Math 141a - Mathematical Logic I

Taught by Sebastien Vasey
Notes by Dongryul Kim

Fall 2018

¡+instructor+¿ ¡+meetingtimes+¿ ¡+textbook+¿ ¡+enrolled+¿ ¡+grading+¿ ¡+courseassistants+¿

Contents

1 September 7, 2018

Logic is roughly studying the foundational objects of math, for instance, sets, statements, proofs, etc.

1.1 Overview

Let me tell you few of the theorems we are going to discuss.

Theorem 1.1 (Gödel's completeness theorem)**.** *Let T be a list of first-order axioms, and let φ be a first-order statement. Then $T \vdash \varphi$ if and only if $T \vDash \varphi$.*

The first symbol $T \vdash \varphi$ means that there is a proof of φ from the axioms in T. The second symbol $T \vDash \varphi$ means that any structure satisfying the axioms in T also satisfies φ. A proof shows that it is true for every structure, but the other direction is subtle. It means that if I can't find a unicorn everywhere, then there is a proof that show that unicorns don't exist.

Example 1.2. Let R be a binary relation, and let

$$\begin{aligned} T &= \text{“}R \text{ is an equivalence relation”} \\ &= \{\forall x R(x,x), \forall x \forall y (R(x,y) \to R(y,x)), \\ &\qquad \forall x \forall y \forall z (R(x,y) \wedge R(y,z) \to R(x,z))\}. \end{aligned}$$

So if there is a statement that is true for every equivalence relation, it has a proof. For instance,

$$\varphi = \forall x \forall y \forall z ((R(x,y) \wedge \neg R(y,z)) \to \neg R(x,z))$$

has a proof.

So it is an interesting relation between syntax and semantics. Some cool consequences include the compactness theorem.

Theorem 1.3 (compactness theorem)**.** *Let T be a list of first-order axioms. If every finite subset of T is satisfied by some structure, then T is satisfied by a structure.*

Consider the structure of $(\mathbb{R}, +, \cdot, 0, 1)$. Let us abstractly look at all the statements that are true for the real numbers and call this set T. For instance, $\forall x \forall y (x \cdot x + y \cdot y = 0 \to x = 0 \wedge y = 0)$. Now what we can do is to consider

$$T' = T \cup \{0 < c, c < 1, c < \tfrac{1}{2}, c < \tfrac{1}{3}, \dots\}.$$

Then every finite subset of $T_0 \subseteq T'$ is a subset of $T \cup \{0 < c, c < 1, \dots, c < \frac{1}{n}\}$ for some n. This is satisfied by $(\mathbb{R}, +, \cdot, 0, 1, c = \frac{1}{n+1})$. By compactness, there is a structure satisfying this, say $\mathbb{R}^*$. One way to actually construct it is to take an ultraproduct of $\mathbb{R}$. Using this, you can do non-standard analysis.

Another application of the compactness theorem is the Ax–Grothendieck theorem.

Theorem 1.4 (Ax–Grothendieck). *If $f : \mathbb{C}^n \to \mathbb{C}^n$ is a polynomial mapping and f is injective, then f is surjective.*

Note that an injective function from a finite set to itself is automatically bijective. In this case, using the compactness theorem, you can pretend that $\mathbb{C}$ is a finite set. There are other proofs, but they are nontrivial.

We can also talk about the back and forth method. You can show that $(\mathbb{Q}, <)$ is the unique countable dense linear order without endpoints. This also shows that the first-order theory of $(\mathbb{Q}, <)$ is decidable, i.e., that is an algorithm that proves of disproves anything about $(\mathbb{Q}, <)$.

1.2 Counting

We can count pass infinity as

$$0, 1, 2, \dots, n, \dots, \omega, \omega + 1, \omega + 2, \dots, \omega + \omega, \dots, \omega \cdot \omega, \dots, \omega^\omega, \dots.$$

These are called **ordinals**. We define an ordinal as the set of ordinals below it, for instance as $\alpha + 1 = \alpha \cup \{\alpha\}$. They will be used to generalize induction to transfinite induction.

We can also define **cardinals**. We say that the two sets X and Y have the same cardinality if there is a bijection between them. We define the cardinality of X as the least ordinal α that has the same cardinality as X.

Proposition 1.5 (well-ordering principle). *The statement that every set has a cardinality is equivalent to the Axiom of Choice.*

2 September 10, 2018

Ordinals are like countings.

