NOTES ON SET THEORY

XINGZHI HUANG

1. Preliminaries

Definition 1.1 (Syntax of one-order logic)**.** A **signature** σ is a set of relation symbols, function symbols and constant symbols, each with a specified arity. A **first-order language** $\mathcal{L}$ over a signature σ consists of:

1. a countable set of variables $x_0, x_1, x_2, \ldots$
2. the symbols in σ
3. the logical symbols $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists, =$
4. the punctuation symbols (,), and ,.

The terms and formulas of $\mathcal{L}$ are defined inductively as follows:

1. every variable and constant symbol is a term
2. if f is an n-ary function symbol and $t_1, \ldots, t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term
3. if R is an n-ary relation symbol and $t_1, \ldots, t_n$ are terms, then $R(t_1, \ldots, t_n)$ is an atomic formula
4. if φ and ψ are formulas, then so are $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$ and $(\varphi \leftrightarrow \psi)$
5. if φ is a formula and x is a variable, then $\forall x\varphi$ and $\exists x\varphi$ are formulas.

A variable x is free in a formula φ if it is not bound by a quantifier in φ. A formula with no free variables is called a sentence.

2. Axioms

Axiom 2.1 (Axiom of Extensionality)**.** Two sets are equal if and only if they have the same elements:

$$\forall A \forall B (\forall x (x \in A \iff x \in B) \iff A = B).$$

Axiom 2.2 (Axiom of Empty Set)**.** There exists a set with no elements, denoted by $\emptyset$.

$$\exists A \forall x (x \notin A).$$

Axiom 2.3 (Axiom of Pairing)**.** For any sets A and B, there exists a set $\{A, B\}$ whose elements are exactly A and B.

$$\forall A \forall B \exists C \forall x (x \in C \iff (x = A \vee x = B)).$$

Axiom 2.4 (Axiom of Union)**.** For any sets A and B, there exists a set $A \cup B$ whose elements are exactly the elements of A or B.

$$\forall A \forall B \exists C \forall x (x \in C \iff (x \in A \lor x \in B)).$$

Axiom 2.5 (Axiom of Power Set)**.** For any set A, there exists a set $\mathcal{P}(A)$ whose elements are exactly the subsets of A.

$$\forall A \exists B \forall x (x \in B \iff x \subseteq A).$$

Axiom 2.6 (Subset Axiom Schema/Axiom of Separation)**.** For any set A and any formula $\varphi(x, t_0, \ldots, t_n)$ not involving A, there exists a set whose elements are exactly the elements of A that satisfy $\varphi(x, t_0, \ldots, t_n)$.

$$\forall t_0, \ldots, t_n \forall A \exists B \forall x (x \in B \iff (x \in A \land \varphi(x, t_0, \ldots, t_n))).$$

Remark 2.7 (Intersection and Union). We can define the intersection/union of a set of sets A as follows(Not strictly):

$$\bigcap_{B \in A} B := \{x : \forall B \in A (x \in B)\}, \quad \bigcup_{B \in A} B := \{x : \exists B \in A (x \in B)\}.$$

Remark 2.8 (Function). A function f from a set A to a set B, denoted by $f : A \to B$, is a subset of $A \times B$ such that for every $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$. The set A is called the domain of f and the set B is called the codomain of f. The element b is called the image of a under f, denoted by $f(a)$.

Axiom 2.9 (Axiom of Choice)**.** For any relation R, there exists a function f such that for every x, if there exists a y where $dom(f) = dom(R)$ and $ran(f) \subseteq ran(R)$, and $(x, f(x)) \in R$.

3. Natural Numbers

Definition 3.1. Let S be a set, we define the successor of S as $S^+ = S \cup \{S\}$.

Remark 3.2. Denote $0 = \emptyset$, $1 = 0^+ = \{\emptyset\}$, $2 = 1^+ = \{\emptyset, \{\emptyset\}\}$, $3 = 2^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, and so on.

Definition 3.3 (Inductive Set)**.** A set A is called inductive if $\emptyset \in A$ and for every $x \in A$, $x^+ \in A$.

Axiom 3.4 (Axiom of Infinity)**.** There exists an inductive set.

$$\exists A (\emptyset \in A \land \forall x (x \in A \to x^+ \in A)).$$

Theorem 3.5. *There exists a set ω consisting of exactly the natural numbers.*

Proof. Suppose A is an inductive set. We use the subset axiom instead of the intersection because the set of all inductive sets may not exist. Let

$$\omega = \{x \in A : \forall B (B \text{ is inductive} \to x \in B)\}.$$

We can show that every element in ω is either $\emptyset$ or the successor of an element in ω. Thus, ω consists of exactly the natural numbers. $\square$

Theorem 3.6. *The set ω is the smallest inductive set, i.e., ω is an inductive set and for any inductive set A, $\omega \subseteq A$.*

Definition 3.7. A set A is called transitive if it satisfies the following equivalent conditions:
1. for every $x \in A$, if $y \in x$, then $y \in A$;
2. $A \subseteq \mathcal{P}(A)$;
3. $\bigcup A \subseteq A$.

