1. Review of set theory

In this lecture, we will review some basics of axiomatic set theory that will be needed later. We will be a little free with notation and incomplete in places. Proofs of Propositions proved in class are usually omitted. The goal is to develop just enough set theory that would be needed and to clear up any ‘mysteries’ about ‘sets’ and ‘classes’ – so that we are comfortable with them in the rest of the course. We follow mostly [Jec03, Chapter 1] and [CL93, Chapter 7].

1.1. Language. The language of set theory is that of first order predicate logic with atomic predicates of two kinds:

(1) $x = y$ (‘set equality’);

(2) $x \in y$ (‘is a member of’)

Date: January 15, 2019.
A *formula* is built out of atomic predicates using the logical connectives
\[ \lor, \land, \neg, \]
and quantifiers
\[ \exists, \forall. \]

For example:

\[ F := \exists v_0 \forall v_1 \neg(v_1 \in v_0) \]  \hspace{1cm} (1.1)

is a formula.

(The above formula of course has several parentheses in addition to the atomic predicates and logical connectives, but these are used only for clarity and we will continue to use them.) The ‘free variables’ in a formula are those which are not ‘bound’ by any quantifiers. A formula without any free variables (such as the one in (1.1)) will be called a *sentence*.

1.2. **ZFC.** Ordinary mathematics is based on the set of axioms called ZFC (Zermelo-Fraenkel+Choice). We introduce them sequentially as follows (two axioms – that of regularity and choice will be introduced in the next lecture).

1. (Extensionality)

\[ \forall v_0 \forall v_1 \forall v_3(v_3 \in v_0 \iff v_3 \in v_1) \iff (v_0 = v_1). \]

(Two sets are equal if and only if they have the same elements.)

2. (Pair)

\[ \forall v_0 \forall v_1 \exists v_3 \forall v_4(v_4 \in v_3) \iff ((v_4 = v_0) \lor (v_4 = v_1)). \]

(For any two sets \( v_0, v_1 \), there exists a set \( v_3 \) containing exactly \( v_0 \) and \( v_1 \) as its members.)

3. (Axiom of the union)

\[ \forall v_0 \exists v_1 \forall v_2(v_2 \in v_1 \iff (\exists v_3(v_3 \in v_0 \land v_2 \in v_3))). \]
(For each set \(v_0\) the union of its element (which we will denote by \(\bigcup v_0\)) is again a set.)

4. (Power set axiom)

\[
\forall v_0 \exists v_1 \forall v_2 v_2 \in v_1 \iff (\forall v_3 (v_3 \in v_2 \Rightarrow v_3 \in v_0)).
\]

(For each set \(v_0\), there exists a set (which we will denote by \(P(v_0)\), whose members are the subsets of \(v_0\).)

5. (Axiom scheme for weak comprehension) For each formula \(F[v_0, v_1, \ldots, v_m]\)

we have the axiom \((5)_F:\)

\[
\forall v_1 \cdots \forall v_m \forall v_{m+1} \exists v_{m+2} \forall v_0 (v_0 \in v_{m+2} \iff (v_0 \in v_{m+1} \iff F[v_0, v_1, \ldots, v_m])).
\]

(For each tuple of ‘parameters’ \(v_1, \ldots, v_m\), and for all set \(v_{m+1}\), the subset of \(v_{m+1}\) consisting of its members \(v_0\) satisfying \(F[v_0, v_1, \ldots, v_m]\) is a set.)

**Remark 1.** Firstly, note it is an ‘axiom scheme’ because it is a list of axioms – one for each formula \(F\). Secondly, its a replacement (or weakening) of the full axiom scheme of comprehension, which would read

“For each formula \(F[v_0, v_1, \ldots, v_m]\), we have the axiom

\[\forall v_1 \cdots \forall v_m \exists v_0 F[v_0, v_1, \ldots, v_m]\]”

Assuming this version of the axiom of comprehension leads to Russell’s paradox. Namely, consider the formula \(F[v_0] := \neg(v_0 \in v_0)\). Not assuming the full axiom of comprehension however leads to other troubles such as not being able to define unions etc. This leads to adding more axioms.

6. (Axiom scheme of replacement) For each formula \(F[w_0, w_1, v_1, \ldots, v_m]\)

we have the axiom \((6)_F:\)

\[
\forall v_0 \forall v_1 \cdots \forall v_m (\forall w_0 \forall w_1 \forall w_2 ((F[w_0, w_1, v_1, \ldots, v_m] \land F[w_0, w_2, v_1, \ldots, v_m] \Rightarrow w_1 = w_2))) \Rightarrow
\]
\[(\exists v_{m+1} \forall v_{m+2}(v_{m+2} \in v_{m+1}) \iff \exists w_0(w_0 \in v_0) \land F[w_0, v_{m+2}, v_1, \ldots, v_m])\].

