1 Lecture 11.09.08

Logic is the science of truth. Truth arises from relations between language and the world. Logic provides mathematical models of such relations. In logic, we study formal languages $L$ and structures $A$ which play the role of language and the world. The central relation is truth of a sentence $\varphi \in L$ in a structure $A$ (we write this as $A \models \varphi$, and we say $\varphi$ is true in $A$, or $A$ satisfies $\varphi$). In terms of this relation, we define the notion of logical consequence: if $\Sigma \subseteq L$ is a set of sentences and $\varphi \in L$ is a sentence we say $\varphi$ is a logical consequence of $\Sigma$ (and write $\Sigma \models \varphi$), if and only if,

$$
\text{for all structures } A, \text{ if } A \models \Sigma, \text{ then } A \models \varphi.
$$

We can also define the set $V$ of valid sentences of $L$, namely, $\varphi \in L$ is valid, if and only if, for every structure $A$, $A \models \varphi$.

One important example of a formal language is first order logic. This language suffices for the formalization of large tracts of scientific discourse. A part of this course will be devoted to answering two interesting epistemological (even technological) questions concerning first order validity.

1. Can we find out that a sentence of first order logic is valid, if in fact it is?
2. Can we determine whether or not a sentence of first order logic is valid?

The answers to both these questions emerged from work of Kurt Gödel, Alonzo Church, and Alan Turing.

1. Gödel’s Completeness Theorem: $V$ is semi-decidable.
2. Church-Turing Theorem: $V$ is not decidable.

Reading: Enderton, Sections 1.1 & 1.2
Exercises: Enderton, Exercise 1.2.10 (Please devote some attention to this exercise, since I would like to go over it during our next class meeting.)
For those who would like to proceed ahead, our next reading will be sections 1.5 and 1.7; exercises 1.7.1-1.7.3.
2 Lecture 11.09.13

Some definitions:
1. \( \mathcal{O} = \{A_i \mid i \in \mathbb{N}\} = \) the set of sentence letters;
2. \( \mathcal{S} = \) the set of sentences generated from \( \mathcal{O} \) using the sentential connectives;
3. \( \mathcal{H} = \{ h \mid h : \mathcal{O} \rightarrow \{T, F\} \} = \) the set of truth assignments;
4. for \( \alpha \in \mathcal{S} \) and \( h \in \mathcal{H} \), \( h \models \alpha \), if and only if, \( h(\alpha) = T \) (\( h \) satisfies \( \alpha \));
5. for \( \Sigma \subseteq \mathcal{S} \) and \( h \in \mathcal{H} \), \( h \models \Sigma \), if and only if, for all \( \varphi \in \Sigma \), \( h \models \varphi \) (\( h \) satisfies \( \Sigma \));
6. for \( \Sigma \subseteq \mathcal{S} \) and \( \alpha \in \mathcal{S} \), \( \Sigma \models \alpha \), if and only if for all \( h \in \mathcal{H} \), if \( h \models \Sigma \), then \( h \models \alpha \). (\( \alpha \) is a logical consequence of \( \Sigma \).)
7. For \( \Sigma \subseteq \mathcal{S} \) let \( \text{Cn}(\Sigma) = \{ \varphi \mid \Sigma \models \varphi \} \). (The set of logical consequences of \( \Sigma \), aka the theory axiomatized by \( \Sigma \).)
8. \( \Sigma \) is equivalent to \( \Gamma \), if and only if, \( \text{Cn}(\Gamma) = \text{Cn}(\Sigma) \).
9. \( \Sigma \) is independent, if and only if, for all \( \alpha \in \Sigma \), \( (\Sigma - \{\alpha\}) \not\models \alpha \).

We discussed the inductive definition of \( \mathcal{S} \) (consult Enderton, Section 1.4 for additional discussion of inductive definitions).

We presented a solution to Enderton, exercise 1.2.10 (a) and (b).

1.2.10(a) Show that if \( \Sigma \subseteq \mathcal{S} \) is finite, then there is a \( \Delta \subseteq \Sigma \) such that \( \Sigma \) is equivalent to \( \Delta \) and \( \Delta \) is independent. We proceeded by induction on the size of \( \Sigma \) and noted the importance of considering the case where \( \Sigma \) is empty, since any set of tautologies is equivalent to the \( \emptyset \). We reduced the induction step to showing that for every \( \Sigma \subseteq \mathcal{S} \) and \( \alpha \in \mathcal{S} \), if \( (\Sigma - \{\alpha\}) \models \alpha \), then \( (\Sigma - \{\alpha\}) \) is equivalent to \( \Sigma \).

It follows at once from the lemma below that for every \( \Sigma \subseteq \mathcal{S} \) and \( \alpha \in \mathcal{S} \), if \( (\Sigma - \{\alpha\}) \models \alpha \), then \( (\Sigma - \{\alpha\}) \) is equivalent to \( \Sigma \). First, for any \( \Sigma \subseteq \mathcal{S} \) we define \( \text{Mod}(\Sigma) = \{ h \in \mathcal{H} \mid h \models \Sigma \} \).

**Lemma 1** For every \( \Sigma, \Gamma \subseteq \mathcal{S} \), if \( \text{Mod}(\Sigma) = \text{Mod}(\Gamma) \), then \( \text{Cn}(\Sigma) = \text{Cn}(\Gamma) \).

