# MATH681
# Mathematical Logic

Pingbang Hu

February 21, 2023

**Abstract**

This is a graduate-level mathematical logic course taught by Matthew Harrison-Trainor, aiming to obtain insights into all other branches of mathematics, such as algebraic geometry, analysis, etc. Specifically, we will cover model theory beyond the basic foundational ideas of logic.

While there are no required textbooks, some books do cover part of the material in the class. For example, Marker's *Model Theory: An Introduction* [Mar02], Hodges's *A Shorter Model Theory* [HH97], and Hinman's *Fundamentals of Mathematical Logic* [Hin05].

This course is taken in Winter 2023, and the date on the covering page is the last updated time.

# Contents

# Chapter 1

# Language, Logic, and Structures

## Lecture 1: Introduction to Mathematical Logic

The goal of mathematical logic is to obtain insights into other areas of mathematics – algebra, analysis, combinatorics, and so on, by formalizing the **process** of mathematics. 5 Jan. 14:30

**Remark.** More concretely, there are different branches:

(a) Model Theory: Study subsets of an object defined by a formula (i.e., first-order logic).

(b) Computability Theory / Recursion Theory: Formalizing what it means to have an algorithm and studying relative computability.

(c) Set Theory: Study the structure of the mathematical universe.

(d) Proof Theory: Study the syntactic nature of proofs.

In this class, we study model theory in nature; specifically, we will cover

- basic definitions of logic:
  - What is a formula?
  - What does it mean for a formula to be true?
  - What is a proof?
- Soundness & completeness theorems:
  - Anything provable is true.
  - Anything true is provable.
- Compactness theorem:
  - Non-standard objects exist.
- Using compactness theorem for applications:
  - Chevalley's theorem.

The main theme of this course will be *syntax* v.s. *semantics*:

| Syntax | v.s. | Semantics |
|---|---|---|
| proofs | | truth |
| form of a formula | | mathematical structures |
| number and type of quantifiers | | isomorphisms, embeddings |

## 1.1 Syntax and Semantics

### 1.1.1 Languages and Structures

Let's start with the fundamental object, language.

**Definition 1.1.1** (Language). A *language* $\mathcal{L}$ consists of:

- a set $\mathcal{F}$ of function symbols $f$ with arities $n_f$;
- a set $\mathcal{R}$ of relation symbols $R$ with arities $n_R$;
- a set $\mathcal{C}$ of constant symbols $c$.

A language is also sometimes called a *signature*, in which case we use $\sigma$ rather than $\mathcal{L}$.

**Note.** A constant is the same as a 0-ary function.

**Remark.** Any or all sets in Definition 1.1.1 might be empty.

**Example** (Graph). The language of graphs, $\mathcal{L}_{\text{graph}} = \{E\}$ where $E$ is a binary (2-ary) relation symbol.

**Example** (Ring). The language of rings, $\mathcal{L}_{\text{ring}} = \{0, 1, +, \cdot, -\}$, where $0, 1$ are constants, $+, \cdot$ are binary functions, and $-$ is a unary function.

**Example** (Ordered ring). The language of ordered rings, $\mathcal{L}_{\text{ord}} = \mathcal{L}_{\text{ring}} \cup \{\leq\}$ where $\leq$ is the binary relation for an ordered ring.

Then, given a language, we can now interpret it in the following way.

**Definition 1.1.2** (Structure). Given a language $\mathcal{L}$, an *$\mathcal{L}$-structure* $\mathcal{M}$ consists of:

- a non-empty set $M$ called the *universe*, *domain*, or *underlying set* of $\mathcal{M}$;
- for each function symbol $f \in \mathcal{F}$, a function $f^{\mathcal{M}} \colon M^{n_f} \to M$;
- for each relation symbol $R \in \mathcal{R}$, a relation $R^{\mathcal{M}} \subseteq M^{n_R}$;
- for each constant symbol $c \in \mathcal{C}$, an element $c^{\mathcal{M}} \in M$.

**Notation** (Interpretation). The *interpretation* of symbols $f, R, c$ in $\mathcal{M}$ is $f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}}$, respectively.

Basically, a structure gives meaning to the symbols from the language, and we often write

$$\mathcal{M} = (M, f^{\mathcal{M}}, \ldots, R^{\mathcal{M}}, \ldots, c^{\mathcal{M}}, \ldots) = (M, f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}} \colon f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C}).$$

**Notation.** We usually use $\mathcal{M}, \mathcal{N}, \ldots, \mathcal{A}, \mathcal{B}, \ldots$ to refer to structures, and $M, N, \ldots, A, B, \ldots$ for the domains.[a]

[a]Some people use $|\mathcal{M}|$ for the domain of $\mathcal{M}$.

It's time to look at some examples.

**Example.** The rationals $\mathbb{Q}$ and integers $\mathbb{Z}$ are both $\mathcal{L}_{\text{ring}}$-structures.

**Proof.** Clearly, the domain is the set of rationals, and naively, we let $+^{\mathbb{Q}} = +$ in $\mathbb{Q}$, $0^{\mathbb{Q}} = 0$ in

$\mathbb{Q}$, $1^{\mathbb{Q}} = 1$ in $\mathbb{Q}$, etc. In this way, $\mathbb{Q} = (\mathbb{Q}, 0, 1, +, \cdot, -)$ is an $\mathcal{L}_{ring}$-structure. Similarly, $\mathbb{Z} = (\mathbb{Z}, 0, 1, +, \cdot, -)$ is as well. ⊛

While the language we have seen are all intuitively correct with their name, e.g., $\mathcal{L}_{\text{ring}}$, $\mathcal{L}_{\text{ord}}$, and $\mathcal{L}_{\text{graph}}$, they are really just the high-level abstraction of the objects in the subscript.

**Example.** Nothing forces an $\mathcal{L}_{\text{ring}}$-structure to be a ring.

**Proof.** Since an $\mathcal{L}_{\text{ring}}$-structure is just any structure with two binary functions, a unary function, and two constants interpreting the symbols of the language; hence we can define an $\mathcal{L}_{\text{ring}}$-structure $\mathcal{M}$ as

- $\mathcal{M} = \{0, 5, 11\}$;
- $0^{\mathcal{M}} = 5$;
- $1^{\mathcal{M}} = 11$;
- $+^{\mathcal{M}}$ is the constant function 0;
- $\cdot^{\mathcal{M}}$ is the function 5;
- $-^{\mathcal{M}}$ is the identity.

This is clearly not a ring since it fails nearly every axiom of a ring. ⊛

**Note.** Later, we will talk about theories that let us restrict to structures we want.

### 1.1.2 Embeddings and Isomorphisms

We can now consider the relation between structures.

**Definition 1.1.3** (Embedding)**.** Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures. A map $\eta\colon \mathcal{M} \to \mathcal{N}$ is an $\mathcal{L}$-*embedding* if it is one-to-one and preserves the interpretation of all symbols of $\mathcal{L}$:

(a) for each function symbol $f \in \mathcal{F}$ of arity $n_f$, and $a_1, \dots, a_{n_f} \in M$,
$$\eta(f^{\mathcal{M}}(a_1, \dots, a_{n_f})) = f^{\mathcal{N}}(\eta(a_1), \dots, \eta(a_{n_f}));$$

(b) for each relation symbol $R \in \mathcal{R}$ of arity $n_R$, and $a_1, \dots, a_{n_R} \in M$,
$$(a_1, \dots, a_{n_R}) \in R^{\mathcal{M}} \Leftrightarrow (\eta(a_1), \dots, \eta(a_{n_R})) \in R^{\mathcal{N}};$$

(c) for each constant symbol $c \in \mathcal{C}$, $c^{\mathcal{M}} = c^{\mathcal{N}}$.

From the definition, an $\mathcal{L}$-embedding is an injection, and naturally, we have the following.

**Definition 1.1.4** (Isomorphism)**.** An $\mathcal{L}$-*isomorphism* is a bijective $\mathcal{L}$-embedding.

**Definition 1.1.5** (Automorphism)**.** An $\mathcal{L}$-*automorphism* of $\mathcal{M}$ is an $\mathcal{L}$-isomorphism from $\mathcal{M}$ to $\mathcal{M}$.

**Definition.** Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures. Suppose $M \subseteq N$ and the inclusion map $\iota\colon \mathcal{M} \hookrightarrow \mathcal{N}$ is an $\mathcal{L}$-embedding.

**Definition 1.1.6** (Substructure)**.** $\mathcal{M}$ is a *substructure* of $\mathcal{N}$.

**Definition 1.1.7** (Extension)**.** $\mathcal{N}$ is an *extension* of $\mathcal{M}$.

**Example.** Ring embeddings are $\mathcal{L}_{\text{ring}}$-embeddings.

This generalizes the notions of embedding and isomorphism for many mathematical structures.

**Remark.** Asking that $\eta$ be injective is the same as (b) in Definition 1.1.3 for the relation $=$ since

$$a = b \in \mathcal{M} \Leftrightarrow \eta(a) = \eta(b) \in \mathcal{N}.$$

The notion of substructure is language sensitive. For groups, there are two possible languages:

(a) $\mathcal{L}_1 = \{e, \cdot\}$;

(b) $\mathcal{L}_2 = \left\{e, \cdot, ^{-1}\right\}$, i.e., with the unary inverse operation.

While both seem valid at the first glance, we should use the second one.

To see why, if we use $\mathcal{L}_2$, the substructure of a group is the same thing as a subgroup. But if we use $\mathcal{L}_1$, then $(\mathbb{N}, +, 0)$ is a substructure of $(\mathbb{Z}, +, 0)$, while $\mathbb{N}$ is not a group for sure.[1]

Similarly, we include $-$ in $\mathcal{L}_{\text{ring}}$ for a similar reason as in the previous example.

**Example.** An $\mathcal{L}_{\text{ring}}$-substructure of a field will be a subring, not a subfield. If we want subfields, use $\mathcal{L}_{\text{ring}} \cup \left\{^{-1}\right\}$.[a]

[a] We can set $0^{-1} = 0$, but never use this.

# Lecture 2: Formulas and First-Order Logic

We start by asking that given a function symbol $f$ of arity $n$, could we replace $f$ with an $(n+1)$-ary $R$ relation to represent its graph? 10 Jan. 14:30

**Example.** Let $\mathcal{L}$ be a language with only relation symbols. Let $\mathcal{A}$ be an $\mathcal{L}$-structure. For any $B \subseteq A$, there is a substructure $\mathcal{B}$ of $\mathcal{A}$ with domain $B$.

**Proof.** For each relation symbol $R$, leting $R^{\mathcal{B}} = R^{\mathcal{A}} \cap B^{n_R}$ will make $\mathcal{B}$ a substructure of $\mathcal{A}$. ⊛

The above is not true for function symbols though.

**Example.** If $G = (\mathbb{Z}, 0, +)$, then $\mathbb{N}$ is not the domain of a subgroup. So if we took $\mathcal{L} = \left\{0, +, ^{-1}\right\}$, where $0$ is the unary relation, $+$ is the ternary relation, and $^{-1}$ is the binary relation, an $\mathcal{L}$-substructure of a group might not be a subgroup.

### 1.1.3 Terms

Intuitive, an $\mathcal{L}$-formula is an expression built using the symbols in a language $\mathcal{L}$, $=$, the logical connectives $\wedge, \vee, \neg$, and variable symbols $v_1, v_2, \ldots, x, y, z$, and also quantifiers $\exists$ and $\forall$.

**Definition 1.1.8** (Term). Given a language $\mathcal{L}$, the set of $\mathcal{L}$-*terms* are defined inductively by:

(a) each constant symbol is a *term*;

(b) each variable symbol $v_1, \ldots$ is a *term*;

(c) if $f$ is a function symbol, and $t_1, \ldots, t_{n_f}$ are terms, then $f(t_1, \ldots, t_{n_f})$ is a *term*.

