Mathematical Logic

Lecture 7, Monday May 22, 2023

Ari Feiglin

7.1 Transfinite Induction

Lemma 7.1.1 (Transfinite Induction):

Let $P(\alpha)$ be some property of ordinals. Suppose that P has the property that if $P(\gamma)$ is true for every $\gamma < \beta$, then $P(\beta)$ is true. Then P is true for all ordinals.

Proof:

Suppose that $P(\alpha)$ is false for some ordinal α. Let

$$X = \{\gamma \leq \alpha \mid P(\gamma) \text{ is false}\}$$

then since X is a set of ordinals, it is well-ordered and since it is non-empty, it has a minimum element β. So $P(\beta)$ is false, but for every $\gamma < \beta$, $\gamma \notin X$ and so $P(\gamma)$ is true. But then $P(\beta)$ is true, in contradiction. ■

Definition 7.1.2:

Two chains $(X, \leq)$ and $(Y, \leq)$ are called **isomorphic** if there exists a bijection $f\colon X \longrightarrow Y$ such that if $x \leq y$ then $f(x) \leq f(y)$.

Since chains are total orders, if $f(x) \leq f(y)$ then since $x \leq y$ or $y < x$, and if $y < x$ then $f(y) < f(x)$ which is a contradiction, two chains are isomorphic if $x \leq y$ if and only if $f(x) \leq f(y)$.

Lemma 7.1.3:

If α and β are ordinals, and are also isomorphic as chains, then $\alpha = \beta$. Furthermore, the identity map is the only isomorphism from α to itself.

Proof:

Let $P(\alpha)$ be the property that α is the unique ordinal isomorphic to itself, and that the unique isomorphism from α to itself is the identity isomorphism. (The α here is a general ordinal, not one referenced in the lemma statement.) Suppose $P(\gamma)$ is true for every $\gamma < \alpha$. Suppose f is an isomorphism from α to some ordinal β. For every $\gamma < \alpha$, the restriction of f to γ is an isomorphism from γ to $f(\gamma)$, and so by $P(\gamma)$, $f(\gamma) = \gamma$ and $f|_{\gamma}$ is the identity. This means that for every $\gamma \in \alpha$, $f(\gamma) = \gamma$ and so f is the identity and so $\alpha = \beta$.

Thus by transfinite induction, this holds for every ordinal. ■

7.2 The Axiom of Choice

Definition 7.2.1:

A function f defined from an ordinal α is called an α**-sequence**. A **sequence** of a set X is an α-sequence whose codomain is X. And an **enumeration** of a set X is an injective sequence of X.

Definition 7.2.2:

The sum of two ordinals $\alpha + \beta$ is the ordinal $\gamma \geq \alpha$ such that the chain $\gamma \setminus \beta$ is isomorphic to the chain β.

By the lemma from the previous section, if the sum of two ordinals exists, then it is unique (as there exists an isomorphism between any two ordinals satisfying the property of the sum).

Example 7.2.3:

(1) The ordinal $\omega + 1$ is the set of all finite ordinals and the set ω, or in other words $\omega \cup \{\omega\}$. Recall that any set of ordinals is well-ordered by $\in$, and so for a set of ordinals to be an ordinal, we must only validate that if $\alpha \in X$ then $\alpha \subseteq X$. This is obviously true for $\omega + 1$, and $\omega + 1 \setminus \omega = \{\omega\}$ which is trivially order-isomorphic (isomorphic) to $1 = \{\varnothing\}$.

(2) $\omega + 2 = \omega + 1 \cup \{\omega + 1\} = \omega \cup \{\omega\} \cup \{\omega \cup \{\omega\}\}$. $\omega + 2 \setminus \omega = \{\omega, \{\omega\}\}$ which is order-isomorphic to $2 = \{\varnothing, \{\varnothing\}\}$.

(3) $\omega + \omega = \{1, 2, \ldots; \omega, \omega + 1, \ldots\}$

Intuitively, $\alpha + \beta$ is the set of all ordinals in α followed by $\alpha + \gamma$ for $\gamma \in \beta$ ($\gamma < \beta$).

Let f be an α-sequence and g be a β-sequence. We define the *concatenation* of f and g to be a $(\alpha + \beta)$-sequence fg defined by

$$fg(\xi) = f(\xi), \quad \xi < \alpha$$
$$fg(\alpha + \zeta) = g(\zeta), \quad \zeta < \beta$$

We now define the *axiom of choice*, which is independent of ZF (very hard to prove), and together with ZF forms a theory called ZFC.