2.1 Ordinals

Definition 2.1. A **chain** is a pair $(A, <)$ where A is a set and $<$ is a binary relation on A which is:

- transitive, if $x < y$ and $y < z$ then $x < z$,
- irreflexive, $x < x$ for all $x < x$,
- total, if $x \neq y$ then either $x < y$ or $y < x$.

Example 2.2. The following are all chains: $(\mathbb{N}, <)$, $(\mathbb{Z}, <)$, $(\mathbb{Q}, <)$, $(\{0, 1\}, <)$. But $(\{\emptyset, \{0\}, \{1\}\}, \subsetneq)$ is not a chain.

For $(A, <)$ and $(B, <)$ chains, a function $f : (A, <) \to (B, <)$ is called **order-preserving** if $a_1 < a_2$ implies $f(a_1) < f(a_2)$. An isomorphism is an order-preserving bijection.

Example 2.3. The function $f : (\mathbb{N}, <) \to (\mathbb{N}, <)$ given by $n \mapsto n + 1$ is order-preserving. But $\mathbb{Z} \to \mathbb{N}$ given by $n \mapsto |n|$ is not order-preserving. In fact, there is no order-preserving map for $\mathbb{Z}$ to $\mathbb{N}$.

We can define $A + B$ for A and B chains, given by $A \amalg B$ with $a < b$ for all $a \in A$ and $b \in B$. We can also define $A \cdot B$ with the lexicographical order.

Definition 2.4. A **well-ordering** is a chain $(A, <)$ such that for every $S \subseteq A$ nonempty, there is a minimal element $x \in A$.

Any finite chain is a well-ordering, but $(\mathbb{Z}, <)$ is not.

Lemma 2.5. *If $(A, <)$ and $(B, <)$ are well-orderings, then either A is isomorphic to an initial segment of A.*

Definition 2.6. For $(A, <)$ a chain, a subset $A_0 \subseteq A$ is called an **initial segment** if for any $a < b$, $b \in A_0$ implies $a \in A_0$. That is, if $a \in A_0$ then

$$\mathrm{pred}_A(a) = \{b \in A : b < a\}$$

is in A_0.

So if you have two well-orderings, they are comparable. If $(A, <)$ is a well-ordering and $A_0 \subseteq A$ is an initial segment, then either $A_0 = A$ or $A \setminus A_0$ has a least element and

$$A_0 = \mathrm{pred}_A(a).$$

Indeed, any well-ordering is isomorphic to the set of predecessors, ordered by inclusion.

Lemma 2.7. *Let $(A,<)$ and $(B,<)$ be well-orderings. Let $f,g:(A,<)\to(B,<)$ be isomorphisms onto initial segments. Then $f=g$.*

Proof. Assume $f\neq g$, and then there exists a minimal $a\in A$ where $f(a)\neq g(a)$. Assume $f(a)<g(a)$, without loss of generality. Because $g[A]$ is an initial segment, we have $f(a)\in g[A]$. If we let $a'\in A$ be such that $g(a')=f(a)$, then $g(a')=f(a)<g(a)$ implies that $a'<a$. But $f(a')=g(a')=f(a)$ gives a contradiction. □

Now we can prove the lemma.

Proof of Lemma 2.5. We look at the set of $a\in A$ such that $\mathrm{pred}(a)$ is not isomorphic to a proper initial segment of B. If this set is nonempty, we may take a minimal a with this property. For any $a_0<a$, we have that $\mathrm{pred}(a_0)$ is isomorphic to $\mathrm{pred}(b_{a_0})$ for some $b_{a_0}\in B$. This is moreover unique. If we let

$$f:\mathrm{pred}(a)\to B;\quad a_0\mapsto b_{a_0},$$

this is order-preserving isomorphism onto an initial segment of B. It cannot be proper by assumption, so it is an isomorphism. Then $f^{-1}:B\to A$ shows that B is an isomorphism to an initial segment of A.

Now assume that all $\mathrm{pred}(a)$ are isomorphic to initial segments of B. If we pick $b_a\in B$ so that $\mathrm{pred}(a)\cong\mathrm{pred}(b_a)$, then

$$f:(A,<)\to(B,<);\quad a\mapsto b_a$$

is an order-preserving isomorphism to an initial segment of B. □

Ordinals are canonical representatives of well-orderings. Every ordinal will be the set of its predecessors.