If $\mathcal{M}$ is an $\mathcal{L}$-structure, and $t$ is a term involving only variables among $v_1, \ldots, v_n$, then $t$ has an interpretation $t^{\mathcal{M}} \colon M^n \to M$ as a function as follows. On input $a_1, \ldots, a_n \in M$,

(a) if $t$ is a constant $c$, $t^{\mathcal{M}}(a_1, \ldots, a_n) = c^{\mathcal{M}}$.

(b) if $t$ is a variable $v_i$, $t^{\mathcal{M}}(a_1, \ldots, a_n) = v_i$;

[1] Simply observe that both $(\mathbb{N}, 0, +), (\mathbb{Z}, 0, +)$ are $\mathcal{L}_1$-structures.

(c) if $t$ is $f(s_1, \dots, s_k)$, then $t^{\mathcal{M}}(a_1, \dots, a_n) = f^{\mathcal{M}}\big(s_1^{\mathcal{M}}(a_1, \dots, a_n), \dots, s_k^{\mathcal{M}}(a_1, \dots, a_n)\big)$.

**Intuition.** We are basically substituting for variables and evaluating the expression.

**Example.** In $(\mathbb{R}, 0, 1, +, \cdot, -)$, a term is essentially just a polynomial with integer coefficients, assuming we interpret them in a ring. Technically, a term looks like

$$\cdot(+(1,1), +(x,y)),$$

but we will write terms the natural way, i.e.,

$$(1+1)(x+y).$$

Also, we will use $\underline{n}$ or $n$ to represent the term $\underline{n} = \underbrace{1+1+\ldots+1}_{n \text{ times}}$. So we could write the above term as $2 \cdot (x+y)$.

### 1.1.4 Formulas

**Definition 1.1.9** (Formula)**.** The set of $\mathcal{L}$-*formulas* is defined inductively:

(a) If $s, t$ are terms, then $s = t$ is a *formula*.

(b) If $R$ is a relation symbol of arity $n_R$ and $s_1, \dots, s_{n_R}$ are terms, then $R(s_1, \dots, s_{n_R})$ is a *formula*.

(c) If $f$ is a formula, then $\neg f$ is a *formula*.

(d) If $\varphi$ and $\psi$ are formulas, then $\varphi \wedge \psi$ and $\varphi \vee \psi$ are *formulas*.

(e) If $\varphi$ is a formula and $v_i$ are variables, then $\exists v_i\ \varphi$ and $\forall v_i\ \varphi$ are *formulas*.

**Notation** (Atomic formula)**.** Definition 1.1.9 (a) and (b) are called *atomic formulas*.

**Notation** (Quantifier-free formula)**.** Definition 1.1.9 (a), (b), (c), and (d) are called *quantifier-free formulas*.

This logic is called *first-order logic* (FO logic), since the quantifiers range over elements of the structures, but not over, e.g., subsets.

**Example.** We can say that an element $x$ of a ring has a square root by $\exists y\ y^2 = x$.

**Example.** A group is torsion of order 2 can be said by $\forall x\ x \cdot x = e$.

**Example.** We can write down all the field/group/... axioms as formulas.

Notice that for the first example, the formula $\exists y\ y^2 = x$ only has meaning if we assign what $x$ is. In this case, we say that $y$ is *bound* by $\exists y$. But this is local:

**Example.** Consider

$$y = 1 \wedge \exists y\ y^2 = x,$$

while the first appearance of $y$ is free, the second appearance of $y$ is bound by (in the scope of) $\exists y$.

While our definitions work perfectly fine with the above example, but sometimes we don't want this to happen. In such a case, we simply replace the bound instances of $y$ with a new variable $z$. This idea of variables being free or bound is defined formally as follows.

**Definition 1.1.10** (Free variable)**.** The *free variables* $\mathrm{FV}(\varphi)$ of a formula $\varphi$ are defined inductively:

(a) $\mathrm{FV}(s = t)$ is the set of variables showing up in $s$ or $t$.

(b) $\mathrm{FV}(R(s_1, \ldots, s_{n_R}))$ is the set of variables showing up in $s_1, \ldots, s_{n_R}$.

(c) $\mathrm{FV}(\neg\varphi) = \mathrm{FV}(\varphi)$.

(d) $\mathrm{FV}(\varphi \wedge \psi) = \mathrm{FV}(\varphi \vee \psi) = \mathrm{FV}(\varphi) \cup \mathrm{FV}(\psi)$.

(e) $\mathrm{FV}(\exists x\ \varphi) = \mathrm{FV}(\forall x\ \varphi) = \mathrm{FV}(\varphi) \setminus \{x\}$.

**Example.** $\mathrm{FV}(\exists y\ y^2 = x) = \{x\}$.

**Example.** $\mathrm{FV}(\forall x\ x \cdot x = e) = \varnothing$.

**Definition 1.1.11** (Sentence)**.** A formula $\varphi$ is called a *sentence* if it has no free variables.

**Notation.** If $\varphi$ is a formula with free variables among $x_1, \ldots, x_n$ we often write $\varphi(x_1, \ldots, x_n)$.

**Remark.** So given $\varphi(x_1, \ldots, x_n)$, we know that $\varphi$ has no other free variables than $x_1, \ldots, x_n$.

**Example.** It's valid to write $\varphi(x, y, z) \coloneqq x = y$.

### 1.1.5 Truths

Finally, we define the notion of truth.

**Definition 1.1.12** (Truth)**.** Given an $\mathcal{L}$-structure $\mathcal{M}$, let $\varphi(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula and let $a_1, \ldots, a_n \in M$. Then we say $\varphi$ is *true* of $\overline{a}$ in $\mathcal{M}$,[a] denoted as $\mathcal{M} \models \varphi(\overline{a})$, as follows:

(a) If $\varphi$ is $s = t$, then $\mathcal{M} \models \varphi(\overline{a})$ if $s^{\mathcal{M}}(\overline{a}) = t^{\mathcal{M}}(\overline{a})$.

(b) If $\varphi$ is $R(t_1, \ldots, t_{n_R})$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\left(t_1^{\mathcal{M}}(\overline{a}), \ldots, t_{n_R}^{\mathcal{M}}(\overline{a})\right) \in R^{\mathcal{M}}$.

(c) If $\varphi$ is $\neg\psi$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\mathcal{M} \not\models \psi(\overline{a})$.

(d) If $\varphi$ is $\psi_1 \wedge \psi_2$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\mathcal{M} \models \psi_1(\overline{a})$ and $\mathcal{M} \models \psi_2(\overline{a})$.

(e) If $\varphi$ is $\psi_1 \vee \psi_2$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\mathcal{M} \models \psi_1(\overline{a})$ or $\mathcal{M} \models \psi_2(\overline{a})$.

(f) If $\varphi$ is $\exists y\ \psi(\overline{x}, y)$, then $\mathcal{M} \models \varphi(\overline{a})$ if there's $b \in M$ such that $\mathcal{M} \models \psi(\overline{a}, b)$.

(g) If $\varphi$ is $\forall y\ \psi(\overline{x}, y)$, then $\mathcal{M} \models \varphi(\overline{a})$ if for all $b \in M$ such that $\mathcal{M} \models \psi(\overline{a}, b)$.

[a] Or $\mathcal{M}$ satisfies $\varphi(\overline{a})$.

**Remark.** Every formula is true, or its negation is.

## Lecture 3: Logical Consequence and Equivalence

**Notation** (Material implication)**.** The *material implication* $\varphi \to \psi$ between two formulas $\varphi, \psi$ is an abbreviation of $\neg\varphi \vee \psi$. 12 Jan. 14:30

**Notation.** We use $\varphi \leftrightarrow \psi$ as an abbreviation of $((\varphi \to \psi) \land (\psi \to \varphi))$.

Essentially, $\to$ and $\leftrightarrow$ is different from $\Rightarrow$ and $\Leftrightarrow$, where the former are only shown in formula. Now, consider the language of graphs $\mathcal{L}_{\text{graph}} = \{E\}$, let's see some examples.

**Example.** An undirected graph can be written as

$$\forall x \forall y\ (xEy \to yEx).$$

**Example.** A vertex has at least three neighbors can be written as

$$\varphi(x) := \exists u \exists v \exists w\ (xEu \land xEv \land xEw \land u \neq v \land v \neq w \land u \neq w)$$

in non-reflexive graphs.

**Example.** For a vertex has exactly three neighbors,

$$\psi(x) := \exists u \exists v \exists w \forall y\ \big(xEu \land xEv \land xEw \land u \neq v \land v \neq w \land u \neq w \land (y = u \lor y = v \lor y = w \lor \neg yEx)\big).$$

**Problem.** Can we say that $x$ has an even number of neighbors?

**Answer.** We can't. Some things are not expressible in FO logic. ⊛

**Example.** For a vertex $x$ has a path of length 4 to $y$,

$$\Theta(x, y) := \exists u \exists v \exists w\ (xEu \land uEv \land vEw \land wEy).$$

We can also express that there is a path of length at most 4.

**Problem.** Can we say that there is a path from $x$ to $y$?

**Answer.** We still can't! Not in FO logic (using compactness theorem). ⊛

**Remark.** When we prove results by induction on formulas, we only need to prove for $\neg, \land, \exists$, instead of for both $\land, \lor$, and both $\exists$ and $\forall$.

**Proof.** Since we can view $\varphi \lor \psi$ as an abbreviation for $\neg(\neg\varphi \land \neg\psi)$ and $\forall x\ \varphi$ as an abbreviation for $\neg(\exists x\ \neg\varphi)$. ⊛

**Remark (Sheffer stroke).** In fact, we can get $\land, \lor, \neg$ from one logical connective, e.g., the *sheffer stroke* $\uparrow$, which is defined as

$$\varphi \uparrow \psi := \neg(\varphi \land \psi),$$

and we can use $\uparrow$ to define $\neg, \lor, \land$.

**Notation.** Let $\Phi$ be a (possibly infinite) set of sentences, we write $\mathcal{M} \models \Phi$ if $\mathcal{M} \models \varphi$ for all $\varphi \in \Phi$.

**Definition 1.1.13 (Logical consequence).** Let $\Phi$ be a set of sentences, and $\varphi$ be a sentence. We say that $\varphi$ is a *logical consequence* of $\Phi$, written $\Phi \models \varphi$, if $\mathcal{M} \models \varphi$ whenever $\mathcal{M} \models \Phi$.

If $\Phi = \varnothing$ is the empty set, Definition 1.1.13 is written as $\models \varphi$, i.e., $\varphi$ is true in all $\mathcal{L}$-structures.[2]

[2]Recall that we always have a language $\mathcal{L}$ implicitly.

**Definition 1.1.14** (Equivalent). Given two formulas $\varphi, \psi$, $\varphi(\overline{x})$ and $\psi(\overline{x})$ are *equivalent* if

$$\models \forall \overline{x}\ \big(\varphi(\overline{x}) \leftrightarrow \psi(\overline{x})\big).$$

**Problem.** Two sentences $\varphi$ and $\psi$ are equivalent if and only if $\varphi \models \psi$ and $\psi \models \varphi$. DIY

**As previously seen.** $\mathcal{A}$ is a substructure of $\mathcal{B}$, or $\mathcal{A} \subseteq \mathcal{B}$, means that $A \subseteq B$ and $\mathrm{id}\colon A \hookrightarrow B$ is an $\mathcal{L}$-embedding.

**Proposition 1.1.1.** Suppose that $\mathcal{A}$ is a substructure of $\mathcal{B}$, and $\varphi(\overline{x})$ is a quantifier-free formula. Let $\overline{a} \in \mathcal{A}$,[a] then $\mathcal{A} \models \varphi(\overline{a})$ if and only if $\mathcal{B} \models \varphi(\overline{a})$.

[a] Formally, we need to write $\mathcal{A}$ to be the Cartesian product with a fixed length.

**Proof.** We start with terms by proving that if $t$ is a term and $\overline{b} \in \mathcal{A}$, then $t^{\mathcal{A}}(\overline{b}) = t^{\mathcal{B}}(\overline{B})$. The proof is induction on terms.