We suggested proving the converse of the foregoing lemma as an exercise (hint: apply the Compactness Theorem).

**Exercise 1** For every \( \Sigma, \Gamma \subseteq \mathcal{S} \), if \( \text{Cn}(\Sigma) = \text{Cn}(\Gamma) \), then \( \text{Mod}(\Sigma) = \text{Mod}(\Gamma) \).

1.2.10(b) Let \( \varphi_n = (A_0 \land \ldots \land A_n) \). Let \( \Sigma = \{ \varphi_n \mid n \in \mathbb{N} \} \). Note that if \( \Gamma \subseteq \Sigma \) and \( \Gamma \) is independent, then \( \Gamma \) contains at most one sentence, whereas if \( \Gamma \) is equivalent to \( \Sigma \) then \( \Gamma \) is infinite. It follows that no subset of \( \Sigma \) is both independent and equivalent to \( \Sigma \).
Let $\Sigma = \{\sigma_0, \sigma_1, \ldots\}$. We may suppose without loss of generality that no finite subset of $\Sigma$ is equivalent to $\Sigma$. We define a sequence of sentences $\delta_i \in \Sigma$ by induction as follows. Let $\delta_0 = \sigma_i$ where $i$ is the least $j$ such that $\sigma_j$ is not a tautology. Some such $j$ exists, for otherwise $\Sigma$ would be equivalent to $\emptyset$. Let $\delta_{n+1} = \sigma_i$ where $i$ is the least $j$ such that $\{\delta_0, \ldots, \delta_n\} \not\equiv \sigma_j$. Such a $j$ exists, for otherwise $\Sigma$ is equivalent to $\{\delta_0, \ldots, \delta_n\}$. Now, let $\gamma_0 = \delta_0$ and $\gamma_{n+1} = (\delta_0 \land \ldots \land \delta_n) \rightarrow \delta_{n+1}$. Let $\Gamma = \{\gamma_n \mid n \in \mathbb{N}\}$. It is easy to verify that $\Gamma$ is equivalent to $\Sigma$ and that $\Gamma$ is independent.

We began to study the expressive power of sentential logic. We first addressed the finite case.

1. $O_n = \{A_i \mid i \leq n\}$;
2. $S_n$ = the set of sentences generated from $O_n$ using the sentential connectives;
3. $H_n = \{h \mid h : O_n \longrightarrow \{\top, \bot\}\}$;
4. for $\varphi \in S_n$, $\text{Mod}_n(\varphi) = \{h \in H_n \mid h \models \varphi\}$.

**Theorem 1 (Expressive Completeness Theorem for Sentential Logic)**

For every $n$ and for every $X \subseteq H_n$, there is a $\varphi \in S_n$, such that $\text{Mod}_n(\varphi) = X$.

A proof of this theorem, essentially the same as we presented in class (with slightly different terminology), may be found in Enderton, section 1.5.

We then began to consider the infinite case. We showed that

**Theorem 2 (Cantor’s Diagonal Theorem)** $H$ is not countable.

Proof: Let $\{h_1, h_2, \ldots\} \subseteq H$. We show that there is an $h \in H$ such that for every $i$, $h \neq h_i$. Let $\text{change}(\top) = \bot$ and $\text{change}(\bot) = \top$. For every $i$, let $h_i(A_i) = \text{change}(h_i(A_i))$.

**Exercise 2** Show that there is a $P \subseteq H$ such that for all $\Sigma \subseteq S$, $\text{Mod}(\Sigma) \neq P$.

**Exercise 3** Show that for every finite $P \subseteq H$ there is a $\Sigma \subseteq S$ such that $\text{Mod}(\Sigma) = P$.

Next time, we will go over solutions to these exercises, and perhaps Exercise 1 as well. We will then proceed to prove the compactness theorem for sentential logic (see Enderton, section 1.7). As part of the proof, we will present solutions to Enderton, exercises 1.7.1 & 2.
4 Lecture 11.09.20

A little set theory (see also Chapter 0 of Enderton, *A Mathematical Introduction to Logic*).

Let $X$ and $Y$ be sets. $X$ is *equipollent to* $Y$, if and only if, there is a bijection from $X$ onto $Y$. We write $X \sim Y$ for $X$ is equipollent to $Y$.

$X \preceq Y$, if and only if, there is an injection from $X$ into $Y$.

**Theorem 3 (Cantor-Schroeder-Bernstein)** If $X \preceq Y$ and $Y \preceq X$, then $X \sim Y$.

We write $X \prec Y$ if and only if $X \preceq Y$ and $X \not\sim Y$.

Let $N$ be the set of natural numbers (aka non-negative integers), $Q$ be the set of rational numbers (ratios of integers) and $R$ be the set of real numbers. Let $X \times Y = \{\langle a, b \rangle \mid a \in X$ and $b \in Y\}$, the cartesian product of $X$ and $Y$. It is easy to see that for every set $X$, $X \preceq X \times X$.

Define $f : N \times N \rightarrow N$, by $f(m, n) = 2^m \cdot 3^n$. Since $f$ is injective, $N \times N \sim N$, by Theorem 3. It follows that $Q \sim N$.

Let $X^2 = \{f \mid f : X \rightarrow \{0, 1\}\}$, the set of 0-1 valued functions with domain $X$.