Theorem 3.8. *Every natural number is a transitive set.*

4. Arithmetic of Natural Numbers

Theorem 4.1. *Let A be a set, $F : A \to A$, $a \in A$. There exists a unique function $f : \omega \to A$ such that.*

$$f(0) = a, \quad f(n^+) = F(f(n))$$

for every $n \in \omega$.

Corollary 4.2. *Let $\mathbb{N}$ be the set of natural numbers with $e \in \mathbb{N}$. There exist unique functions $\sigma : \mathbb{N} \to \mathbb{N}$ such that:*
1. *$\sigma(0) = e$;*
2. *$\sigma(n^+) = (\sigma(n))^+$ for every $n \in \mathbb{N}$.*

Definition 4.3. We can define $A_m : \mathbb{N} \to \mathbb{N}$ as follows:

$$A_m(0) = m, \quad A_m(n^+) = (A_m(n))^+$$

Definition 4.4. For $m, n \in \mathbb{N}$, we define the addition of m and n as:

$$m + n = A_m(n).$$

where $+(-,-) : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is a function defined by recursion.

Theorem 4.5. *The addition on $\mathbb{N}$ satisfies the following properties:*
1. *$m + 0 = m$ for every $m \in \mathbb{N}$;*
2. *$m + n^+ = (m + n)^+$ for every $m, n \in \mathbb{N}$;*
3. *$m + n = n + m$ for every $m, n \in \mathbb{N}$;*
4. *$(m + n) + k = m + (n + k)$ for every $m, n, k \in \mathbb{N}$.*

Definition 4.6. We can define $M_m : \mathbb{N} \to \mathbb{N}$ as follows:

$$M_m(0) = 0, \quad M_m(n^+) = M_m(n) + m$$

Theorem 4.7. *The multiplication on $\mathbb{N}$ satisfies the following properties:*
1. *$m \cdot 0 = 0$ for every $m \in \mathbb{N}$;*
2. *$m \cdot n^+ = m \cdot n + m$ for every $m, n \in \mathbb{N}$;*
3. *$m \cdot n = n \cdot m$ for every $m, n \in \mathbb{N}$;*
4. *$(m \cdot n) \cdot k = m \cdot (n \cdot k)$ for every $m, n, k \in \mathbb{N}$;*
5. *$m \cdot (n + k) = m \cdot n + m \cdot k$ for every $m, n, k \in \mathbb{N}$.*

5. Integers

Definition 5.1 (Equivalence Relation)**.** A relation R on a set A is called an equivalence relation if it satisfies the following properties:

1. Reflexivity: for every $a \in A$, $(a, a) \in R$;
2. Symmetry: for every $a, b \in A$, if $(a, b) \in R$, then $(b, a) \in R$;
3. Transitivity: for every $a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

Definition 5.2 (Equivalence Class)**.** Let R be an equivalence relation on a set A. For every $a \in A$, the equivalence class of a is defined as:

$$[a] = \{b \in A : (a, b) \in R\}.$$

Definition 5.3. A function $f : A \to B$ where A and B are sets equipped with equivalence relations R_A and R_B respectively is called compatible with the equivalence relations if for every $a_1, a_2 \in A$, if $(a_1, a_2) \in R_A$, then $(f(a_1), f(a_2)) \in R_B$.

Theorem 5.4. *Let $f : A \to B$ be a function compatible with the equivalence relations R_A and R_B. Then f induces an unique well-defined function $\bar{f} : A/R_A \to B/R_B$ defined by:*

$$\bar{f}([a]) = [f(a)]$$

for every $[a] \in A/R_A$.

Definition 5.5 (Integers)**.** We define the set of integers $\mathbb{Z}$ as the set of equivalence classes of the relation R on $\mathbb{N} \times \mathbb{N}$ defined by:

$$((a, b), (c, d)) \in R \iff a + d = b + c.$$

Definition 5.6 (Addition)**.** We define the addition on $\mathbb{Z}$ as follows:

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$

for every $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Proposition 5.7. *The addition on $\mathbb{Z}$ is well-defined and satisfies the following properties:*

1. *$x + 0 = x$ for every $x \in \mathbb{Z}$;*
2. *$x + y = y + x$ for every $x, y \in \mathbb{Z}$;*
3. *$(x + y) + z = x + (y + z)$ for every $x, y, z \in \mathbb{Z}$.*
4. *For every $x \in \mathbb{Z}$, there exists $-x \in \mathbb{Z}$ such that $x + (-x) = 0$.*
5. *$[(0, x)] + [(0, y)] = [(0, x + y)]$ for every $x, y \in \mathbb{N}$.*

Definition 5.8. We define the multiplication on $\mathbb{Z}$ as follows:

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)]$$

for every $[(a, b)], [(c, d)] \in \mathbb{Z}$.