(a) If $t$ is a constant symbol $c$, then $t^{\mathcal{A}}(\overline{b}) = c^{\mathcal{A}} = c^{\mathcal{B}} = t^{\mathcal{B}}(\overline{b})$.

(b) If $t$ is a variable $x_i$, then $t^{\mathcal{A}}(\overline{b}) = b_i = t^{\mathcal{B}}(\overline{b})$.

(c) If $t$ is a function symbol $f(s_1, \dots, s_n)$ where $s_i$ are terms, then $t^{\mathcal{A}}(\overline{b}) = f^{\mathcal{A}}\big(s_1^{\mathcal{A}}(\overline{b}), \dots, s_n^{\mathcal{A}}(\overline{b})\big)$. By the induction hypothesis, $s_i^{\mathcal{A}}(\overline{b}) = s_i^{\mathcal{B}}(\overline{b}) \in \mathcal{A}$, and hence

$$t^{\mathcal{B}}(\overline{b}) = f^{\mathcal{B}}\big(s_1^{\mathcal{B}}(\overline{b}), \dots, s_n^{\mathcal{B}}(\overline{b})\big) = f^{\mathcal{A}}\big(s_1^{\mathcal{A}}(\overline{b}), \dots, s_n^{\mathcal{A}}(\overline{b})\big) = t^{\mathcal{A}}(\mathcal{B}),$$

i.e., $f^{\mathcal{B}} \restriction_{\mathcal{A}} = f^{\mathcal{A}}$, so $t^{\mathcal{A}}(\overline{b}) = t^{\mathcal{B}}(\overline{b})$.

Now we turn to formulas, and prove that for $\varphi$ quantifier-free, then $\mathcal{A} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{B} \models \varphi(\overline{a})$ for $\overline{a} \in \mathcal{A}$. The proof is, again, induction on formulas.[a]

(a) If $\varphi$ is $s = t$, then $s^{\mathcal{A}}(\overline{a}) = s^{\mathcal{B}}(\overline{a})$ and $t^{\mathcal{A}}(\overline{a}) = t^{\mathcal{B}}(\overline{a})$, so

$$\mathcal{A} \models \varphi(\overline{a}) \Leftrightarrow s^{\mathcal{A}}(\overline{a}) = t^{\mathcal{A}}(\overline{a}) \Leftrightarrow s^{\mathcal{B}}(\overline{a}) = t^{\mathcal{B}}(\overline{a}) \Leftrightarrow \mathcal{B} \models \varphi(\overline{a}).$$

(b) If $\varphi$ is $R(s_1, \dots, s_n)$, then

$$A \models \varphi(\overline{a}) \Leftrightarrow \big(s_1^{\mathcal{A}}(\overline{a}), \dots, s_n^{\mathcal{A}}(\overline{a})\big) \in R^{\mathcal{A}} \Leftrightarrow \big(s_1^{\mathcal{B}}(\overline{a}), \dots, s_n^{\mathcal{B}}(\overline{a})\big) \in R^{\mathcal{B}} \Leftrightarrow \mathcal{B} \models \varphi(\overline{a}).$$

(c) If $\varphi$ is $\neg\psi$,

$$\mathcal{A} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{A} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{B} \not\models \psi(\overline{a}) \Leftrightarrow \mathcal{B} \models \varphi(\overline{a}),$$

where we use the induction hypothesis in the second $\Leftrightarrow$.

(d) If $\varphi$ is $\psi_1 \vee \psi_2$,

$$\mathcal{A} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{A} \models \psi_1(\overline{a}) \text{ or } \mathcal{A} \models \psi_2(\overline{a}) \Leftrightarrow \mathcal{B} \models \psi_1(\overline{a}) \text{ or } \mathcal{B} \models \psi_2(\overline{a}) \Leftrightarrow \mathcal{B} \models \varphi(\overline{a}),$$

where we use the induction hypothesis in the second $\Leftrightarrow$.

■

[a] Recall that we only need to show one of $\vee$ or $\wedge$, and here we pick $\vee$ and treat $\wedge$ as an abbreviation.

**As previously seen** (Characteristic). Given a field $K$, the *characteristic* $p$ of $K$ is the number of 1 you need to add 1 in order to get 0, i.e., $\underbrace{1 + 1 + \ldots + 1}_{p} = 0$.

**Example.** Let $L$ be a subfield of $K$, for each $p > 0$, $\varphi_p := \underbrace{1 + 1 + \ldots + 1}_{p} = 0$, which says the characteristic $p$. $\varphi_p$ is quantifier-free, so

$$L \models \varphi_p \Leftrightarrow K \models \varphi_p.$$

**Example.** Consider $\mathbb{Z} = (\mathbb{Z}, 0, 1, +, -, \cdot)$, and let $\varphi(x) := \neg\exists y\ y + y = x$. We see that $\mathbb{Z} \models \varphi(1)$ but $\mathbb{Q} \models \neg\varphi(1)$.

**Proposition 1.1.2.** Suppose that $\mathcal{A}$ is a substructure of $\mathcal{B}$, and $\varphi(\overline{x}, y_1, \ldots, y_n)$ is a quantifier-free formula. Let $\overline{a} \in \mathcal{A}$, then

(a) if $\mathcal{A} \models \exists y_1 \ldots \exists y_n\ \varphi(\overline{a}, y_1, \ldots, y_n)$, then $\mathcal{B} \models \exists y_1 \ldots \exists y_n\ \varphi(\overline{a}, y_1, \ldots, y_n)$;

(b) if $\mathcal{B} \models \forall y_1 \ldots \forall y_n\ \varphi(\overline{a}, y_1, \ldots, y_n)$, then $\mathcal{A} \models \forall y_1 \ldots \forall y_n\ \varphi(\overline{a}, y_1, \ldots, y_n)$.

**Proof.** Suppose that $\mathcal{A} \models \exists y_1 \ldots \exists y_n\ \varphi(\overline{a}, y_1, \ldots, y_n)$, so there are $b_1, \ldots, b_n \in \mathcal{A}$ such that $\mathcal{A} \models \varphi(\overline{a}, b_1, \ldots, b_n)$. Since $\varphi$ is quantifier-free, so $\mathcal{B} \models \varphi(\overline{a}, b_1, \ldots, b_n)$ from Proposition 1.1.1, and hence $\mathcal{B} \models \exists y_1 \ldots \exists y_n\ \varphi(\overline{a}, y_1, \ldots, y_n)$.

On the other hand, it's easy to see that (b) is implied by (a). ■

**Notation** (Existential)**.** In Proposition 1.1.2, formulas as in (a) are called *existential ($\exists_1$ or $\exists$) formulas.*

**Notation** (Universal)**.** In Proposition 1.1.2, formulas as in (b) are called *universal ($\forall_1$ or $\forall$) formulas.*

**Example.** Recall $\mathcal{L}_1 = \{e, \cdot\}$, $\mathcal{L}_2 = \left\{e, \cdot, {}^{-1}\right\}$.

- Associativity: $\forall x \forall y \forall z\ (xy)z = x(yz)$.
- Identity: $\forall x\ ex = xe$.

These are $\forall$-formulas in either language.

- Inverses in $\mathcal{L}_1$: $\forall x \exists y\ xy = yx = e$, which is **not** an $\forall$-formula.
- Inverses in $\mathcal{L}_2$: $\forall x\ xx^{-1} = x^{-1}x = e$, which is an $\forall$-formula.

Hence, group axioms in $\mathcal{L}_1$ are not universal, but in $\mathcal{L}_2$ they are.

The above discrepancy is the reason why $\mathcal{L}_2$ is better than $\mathcal{L}_1$, i.e., $\mathcal{L}_1$-substructure might not be a group.

**Problem.** Show that $\forall x \exists y\ xy = yx = e$ in the above example is not equivalent to an $\forall$-formula.

## Lecture 4: Theories and Axioms

17 Jan. 14:30

**Example.** Let $\mathcal{L}_1 = \{E\}$, where $E$ is a binary relation representing edge relation; and $\mathcal{L}_2 = \{V, E, I\}$, where $V, E$ are unary relations and $I$ is a binary relation representing incidence such that $I(v, e)$ for $v \in V$, $e \in E$ means that $v$ is a vertex on edge $e$. Then,

- Let $G$ be a graph, viewed as an $\mathcal{L}_1$-structure. A substructure of $G$ is an induced subgraph $H \subseteq G$ such that any edge in $G$ between two vertices of $H$ is in $H$.
- If we view $G$ as an $\mathcal{L}_2$-substructure, a substructure is a subgraph $H$ such that $H$ has some vertices and edges from $G$.[a]

[a]But there might be edges in $H$ with no vertices, which can be fixed by having two functions $I_1(e) = v$, $I_2(e) = w$ when $e\colon v \to w$.

The difference is that for $\mathcal{L}_1$, having an edge is quantifier-free, while in $\mathcal{L}_2$ is existential. To elaborate a bit further, for $\mathcal{L}_2$, $vEw$ is quantifier-free, while in $\mathcal{L}_2$,

$$\exists\ (v \in V \wedge w \in V \wedge e \in E \wedge I(v, e) \wedge I(w, e))$$

is not quantifier-free.

## 1.2 Theories

Let's start by the notion of theory.

**Definition 1.2.1** (Theory). An $\mathcal{L}$-*theory* is a set of $\mathcal{L}$-sentences.

**Definition 1.2.2** (Model). $\mathcal{M}$ is a *model* of a theory $T$, written as $\mathcal{M} \models T$, if $\mathcal{M} \models \varphi$ for all $\varphi \in T$.

**Note.** Not every theory has a model, e.g., $\{\exists x\ x \neq x\}$.

The above note motivates the following.

**Definition 1.2.3** (Satisfiable). A theory is *satisfiable* if it has a model.

**Definition 1.2.4** (Elementary class). A class $\mathcal{K}$ of $\mathcal{L}$-structures $\mathcal{M}$ is called an *elementary class* if there is an $\mathcal{L}$-theory $T$ such that

$$\mathcal{K} = \{\mathcal{M} \mid \mathcal{M} \models T\}.$$

One way to get an elementary class is to take an $\mathcal{L}$-structure $\mathcal{M}$ and take the full theory.

**Definition 1.2.5** (Full theory). The *full theory* $\mathrm{Th}(\mathcal{M})$ of an $\mathcal{L}$-structure $\mathcal{M}$ is defined as $\mathrm{Th}(\mathcal{M}) = \{\varphi \mid \mathcal{M} \models \varphi\}$.

From the definition, $\mathcal{M} \models \mathrm{Th}(\mathcal{M})$, and $\mathrm{Th}(\mathcal{M})$ characterizes the structures satisfying the same sentences as $\mathcal{M}$.

**Definition 1.2.6** (Complete). A theory $T$ is *complete* if for any sentence $\varphi$, either $\varphi \in T$ or $\neg\varphi \in T$.

**Remark.** $\mathrm{Th}(\mathcal{M})$ is complete.

**Definition 1.2.7** (Elementarily equivalent). $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent*$\mathcal{M} \equiv \mathcal{N}$ if for all sentences $\varphi$,

$$\mathcal{M} \models \varphi \Leftrightarrow \mathcal{N} \models \varphi.$$

**Remark.** There are $\mathcal{N} \models \mathrm{Th}(\mathbb{N})$, but $\mathcal{N}$ is not isomorphic to $\mathbb{N}$. $\mathcal{N}$ is called a *non-standard model of arithmetic*, and $\mathcal{N}$ might have *infinite element* larger than all of $\mathcal{M}$. Here, $\mathbb{N} = (\mathbb{N}, 0, 1, +, \cdot, -)$

**Example.** $\mathbb{Z} \oplus \mathbb{Z} \not\equiv \mathbb{Z}$ as groups.

The other way to define a theory is to write down axioms.

