_B$ Want to show $\forall b \in B \exists a\, F(a) = b$ Take $a = G(b) \to F(a) = F(G(b)) = b$
Conversely, suppose F is onto. We want to define G, given $b \in B$ want to define $G(b)$ such that $F(G(b)) = b$, equivalently, want $G(b) \in F^{-1}(\{b\})$. Since F is onto $F^{-1}(\{b\})$ is nonempty. Let $G(b)$ be any element of $F^{-1}(b)$, equivalently $G \subseteq F^{-1}$ and $\text{dom}(G) = B = \text{dom}(F^{-1})$.

Example 3.2.2. Suppose $A = \mathbb{N}$, let $G = \{(b, a) \in B \times \mathbb{N} : a \text{ is least satisfying } f(a) = b\}$

- Don't have a method to specify such elements in gneral.

Axiom 3.2.3 (Axiom of Choice - Form I)**.** For every relation R, there is a function $G \subseteq R$ with $\text{dom}(G) = \text{dom}(R)$

3.2.2 Infinite Cartesion Products

$A \times B = \{\langle x, y\rangle \in \mathcal{P}\mathcal{P}(A \cup B) \,|\, x \in A \wedge y \in B\}$

Definition 3.2.4. Let M be a function with domain I such that for every $i \in I$, $H(i)$ is a set. Let

$$\bigtimes_{i \in I} H(i) - \{f : I \to \bigcup H(i) \mid f(i) \in H9 = (i)\}$$

Example 3.2.5. Let ω_g be $\{G \subseteq \mathbb{R} \mid 0 \neq G, G \cup \{0\}$ is closed under addition $\}$
$\bigtimes_{G \in \omega_g} = \bigtimes_{G \in \omega_g} H(G)$ is a function such that for each $G \in \omega_g$, you get an element of G.
Observation: If one of the $H(i)$ is $\varnothing$, then $\bigtimes_{i \in I} H(i) = \varnothing$

Axiom 3.2.6 (Axiom of Choice - Form II)**.** If H is a function with domain I such that $H(i) \neq \varnothing \; \forall i \in I$, then $\bigtimes_{i \in I} H(i) \neq \varnothing$

(ACI) $\to$ (ACII): We are given H with $H(i) \neq \varnothing$ for all i. Want $f : I \to H(i)$ with $f(i) \in H(i) \; \forall i \in I$. Let $R = \{\langle i, h \rangle \in I \times \bigcup_{i \in I} H(i) \mid h \in H(i)\}$. $\mathrm{dom}(R) = I$, since $H(i) \neq \varnothing$ there is $h \in H(i)$ so $\langle i, h \rangle \in R$. BY ACI, there is $F \subseteq R$ with $\mathrm{dom}(F)$=$\mathrm{dom}(R) = I$. $\forall i$, $\langle i, f(i) \rangle \in R$ so $f(i) \in H(i)$

3.3 September 8

3.3.1 Natural Numbers

Idea: each natural number is the set of all the previous numbers.
$0 = \varnothing, 1 = \{\varnothing\}, 2 = \{\varnothing, \{\varnothing\}\}, \ldots, n = \{0, 1, \ldots, n-1\}, \ldots$

Definition 3.3.1. The succesor of a set a is defined as $a^+ = a \cup \{a\}$

Definition 3.3.2. A set I is inductive if $\varnothing \in I$ and $\forall a \in I, a^+ \in I$

Definition 3.3.3. a is a natural number if it belongs to all inductive sets, $\forall I(I \text{ inductive} \to a \in I)$

If I is any inductive set, let $\omega = \{a \in I \mid a$ belongs to all inductive sets$\}$=the minimal inductive set.
Observation: ω is inductive because $\varnothing$ is in all inductive sets and if n belongs to all inductive sets then so does n^+

Axiom 3.3.4 (Ifinity Axiom)**.** There is an inductive set.