**Theorem 4 (Cantor Diagonal Theorem)** $X \prec X^2$.

Proof: Let $X$ be a set and let $G : X \rightarrow X^2$. It suffices to show that $G$ is not surjective. Define $f : X \rightarrow \{0, 1\}$ as follows: for every $a \in X$,

$$f(a) = 1 - [G(a)](a).$$

It is easy to see that for all $b \in X, G(b) \neq f$.

We write $P(X)$ for the *powerset* of $X$, that is, $\{Y \mid Y \subseteq X\}$. Observe that $P(X) \sim X^2$.

**Theorem 5** $R \sim N^2$.

Proof: For $r \in R$ define $D(r) = \{q \in Q \mid q < r\}$ (the left, open Dedekind cut in $Q$ determined by $r$). It follows at once from the fact that for all $r, s \in R$ with $r < s$, there is a $q \in Q$ such that $r < q < s$, that $D$ is an injection from $R$ into $P(Q)$. Hence, $R \preceq N^2$. On the other hand, for each $f \in N\{0, 2\}$ define $C(f) = \sum_{i=0}^{\infty} f(i) \cdot 3^i$. It follows from the least upper bound principle (which allows us to show that the summation of an infinite series is well-defined) that $C$ is an injection. Thus, $N^2 \preceq R$.

In light of the fact that $\aleph_1 \leq R$ the following question is quite natural. Is there an infinite set $Y \subset R$ such that $Y \not\sim N$ and $Y \not\sim R$? Cantor conjectured that the answer to this question is negative (Cantor’s Continuum Hypothesis - CH) and Hilbert placed the question first on the famous list of problems he promulgated in his address to the 1900 International Congress of Mathematicians. The question is yet to be resolved. Indeed, the solution will require new insights into the nature of sets, since the current definitive axiomatization of set theory, Zermelo-Fraenkel set theory with the axiom of choice (ZFC), fails to settle the question, as the following results show.
Theorem (Gödel, 1939): CH is not refutable in ZFC.
Theorem (Cohen, 1963): CH is not provable in ZFC.
5 Lecture 11.09.22

We began by exploring the expressive power of sentential logic in the infinite case. First we showed, in contrast to the finite case, that

**Proposition 1** There is a $P \subseteq H$ such that for all $\Sigma \subseteq S$, $\text{Mod}(\Sigma) \neq P$.

Proof: It is easy to see that $P(S) \sim H$, from which it follows, by Theorem 4, that $P(S) \prec P(H)$.

We next showed that

**Proposition 2** For every finite $P \subseteq H$, there is a $\Sigma \subseteq S$ such that $\text{Mod}(\Sigma) = P$.

Proof: Let $P = \{h_1, \ldots, h_n\}$. Recall that $\text{Th}_{\text{lit}}(h) = \{\lambda \mid \lambda$ is a literal and $h \models \lambda\}$. The important properties of $\text{Th}_{\text{lit}}(h)$ are

1. $h \models \text{Th}_{\text{lit}}(h)$;
2. for every $g \in H$, if $g \models \text{Th}_{\text{lit}}(h)$, then $g = h$.

Let

$$\lambda_{ik} = \begin{cases} A_k & \text{if } h_i(A_k) = \top; \\
\neg A_k & \text{if } h_i(A_k) = \bot. \end{cases}$$

Note that $\text{Th}_{\text{lit}}(h_i) = \{\lambda_{ik} \mid k \geq 1\}$. Now, let $\alpha_{ij}$ be the sentence $\lambda_{i1} \land \lambda_{i2} \land \ldots \land \lambda_{ij}$, and let $\beta_j$ be the sentence $\alpha_{1j} \land \alpha_{2j} \land \ldots \land \alpha_{nj}$.

Finally, let

$$\Sigma = \{\beta_j \mid j \geq 1\}.$$

It is straightforward to verify that for each $1 \leq i \leq n$, $h_i \models \Sigma$. It then remains to show that for every $h \in H$, if $h \models \Sigma$, then for some $1 \leq i \leq n$, $h = h_i$. Suppose $h \in H$ and $h \models \Sigma$. Note that for every $1 \leq i < i' \leq n$, there is a $j$ such that $\lambda_{ij} \neq \lambda_{i'j}$. It follows that for some $l$, for all $l \leq j$ and all $1 \leq i < i' \leq n$, $h \not\models (\alpha_{ij} \land \alpha_{i'j})$. Hence, since $h \models \Sigma$, there is an $i$ and an $l$ such that for every $l \leq j$, $h \models \alpha_{ij}$. It follows immediately that $h = h_i$.

Recall that $\Sigma$ is satisfiable if and only if there an $h$ such that $h \models \Sigma$ and that $\Sigma$ is finitely satisfiable if and only if for every finite $\Delta \subseteq \Sigma$, $\Delta$ is satisfiable. We stated the

**Theorem 6 (Compactness Theorem for Sentential Logic)** If $\Sigma \subseteq S$ is finitely satisfiable, then $\Sigma$ is satisfiable.

We applied the Compactness Theorem to provide a solution to Exercise 1.