**Example** (Infinite set). Let $\mathcal{L} = \varnothing$, and let $T$ consist of

$$\varphi_n \coloneqq \exists x_1 \dots \exists x_n \bigwedge_{i \neq j} x_i \neq x_j.$$

**Example** (Linear order). Let $\mathcal{L} = \{\leq\}$, and let $T$ consist of the axioms of linear orders, e.g.,

$$\forall x \forall y\ (x \leq y \land y \leq x \to x = y).$$

There are other interesting theories of linear orders, e.g., dense ones.

**Example** (Dense linear order). Consider

$$\forall x \forall y\ (x < y \to \exists z\ x < z < y),$$

where we use $a < b$ as shorthand of saying $a \leq b \land a \neq b$.

**Example** (Group). In $\mathcal{L}_{\text{group}} = \{e, \cdot, ^{-1}\}$, let $T$ be the group axioms.

Other theories of groups include Abelson group, divisible, etc.

**Definition 1.2.8** (Finitely axiomatizable). A theory is *finitely axiomatizable* if it has a finite set of axioms.

Given a theory, consider $T^{\models} = \{\varphi \mid T \models \varphi\}$,[3] so $\mathcal{M} \models T$ if and only if $\mathcal{M} \models T^{\models}$. Often we think of $T$ and $T^{\models}$ as the same. A theory $T$ is finitely axiomatizable if there is a finite $\Phi$ such that $T^{\models} = \Phi^{\models}$.

### 1.2.1 Elementary Embeddings

Let's now consider the following notion.

**Definition 1.2.9** (Elementary embedding). Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures, and $f \colon \mathcal{M} \to \mathcal{N}$ an $\mathcal{L}$-embedding. Then $f$ is an *elementary embedding* if for any formula $\varphi(\overline{x})$ and $\overline{a} \in M$,

$$\mathcal{M} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{N} \models \varphi(f(\overline{a})).$$

**Definition 1.2.10** (Elementary substructure). If $f \colon \mathcal{M} \hookrightarrow \mathcal{N}$ is a elementary embedding where $\mathcal{M}$ is a substructure of $\mathcal{N}$, then $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$, written as $\mathcal{M} \preceq \mathcal{N}$.

**Example.** As groups, $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is not elementary. In fact, $\mathbb{Z} \not\equiv \mathbb{Q}$. Wheres, if $f \colon \mathcal{M} \hookrightarrow \mathcal{N}$ is an elementary embedding, $\mathcal{M} \equiv \mathcal{N}$.[a]

[a] And also much more is true.

**Proposition 1.2.1.** Every isomorphism is an elementary embedding.

**Proof.** Let $f \colon \mathcal{M} \to \mathcal{N}$ be an isomorphism. We will argue by induction on formulas $\varphi$, that for all $\overline{a} \in M$,

$$\mathcal{M} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{N} \models \varphi(f(\overline{a})).$$

Firstly, observe that all cases except quantifiers are the same as Proposition 1.1.1. For quantifiers, suppose that $\varphi(\overline{x})$ is $\exists y\ \psi(\overline{x}, y)$ and $\mathcal{M} \models \varphi(\overline{a})$. This means that there is $b \in M$ such that $\mathcal{M} \models \psi(\overline{a}, b)$. By the induction hypothesis, $\mathcal{N} \models \psi(f(\overline{a}), f(b))$, so $\mathcal{N} \models \varphi(f(\overline{a}))$.

Now suppose $\mathcal{N} \models \varphi(f(\overline{a}))$, then there is $c \in N$ such that $\mathcal{N} \models \psi(f(\overline{a}), c)$. Since $f$ is an isomorphism, so there is a $b \in M$ such that $f(b) = c$. By the induction hypothesis, $\mathcal{M} \models \psi(\overline{a}, b)$,

[3] Recall Definition 1.1.13.

so $\mathcal{M} \models \varphi(\overline{a})$. ∎

**Corollary 1.2.1.** If $\mathcal{M} \cong \mathcal{N}$, then $\mathcal{M} \equiv \mathcal{N}$.

### 1.2.2 Definable Sets

Consider the following.

**Definition 1.2.11** (Definable). Let $\mathcal{M}$ be an $\mathcal{L}$-structure, then $X \subseteq M^n$ is *definable* if there is a formula $\varphi(x_1, \ldots, x_n, \overline{y})$ and $\overline{b} \in M$ such that

$$X = \left\{\overline{a} \in M^n \mid \mathcal{M} \models \varphi(\overline{a}, \overline{b})\right\}.$$

**Notation** (Define). We say that $\varphi(\overline{x}, \overline{b})$ *defines* $X$ over $\overline{b}$, written as $X = \varphi(\mathcal{M}, \overline{b})$.

**Notation** (Parameter). The tuple $\overline{b}$ is called the *parameters* when $X$ is definable over $\overline{b}$.

**Remark.** Sometimes $X$ is definable without parameters, or definable over $\varnothing$.

**Example.** Take $\mathbb{R} = (\mathbb{R}, 0, 1, +, \cdot, -)$ in $\mathcal{L}_{\text{ring}}$, then

$$\leq = \{(a, b) \colon a \leq b\}$$

is definable.

**Example.** Let $\mathbb{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$, then $\mathbb{N}$ is $\varnothing$-definable in $\mathbb{Z}$ by[a]

$$\mathbb{N} = \left\{z \in \mathbb{Z} \colon \exists u, v, x, y\ u^2 + v^2 + x^2 + y^2 = z\right\}.$$

[a]From the Langrange's four-square theorem, which says that every natural number is the sum of four squares.

**Example.** $\mathbb{Z}$ is $\varnothing$-definable in $\mathbb{Q} = (\mathbb{Q}, +, -, \cdot, 0, 1)$. This is a result of Julia Robinson [Rob49], and the formulation is very complicated.

**Problem.** How does one show that a set is not definable? For example, $\mathbb{R}$ is not definable in $\mathbb{C} = (\mathbb{C}, 0, 1, +, \cdot, -)$.

## Lecture 5: Hilbert-Style Deductive System

We start by asking whether $\mathbb{R}$ is definable in $\mathbb{C} = (\mathbb{C}, 0, 1, +, \cdot, -)$? 19 Jan. 14:30

**Proposition 1.2.2.** Let $\mathcal{M}$ be an $\mathcal{L}$-structure, and let $X \subseteq M^n$ be a set which is definable over $\overline{a}$. Then any automorphism of $\mathcal{M}$ that fixes $\overline{a}$ pointwise[a] fixes $X$ setwise.[b]

[a]If $\overline{a} = (a_1, \ldots, a_m)$, then $f(a_i) = a_i$.
[b]If $b \in X$, then $f(b) \in X$.

**Proof.** Let $f$ be an automorphism of $\mathcal{M}$ fixing $\overline{a}$ pointwise, and $X = \left\{\overline{b} \in M^n \colon \mathcal{M} \models \varphi(\overline{b}, \overline{a})\right\}$. Fix $\overline{b}$, and suppose $\overline{b} \in X$, so $\mathcal{M} \models \varphi(\overline{b}, \overline{a})$. Because $f$ is an elementary embedding from Proposition 1.2.1,

$$\mathcal{M} \models \varphi(f(\overline{b}), f(\overline{a})) \Rightarrow \mathcal{M} \models \varphi(f(\overline{b}), \overline{a}),$$

hence $f(\bar{b}) \in X$. Similarly, if $\bar{b} \notin X$, $\mathcal{M} \models \neg\varphi(\bar{b}, \bar{a}) \Rightarrow \mathcal{M} \models \neg\varphi(f(\bar{b}, \bar{a}))$, so $f(\bar{b}) \notin X$. ■

**Remark.** If $X$ is $\varnothing$-definable, it is fixed setwise by any automorphism.

**Example.** $\mathbb{N}$ is fixed setwise by any automorphism of the ring $\mathbb{Z}$. In fact, the only automorphism of $\mathbb{Z}$ is the identity.

**Example.** $\mathbb{N}$ is not $\varnothing$-definable in $\mathbb{Z} = (\mathbb{Z}, 0, +)$.

**Proof.** Consider an automorphism $f(x) = -x$ of the group $\mathbb{Z}$, which does not fix $\mathbb{N}$ setwise. ⊛

**Problem.** Is $\mathbb{N}$ definable in $\mathbb{Z} = (\mathbb{Z}, 0, +)$ over some parameters $\bar{a}$?

**Answer.** For example, if $\bar{a} = (1)$, then $f$ does not fix 1. In fact, any automorphism fixing 1 also fixes all of $\mathbb{Z}$, but $\mathbb{N}$ is not definable in $(\mathbb{Z}, 0, +)$. To prove this we need compactness. ⊛

**As previously seen.** Given a field $F$, then $F(a) \cong F(b)$ if $a$ and $b$ have the same minimal polynomial over $F$ or if both do not satisfy any polynomial over $F$.

**Example.** $\mathbb{Q}(\pi) \cong \mathbb{Q}(e)$ because $\pi$ and $e$ are both transcendental.

We now return to the big question: is $\mathbb{R}$ definable in $\mathbb{C} = (\mathbb{C}, 0, 1, +, \cdot, -)$? If $f\colon \mathbb{Q}(a) \to \mathbb{Q}(b)$ such that $a \mapsto b$, then there is an automorphism $\hat{f}\colon \mathbb{C} \to \mathbb{C}$ such that $a \mapsto b$, i.e., $\hat{f}$ extends $f$. In other words, we need to find such an $f$ with $a \in \mathbb{R}$ and $b \notin \mathbb{R}$.

**Example.** $a = \pi$, $b = i\pi$ are both transcendental.

**Example.** $a$ is a real $\sqrt[4]{2}$, $b$ is a complex $\sqrt[4]{2}$.

The above two examples show that $\mathbb{R}$ is not $\varnothing$-definable in $\mathbb{C}$. In fact, $\mathbb{R}$ is not definable over any $\bar{a}$ because there are elements of $\mathbb{R}$ and $\mathbb{C} \setminus \mathbb{R}$ transcendental over any $\bar{a}$.

**Intuition.** There are so many $a, b$ such that given any $\bar{a}$, we can still find a pair that works.

## 1.3 Completeness and Compactness

In this section, we're going to formalize proofs.

### 1.3.1 Proofs

There are all sorts of different proof systems, and the one we use is the so-called Hilbert-style deductive system. Before that, we first see some common notions.

**Notation** (Schema). A *schema* is written in symbols for formulas, variables, etc.

**Example.** $\varphi \to (\psi \to \varphi)$ is a schema, i.e., an infinite set with all possible choices of $\varphi$ and $\psi$.

Specifically, every logical axiom is written in schema, meaning that any instance of a symbol for a formula, e.g., $\varphi$, can be replaced by any formula.

**Definition 1.3.1** (Generalization). A formula $\varphi$ is a *generalization* of a formula $\psi$ if $\varphi$ is $\forall x_1 \ldots \forall x_n\ \psi$ where $x_1, \ldots, x_n$ are variables.

**Notation** (Hypothesis). *Hypotheses* are formulas that we may assume in a proof.

**Definition 1.3.2** (Proof). A *proof* is a sequence of formulas $\{\varphi_i\}_{i=1}^n$ such that $\varphi_n$ is the conclusion, and each formula is either an axiom or is obtained from the previous formulas by a rule of inference.

Moreover, for a proof based on a set of hypotheses $\Gamma$, then in addition to a logical axiom, we can assert a formula $\varphi \in \Gamma$. If we prove $\psi$ using $\Gamma$ as hypotheses, we write $\Gamma \vdash \psi$.

**Definition 1.3.3** (Valid). If we prove $\psi$ without hypotheses, we write $\vdash \psi$ and say $\psi$ is *valid*.

**Definition 1.3.4** (Logical axioms). The *logical axioms* are the following formulas written in schema, as well as all of their generalizations:

**Definition 1.3.5** (Propositional axioms). The *propositional axioms* are

(A1) $\varphi \to (\psi \to \varphi)$.

(A2) $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$.