(The formula
\[\forall v_1 \ldots \forall v_m (\forall w_0 \forall w_1 \forall w_2((F[w_0, w_1, v_1, \ldots, v_m] \land F[w_0, w_2, v_1, \ldots, v_m] \Rightarrow w_1 = w_2)))\]
states the for all values of the ‘parameters’ \(v_1, \ldots, v_m\), the formula \(F[w_0, w_1, v_1, \ldots, v_m]\) defines a partial function defined on a subset of \(w_0\) (we say that \(F\) is ‘functional’ on \(w_0\)). The axiom (6)\(_F\) then states that if \(F\) is functional on \(w_0\), then for all values of the parameters \(v_1, \ldots, v_m\), and for each set \(v_0\), the ‘image’ of the partial function defined by \(F\) on \(v_0\) is a set.)

**Exercise 1.** Prove that the axiom scheme (6) implies the axiom scheme (5). (We include the axiom scheme (5) for historical reasons. More precisely, the axioms (1), (2), (5), (3), (4) and (7) (introduced later) is what is known as Zermelo set theory (denoted \(Z\)), while axioms (1), (2), (3), (4), (6), and (7) (introduced later) constitute a stronger theory called Zermelo-Fraenkel set theory (denoted \(ZF\)).)

**Definition 1** (Ordered pairs and Cartesian products). Given two sets \(a\) and \(b\), we call the set \(\{\{a\}, \{a, b\}\}\) the ordered pair \(a, b\) and denote it by \((a, b)\). It exists by using the axiom of pairs three times.

For sets \(x, y\), the collection of all ordered pairs \((a, b), a \in x, b \in y\) is a set and will be denoted by \(x \times y\).

**Exercise 2.** Prove that the collection of all ordered pairs \((a, b), a \in x, b \in y\) is a set. (Hint. Notice that \(x \times y \subset P(P(x \cup y))\). Use Axioms (3) and (5).)

**Exercise 3.** Now prove that there exists a set (denoted \(y^x\)) whose members are functions \(x \rightarrow y\). (Hint. A function is a binary relation satisfying a certain extra condition – so \(y^x \subset P(x \times y)\).

1.3. **Classes.** As mentioned above the “full comprehension axiom” leads to Russell’s paradox. Nevertheless, for any fixed formula
\[F[v_0, v_1, \ldots, v_n],\]
and any fixed tuple of sets \((p_1, \ldots, p_n)\) it makes sense to consider the collection of sets \(\{x \mid F[x, p_1, \ldots, p_n]\}\), except that this might not be a set. We call the collection \(\{x \mid F[x, p_1, \ldots, p_n]\}\) a class definable from \(p_1, \ldots, p_n\). We will say that a class is \textit{definable} if it is defined by a formula \(F[v_0]\) with no parameters (i.e. \(n = 0\)).

We will denote classes by bold letters (with a few standard exceptions).

If \(C\) is the class defined by \(F[v_0, v_1, \ldots, v_n]\) for a fixed tuple \((p_1, \ldots, p_n)\) of sets, we say that a set \(x\) is a member of \(C\) if \(F[x, p_1, \ldots, p_n]\) is true, and denote \(x \in C\). This extends the membership relation to classes. However, note that the left hand side of every use of \(\in\) must always be a set.

Every set is a class. Take \(F[v_0, v_1] := (v_0 \in v_1)\). For each set \(p\), the class defined by \(F\) is equal to \(p\).

But not all classes are sets. For example, the class (denoted \(V\)) of all sets. \(V\) is defined by the formula \(F[v_0] := (v_0 = v_0)\) (with no parameters, and hence \(V\) is a definable class). A class that is not a set is called a \textit{proper class}. \(V\) is a proper class (otherwise, you get contradiction from Russell’s paradox).

One can define the notion of being a subclass of a class. If \(C\) and \(D\), then one can define the class \(C \times D\) and the notion of relations and functions as subclasses of the class \(C \times D\). We will denote such class functions/relations by bold letters as well.

1.4. \textbf{Order.} We discuss some properties of orders. Recall the notion of linear and partial order on sets.

\textbf{Definition 2.} A (partial) order \(\prec\) on a set \(x\) is a binary relation on \(x \times x\), which is irreflexive and transitive. A partial order \(\prec\) on \(x\) is a linear (also sometimes called total) order if for every \(a, b \in x\), exactly one of three alternatives, \(a = b, a < b, b < a\) is true.

Given a partially ordered set \((x, \prec)\) and a subset \(w \subseteq x\), the notions of sup, inf, greatest, least element etc. of \(w\) coincides with the usual mathematical definitions of these terms. A subset \(w\) is a \textit{chain} if the induced order on \(w\) is a linear order. A subset \(w\) is an initial segment of \(x\) if it satisfies \(\forall u \forall v (v \in w) \land (u \in x) \land (u < v) \Rightarrow (v \in w)\).
Definition 3. Given two linearly ordered sets \((P, <_P)\) and \((Q, <_Q)\), a map \(f : P \rightarrow Q\) is called an isomorphism if \(f\) is order-preserving and bijective.