Inductivion Principle: If $A \subseteq \omega$ is inductive set $A = \omega$

Example 3.3.5. Every natural number is 0 or the succesor of some natural number.
Let $A = \{n \in \omega \mid n = 0 \vee \exists m \in \omega \, n = m^+\}$. A is inductive so $A = \omega$

Definition 3.3.6. A set A is transitive if one of the following equivalent conditions holds:

- if $x \in a \in A$, then $x \in A$
- $\bigcup A \subseteq A$

- if $a \in A$, then $a \subseteq A$
- $A \in \mathcal{P}(A)$

Example 3.3.7. Transitive sets includ $\varnothing$, each natural number, ω, V_ω

Claim: $A = \{n \in \omega \mid n \text{ is transitive }\}$ is inductive (implies all nautrual numbers are transitiev)

- Base: $0 \in A$ since $\varnothing$ is transitive
- Inductive Step: Suppose $n \in A$ transitive, want to show n^+ is transitive.
  Consider $x \in a \in n^+ = n \cup \{n\}$. If $a = n$, $x \in n \subseteq n^+$. If $a \in n$, $x \in a \in$ so by transitivity $x \in\subseteq n^+$ so $x \in n^+$

Theorem 3.3.8. If a is tansitive, then $\bigcup a^+ = a$

Proof. ($\supseteq$) $a = \bigcup\{a\} \subseteq \bigcup(a \cup \{a\} = \bigcup a^+)$ ($a \in a^+$ so $a \subseteq \bigcup a^+$)
($\subseteq$) Take $x \in \bigcup a^+$, then let $b \in a^+$ with $x \in b$. If $b = a$, $x \in a$. If $b \in a$, $x \in b \in a$ so $x \in a$.

- If a, b transitive and $a^+ = b^+$ then $a = \bigcup a^+ = \bigcup b^+ = b$ so succesor function is one to one on transitive sets, more specifically ω.

Fix a number $k \in \omega$. Consdier the following functions:

- $A_k : \omega \to \omega$ by $A_k(0) = 0$, $A_k(n^+) = A_k(n)^+$
- $M_k : \omega \to \omega$ by $M_k(0) = 0$, $M_k(n^+) = A_k(M_k(n))$

3.4 September 13

3.4.1 Operations on the Natural Numbers

Theorem 3.4.1. Let A be a set, $a \in A$ and $F : A \to A$. Then there is a unique function $h : \omega \to A$ such that:

1. $h(0) = a$
2. $h(n^+) = F(h(n))$ for all $n \in \omega$

Proof. Let $h = \{\langle n, b\rangle \in \omega \times A \mid \text{there is } g : n^+ \to A \text{ such that } g(0) = a, g(i^+) = F(g(i)) \wedge g(n) = b\}$
Claim 1: For all n there is a $g : \{0, \dots, n\} \to A$ such that $g(0) = a$, $g(i^+) = F(g(i))$
Claim 2: Such a g is unique.

Proof of Claim 1. Let $I = \{n \in \omega \mid \text{ such a } g \text{ exists}\}$. Want to show that I is inductive.

1. $0 \in I$: let $g : \{0\} \to A$ be such that $g(0) = a$ eg. $g = \{\langle 0, a\rangle\}$
2. Suppose $n \in I$, we know such a g exists for n, $g : \{0, \dots, n\} \to A$. We want $\tilde{g} : \{0, \dots, n, n^+\} \to A$. Let $\tilde{g} = g \cup \{\langle n^+, F(g(n))\rangle\}$

□

Proof of Claim 2. Suppose $g, \tilde{g} : \{0, \dots, n\} \to A$ such that $g(0) = a = \tilde{g}(0)$, $g(i^+) = F(g(i))$, $\tilde{g}(i^+) = F(\tilde{g}(i^+)), i < n$. We want to show $g(i) = \tilde{g}(i)\ \forall i \leqslant n$. $g(0) = \tilde{g}(0)$, $g(i^+) = F(g(i)) = F(\tilde{g}(i)) = \tilde{g}(i^+)$
Can formally show this by induction using $I = \{i \in \omega \mid i \in n^+ \wedge g(i) = \tilde{g}(i) \vee i \notin n^+\}$ ☐

Claim 3: $\forall n \in \omega,\ h(n^+) = F(H(n))$

Definition 3.4.2. Given $k \in \omega$, define $A_k : \omega \to \omega$ by $A_k(0) = k$, $A_k(n^+) = (A_k(n))^+$. Define $n+k = A_k(n)$
Define $M_k : \omega \to \omega$ by $M_k(0) = 0$, $M_k(n^+) = A_k(M_k(n))$, let $n \times k = M_k(n)$.
Let $m < n$ if $m \in n$

Theorem 3.4.3. We can show the associativity of addition: $\forall a, b, v \in \omega((a + b) + c = a + (b + c))$, commutativity of addition: $\forall a, b \in \omega a + b = b + a$, etc.