(A3) $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$.

(A4) $\forall x\ \varphi(x, \ldots) \to \varphi(t, \ldots)$ where $t$ is any term.

(A5) $[\forall x\ (\varphi \to \psi)] \to [(\forall x\ \varphi) \to (\forall x\ \psi)]$.

(A6) $\varphi \to \forall x\ \varphi$, where $x$ is not free in $\varphi$.

**Definition 1.3.6** (Axioms for equality). The *axioms for equality* is

(A7) for any terms $t, u, v, \ldots$, function symbols $f$, and relation symbols $R$,

(a) $t = t$.
(b) $t = u \to u = t$.
(c) $(t = u \wedge u = v) \to (t = v)$.
(d) $(u_1 = t_1 \wedge \ldots \wedge u_{n_f} = t_{n_f}) \to f(u_1, \ldots, u_{n_f}) = f(t_1, \ldots, t_{n_f})$.
(e) $(u_1 = t_1 \wedge \ldots \wedge u_{n_R} = t_{n_R}) \to (R(u_1, \ldots, u_{n_R}) \leftrightarrow R(t_1, \ldots, t_{n_R}))$.

**Definition 1.3.7** (Rule of inference). From $\varphi$ and $\varphi \to \psi$, deduces $\psi$.[a]

[a] This is called modus ponens.

These formulas might have free variables.

**Example.** A proof from calculus of a limit, e.g., $\forall\epsilon\exists\delta\ldots$. And we start by stating

1. let $\epsilon > 0$,
2. choose $\delta = \epsilon$,

$\vdots$

$n$. $|f(x) - f(y)| < \epsilon$.

We should interpret free variables as anything.

**As previously seen** (Propositional logic). $(p \wedge q) \vee (r \wedge \neg q)$.

**Remark.** We can check whether the propositional axioms are true with a truth table.

**Definition 1.3.8** (Propositional tautology)**.** A *propositional tautology* is a boolean combination $\vee, \wedge, \neg$ of formulas $\varphi_1, \ldots, \varphi_n$ which is true via a truth table assigning true or false to each of $\varphi_1, \ldots, \varphi_n$.

So instead of using propositional axioms, we could instead allow as logical axioms any propositional tautology. To prove completeness, we will need 5 propositional tautologies. We will prove some of these, but take others on faith.

**Remark.** Propositional axioms are enough to prove all propositional tautologies.

**Notation.** We write $\Gamma \vdash_{\mathcal{L}} \varphi$ if there is a proof of $\varphi$ from $\Gamma$ in the language $\mathcal{L}$.

**Note.** Passing to a larger language will not let you prove more, so we can just write $\vdash$.

## Lecture 6: Soundness Theorem

To see why propositional axioms are enough to prove all propositional tautologies, we see one example. 24 Jan. 14:30

**Problem.** Prove $\varphi \to \varphi$ using propositional axioms.

**Answer.** We see that

1. $\varphi \to ((\psi \to \varphi) \to \varphi)$ from (A1), where $\psi$ is any formula (possibly $\psi = \varphi$).
2. $[\varphi \to ((\psi \to \varphi) \to \varphi)] \to [(\varphi \to (\psi \to \varphi)) \to (\varphi \to \varphi)]$ from (A2).
3. $(\varphi \to (\psi \to \varphi)) \to (\varphi \to \varphi)$ from (MP) and the two above.
4. $\varphi \to (\psi \to \varphi)$ from (A1).
5. $\varphi \to \varphi$ from (MP) and the two above.

⊛

In general, we can prove

(a) $\varphi \to \varphi$;

(b) $\varphi \to \neg\neg\varphi$;

(c) $\neg\neg\varphi \to \varphi$;

(d) $(\varphi \to \psi) \to ((\neg\varphi \to \psi) \to \psi)$;

(e) $\varphi \to (\psi \to (\varphi \to \psi))$,

and so on.

**Note.** As we said, we may replace propositional axioms by every propositional tautologies.

Some proof system also have a second rule about universal quantifiers, but in our system, we have built this into the axioms. We can prove, as a theorem, what the other proof systems take as a rule.

**Theorem 1.3.1.** If $\Gamma \vdash \varphi$, and $x$ does not occur freely in $\Gamma$, then $\Gamma \vdash \forall x\ \varphi$.

**Proof.** Fix $\Gamma$ and $x$, we use *induction on proofs*. Consider the set $\{\varphi \mid \Gamma \vdash \forall x\ \varphi\}$, we will show that this set contains all the logical axioms, formulas from $\Gamma$, and is closed under modus ponens.[a]

(a) If $\varphi$ is a logical axiom, so is its generalization $\forall x\ \varphi$, so $\Gamma \vdash \forall x\ \varphi$.

(b) If $\varphi \in \Gamma$, then $x$ is not free in $\varphi$, so from (A6), $\varphi \to \forall x\ \varphi$, and from (MP), $\forall x\ \varphi$. The above are based on $\Gamma$, hence $\Gamma \vdash \forall x\ \varphi$.

(c) Suppose $\Gamma \vdash \forall x\ \varphi$ and $\Gamma \vdash \forall x\ (\varphi \to \psi)$, we want to show that $\Gamma \vdash \forall x\ \psi$.

1. By (A5), $\forall x\ (\varphi \to \psi) \to (\forall x\ \varphi \to \forall x\ \psi)$, $\Gamma$ proves this.
2. By (MP), $\Gamma \vdash \forall x\ \varphi \to \forall x\ \psi$.
3. By (MP) again, $\Gamma \vdash \forall x\ \psi$.

■

[a] Thus, if $\Gamma \vdash \theta$, then $\theta \in \{\varphi \mid \Gamma \vdash \forall x\ \varphi\}$.

**Corollary 1.3.1.** If $\vdash \varphi$, then $\vdash \forall x\ \varphi$. So the generalization of anything valid is also valid.

We now ask a critical question: is our proof system a good one?

### 1.3.2 Soundness Theorem

The first thing we should check is whether our proofs are sound.

**Definition 1.3.9** (Sound). A proof system is *sound* if any provable sentence $\varphi$ is true.

The idea is that if an $\mathcal{L}$-sentence $\varphi$ is provable, then it is true in all $\mathcal{L}$-structures, i.e., every thing we prove should be true, in other words, we can't prove wrong things.

**Lemma 1.3.1** (Soundness). If $\Gamma$ is a set of $\mathcal{L}$-sentences and $\varphi$ is a sentence, and $\Gamma \vdash_{\mathcal{L}} \varphi$, then $\Gamma \models \varphi$.

**Proof.** Suppose that $\Gamma \vdash \varphi$, let $\psi_1, \psi_2, \dots, \psi_n = \varphi$ be such a proof.[a] Let $\overline{x} = (x_1, \dots, x_m)$ be the free variable that appears in the $\psi_i$. Let $\mathcal{M}$ be an $\mathcal{L}$-structure, $\mathcal{M} \models \Gamma$. To show $\mathcal{M} \models \varphi$, we show that by induction on $i$, for all $\overline{a} \in M^m$, $\mathcal{M} \models \psi_i(\overline{a})$. For $\psi_i$, we have three cases.

(a) If $\psi_i \in \Gamma$, then $\mathcal{M} \models \Gamma$ so $\mathcal{M} \models \psi_i$.

(b) If $\psi_i$ is a (generalization of) a logical axiom, then we can check that $\mathcal{M} \models \psi_i(\overline{a})$. For example, if $\psi_i$ is (A1), $\theta \to (\gamma \to \theta)$, it's easy to check that

$$\mathcal{M} \models \theta(\overline{a}) \to (\gamma(\overline{a}) \to \theta(\overline{a})).$$

(c) If there are $j, k < i$ such that $\psi_k$ is $\psi_j \to \psi_i$, from inductive hypothesis, for all $\overline{a}$, $\mathcal{M} \models \psi_j(\overline{a}), \mathcal{M} \models \psi_k(\overline{a})$, then $\mathcal{M} \models \psi_j(\overline{a}) \to \psi_i(\overline{a})$. Checking our definition of truth, we get $\mathcal{M} \models \psi_i(\overline{a})$.

■

[a] Some $\psi_i$ might be formulas, but $\varphi$ should be a sentence.

There are remarks to make about some obvious properties of $\vdash_{\mathcal{L}}$.

**Remark.** If $\varphi \in \Gamma$, then $\Gamma \vdash \varphi$.

**Remark.** If $\Delta \subseteq \Gamma$, and $\Delta \vdash \varphi$, then $\Gamma \vdash \varphi$.

**Remark.** If $\Gamma \vdash_{\mathcal{L}} \varphi$, and $\mathcal{L}^+ \supseteq \mathcal{L}$, then $\Gamma \vdash_{\mathcal{L}^+} \varphi$.

**Remark.** If $\Gamma \vdash \varphi$, then there is a finite $\Delta \subseteq \Gamma$ such that $\Delta \vdash \varphi$.

We can prove the following.

**Theorem 1.3.2** (Deduction theorem). For any set of formulas $\Gamma$, formulas $\theta$ and $\psi$,

$$\Gamma \cup \{\theta\} \vdash \psi \Leftrightarrow \Gamma \vdash \theta \to \psi.$$

**Proof.** The backward direction is easier. Suppose $\Gamma \vdash \theta \to \psi$, then $\Gamma \cup \{\theta\} \vdash \psi$ since we can have a proof like:

1. $\theta$

   $\vdots$ (the proof of $\Gamma \vdash \theta \to \psi$)

$n$. $\theta \to \psi$

$n+1$. $\psi$.

Now, suppose that $\Gamma \cup \{\theta\} \vdash \psi$, then there is a proof $\psi_1, \ldots, \psi_n = \psi$ from $\Gamma \cup \{\theta\}$. We argue inductively that $\Gamma \vdash \theta \to \psi_i$. For $i$, we have three cases.

(a) If $\psi_i \in \Gamma$ or it is a logical axiom. By (A1), $\psi_i \to (\theta \to \psi_i)$, so $\Gamma \vdash \theta \to \psi_i$.

(b) If $\psi_i = \theta$. Then $\Gamma \vdash \theta \to \theta$ by (A1) and (A2) from here, hence $\Gamma \vdash \theta \to \psi_i$.

(c) If $\psi_i$ follows from $\psi_j$, $\psi_k = \psi_j \to \psi_i$, using (MP) with $j, k < i$.

   1. From the induction hypothesis, $\Gamma \vdash \theta \to \psi_j$ and $\Gamma \vdash \theta \to (\psi_j \to \psi_i)$.
   2. By (A2), $\Gamma \vdash [\theta \to (\psi_j \to \psi_i)] \to [(\theta \to \psi_j) \to (\theta \to \psi_i)]$.
   3. By (MP), $\Gamma \vdash (\theta \to \psi_j) \to (\theta \to \psi_i)$.
   4. By (MP), $\Gamma \vdash \theta \to \psi_i$.

■

## Lecture 7: Soundness, Completeness, and Compactness

26 Jan. 14:30

**Proposition 1.3.1** (Contraposition). If $\Gamma \cup \{\varphi\} \vdash \neg\psi$, then $\Gamma \cup \{\psi\} \vdash \neg\varphi$.

**Proof.** Suppose $\Gamma \cup \{\varphi\} \vdash \neg\psi$, by the deduction theorem says that $\Gamma \vdash \varphi \to \neg\psi$. From (A1), (A2), and (A3), we can prove $(\varphi \to \neg\psi) \to (\psi \to \neg\varphi)$. By (MP), $\Gamma \vdash \psi \to \neg\varphi$, then from the deduction theorem, $\Gamma \cup \{\psi\} \vdash \neg\varphi$. ■

Now we introduce an important notion.

**Definition 1.3.10** (Consistent). A theory $T$ is *consistent* if for all $\varphi$, it is not the case that $T \vdash \varphi$ and $T \vdash \neg\varphi$.

**Definition 1.3.11** (Inconsistent). If a theory $T$ is not consistent, then it's *inconsistent*.

We could make the same definition for a set of formulas.