Definition 4. A set is well-ordered by a linear order \(<\) if every non-empty subset has a least element.

Exercise 4. Suppose that \(x\) is a set well-ordered by \(<\) and \(w \subset x\) is a proper (i.e. \(w \neq x\)) initial segment of \(x\). Then, there exists \(v \in x\) such that \(w = \{u \in x | u < v\}\).

The following proposition was proved in class.

Proposition 1. Let \((x,<_x),(y,<_y)\) be two well-ordered sets. Then, one of the following two alternatives (or both) must hold.

1. There exists a unique initial segment \(y_1 \subset y\), and a unique isomorphism \(f : (x,<_x) \rightarrow (y_1,<_y|y_1)\);

2. There exists a unique initial segment \(x_1 \subset x\), and a unique isomorphism \(g : (y,<_y) \rightarrow (x_1,<_x|x_1)\);

If both alternatives hold, then \(x_1 = x\), \(y_1 = y\) and \(f, g\) are inverses.

Exercise 5. No well-ordered set is isomorphic to an initial segment of itself.

Definition 5. A set \(x\) is said to have the transitive property if \(y \in x \rightarrow y \subset x\). In other words, \(\alpha \in x \land \beta \in \alpha \Rightarrow \beta \in x\).

1.5. Ordinals.

Definition 6. An ordinal is a transitive set which is well-ordered by the \(\in\) relation (i.e. A set \(\alpha\) is an ordinal if and only if \(\alpha\) is transitive and the relation \(\beta < \gamma \iff \beta \in \gamma\) on members \(\beta, \gamma \in \alpha\) is a well-ordering.

The following propositions were proved in class.

Proposition 2. Suppose \(\alpha, \beta\) are ordinals and \(f : \alpha \rightarrow \beta\) is an isomorphism. Then, \(\alpha = \beta\) and \(f\) is the identity map.
Proposition 3. Suppose $\alpha, \beta$ are ordinals. Then, exactly, one of the following three alternatives hold.

$$\alpha = \beta, \alpha \in \beta, \beta \in \alpha.$$ 

Exercise 6. Suppose $\alpha$ is an ordinal.

1. Prove that $\alpha \not\in \alpha$.

2. Then, prove that $\alpha \cup \{\alpha\}$ is also an ordinal, and that it is the least ordinal not equal to $\alpha$. We will denote the ordinal $\alpha \cup \{\alpha\}$ by $\alpha + 1$ and call it the successor ordinal of $\alpha$. An ordinal which is not a successor ordinal will be called a limit ordinal.

Exercise 7. (1) Prove that there exists a formula $\text{On}[v_0]$ such that a set $\alpha$ is an ordinal if and only if $\text{On}[\alpha]$ is true. Deduce that the ordinals form a definable class (which we will denote by $\text{Ord}$).

2. Prove that if $\alpha \in \text{Ord}$, and $\beta \in \text{Ord}$, then $\beta \in \text{Ord}$. (Thus, the class of ordinals itself has the ‘transitive’ property).

3. Prove that if $C$ is a non-empty subclass of $\text{Ord}$, then $C$ has a least element.

4. Prove that $\text{Ord}$ is a proper class. (Hint. If $\text{Ord}$ is a set, then it will be itself an ordinal.)

Definition 7 (Finite and infinite ordinals). An ordinal that is non-empty and not a successor ordinal is called a limit ordinal. An ordinal $\alpha$ is a finite ordinal if neither $\alpha$ nor any of its members is a limit ordinal. An ordinal is an infinite ordinal if it is not a finite ordinal.

(7) (Axiom of infinity) There exists an infinite ordinal.

Till now we could not deduce if the class $V$ of sets is actually non-empty. Axiom (7) assures us that $V$ is non-empty.

Definition 8. The least infinite ordinal (which exists by Part (3) of Exercise (7)) will be denoted by $\omega$. 

Exercise 8. Prove that $\omega$ is equal to the set of all finite ordinals. Also, the empty set exists.

Exercise 9. Deduce from Axioms (7) and (5) that there exists an empty set (which we will denote by $\emptyset$).

Example 1. The following ordinals are finite.

$$
0 := \emptyset, \\
1 := \{0\}, \\
2 := \{0, 1\}, \\
: 
$$

The sets $0, 1, 2 \ldots \in \omega$, but there might very well be finite ordinals not belonging to this list but which nevertheless belong to $\omega$. We will call them non-standard natural numbers.