3.4.2 Integers

Let $\sim$ be the following equivalence relation on $\omega \times \omega$ by $\langle a, b\rangle \sim \langle c, d\rangle \leftrightarrow a + d = b + c$
Define $\mathbb{Z} = \omega \times \omega / \sim$. $0_{\mathbb{Z}} = [\langle 0, 0\rangle]$, $1_{\mathbb{Z}} = [\langle 1, 0\rangle]$
Let $[\langle a, b\rangle] +_{\mathbb{Z}} [\langle c, d\rangle] = [\langle a+c, b+d\rangle]$. One needs to show this is well defined eg. if $\langle a, b\rangle \sim \langle a', b'\rangle, \langle c, d\rangle \sim \langle c', d'\rangle$ then $\langle a + c, b + d\rangle \sim \langle a' + c', b' + d'\rangle/$
Let $[\langle a, b\rangle] \times_{\mathbb{Z}} [\langle c, d\rangle] = [\langle ac + bd, ad + bc\rangle]$
Let $E : \omega \to \mathbb{Z}$ by $E(n) = [\langle n, 0\rangle]$

3.4.3 Rationals

Let $\sim$ be the following equivalence relation on $\mathbb{Z} \times \mathbb{Z}\backslash\{0\}$. $\langle a, b\rangle \sim \langle c, d\rangle \iff a \times_{\mathbb{Z}} d = b \times_{\mathbb{Z}} c$
Define $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}\backslash\{0\}/\sim$. $0_{\mathbb{Q}} = [\langle 0, 1\rangle]$, $1_{\mathbb{Q}} = [\langle 1, 1, \rangle]$
Let $[\langle a, b\rangle] \times_{\mathbb{Q}} [\langle c, d\rangle] = [\langle a \times c, b \times d\rangle]$
Let $[\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ad + bc, bd\rangle]$
$E : \mathbb{Z} \to \mathbb{Q}$ by $E(z) = [\langle z, 1\rangle]$

3.5 September 15

3.5.1 Reals (Dedekind Cuts)

Definition 3.5.1. A dedekind cut is a subset $D \subseteq \mathbb{Q}$ such that

- $\varnothing \neq D \neq \mathbb{Q}$
- D is closed downwards, if $d \in D$, $c < d \to c \in D$
- D has no greatest element.

Let $\mathbb{R} = \{D \in \mathcal{P}(\mathbb{Q}) \mid D \text{ is a dedekind cut }\}$
$\sqrt{2} = \{q \in \mathbb{Q} \mid q \times_{\mathbb{Q}} q < 2\}$, $e = \{q \in \mathbb{Q} \mid exn \in \omega\, q <_{\mathbb{Q}} (1 + \frac{1}{N})^N\}$ For $r \in \mathbb{R}$, $-r = \{q \in \mathbb{Q} \mid -q \in r\}\backslash\{-\sup(r)\}$
For $r_1, r_2 \in \mathbb{R}$, $r_1 \leqslant_{\mathbb{R}} r_2 \iff r_1 \subseteq r_2$
$r_1 \times r_2 = \{q \in \mathbb{Q} \mid \exists q \leqslant 0 \in r \exists b \leqslant 0 \in r_2\, q, a \times_{\mathbb{Q}} b$ if $r_1, r_2 > 0, \dots$

Theorem 3.5.2. $(\mathbb{R}, 0, 1, +, \times, \leqslant)$ is an ordered field.

$E : \mathbb{Q} \to \mathbb{R}$ is a field embedding.

3.5.2 Cardinality

Definition 3.5.3. A is equinumerous to B (written $A \approx B$) if there is a bijection $f : A \to B$

Theorem 3.5.4. For every A, B, C

- $A \approx A$
- If $A \approx B$, $B \approx B$
- If $A \approx B$, $B \approx C$ then $A \approx C$

Lemma 3.5.5. $\mathbb{Z} \approx \omega$

Proof. For $z \in Z$, $f(z) = \begin{cases} -2z & z \leqslant 0 \\ 2z+1 & z > 0 \end{cases}$

Lemma 3.5.6. $\mathbb{Q} \approx \omega$

Proof. $f : \omega \to \mathbb{Z} \times \mathbb{Z}^+$, $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^+/\sim$
$f' : \omega \to \mathbb{Q}$, $f'(n) =$ least $i \in \omega$ $g(i) \notin \{f(1), \ldots, f(n-1)\}$

Lemma 3.5.7. $\mathbb{R} \approx (0, 1)_{\mathbb{R}}$