**Proposition 1.3.2** (Proof by contradiction)**.** If $\Gamma \cup \{\varphi\}$ is inconsistent, then $\Gamma \vdash \neg\varphi$.

**Proof.** There is $\psi$ such that $\Gamma \cup \{\varphi\} \vdash \psi$ and $\Gamma \cup \{\varphi\} \vdash \psi$, so $\Gamma \vdash \varphi \to \psi$ and $\Gamma \vdash \varphi \to \neg\psi$ by the deduction theorem. Using (A1), (A2), and (A3), we can prove that

$$(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi).$$

By (MP), $\Gamma \vdash (\varphi \to \neg\psi) \to \neg\varphi$, and by (MP) again, we have $\Gamma \vdash \neg\varphi$. ■

**Proposition 1.3.3.** If a theory $T$ is consistent, and $\varphi$ is a sentence, then either $T \cup \{\varphi\}$ or $T \cup \{\neg\varphi\}$ is consistent.

**Proof.** If they were both inconsistent, $T \vdash \neg\varphi$ and $T \vdash \neg\neg\varphi$, so $T$ would be inconsistent ↯ ■

**Note.** The above is also true for formulas.

**Remark.** If $T$ is inconsistent, then $T \vdash \varphi$ for any $\varphi$.

**Proof.** If $T$ is inconsistent, then $T \cup \{\neg\varphi\}$ is inconsistent for all $\varphi$. Hence, from proof by contradiction, $T \vdash \neg\neg\varphi$ for all $\varphi$, which is just $T \vdash \varphi$. ⊛

**Definition 1.3.12** (Maximal)**.** A theory $T$ is *maximal* if it is consistent and for all sentences $\varphi$, either $\varphi \in T$ or $\neg\varphi \in T$.

In particular, if $T \vdash \varphi$, then $\varphi \in T$.

**Intuition.** Basically, a maximal consistent theory has opinion on everything.

Now, we want to see that given a consistent theory, whether we can extend it to a maximal one. To do this, we need the following.

**Definition.** Let $(P, \leq)$ be a partially ordered set.

**Definition 1.3.13** (Chain)**.** A *chain* is a set $C \subseteq P$ such that for every $p, q \in C$, either $p \leq q$ or $q \leq p$.

**Definition 1.3.14** (Upper bound)**.** If $X \subseteq P$ is a set, an *upper bound* for $X$ is an element $p \in P$ such that $p \geq q$ for all $q \in X$.

**Definition 1.3.15** (Maximal)**.** An element $p \in P$ is *maximal* if there is no $q \in P$ with $q > p$.

**Note.** Note that a maximal element might not be greater than everything, there is just nothing greater than it.

**Theorem 1.3.3** (Zorn's lemma)**.** Let $(P, \leq)$ be a partially ordered set. If every non-empty chain in $P$ has an upper bound, then $P$ has a maximal element.

**Theorem 1.3.4.** Any consistent theory $T$ can be extended to a maximal consistent theory $T' \supseteq T$.

**Proof.** We first consider the case that $T$ is countable by considering $\mathcal{L}$ is countable since if $\mathcal{L}$ is countable, then there are only countable many formulas since there are only countable many formulas of each length.

**Claim.** The result holds for $\mathcal{L}$ being countable.

**Proof.** Firstly, list out all sentences $\varphi_1, \varphi_2, \ldots$, start with $T_0 = T$. Given $T_i$ consistent, one of $T_i \cup \{\varphi_i\}$ or $T_i \cup \{\neg\varphi_i\}$ is consistent from Proposition 1.3.3. Let $T_{i+1}$ be one of these that is consistent. Let $T^* = \bigcup_i T_i$, which is maximal, and we now show that $T^*$ is consistent.

Suppose not, then $T^* \vdash \theta$ and $T^* \vdash \neg\theta$ for some $\theta$. In this case, there is some $T_i$ such that $T_i \vdash \theta$ and $T_i \vdash \neg\theta$ because proofs are finite, with $T_i$ being consistent, a contradiction $\lightning$ ⊛

**Claim.** The result holds for arbitrary $\mathcal{L}$.

**Proof.** For arbitrary $\mathcal{L}$, let $(P, \leq)$ be the set of consistent theories extending $T_i$ ordered by inclusion. Let $C$ be a non-empty chain, and let $T^* = \bigcup_{T' \in C} T' \supseteq T$.

We see that $T^*$ is consistent because if $T^* \vdash \theta$ and $T^* \vdash \neg\theta$, there are finitely many formulas used in those proofs, from, say, $T_1, \ldots, T_n \in C$. Because $C$ is a chain, by reordering, we may assume that $T_1 \subseteq \ldots \subseteq T_n$. So $T_n \vdash \theta$ and $T_n \vdash \neg\theta$, contradicting the consistency of $T_n$, so $T^*$ is consistent, i.e., $T^* \in P$. Furthermore, $T^*$ is an upper bound on $C$,[a] so $(P, \leq)$ has a maximal consistent theory $T^* \supseteq T$ from Zorn's lemma.

If $T^*$ is not maximal, then there is $\varphi$ where $\varphi \notin T^*$, $\neg\varphi \notin T^*$. From Proposition 1.3.3, one of $T^* \cup \{\varphi\}$ or $T^* \cup \{\neg\varphi\}$ is consistent, hence in $P$, contradicting to $T^*$ being maximal $\lightning$ ⊛

[a] Note that $C$ is arbitrary.

■

**Remark.** We can do that same proof for any $\mathcal{L}$ using transfinite recursion for the uncountable case.

Motivated by Lemma 1.3.1 and Theorem 1.3.4, we close this section with the following.

**Theorem 1.3.5 (Soundness).** Let $T$ be a theory and $\varphi$ be a sentence.

(a) If $T \vdash \varphi$, then $T \models \varphi$.

(b) If $T$ is satisfiable, then it is consistent.

**Proof.** (a) is exactly Theorem 1.3.5. For (b), let $\mathcal{M} \models T$, suppose that $T$ was inconsistent, then $T \vdash \varphi$ and $T \vdash \neg\varphi$ for some $\varphi$. By (a), $T \models \varphi$ and $T \models \neg\varphi$, so $\mathcal{M} \models \varphi$ and $\mathcal{M} \models \neg\varphi$. But $\mathcal{M} \models \neg\varphi$ means $\mathcal{M} \not\models \varphi$, so this is a contradiction, hence $T$ is consistent. ■

### 1.3.3 Completeness and Compactness Theorems

After knowing our proof system is sound, we now ask the converse: is our proof system complete?

**Definition 1.3.16 (Complete).** A proof system is *complete* if any true sentence $\varphi$ is provable.

And indeed, this is the case.

**Theorem 1.3.6 (Completeness).** Let $T$ be a theory and $\varphi$ be a sentence.

(a) If $T \models \varphi$, then $T \vdash \varphi$.

(b) If $T$ is consistent, then it is satisfiable.

(b) implies (a) is easy to see. Suppose that $T \models \varphi$, so $T \cup \{\neg\varphi\}$ is not satisfiable. By (b), $T \cup \{\neg\varphi\}$ is inconsistent. By proof by contradiction, $T \vdash \varphi$. One important consequence of the completeness theorem is the compactness theorem.

**Theorem 1.3.7 (Compactness).** Let $T$ be a theory and $\varphi$ be a sentence.

(a) If $T \models \varphi$, then there is a finite $T_0 \subseteq T$ such that $T_0 \models \varphi$.

(b) $T$ is satisfiable if and only if every finite subset of $T$ is satisfiable.

**Proof.** Consider the following.

(a*) If $T \vdash \varphi$, then there is a finite $T_0 \subseteq T$ such that $T_0 \vdash \varphi$.

(b*) If $T$ is consistent if and only if every finite subset of $T$ is consistent.

We see that (a*) and (b*) are true because proofs are finite, and soundness and completeness translate directly between (a) and (a*) (and (b) and (b*)). ∎

**Remark.** The compactness theorem does have something to do with topological compactness; consider the topological space of complete satisfiable theories, with the basic open sets being the sets

$$U_\varphi \coloneqq \{T : T \models \varphi\},$$

then this topological space is compact.

Let's see one cool example using compactness.

**Example.** Let $\mathcal{L} = \{0, 1, +, \cdot, -, <\}$, and $\mathcal{L}^* = \mathcal{L} \cup \{c\}$, where $c$ is a new constant symbol. Let

$$T = \mathrm{Th}_{\mathcal{L}}(\mathbb{N}) \cup \{c > \underline{n} \mid n \in \mathbb{N}\},$$

then $T$ is finitely satisfiable.

**Proof.** Given $T_0 \subseteq T$ finite, $T_0 \subseteq \mathrm{Th}_{\mathcal{L}}(\mathbb{N}) \cup \{c > \underline{n}, \ldots, c > \underline{n_\ell}\}$, and may assume they are equal and show that $T_0$ is satisfiable. Let $\mathcal{N}$ be the $\mathcal{L} \cup \{c\}$-structure which is the expansion of the $\mathcal{L}$-structure $\mathbb{N}$, with

$$c^{\mathcal{N}} = 1 + \max(n_1, \ldots, n_\ell),$$

then $\mathcal{N} \models T_0$, and $T_0$ is satisfiable. By compactness, $T$ is satisfiable, say $\mathcal{A} \models T$. Then $\mathcal{A} \equiv \mathbb{N}$ and $\mathcal{A}$ contains an element $c^{\mathcal{A}}$ bigger than $1$, $1+1$, $1+1+1$, ..., but $\mathcal{A} \not\cong \mathbb{N}$, so $\mathcal{A}$ is a non-standard model of arithmetic. ⊛

We now start a long journey toward proving completeness theorem, specifically (b).

# Lecture 8: Henkin Constants

## 1.3.4 Henkin Construction

31 Jan. 14:30

To prove Theorem 1.3.6 (b), we need an additional definition and a technical lemma due to Henkin.

**Definition 1.3.17** (Henkin constant)**.** An $\mathcal{L}^*$-theory $T^*$ has *Henkin constants* if for each formula $\varphi(x)$ with one free variable, there is a constant symbol $c \in \mathcal{L}^*$ such that

$$\big(\exists x\ \varphi(x)\big) \to \varphi(c) \text{ is in } T^*.$$

We see that the above is equivalent to

$$\big(\neg\forall x\ \varphi(x)\big) \to \neg\varphi(c) \text{ is in } T^*,$$

and we will use this version ($\forall$) and view $\exists$ being a shorthand for $\neg\forall\neg$; also, we will use $\to$ and $\neg$ as primitive, and $\wedge, \vee$ are shorthand.

**Lemma 1.3.2.** If $\Gamma \vdash \varphi(c)$, and $c$ does not occur in $\Gamma$ or in $\varphi(x)$, then there is a variable $y$ not appearing in $\varphi(x)$, such that $\Gamma \vdash \forall y\ \varphi(y)$. Moreover, there is a proof of $\forall y\ \varphi(y)$ in which $c$ does not appear.

**Proof.** Let $\alpha_1(c), \ldots, \alpha_n(c) = \varphi(c)$ be a proof of $\varphi(c)$ from $\Gamma$, and let $y$ be a variable not appearing in this proof. We claim that $\alpha_1(y), \ldots, \alpha_n(y) = \varphi(y)$ is still a valid proof of $\varphi(y)$. There are three cases to consider (for each $i = 1, \ldots, n$):

(a) If $\alpha_i(c)$ is in $\Gamma$, then $c$ does not actually occur in $\alpha_i(c)$ because it does not appear in $\Gamma$. So $\alpha_i(y)$ is the same as $\alpha_i(c)$, hence in $\Gamma$.

(b) If $\alpha_i(c)$ is a logical axiom, then $\alpha_i(y)$ is a logical axiom as well. For most of these it is easy to check, but for (A6), i.e., $\varphi \to \forall x\ \varphi$ if $x$ is not free in $\varphi$, there is a little more. But $y$ did not appear in $\alpha_i(c)$, so $y \neq x$, and substituting $y$ for $c$ will not stop $x$ from being not free.