Definition 9 (Disjoint Union). For $a, b$ sets we will denote by $x \cup y$ the set $\{(x, \emptyset)|x \in a\} \cup \{(y, \{\emptyset\})|y \in b\}$.

Proposition 4. Let $(x <)$ be a well-ordered set. Then, there exists a unique ordinal $\alpha$ such that $x$ is isomorphic to $\alpha$, and there is a unique isomorphism from $\alpha$ onto $x$.

1.6. Ordinal Arithmetic.

(1) (Ordinal sum) Let $\alpha, \beta$ be ordinals. Let $<$ be the order on $\alpha \cup \beta$ defined as follows. Let

$$
\alpha' = \{x \in \alpha \cup \beta | \exists uu \in \alpha \land x = (u, \emptyset)\},
$$

and

$$
\beta' = \{x \in \alpha \cup \beta | \exists vv \in \beta \land x = (v, \{\emptyset\})\}.
$$

For $x, y \in \alpha \cup \beta$, $x < y$ if and only if $x \in \alpha'$ and $y \in \beta'$, or else $x = (u, \emptyset), y = (v, \emptyset) \in \alpha'$ and $u \in v$, or $x = (u, \{\emptyset\}), y = (v, \{\emptyset\}) \in \beta'$ and $u < v$. 
Exercise 10. Prove that the ordering defined above on $\alpha \uplus \beta$ is a well-ordering.

We denote the unique ordinal isomorphic to the $\alpha \uplus \beta$ (well-ordered by the ordering described above) as $\alpha + \beta$.

Exercise 11. (a) Prove that $\alpha + 0 = \alpha$.

(b) Prove that the definition of $\alpha + 1$ is consistent with the definition of $\alpha + 1$ in Part 2 in Exercise 6.

(2) (Ordinal product) Let $\alpha, \beta$ be ordinals. Define an order on $\alpha \times \beta$ by $(x, y) < (x', y') \Rightarrow (y < y') \lor ((y = y') \land (x < x'))$.

Exercise 12. Prove that this defines an well-ordering on $\alpha \times \beta$.

We abuse notation and denote the unique ordinal isomorphic to the $\alpha \times \beta$ (well ordered as above), also by $\alpha \times \beta$.

(3) (Ordinal exponentiation) Given ordinal $\alpha, \beta$, recall that $\alpha^\beta$ is the set of functions $f : \beta \to \alpha$. We order $\alpha^\beta$ as follows. Given $f, f' \in \alpha^\beta$, $f < f'$ if and only if $f \neq f'$ and $f(\gamma) < f'(\gamma)$, where $\gamma$ is the least element of the non-empty subset $\{x \in \beta | f(x) \neq f'(x)\}$.

Exercise 13. Prove that the above order defined above is a well-ordering of $\alpha^\beta$.

We again abuse notation and denote by $\alpha^\beta$ the unique ordinal isomorphic to the set $\alpha^\beta$ well-ordered as above.

Exercise 14. Let $\alpha, \beta, \gamma$ be ordinals. Prove that:

(i) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$

(ii) $1 + \omega = \omega < \omega + 1$

(ordinal addition is associative but not commutative in general (!));
(iii) \[ \alpha \times (\beta \times \gamma) = (\alpha \times \beta) \times \gamma \]

(iv) \[ 2 \times \omega = \omega < \omega \times 2 \]

(ordinal multiplication is associative but not commutative in general (!));

(v) \[ \alpha \times (\beta + \gamma) = (\alpha \times \beta) + (\alpha \times \gamma); \]

(vi) also prove that \((\beta + \gamma) \times \alpha\) need not equal \((\beta) + (\gamma \times \alpha)\) by showing

\[ 2 \times \omega = (1 + 1) \times \omega \neq \omega + \omega; \]

(vii) \[ \alpha + 0 = \alpha = 0 + \alpha; \]

(viii) \[ \alpha \times 0 = 0 = \alpha \times 0; \]

(ix) \[ \alpha \times 1 = \alpha = 1 \times \alpha; \]

(x) if \(\alpha, \beta\) are finite ordinals, then so are \(\alpha + \beta, \alpha \times \beta, \alpha^\beta; \)

(xi) if \(\alpha + 1 = \beta + 1\), then \(\alpha = \beta; \)

(xii) addition and multiplication of finite ordinals are commutative.

**Exercise 15.** If \(A\) is a set of ordinals prove that \(\bigcup A\) is also an ordinal, and \(\bigcup A = \sup A\).

Anticipating the formal definition of a ‘structure’ which will come later:

**Definition 10.** We will call the tuple \(\langle \omega, 0, 1, +, \times \rangle\) the structure of natural numbers and denote it by \(\mathbb{N}\).


REFERENCES


Department of Mathematics, Purdue University, West Lafayette, IN 47906, U.S.A.

E-mail address: sbasu@math.purdue.edu