**Corollary 1** For every $\Sigma, \Gamma \subseteq S$, if $\text{Cn}(\Sigma) = \text{Cn}(\Gamma)$, then $\text{Mod}(\Sigma) = \text{Mod}(\Gamma)$. 
Proof: Suppose that $\text{Cn}(\Sigma) = \text{Cn}(\Gamma)$, but that $\text{Mod}(\Sigma) \neq \text{Mod}(\Gamma)$. We may suppose, without loss of generality, that for some $h \in H$, $h \in \text{Mod}(\Sigma)$ and $h \not\in \text{Mod}(\Gamma)$. It follows at once that $\Gamma \cup \text{Th}_{\text{lit}}(h)$ is not satisfiable (recall that $h$ is the unique truth assignment satisfying $\text{Th}_{\text{lit}}(h)$). But then, by the Compactness Theorem, for some $\{\lambda_1, \ldots, \lambda_k\} \subseteq \text{Th}_{\text{lit}}(h)$, 

$$\Gamma \models \neg(\lambda_1 \land \ldots \land \lambda_k).$$

But this contradicts the hypothesis that $\text{Cn}(\Sigma) = \text{Cn}(\Gamma)$ and $h \in \text{Mod}(\Sigma)$.

We then proceeded to begin the proof of the Compactness Theorem.

Proof: The Theorem is a corollary of the following two lemmas. First recall that a set of sentences $\Sigma'$ is complete if and only if for every $\alpha \in S$, $\alpha \in \Sigma'$ or $(\neg \alpha) \in \Sigma'$.

**Lemma 2 (Completion Lemma)** If $\Sigma$ is finitely satisfiable, then there is a $\Sigma'$ such that

1. $\Sigma \subseteq \Sigma'$;
2. $\Sigma'$ is finitely satisfiable;
3. $\Sigma'$ is complete.

The canonical truth assignment, $h_{\Sigma'}$ for $\Sigma'$ is defined as follows: for every sentence letter $A \in \mathcal{O}$,

$$h_{\Sigma'}(A) = \top \text{ if and only if } A \in \Sigma'.$$

**Lemma 3 (Canonical Truth Assignment Lemma)** Let $\Sigma' \subseteq S$. If $\Sigma'$ is finitely satisfiable and complete, then $h_{\Sigma'} \models \Sigma'$. 
6 Lecture 11.09.27

Proof of Lemma 2: Let $S = \{\alpha_1, \alpha_2, \ldots\}$. We construct a sequence of sets of sentences $\Sigma_0, \Sigma_1, \ldots$ to satisfy the following conditions (i)-(iv), and then define $\Sigma'$ to be $\bigcup_{i \in \mathbb{N}} \Sigma_i$.

(i) $\Sigma_0 = \Sigma$;
(ii) $\Sigma_n \subseteq \Sigma_{n+1}$, for all $n$;
(iii) $\Sigma_n$ is finitely satisfiable, for all $n$;
(iv) $\alpha_n \in \Sigma_n$ or $(\neg \alpha_n) \in \Sigma_n$, for all $n > 0$.

Note that conditions (i) and (iv) immediately imply that $\Sigma'$ satisfies conditions 1. and 3. of Lemma 1, while conditions (ii) and (iii) imply that $\Sigma'$ satisfies condition 2. of the Lemma 1.

At stage 0 of the construction we set $\Sigma_0 = \Sigma$. At stage $n + 1$ we set

$$
\Sigma_{n+1} = \begin{cases} 
\Sigma_n \cup \{\alpha_{n+1}\} & \text{if } \Sigma_n \cup \{\alpha_{n+1}\} \text{ is consistent;} \\
\Sigma_n \cup \{\neg \alpha_{n+1}\} & \text{otherwise}.
\end{cases}
$$

We first show by induction that for all $n$, $\Sigma_n$ is finitely satisfiable. $\Sigma_0 = \Sigma$ is finitely satisfiable by hypothesis. Suppose $\Sigma_n$ is finitely satisfiable. The following sublemma then guarantees that $\Sigma_{n+1}$ is finitely satisfiable, and thereby concludes the proof of Lemma 2.

Sublemma 1 Let $\Gamma \subseteq S$ and $\alpha \in S$. If $\Gamma$ is finitely satisfiable, then $\Gamma \cup \{\alpha\}$ or $\Gamma \cup \{\neg \alpha\}$ is finitely satisfiable.

Proof of Sublemma 1: Suppose, for reductio, that $\Gamma$ is finitely satisfiable and that for some $\alpha$ neither $\Gamma \cup \{\alpha\}$ nor $\Gamma \cup \{\neg \alpha\}$ is finitely satisfiable. Then there are finite $\Delta, \Delta' \subseteq \Gamma$ such that neither $\Delta \cup \{\alpha\}$ nor $\Delta' \cup \{\neg \alpha\}$ is satisfiable. But then, $\Delta \cup \Delta' \subseteq \Gamma$ is finite and is not satisfiable, contrary to hypothesis.

Proof Sketch of Lemma 3: Let $h_{\Sigma'}$ be the canonical truth assignment for $\Sigma'$. We show by induction on sentences that for every sentence $\alpha$,

$$
h_{\Sigma'} \models \alpha \iff \alpha \in \Sigma'.
$$

Observe that the basis case of the induction is immediate from the definition of canonical truth assignment. The induction step is a straightforward application of the definitions of satisfaction, completeness, and finite satisfiability. We went over the case of disjunction in detail in class.

With the proof of the Compactness Theorem thus concluded, we went on to derive the following corollary.