(c) If $\alpha_i(c)$ follows by (MP) from $\alpha_j(c)$ and $\alpha_k(c) = \alpha_j(c) \to \alpha_i(c)$ for $j, k < i$, then $\alpha_i(y)$ follows by (MP) from $\alpha_j(y)$ and $\alpha_k(y) = \alpha_j(y) \to \alpha_i(y)$.

So $\Gamma \vdash \varphi(y)$ and the proof does not involve $c$. Let $\Phi \subseteq \Gamma$ be the subset of $\Gamma$ that was used in the proof, so $y$ does not appear in $\Phi$, hence $\Phi \vdash \varphi(y)$ and $\Phi \vdash \forall y\ \varphi(y)$, so $\Gamma \vdash \forall y\ \varphi(y)$. ■

So Lemma 1.3.2 implies that we have $\Gamma \vdash \varphi(y)$ and the proof does not involve $c$. And sometimes, we want to be able to choose the variable $y$ from above.

**Corollary 1.3.2.** If $\Gamma \vdash \varphi(c)$, and $c$ does not occur in $\Gamma$ or in $\varphi(x)$, then $\Gamma \vdash \forall x\ \varphi(x)$. Moreover, there is a proof of $\forall x\ \varphi(x)$ not involving $c$.[a]

[a] Here, $x$ is any variable that does not appear in $\varphi(c)$.

**Proof.** We know that for some $y$, $\Gamma \vdash \forall y\ \varphi(y)$, (A4) says $\forall y\ \varphi(y) \to \varphi(x)$. So $\forall y\ \varphi(y) \vdash \varphi(x)$ since $x$ does not appear in $\forall y\ \varphi(y)$, $\forall y\ \varphi(y) \vdash \forall x\ \varphi(x)$. ■

**Note.** $x$ might appear in $\Gamma$.

**Theorem 1.3.8.** Let $T$ be a consistent $\mathcal{L}$-theory. There is a language $\mathcal{L}^* \supseteq \mathcal{L}$ and $T^* \supseteq T$ a consistent $\mathcal{L}^*$-theory such that $T^*$ has Henkin constants. We can choose $\mathcal{L}^*$ such that $|\mathcal{L}^*| = |\mathcal{L}| + \aleph_0$, and all new symbols in $\mathcal{L}^*$ are constants.

**Proof.** Let $\mathcal{L}_0 = \mathcal{L}$ and $T_0 = T$. Let $\mathcal{L}_1$ be the expansion of $\mathcal{L}_0$ by adding a new constant symbol $c_\varphi$ for each $\mathcal{L}_0$-formula $\varphi$ w.r.t. the Henkin construction. First, we show that after this procedure, $T_0$ is still a consistent $\mathcal{L}_1$-theory.

**Remark.** Technically, $\vdash$ is really $\vdash_{\mathcal{L}}$, so this is a key step for seeing that it does not matter.

**Claim.** $T_0$ is still a consistent $\mathcal{L}_1$-theory after the expansion of $\mathcal{L}_0$.

**Proof.** If not, there is a proof of a contradiction from $T_0$, and which uses only finitely many of the new constants symbols. By Corollary 1.3.2, we can replace these constants one-by-one by variables, e.g., if the original contradiction was $\varphi(c_1, \ldots, c_n)$ and $\neg\varphi(c_1, \ldots, c_n)$, then $T_0$ proves $\forall x_1, \ldots, \forall x_n\ \varphi(x_1, \ldots, x_n)$ and $\forall x_1, \ldots, \forall x_n\ \neg\varphi(x_1, \ldots, x_n)$. Moreover, these proofs take place in $\mathcal{L}_0$, so by (A4), $T_0 \vdash_{\mathcal{L}_0} \varphi(x_1, \ldots, x_n)$, and $T_0 \vdash_{\mathcal{L}_0} \neg\varphi(x_1, \ldots, x_n)$ $\lightning$ ⊛

To construct $T_1$ w.r.t. the Henkin construction, it's natural to consider the following: if $\varphi$ is of the form $\neg\forall x\ \psi(x)$, then let

$$\theta_\varphi := (\neg\forall x\ \psi(x)) \to \neg\psi(c_\varphi), \text{ i.e., } (\exists x\ \neg\psi(x)) \to \neg\psi(c_\varphi),$$

otherwise, let $\theta_\varphi := \forall x\ (x = x)$ (trivially true). Let $\Theta = \{\theta_\varphi \mid \varphi \text{ an } \mathcal{L}_0\text{-formula}\}$, and we let that $T_1 = T_0 \cup \Theta$. We claim that $T_1$ is still consistent.

**Claim.** $T_1 = T_0 \cup \Theta$ is a consistent $\mathcal{L}_1$-language after the expansion of $\mathcal{L}_0$.

**Proof.** If not, then there are $\varphi_1, \ldots, \varphi_{m+1}$ such that $T_0 \cup \{\theta_{\varphi_1}, \ldots, \theta_{\varphi_m}, \theta_{\varphi_{m+1}}\}$ is inconsistent. Taking $m$ to be as small as possible, $T_0 \cup \{\theta_{\varphi_i}\}_{i=1}^m$ is consistent, so $T_0 \cup \{\theta_{\varphi_i}\}_{i=1}^m \vdash \neg\theta_{\varphi_{m+1}}$ with $\varphi_{m+1}$ being of the form $\neg\forall x\ \psi(x)$, $\theta_{\varphi_{m+1}}$ is $\neg\forall x\ \psi(x) \to \neg\psi(c_\varphi)$. By (A1), (A2), (A3),

$$T_0 \cup \{\theta_{\varphi_1}, \ldots, \theta_{\varphi_m}\} \vdash \neg\forall x\ \psi(x) \text{ and } T_0 \cup \{\theta_{\varphi_1}, \ldots, \theta_{\varphi_m}\} \vdash \psi(c_{\varphi_{m+1}}).$$

Since $c_{\varphi_{m+1}}$ does not appear in $T_0 \cup \{\theta_{\varphi_i}\}_{i=1}^m$, so $T_0 \cup \{\theta_{\varphi_i}\}_{i=1}^m \vdash \forall x\ \psi(x)$, i.e., $T_0 \cup \{\theta_{\varphi_i}\}_{i=1}^m$ is inconsistent, contradicting to the fact that $m$ is the smallest choice $\lightning$ [a] ⊛

[a]If $m = 0$, then we violate the consistency of $T_0$.

It might be that $T_1$ does not have Henkin constants since there are new $\mathcal{L}_1$-formulas which are not $\mathcal{L}_0$-formulas. But we know that $T_1$ does have Henkin constants for $\mathcal{L}_0$-formulas, hence we can repeat that process and keep fixing things. In general, given $T_i$ and $\mathcal{L}_i$, define a $T_{i+1}$ and $\mathcal{L}_{i+1}$ in the above way. Since each $T_i$ is consistent, so $T^* = \bigcup T_i$ is an $\mathcal{L}^* = \bigcup \mathcal{L}_i$-theory. Note that $T^*$ is consistent as a nested union of consistent theories, and $T^*$ has Henkin constants because every $\mathcal{L}^*$-formula $\varphi$ is an $\mathcal{L}_i$-formula for some $i$, and $\theta_\varphi \in T_{i+1} \subseteq T^*$.

**Intuition.** This is like "chasing its own tail," which basically fixes new errors introduced every time and then takes the union in the end.

Finally, we want to show that $|\mathcal{L}^*| = |\mathcal{L}| + \aleph_0$. Given $\mathcal{L}_i$, we define $\mathcal{L}_{i+1}$ to be $\mathcal{L}_i$ plus new constants $c_\varphi$ for $\varphi$ on $\mathcal{L}_i$-formula. Then, we have

$$|\mathcal{L}_{i+1}| \leq |\mathcal{L}_i| + \underbrace{|\mathcal{L}_i| + \aleph_0}_{\#\text{ of } \mathcal{L}_i\text{-formulas}} = |\mathcal{L}_i| + \aleph_0.$$

So for all $i$, $|\mathcal{L}_i| \leq |\mathcal{L}| + \aleph_0$, and $\mathcal{L}^* = \bigcup_i \mathcal{L}_i$ is a countable union, so $|\mathcal{L}^*| \leq |\mathcal{L}| + \aleph_0$, and in fact, $|\mathcal{L}^*| = |\mathcal{L}| + \aleph_0$. ■

After proving Theorem 1.3.8, we see that to prove Theorem 1.3.6 (b), we can proceed by:

1. extend $T^*$ to a maximal theory $T^{**}$;[4]
2. turn $T^{**}$ into a model. The elements of the model are constant symbols from $\mathcal{L}^*$, modulo the equivalence relation $c \sim d$ if $c = d$ is in $T^{**}$, i.e., $T^{**} \vdash c = d$.

Thankfully, the first step is easy from Theorem 1.3.4, so we just need to show the second step, and we're done.

## Lecture 9: Proving the Completeness Theorem

To finish the proof of Theorem 1.3.6 (b), we follow the plan mentioned last lecture, and prove the following. 2 Feb. 14:30

**Theorem 1.3.9.** If $T$ is a maximal consistent $\mathcal{L}$-theory with Henkin constants, then $T$ has a model.

**Proof.** The model we build is called a "canonical model." Let $\mathcal{C}$ be the set of constants in $\mathcal{L}$, and define an equivalence relation $\sim$ on $\mathcal{C}$ by $c \sim d$ if and only if $c = d$ is in $T$.

**Claim.** The relation $\sim$ on $\mathcal{C}$ defined by $c \sim d \Leftrightarrow c = d \in T$ is an equivalence relation.

[4]Which still has Henkin constants.

**Proof.** We check the axioms for being an equivalence relation.

(a) $c \sim c$ because $c = c$ is in $T$ by (A7) (a).[a]

(b) If $c \sim d$, then $c = d$ is in $T$ so $d = c$ is in $T$ by (A7) (b), i.e., $d \sim c$.

(c) If $c \sim d$ and $d \sim e$, then $c = d$ and $d = e \in T \Rightarrow c = e \in T$ by (A7) (c), so $c \sim e$.

⊛

[a]Otherwise, $c \neq c$ is in $T$ from the maximality, so $T \vdash c \neq c$ with $T \vdash c = c$, so $T$ would be inconsistent.

Let $[c]$ be the equivalence class of $c$. Define an $\mathcal{L}$-structure $\mathcal{M}$ with domain $M = \mathcal{C} / \sim = \{[c] \mid c \in \mathcal{C}\}$, with functions, relations, and constants defined as follows:

(a) $c^{\mathcal{M}} = [c]$.

(b) $R^{\mathcal{M}}([c_1], \ldots, [c_n])$ true if $R(c_1, \ldots, c_n)$ is in $T$. This is well-defined by (A7) (e).

(c) $f^{\mathcal{M}}([c_1], \ldots, [c_n]) = [d]$ if $f(c_1, \ldots, c_n) = d$ is in $T$. Such a $d$ exists because $\exists x\, f(c_1, \ldots, c_n) = x$, i.e., $\neg \forall x\, f(c_1, \ldots, c_n) \neq x$, is in $T$.[b] If this is in $T$, then there is a Henkin constant $d$ with $f(c_1, \ldots, c_n) = d$ in $T$. To show that this is well-defined, from (A7) (d), i.e.,

$$(t_1 = u_1 \wedge \ldots \wedge t_n = u_n) \to f(t_1, \ldots, t_n) = f(u_1, \ldots, u_n).$$

So if $[c_1] = [d_1], \ldots, [c_n] = [d_n]$, then $c_1 = d_1, \ldots, c_n = d_n$ are in $T$. So $f(c_1, \ldots, c_n) = f(d_1, \ldots, d_n)$ is in $T$ by (A7) (d). If $a$ and $b$ are constants such that $f(c_1, \ldots, c_n) = a$ and $f(d_1, \ldots, d_n) = b$ are in $T$, so $a = b$ is in $T$ by (A7) (c), i.e., the transitivity of $=$.