Axiom 7.2.4 (Axiom of Choice):

If X is a set such that $\varnothing \notin X$ then there exists a function $f \colon X \longrightarrow \bigcup X$ such that for every $A \in X$, $f(A) \in A$. This means that for every $A \in X$, we can "choose" an element $f(A)$ from A.

An equivalent formulation of this is that given a family of non-empty sets $\{X_\lambda\}_{\lambda \in \Lambda}$, there exists a function $f \colon \Lambda \longrightarrow \bigcup_{\lambda \in \Lambda} X_\lambda$ such that $f(\lambda) \in X_\lambda$ for every $\lambda \in \Lambda$, or in other words, $\prod_{\lambda \in \Lambda} X_\lambda$ (the set of precisely all these functions) is non-empty.

Other less-obvious equivalent formulations are for example:

(1) **Well-Ordering Theorem**: Every set can be well ordered.

(2) **Zorn's Lemma**: Let X be a non-empty family of sets such that every chain in X has an upper bound in X, then X has a maximal element.

We will not be proving all of the equivalences.

Proposition 7.2.5:

Zorn's Lemma implies the Well-Ordering Theorem.

Proof:

Let M be an arbitrary set. Let $\mathfrak{M}$ be the set of all $(A, \leq_A)$ where $A \subseteq M$ and $\leq_A$ is a well-ordering of A. We define an order relation on $\mathfrak{M}$ by $(A, \leq_A) \leq_{\mathfrak{M}} (B, \leq_B)$ if there exists a $b \in B$ such that $A = \{a \in B \mid a <_B b\}$ and $\leq_A$ and $\leq_B$ coincide on A (this means that A is an *initial segment* of B's).

We will now prove that $\mathfrak{M}$ has a maximal element. Let $\mathfrak{C}$ be a chain in $\mathfrak{M}$, then $\bigcup \mathfrak{C}$ is in $\mathfrak{M}$ and is an upper bound. To be precise, let $B = \left(\bigcup_{(C, \leq_C) \in \mathfrak{C}} C, \leq_B \right)$ where if $m, n \in B$ then $m, n \in C$ for some $C \in \mathfrak{C}$ (since $m \in C_1$ and $n \in C_2$ then since $\mathfrak{C}$ is a chain, one must be contained within the other), then $m \leq_B n$ if and only if $m \leq_C n$. For this same reason B is totally ordered. This is well-defined because $\mathfrak{C}$ is a chain and the orders of the elements in this chain must agree (by the definition of $\leq_{\mathfrak{M}}$). This is also a well-ordering since if $S \subseteq B$ then let $x \in S$, if x is not a minimal element then $x \in C$ for some $C \in \mathfrak{C}$, so let $S' = \{a \in C \mid a <_C x\} \subseteq C$. Then S' has a minimal element and every element not in S' is greater than it (B is totally ordered).

And it is trivial to see that B is an upper bound of $\mathfrak{C}$'s. Thus by Zorn's Lemma, $\mathfrak{M}$ has a maximal element, $(A, \leq_A)$.

We claim that $A = M$, otherwise for $x \in M \setminus A$, let us set $x > a$ for all $a \in A$. This gives a well-ordered set $A \cup \{x\}$, and A is an initial segment of this, which contradicts A being maximal in $\mathfrak{M}$. So $(M, \leq_M)$ is a well-ordering (and maximal in $\mathfrak{M}$), as required. $\blacksquare$

7.3 Cardinal Numbers

Another equivalent definition is to define the relations between cardinalities. $|A| = |B|$ if and only if there exists a bijection between A and B.

By the Cantor-Bernstein theorem, if there exists injections $A \hookrightarrow B$ and $B \hookrightarrow A$ then $|A| = |B|$. The definition of cardinal arithmetic is done as usual.

Theorem 7.3.2:

If α and β are cardinal numbers such that $1 \leq \beta \leq \alpha$ and α is infinite, then

(1) $\alpha + \beta = \alpha$

(2) $\alpha \cdot \beta = \alpha$

Proof:

It is clear that $\alpha \leq \alpha + \beta \leq \alpha + \alpha$ and $\alpha \leq \alpha \cdot \beta \leq \alpha \cdot \alpha$ so we will prove this for the case $\alpha = \beta$, then the result follows from Cantor-Bernstein. Let $|A| = \alpha$