Corollary 2 (Compactness Theorem for Tautological Consequence) For every $\Sigma \subseteq S$ and every $\alpha \in S$, if $\Sigma \models \alpha$, then for some finite $\Delta \subseteq \Sigma$ such that $\Delta \models \alpha$. 
Proof: Suppose $\Sigma \models \alpha$. Then, $\Sigma \cup \{\neg \alpha\}$ is not satisfiable. It follows from the Compactness Theorem (for sentential satisfiability) that there is a finite $\Delta \subseteq \Sigma$ such that $\Delta \cup \{\neg \alpha\}$ is not satisfiable. It follows that $\Delta \models \alpha$.

We began to discuss the expressive power of first-order logic. We considered two structures, $\text{UDT}$, an undirected triangle, and $\text{BIC}$, an undirected bi-infinite chain. We observed that both these structures are 2-regular simple graphs, a condition that is expressible by the conjunction of the following three first-order sentences.

- $(\forall x) \neg Exx$ (irreflexivity)
- $(\forall x)(\forall y)(Exy \rightarrow Eyx)$ (symmetry)
- $(\forall x)(\exists y)(\exists z)(y \neq z \land (\forall w)(Exw \leftrightarrow (w = y \lor w = z)))$ 2-regularity

We noted that $\text{UDT}$ is characterized up to isomorphism by the additional condition that the universe has exactly three members, which is expressible by a first-order sentence. We asked whether $\text{BIC}$ can be characterized up to isomorphism by a set of first-order sentences. We will pursue this, and related questions, next time.
7 Lecture 11.09.29

We began to study the expressive power of first-order logic by giving some simple examples of first-order definable classes of structures and of first-order definable relations on a fixed structure. For a first-order sentence $\alpha$, we define $\text{Mod}(\alpha) = \{ A \mid A \models \alpha \}$. We say a collection of structures $C$ is first-order definable if and only if for some first order sentence $\alpha$, $C = \text{Mod}(\alpha)$. Given a structure $A$ and a formula $\alpha(x_1, \ldots, x_n)$, with at most the variables indicated free, we define the $n$-ary relation defined by $\alpha$ on $A$ as follows:

$$\alpha[A] = \{ <a_1, \ldots, a_n> \mid A \models \alpha([x_1|a_1], \ldots, (x_n|a_n)) \}.$$

We presented solutions to problems 2.2.9 and 2.2.11 in Enderton, which deal with definable collections of structures and definability within a fixed structure respectively.

Let $A = \langle |A|, P^A \rangle$ be a structure for a language with a binary relation $P$ and with no further relation, function, or constant symbols other than identity. We will often use $A$, rather than $|A|$, to denote the universe of $A$ when no confusion is likely to result. If $f$ is a function with domain $A$ and range contained in $A$, that is, a function from $A$ into $A$, we say that $P^A$ is the graph of $f$ if and only if for all $a, b \in A$,

$$(a, b) \in P^A \iff f(a) = b.$$

Let $\alpha$ be the sentence

$$\forall x \exists y Pxy \land \forall x \forall y \forall z ((Pxy \land Pxz) \rightarrow y = z).$$

Note that $\text{Mod}(\alpha)$ is the collection of all structures $A$ such that $P^A$ is the graph of a function from $A$ into $A$. Let $\beta$ be the sentence

$$\forall x \forall y \forall z ((Pxz \land Pyz) \rightarrow x = y).$$

Note that $\text{Mod}(\alpha \land \beta)$ is the collection of all structures $A$ such that $P^A$ is the graph of an injection (that is, 1-1 function) from $A$ into $A$. Let $\gamma$ be the sentence

$$\forall x \exists y Pyx.$$

Note that $\text{Mod}(\alpha \land \gamma)$ is the collection of all structures $A$ such that $P^A$ is the graph of a surjection from $A$ onto $A$. Finally, note that $\text{Mod}(\alpha \land \beta \land \gamma)$ is the collection of all structures $A$ such that $P^A$ is the graph of a permutation of $A$, that is, a bijection from $A$ onto $A$.

We next considered definability within the fixed structure $\mathbb{N} = \langle N, +, \cdot \rangle$ where $N = \{0, 1, 2, \ldots \}$ and $+$ and $\cdot$ are the usual arithmetic operations on $N$. We considered the definability of simple sets and relations on $\mathbb{N}$ per exercise 2.2.11.

(a) $\forall y (x + y = y)[\mathbb{N}] = \{0\}$.

(b) $\forall y (x \cdot y = y)[\mathbb{N}] = \{1\}$. 
(c) \( \exists z (\forall w (z \cdot w = w) \land x + z = y)[N] = \{ (m, n) \mid n = m + 1 \} \).

(d) \( \exists z (\forall w (z + w \neq w) \land x + z = y)[N] = \{ (m, n) \mid m < n \} \).

We next considered the structures \( N = \langle N, < \rangle \) and \( Z = \langle Z, < \rangle \) where \( Z = \{ \ldots -1, 0, 1, \ldots \} \). We noted that \( \forall y - (y < x)[N] = \{ 0 \} \) and asked whether \( \{ 0 \} \) is definable in \( Z \). The general sentiment was negative, but we agreed that we’d need a new idea to settle the question. To this end, we introduced the notion of an isomorphism of one structure onto another and of an automorphism, that is, an isomorphism of a structure onto itself. We say that \( f \) is an isomorphism of \( A \) onto \( B \) if and only if \( f \) is a bijection of \( A \) onto \( B \) and for all \( a, b \in A \)

\[ \langle a, b \rangle \in P^A \iff \langle f(a), f(b) \rangle \in P^B. \]

An automorphism of \( A \) is an isomorphism of \( A \) onto \( A \). We write \( \text{Aut}(A) \) for the set of automorphisms of \( A \). We stated the following theorem, which says that first-order logic satisfies a natural desideratum for a language to be logical – it does not distinguish between structurally identical models.