Definition 2.8. An **ordinal** is a set α which is

- transitive, $x\in\alpha$ and $y\in x$ then $y\in\alpha$,
- $(\alpha,\in)$ is a well-ordering,

Examples include

$$0=\emptyset,\quad 1=\{\emptyset\},\quad 2=\{0,1\},\quad \ldots,\quad \omega=\{0,1,2,\ldots\},\quad \omega+1=\omega\cup\{\omega\},\ldots.$$

If α is an ordinal, you can take $\alpha+1=\alpha\cup\{\alpha\}$, which is again an ordinal. If $(\alpha_i)_{i\in I}$ are ordinals, then

$$\alpha=\bigcup_{i\in I}\alpha_i$$

is an ordinal, called $\sup_{i\in I}\alpha_i$. For instance, $\omega=\sup_{n\in\omega}n$. If $x\in\alpha$, then

$$\mathrm{pred}_{(\alpha,\in)}(x)=x.$$

Lemma 2.9. *If α and β are isomorphic ordinals, then $\alpha=\beta$.*

Proof. Let $f : (\alpha, \in) \cong (\beta, \in)$. We claim that f is the identity. If not, there exists a minimal $a \in \alpha$ such that $f(a) \neq a$. Then

$$f(a) = \mathrm{pred}_{(\beta,\in)}(f(a)) = f[a] = a$$

because f is the identity on a. $\square$

Lemma 2.10. *Any well-ordering is uniquely isomorphic to a unique ordinal.*

Proof. We claim that if $a \in A$ has $\mathrm{pred}(a) \cong (\alpha_a, \in)$, then we can take

$$\alpha = \{\alpha_a : a \in A\}$$

and then α is an ordinal and $a \mapsto \alpha_a$ is the desired isomorphism. If there is $a \in A$ such that $\mathrm{pred}(a)$ is not isomorphic to an ordinal, we can take the minimal one. Then applying the claim gives a contradiction. $\square$

3 September 14, 2018

Last time we defined an ordinal as a transitive set such that $(\alpha, \in)$ is a well-ordering. We showed that any well-ordering is isomorphic to a unique ordinal. The intuition is that an ordinal is the set of its predecessors. For α, β ordinals, we are going to write $\alpha < \beta$ instead of $\alpha \in \beta$. In the homework, you are going to show that for α and β ordinals, either $\alpha = \beta$ or $\alpha < \beta$ or $\beta < \alpha$.

3.1 Operations on ordinals

- Given an ordinal α, we define $\alpha + 1 = \alpha \cup \{\alpha\}$.
- Given $(\alpha_i)_{i \in I}$ a set of ordinals, we define $\sup_{i \in I} \alpha_i = \bigcup_{i \in I} \alpha_i$. This is the least α such that $\alpha \geq \alpha_i$ for all $i \in I$.

Definition 3.1. For ordinals α and β, we define $\alpha + \beta$ to be the unique ordinal isomorphic to $(\alpha, \in) + (\beta, \in)$. Likewise, $\alpha \cdot \beta$ is the unique ordinal isomorphic to $(\alpha, \in)(\beta, \in)$, which is α copied β times.

On finite ordinals, these are usual addition and multiplication. We have

$$1 + \omega = \omega, \quad \omega + 1 > \omega, \quad \omega \cdot 2 = \omega + \omega, \quad 2 \cdot \omega = \omega.$$

You can do division: if α is an ordinal and $\beta > 0$, then there exist unique ordinals γ and $\delta < \beta$ such that

$$\alpha = \beta \cdot \gamma + \delta.$$

Lemma 3.2 (transfinite induction)**.** *Any nonempty collection S of ordinals has a minimal element.*

Proof. Pick $\alpha \in S$. If α is minimal, we are done. Otherwise, we can take the minimal element in $S \cap \alpha$. □

Corollary 3.3. *Let $P(x)$ be a property of ordinals. Suppose that*

> *For any ordinal α, $P(\beta)$ for all $\beta < \alpha$ implies $P(\alpha)$.*

Then $P(\alpha)$ for all ordinal α.

Proof. If not there is a minimal α such that $P(\alpha)$ is false. This contradicts our assumptions. □

There are three types of ordinals. That is, for any ordinal α, exactly one of the following three is true:

- $\alpha = 0$
- $\alpha = \beta + 1$ for some β (these are called **successors**)
- $\alpha > 0$ and $\beta + 1 < \alpha$ for any $\beta < \alpha$ (these are called **limit ordinals**).

So we can we can restate transfinite induction as the following.