Proposition 5.9. *The multiplication on $\mathbb{Z}$ is well-defined and satisfies the following properties:*

1. *$x \cdot 1 = x$ for every $x \in \mathbb{Z}$;*
2. *$x \cdot y = y \cdot x$ for every $x, y \in \mathbb{Z}$;*
3. *$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for every $x, y, z \in \mathbb{Z}$;*
4. *$x \cdot (y + z) = x \cdot y + x \cdot z$ for every $x, y, z \in \mathbb{Z}$;*
5. *$[(0, x)] \cdot [(0, y)] = [(0, xy)]$ for every $x, y \in \mathbb{N}$.*

Definition 5.10. We define the order relation on $\mathbb{Z}$ as follows:

$$[(a,b)] < [(c,d)] \iff b+c < a+d$$

for every $[(a,b)], [(c,d)] \in \mathbb{Z}$.

Proposition 5.11. *The order relation on $\mathbb{Z}$ is well-defined and satisfies the following properties:*

1. *For every $x, y \in \mathbb{Z}$, exactly one of the following holds: $x < y$, $x = y$, $x > y$;*
2. *For every $x, y, z \in \mathbb{Z}$, if $x < y$ and $y < z$, then $x < z$;*
3. *For every $x, y, z \in \mathbb{Z}$, if $x < y$, then $x + z < y + z$;*
4. *For every $x, y, z \in \mathbb{Z}$, if $0 < x$ and $0 < y$, then $0 < x \cdot y$.*

6. Rational Numbers

Definition 6.1. We define the equivalence relation R on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ as follows:

$$((a,b),(c,d)) \in R \iff ad = bc.$$

Definition 6.2. We define the set of rational numbers $\mathbb{Q}$ as the set of equivalence classes of the relation R on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Definition 6.3 (Addition)**.** We define the addition on $\mathbb{Q}$ as follows:

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$

for every $[(a,b)], [(c,d)] \in \mathbb{Q}$.

Definition 6.4 (Multiplication)**.** We define the multiplication on $\mathbb{Q}$ as follows:

$$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

for every $[(a,b)], [(c,d)] \in \mathbb{Q}$.

Definition 6.5 (Order Relation)**.** We define the order relation on $\mathbb{Q}$ as follows:

$$[(a,b)] < [(c,d)] \iff ad < bc$$

for every $[(a,b)], [(c,d)] \in \mathbb{Q}$.

7. Real Numbers

Strategy 1: Dedekind Cuts

Definition 7.1 (Dedkind Set)**.** A subset A of $\mathbb{Q}$ is called a Dedekind set if it satisfies the following properties:

1. A is non-empty and not equal to $\mathbb{Q}$;
2. for every $x, y \in \mathbb{Q}$, if $x \in A$ and $y < x$, then $y \in A$;
3. for every $x \in A$, there exists $y \in A$ such that $x < y$.

Definition 7.2 (Real Numbers)**.** We define the set of real numbers $\mathbb{R}$ as the set of all Dedekind sets or the set of all Cauchy sequences in $\mathbb{Q}$.

Strategy 2: Cauchy Sequences

Definition 7.3 (Cauchy Sequence)**.** A sequence (a_n) in $\mathbb{Q}$ is called a Cauchy sequence if for every $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for every $m, n > N$, $|a_n - a_m| < \epsilon$.

Definition 7.4. We define the equivalence relation R on the set of Cauchy sequences in $\mathbb{Q}$ as follows:

$$((a_n),(b_n)) \in R \iff \lim_{n\to\infty} |a_n - b_n| = 0.$$

Definition 7.5 (Real Numbers)**.** We define the set of real numbers $\mathbb{R}$ as the set of equivalence classes of the relation R on the set of Cauchy sequences in $\mathbb{Q}$.

Arithmetic Properties of Real Numbers In this subsection, we will use the Dedekind cut approach to define the arithmetic operations and order relation on $\mathbb{R}$.

Theorem 7.6 (Least Upper Bound Property)**.** *Every non-empty subset of $\mathbb{R}$ that is bounded above has a least upper bound in $\mathbb{R}$.*

Definition 7.7. We define the addition on $\mathbb{R}$ as follows:

$$A + B = \{x + y : x \in A, y \in B\}$$

for every $A, B \in \mathbb{R}$.

References