**Theorem 7 (Isomorphism Theorem)** Suppose \( f \) is an isomorphism of \( A \) onto \( B \). Then for every formula \( \alpha(x_1, \ldots, x_n) \), with at most the variables indicated free, and for all \( a_1, \ldots, a_n \in A \),

\[ A \models \alpha((a_1|a_1), \ldots, (a_n|a_n)) \iff B \models \alpha((x_1|f(a_1)), \ldots, (x_n|f(a_n))). \]

As a corollary to the Isomorphism Theorem, we have the

**Corollary 3 (Automorphism Theorem)** If \( f \) is an automorphism of \( A \) and \( \alpha(x) \) is a formula with at most \( x \) free, then for all \( a \in A \),

\[ a \in \alpha[A] \iff f(a) \in \alpha[A]. \]

We applied the automorphism theorem to show that the only sets definable in \( Z = \langle Z, < \rangle \) are \( Z \) and \( \emptyset \). This follows from the observation that for every \( p \in Z \) the function \( f_p \in \text{Aut}(Z) \), where \( f_p(q) = p + q \), for all \( q \in Z \).

We reflected on this last resulted and introduced the notion of an orbit. Let \( a \in A \);

\[ \text{Orb}(a, A) = \{ f(a) \mid f \in \text{Aut}(A) \}. \]

As a corollary to the Automorphism Theorem, we noted that for every structure \( A, a \in A \) and \( X \subseteq A \), if \( X \) is definable on \( A \), then \( \text{Orb}(a, A) \subseteq X \) or \( \text{Orb}(a, A) \cap X = \emptyset \).

**Exercise 4** Let \( A \) be a structure and for all \( a, b \in A \) let \( a \approx b \) if and only if \( b \in \text{Orb}(a, A) \). Show that \( a \approx b \) is an equivalence relation, that is, a reflexive, symmetric, and transitive relation.

We asked whether the usual order on \( N \) is definable over \( \langle N, \cdot \rangle \). We observed that the answer is no, since for every permutation \( f \) of the set of prime numbers \( P \), there is an automorphism \( g \) of \( \langle N, \cdot \rangle \) such that \( g|P = f \).

**Exercise 5** Show that \( \frac{\mathbb{N}}{\mathbb{N}} \sim \mathbb{N}_2 \).
8 Lecture 11.10.04

A structure $A$ is rigid if and only if $\text{card}(\text{Aut}(A)) = 1$. If $A$ is rigid, then the Automorphism Theorem cannot be deployed directly to analyze the collection of sets definable over $A$. We observed that $\mathbb{N} = \langle \mathbb{N}, 0, S \rangle$ (the natural numbers equipped with zero and the successor function) is a rigid structure. We noted that every finite and co-finite subset of $\mathbb{N}$ is definable. We explore the matter further in an exam problem.

With Exercise 2.2.16 we meet another measure of expressive power that is specially suited to measure expressiveness in the context of finite structures. Given a first-order sentence $\alpha$, we define the spectrum of $\alpha$ as follows:

$$\text{Spec}(\alpha) = \{ n \in \mathbb{N} \mid \exists A (\text{card}(A) = n \text{ and } A \models \alpha) \}.$$

We are asked to exhibit a sentence $\alpha$ whose spectrum is the set of positive even numbers. Here is such a sentence:

$$\forall x \neg Rxx \land \forall x \forall y (Rxy \rightarrow Ryx) \land \forall x \exists y \forall z (Rxz \leftrightarrow z = y).$$

The sentence is true in a structure just in case that structure is a loop-free undirected graph which is 1-regular, that is, all vertices have degree 1. It is easy to see that such a graph must have an even number of elements, and that for every even number $n$, there is such a graph of size $n$.

We proceeded to give an example of a sentence $\varphi$ whose spectrum is the set of perfect squares. The sentence used one ternary relation symbol $R$ and one unary relation symbol $F$. A structure $A$ satisfies $\varphi$ if and only if $R^A$ is the graph of a bijection of $F^A \times F^A$ onto $|A|$. We may choose $\varphi$ to be the conjunction of the following sentences.

- $(\forall x)(\forall y)(\exists z)(\forall w)((Fx \land Fy) \rightarrow (Rxyw \leftrightarrow w = z))$
- $(\forall x)(\forall y)(\forall v)(\forall w)((Rxzy \land Rwz) \rightarrow (Fx \land Fy \land x = v \land y = w))$
- $(\forall z)(\exists x)(\exists y)Rxyz$

It is unusual that $\text{Spec}(\neg \varphi) = \mathbb{N} - \text{Spec}(\varphi)$. An exam problem illustrates just how badly this identity fails. We briefly discussed the Spectrum Problem: Is the collection of first-order spectra closed under complementation? We remarked that this problem is equivalent to the closure of NEXP under complementation, a deep question in the theory of computational complexity.