Corollary 3.4. *Let $P(x)$ be a property of ordinals. Suppose that*

- $P(0)$,
- $P(\alpha)$ *implies* $P(\alpha+1)$,
- $P(\beta$ *for all* $\beta < \alpha$ *implies* $P(\alpha)$, *if* α *is a limit.*

Then $P(\alpha)$ *for all ordinals* α.

We can also define objects by transfinite induction. We define

- $\alpha + 0 = \alpha$,
- $\alpha + (\beta + 1) = (\alpha + \beta) + 1$,
- $\alpha + \beta = \sup_{\gamma<\beta} \alpha + \gamma$ if β is a limit ordinal.

This, you can check again by induction, is equivalent to the previous definition. Similarly, we can define

- $\alpha \cdot 0 = 0$,
- $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$,
- $\alpha \cdot \beta = \sup_{\gamma<\beta} \alpha \cdot \gamma$ if β is a limit ordinal.

We can even define exponentiation as

- $\alpha^0 = 1$,
- $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$,
- $\alpha^\beta = \sup_{\gamma<\beta} \alpha^\gamma$.

Any ordinal has a base ω representation, so we can write

$$\alpha = c_1\omega^{\beta_1} + c_2\omega^{\beta_2} + \cdots + c_n\omega^{\beta_n},$$

where $c_i < \omega$.

3.2 Cardinalities

Theorem 3.5. *For any set X, there is an ordering such that $(X, <)$ is a well-ordering.*

For instance, for $X = \mathbb{R}$, the new ordering doesn't need to have anything to do with the usual ordering. For instance, we can pick things $a_0 = 0$, $a_1 = -1$, $a_2 = \frac{1}{2}$, $a_3 = \pi$, $a_4 = \sqrt{2}$, and so on. So we keep arbitrarily picking these elements. This is not a rigorous proof, and we are going to see the rigorous proof next time.

Definition 3.6. The **cardinality** $|X|$ of a set X is the minimal ordinal α such that there is a well-ordering of X isomorphic to α.

For instance,

$$|\omega| = \omega, \quad |\omega + 1| = \omega.$$

Definition 3.7. An ordinal is a **cardinal** if $\alpha = |\alpha|$.

For example, n is a cardinal for any $n < \omega$. Although ω is a cardinal, $\omega+1, \omega+2, \dots, \omega+\omega, \dots, \omega\cdot\omega$ are all not cardinals. For sets X and Y, there is a bijection from X to Y if and only if $|X| = |Y|$. There is an injection from X to Y if and only if $|X| \leq |Y|$. Note that if X and Y are two sets, either $|X| < |Y|$ or $|X| > |Y|$ or $|X| = |Y|$.

Theorem 3.8 (Cantor)**.** *For any set X, $|X| < |\mathcal{P}(X)|$.*

Proof. We have $|S| \leq |\mathcal{P}(X)|$ because $x \mapsto [x]$ is injective. Suppose for a contradiction that $|X| = |\mathcal{P}(X)|$. Then there should be a bijection

$$F : X \to \mathcal{P}(X).$$

Now consider the set

$$Y = \{x \in X : x \notin F(x)\} \subseteq X.$$

Then there is a $x \in X$ such that $F(x) = Y$. If $x \in Y$, then $x \in Y = F(x)$ so $x \notin Y$. On the other hand, if $x \notin Y$ then $x \notin F(x) - Y$ implies $x \in Y$. This gives a contradiction. □

Corollary 3.9. *For any cardinal κ, there is a cardinal $\lambda > \kappa$.*

Definition 3.10. Let κ^+ be the minimal cardinal above κ.

Then we can play around with the definitions. We can define

- $\aleph_0 = \omega$,
- $\aleph_{\alpha+1} = (\aleph_\alpha)^+$,
- $\aleph_\alpha = \sup_{\beta<\alpha} \aleph_\beta$ if α is a limit.

We can think of $\aleph_\alpha$ as the αth infinite cardinal.

Theorem 3.11. *For any cardinal λ, there is α such that $\lambda = \aleph_\alpha$.*

Proof. We do this by induction on λ. Take the minimal λ where this fails. Then either $\lambda = \kappa^+$ or $\kappa^+ < \lambda$ for all $\kappa < \lambda$. Apply the induction hypothesis. □

The continuum hypothesis states that $\aleph_1 = |\mathbb{P}(\mathbb{N})| = 2^{\aleph_0}$. The generalized continuum hypothesis that $\kappa^+ = |\mathcal{P}(\kappa)|$ for every infinite cardinal κ.

Index