We showed that for every finite directed graph $A$, there is a sentence $\varphi_A$ such that for all directed graphs $B$,

$$B \models \varphi_A \iff A \cong B.$$

**Definition 1** The first-order theory of $A$ ($\text{Th}(A)$) is equal to $\{ \varphi \mid A \models \varphi \}$. $A$ is elementarily equivalent to $B$ ($A \cong B$) if and only if $\text{Th}(A) = \text{Th}(B)$. 
We began to explore the question whether there is an infinite structure $A$ such that for all $B$, if $B \equiv A$, then $B \cong A$. In particular, we started to axiomatize $\text{Th}(\langle N, 0, S \rangle)$ and investigate structures not isomorphic to $\langle N, 0, S \rangle$ which satisfy our axioms.
We continued our study of $\mathbb{N} = \langle \mathbb{N}, 0, S \rangle$. Much of the material we covered may be found in Enderton, Section 3.1. Last time we introduced the following set of sentences $\Gamma$, all true in the structure $\mathbb{N}$, as a potential axiomatization of $\text{Th}(\mathbb{N})$.

1. $(\forall x) Sx \neq 0$
2. $(\forall x)(\forall y)(Sx = Sy \rightarrow x = y)$
3. $(\forall x)(x \neq 0 \rightarrow (\exists y) Sy = x)$
4. for each $n$, the sentence $(\forall x)S^n x \neq x$

We considered how well these sentences describe $\mathbb{N}$.

**Definition 2** A satisfiable set of sentences $\Sigma$ is categorical if and only if for all $A, B \in \text{Mod}(\Sigma)$, $A \cong B$. Let $\kappa$ be an infinite cardinal (see the notes on set theory at the end of this memoir for explanation). A satisfiable set of sentences $\Sigma$ is $\kappa$-categorical if and only if for all $A, B \in \text{Mod}(\Sigma)$, if $\text{card}(A) = \text{card}(B) = \kappa$, then $A \cong B$.

We observed that the Peano induction axiom, a sentence of monadic second-order logic, that is, a sentence involving quantification over subsets of the universe of discourse as well as elements of the universe of discourse, when conjoined with sentences 1-3 above, provides a categorical description of $\mathbb{N}$.

**Induction Axiom:** $(\forall P)((P0 \land (\forall x)(Px \rightarrow PSx)) \rightarrow (\forall x)Px)$

We discussed a first-order formulation of the induction axiom as an axiom schema yielding infinitely many induction axioms, one for each substitution instance of a first-order formula. We considered the possibility that the addition of these axioms to $\Gamma$ might provide a better description of $\mathbb{N}$ than $\Gamma$ alone, perhaps even a categorical description.

We analyzed the models of $\Gamma$ up to isomorphism. For each cardinal number $\kappa \geq 0$ there is a model $A_\kappa \models \Gamma$ where $A_\kappa$ consists of a copy of $\mathbb{N}$ together with $\kappa$ many copies of $\langle \mathbb{Z}, S \rangle$ (the integers equipped with the usual successor function). It follows at once that $\Gamma$ is $\kappa$-categorical for all $\kappa > \aleph_0$.

**Theorem 8 (Łoś-Vaught Test)** If $\Sigma$ is $\kappa$-categorical for some infinite cardinal $\kappa$ and $\Sigma$ has no finite models, then $\text{Cn}(\Sigma)$ is complete.

It follows at once that $\text{Cn}(\Gamma) = \text{Th}(\mathbb{N})$.

**Addendum: notes on set theory**

Let $X$ be a set and $R$ be a binary relation on $X$, that is, $R \subseteq X \times X$. $R$ is a well-ordering of $X$, if and only if, $R$ is transitive and asymmetric, and every nonempty subset of $X$ has an $R$-least element.

Ordinal numbers provide representatives for well-orderings. Suppose $X$ is a set of sets. We say $X$ is a transitive set, if and only if, for every $y \in X$, $y \subseteq X$. A
set of sets \( X \) is an (von Neumann) ordinal number, if and only if, \( X \) is transitive and \( X \) is well-ordered by \( \in \) (restricted to \( X \)). The (proper class of) ordinals is itself, in the obvious sense, well-ordered by \( \in \). Every ordinal is equal to its set of predecessors. The successor of an ordinal \( \alpha \) is \( \alpha \cup \{ \alpha \} \); the supremum of a set of ordinals is its union. For every well-ordering \( \langle X, R \rangle \) there is a unique ordinal number \( \alpha \) such that \( \langle X, R \rangle \) is isomorphic to \( \langle \alpha, \in \rangle \).

Some ordinals: \( 0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \omega + \omega, \ldots, \omega \times \omega, \ldots \)

Zermelo’s Well-Ordering Principle (a version of the Axiom of Choice): For every set \( X \), there is an ordinal \( \alpha \) such that \( X \sim \alpha \).

We call the least ordinal number \( \alpha \) such that \( X \sim \alpha \) the cardinality of \( X \). An ordinal number \( \alpha \) is a cardinal number, if and only if, the cardinality of \( \alpha \) is \( \alpha \).

For any set \( X \), the power set of \( X \) (written \( P(X) \)) is the set of all subsets of \( X \) and \( X^2 = \{ f \mid f : X \to \{0, 1\} \} \). Observe that \( X^2 \sim P(X) \). If \( \kappa \) is a cardinal number, we write \( 2^\kappa \) for the cardinality of \( ^\kappa 2 \). By Cantor’s Diagonal Theorem, for every cardinal number \( \kappa \), \( \kappa < 2^\kappa \). The infinite cardinals form a well-ordered class. For each ordinal \( \alpha \), we denote the \( \alpha \)th infinite cardinal by \( \aleph_\alpha \). Thus, \( \aleph_0 = \omega = \{0, 1, 2, \ldots \} \) is the smallest infinite cardinal. We say a set is countable, if and only if, its cardinality is less than or equal to \( \aleph_0 \). Note that \( \aleph_1 \), the first uncountable cardinal, is the set of countable ordinals. Thus, we can restate Cantor’s Continuum Hypothesis (CH) as \( 2^{\aleph_0} = \aleph_1 \).
10 Lecture 11.10.13

We proved Theorem 8. The proof relied on

**Theorem 9 (Łöwenheim-Skolem Theorem)** If a countable set of first-order sentences has an infinite model, then for every infinite cardinal $\kappa$, it has a model of cardinality $\kappa$.

**Proof** (of Theorem 8): Suppose $\Gamma$ is a countable set of first-order sentences which has no finite models and $\kappa$ is an infinite cardinal such that $\Gamma$ is $\kappa$-categorical. Suppose, for reductio that $\Gamma$ is not complete. Then there is a sentence $\varphi$ such that $\Gamma \not|= \varphi$ and $\Gamma \not|= \neg \varphi$. Since $\Gamma$ has no finite models, it follows at once, from Theorem 8, that there are models $A$ and $B$ of $\Gamma$ such that $A |= \varphi$ and $B |= \neg \varphi$ and $\text{card}(A) = \text{card}(B) = \kappa$. Hence, $A \cong B$.

In order to prove Theorem 9, we divided the result into its upward and downward aspects.

**Theorem 10 (Upward Łöwenheim-Skolem Theorem)** If a set of first-order sentences has an infinite model, then for every infinite cardinal $\kappa$, it has a model of cardinality $\geq \kappa$.

Theorem 10 is a corollary of the following fundamental result about first-order logic.

**Theorem 11 (Compactness Theorem)** If a set of first-order sentences is finitely satisfiable, then it is satisfiable.

**Proof** (of Theorem 10): Suppose $\Gamma$ is a set of first-order sentence with an infinite model and $\kappa$ is an infinite cardinal. Let $\{c_\xi \mid \xi < \kappa\}$ be a set of distinct constant symbols disjoint from the language of $\Gamma$. Let $\Delta = \{c_\xi \neq c_\zeta \mid \xi < \zeta < \kappa\}$. Since $\Gamma$ has an infinite model, $\Gamma \cup \Delta$ is finitely satisfiable. The result now follows immediately from Theorem 11.

In order to state the downward aspect we require a definition.

**Definition 3** $A$ is an elementary substructure of $B$ (equivalently, $B$ is an elementary extension of $A$, written $A \preceq B$), if and only if, $A$ is a substructure of $B$ and for every first order formula $\varphi(x_1,\ldots,x_n)$ and every $a_1,\ldots,a_n \in A$,

$$A |= \varphi(a_1,\ldots,a_n) \iff B |= \varphi[a_1,\ldots,a_n].$$

**Theorem 12 (Downward Łöwenheim-Skolem Theorem)** Suppose $B$ is infinite. Moreover, suppose the signature of $B$ is countable. If $X$ is contained in the universe of $B$, then there is a structure $A$ such that $X \subseteq A$, $A \preceq B$ and $\text{card}(A) = \max(\aleph_0,\text{card}(X))$.

The following useful criterion for one structure to be an elementary substructure of another may be established by a straightforward induction on formulas.

**Theorem 13 (Tarski-Vaught Criterion)** Suppose $A$ is a substructure of $B$. Then, $A \preceq B$, if and only if, for every formula $\varphi$ and every assignment $s$ in $A$, if $B |= \exists x \varphi[s]$, then for some $a \in A$ $B |= \varphi[s(x|a)]$. 
Proof (of Theorem 12): Now, suppose that $B$ is an infinite structure with a countable signature. For each formula in the language of $B$ of the form $\varphi(y, x_1, \ldots, x_n)$ let $f_\varphi : B^n \to B$ satisfy the following condition:

$$\forall a_1, \ldots, a_n \in B (B \models \exists y \varphi[a_1, \ldots, a_n] \to B \models \varphi[f_\varphi(a_1, \ldots, a_n), a_1, \ldots, a_n]).$$

The existence of such an $f_\varphi$ is guaranteed by the axiom of choice. The set of all the $f_\varphi$ for $\varphi$ a formula in the language of $B$ is called a set of Skolem functions for $B$. Note that this set is countable, since the signature of $B$ is countable. For $X \subseteq B$ let $H(X)$ be the closure of $X$ under a set of Skolem functions for $B$ and let $\mathcal{H}(X)$ be the substructure of $B$ with universe $H(X)$. $\mathcal{H}(X)$ is called the Skolem hull of $X$ in $B$. Now, for every formula $\varphi(y, x_1, \ldots, x_n)$ in the language of $B$

$$\forall a_1, \ldots, a_n \in H(X) (B \models \exists y \varphi[a_1, \ldots, a_n] \to \exists b \in H(X) (B \models \varphi[b, a_1, \ldots, a_n])).$$

It follows at once, by the Tarski-Vaught Criterion, that $\mathcal{H}(X) \preceq B$. 