Now we need to show that $\mathcal{M} \models T$, i.e., we claim that

$$\mathcal{M} \models \varphi([c_1], \ldots, [c_n]) \Leftrightarrow \varphi(c_1, \ldots, c_n) \text{ is in } T.$$

We prove this by induction on terms and then formulas.

1. Terms: Show that $t^{\mathcal{M}}([c_1], \ldots, [c_n]) = [d]$ if and only if $t(c_1, \ldots, c_n) = d$ is in $T$.

   (a) If $t$ is a constant $e$, $t^{\mathcal{M}}([c_1], \ldots, c_n) = e^{\mathcal{M}} = [e]$, and

   $$[e] = t^{\mathcal{M}}([c_1], \ldots, [c_n]) = [d] \Leftrightarrow [e] = [d] \Leftrightarrow e = d \text{ is in } T.$$

   (b) If $t$ is $x_i$, $t^{\mathcal{M}}([c_1], \ldots [c_n]) = [c_i]$. This is equal to $[d]$ if and only if $c_i = d$ is in $T$.

   (c) Suppose that $t(x_1, \ldots, x_n) = f(s_i(x_1, \ldots, x_n), \ldots, s_m(x_1, \ldots, x_n))$. Let

   $$[d_i] = s_i^{\mathcal{M}}([c_1], \ldots, [c_n]),$$

   by the inductive hypothesis, $d_i = s_i(c_1, \ldots, c_n)$ is in $T$. Let $[e] = f^{\mathcal{M}}([d_1], \ldots, [d_m]) = t^{\mathcal{M}}([c_1], \ldots, [c_n])$. By the definition of $f$, $e = f(d_1, \ldots, d_m)$ is in $T$. By (A7) (d),

   $$e = f(s_1(c_1, \ldots, c_n), \ldots, s_m(c_1, \ldots, c_n))$$

   is in $T$. This is the direction ($\Rightarrow$).
   Now suppose that $t(c_1, \ldots, c_n) = e'$ is in $T$. We want to show that $[e] = [e']$, i.e., $e = e'$ is in $T$. Since $e = t(c_1, \ldots, c_n)$ is in $T$, and $e' = t(c_1, \ldots, c_n)$ is in $T$. By (A7) (c), $e = e'$ is in $T$, so $[e'] = [e] \ = t^{\mathcal{M}}([c_1], \ldots, [c_n])$. This is ($\Leftarrow$).

2. Formulas: Show that $\mathcal{M} \models \varphi([c_1], \ldots, [c_n])$ if and only if $\varphi(c_1, \ldots, c_n)$ is in $T$.[c]

   (a) If $\varphi$ is $s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$:

($\Rightarrow$) If $\mathcal{M} \models s([c_1], \ldots, [c_n]) = t([c_1], \ldots, [c_n])$,

$$s^{\mathcal{M}}([c_1], \ldots, [c_n]) = t^{\mathcal{M}}([c_1], \ldots, [c_n]).$$

Let $[d]$ be this element equal to the above, so $d = s(c_1, \ldots, c_n)$ and $d = t(c_1, \ldots, c_n)$ are in $T$ so $\underbrace{s(c_1, \ldots, c_n) = t(c_1, \ldots, c_n)}_{\varphi(c_1, \ldots, c_n)}$ is in $T$ by (A7) (c).

($\Leftarrow$) If $s(c_1, \ldots, c_n) = t(c_1, \ldots, c_n)$ is in $T$, let

$$[d] = s^{\mathcal{M}}([c_1], \ldots, [c_n]) \text{ and } [e] = t^{\mathcal{M}}([c_1], \ldots, [c_n]),$$

so $d = s(c_1, \ldots, c_n)$ and $e = t(c_1, \ldots, c_n)$ are in $t$, so $d = e$ is in $t$, and $[e] = [d]$.

(b) If $\varphi$ is $R(t_1(\overline{x}), \ldots, t_m(\overline{x}))$: Let $[d_i] = t_i^{\mathcal{M}}([c_1], \ldots, [c_n])$,

$$\begin{array}{ccc}
R^{\mathcal{M}}([d_1], \ldots, [d_m]) \text{ is true} & \Longleftrightarrow & R(d_1, \ldots, d_m) \text{ is in } T \\
\Updownarrow & & \Updownarrow \\
R^{\mathcal{M}}(t_1^{\mathcal{M}}[\overline{c}], \ldots, t_m^{\mathcal{M}}[\overline{c}]) \text{ is true} & & R(t_1(\overline{c}), \ldots, t_m(\overline{c})) \text{ is in } T \\
\Updownarrow & & \\
\mathcal{M} \models \varphi([c_1], \ldots, [c_n]) & &
\end{array}$$

(c) If $\varphi$ is $\neg\psi$: Then

$$\mathcal{M} \models \varphi(\overline{c}) \Leftrightarrow \mathcal{M} \not\models \psi([\overline{c}]) \Leftrightarrow \psi(\overline{c}) \text{ is not in } T \Leftrightarrow \varphi(\overline{c}) \text{ is in } T$$

where the last $\Leftrightarrow$ follows from the fact that $T$ is maximal and consistent.

(d) If $\varphi$ is $\psi \to \theta$:

- If $\psi(\overline{c}) \to \theta(\overline{c})$ is in $T$: then if $\psi(\overline{c})$ is in $T$, then $\theta(\overline{c})$ is in $T$ by (MP).then by the induction hypotheses, if $\mathcal{M} \models \psi([\overline{c}])$, then $\mathcal{M} \models \theta([\overline{c}])$.
- If $\mathcal{M} \models \psi([\overline{c}]) \to \theta([\overline{c}])$: then either $\mathcal{M} \models \theta([\overline{c}])$ or $\mathcal{M} \models \neg\psi([\overline{c}])$. So either
  i. $\theta(\overline{c})$ is in $T$: by (A1), $\theta(\overline{c}) \to (\psi(\overline{c}) \to \theta(\overline{c}))$, so $\psi(\overline{c}) \to \theta(\overline{c})$ is in $T$.
  ii. $\neg\psi(\overline{c})$ is in $T$: $T \cup \{\psi(\overline{c})\}$ is now inconsistent, so $T \cup \{\psi(\overline{c})\} \vdash \theta(\overline{c})$. From the deductive theorem, $T \vdash \psi(\overline{c}) \to \theta(\overline{c})$. Because $T$ is maximal and consistent, $\psi(\overline{c}) \to \theta(\overline{c})$ is in $T$.

[b]Otherwise, $\forall x\ f(c_1, \ldots, c_n) \neq x$ is in $T$. By (A4), $f(c_1, \ldots, c_n) \neq f(c_1, \ldots, c_n)$ is in $T$, contradicts to (A7) (a).
[c]In particular, for a sentence $\varphi$, $\mathcal{M} \models \varphi \Leftrightarrow \varphi$ is in $T$, and so $\mathcal{M} \models T$.

# Lecture 10: Introduction to Model Theory

Let's start by finishing the proof of Theorem 1.3.9. 7 Feb. 14:30

**Proof of Theorem 1.3.9 (Continued).** There's one final case left:

(e) If $\varphi$ is $\forall x\ \psi(x, \overline{y})$: Because $T$ has Henkin constants, there is $d$ such that $\neg\forall x\ \psi(x, \overline{c}) \to \neg\psi(d, \overline{c})$ is in $T$.

- If $\varphi(c_1, \ldots, c_n)$ is not in $T$, i.e., $\forall x\ \psi(x, \overline{c})$ is in $T$, then since $T$ is maximal, $\neg\forall x\ \psi(x, \overline{c})$ is in $T$. So by (MP), $\neg\psi(d, \overline{c})$ is in $T$. So, $\mathcal{M} \models \neg\psi([d], [\overline{c}])$ by induction hypotheses, hence $\mathcal{M} \models \neg\forall x\ \psi(x, [\overline{c}])$, i.e., $\mathcal{M} \not\models \varphi([\overline{c}])$.
- If $\mathcal{M} \not\models \varphi([\overline{c}])$, then $\mathcal{M}\neg \models \forall x\ \varphi(x, [\overline{c}])$, so there is $[e]$ such that $\mathcal{M} \models \neg\psi([e], [\overline{c}])$. Hence, $\neg\psi(e, \overline{c})$ is in $T$. Suppose for a contradiction that $\varphi(\overline{c})$, i.e., $\forall x\ \psi(x, \overline{c})$ is in $T$, by (A4), $\forall x\ \psi(x, \overline{c}) \to \psi(e, \overline{c})$, so $\psi(e, \overline{c})$ is in $T$ by maximality and by consistency. But then $T$ is inconsistent, a contradiction $\lightning$ Hence $\varphi(\overline{c})$ is not in $T$.

Thus, $\mathcal{M} \models T$, so $T$ is satisfiable, proving the theorem. ∎

**Remark.** We see that when proving the above, when we talk about $\mathcal{M}$, the witness comes for free, while for $T$, we need Henkin constants for getting a witness.

Now, we can complete the proof of completeness theorem by putting everything together.

**Claim.** The completeness theorem (b) holds.

**Proof.** We see that

1. Theorem 1.3.8: There is a consistent $T^* \supseteq T$ and $\mathcal{L}^*$-theory (with $\mathcal{L}^* \supseteq \mathcal{L}$) and $T^*$ has Henkin constants.
2. Theorem 1.3.4: There is a maximal consistent $\mathcal{L}^*$-theory $T^{**} \supseteq T^*$, where $T^{**}$ still has Henkin constants.
3. Theorem 1.3.9: $T^{**}$ has a model $\mathcal{M}^*$ an $\mathcal{L}^*$-structure. Let $\mathcal{M}$ be the reduct of $\mathcal{M}^*$ to an $\mathcal{L}$-structure.

Hence, $\mathcal{M} \models T$. ⊛

**As previously seen** (Problem set 1). Let $\mathcal{L}^* \supseteq \mathcal{L}$. If $\mathcal{M}^*$ is an $\mathcal{L}^*$-structure, then by ignoring the interpretation of the symbols in $\mathcal{L}^* - \mathcal{L}$, we get an $\mathcal{L}$-structure $\mathcal{M}$.

**Notation** (Reduct). $\mathcal{M}$ is a *reduct* of $\mathcal{M}^*$.

**Notation** (Expansion). $\mathcal{M}^*$ is an *expansion* of $\mathcal{M}$.

**Remark.** We see that $\vdash$ and $\models$ are the same.

### 1.3.5 Consequences of Completeness Theorem

Now, let's step back and look at the proof of the completeness theorem, and ask the following.

**Problem.** When we did the Henkin construction of $\mathcal{M}^* \models T^{**}$, how big was $M$?

This can be answered by the following.

**Theorem 1.3.10.** If $T$ is a satisfiable $\mathcal{L}$-theory, then it has a model of size at most $|\mathcal{L}| + \aleph_0$.

**Proof.** Since $|M| \leq |\mathcal{L}^*|$ since $\mathcal{M} = \mathcal{C} / \sim$, and in step one, $|\mathcal{L}^*| \leq |\mathcal{L}| + \aleph_0$, so $|M| \leq |\mathcal{L}| + \aleph_0$. ■

**Example.** Let $\mathcal{L} = \{f\}$, $T$ says that $f$ is injective but not surjective.

**Example.** Let $\mathcal{L} = \{\leq\}$, $T$ says that $\leq$ is a linear order with no greatest element.

**Example.** Let $\mathcal{L} = \varnothing$, $T$ says that there are at least $n$ elements for each $n$.

**As previously seen.** $\vdash$ and $\models$ are actually $\vdash_{\mathcal{L}}$[a] and $\models_{\mathcal{L}}$[b]

[a] Proofs can only use $\mathcal{L}$-formulas.
[b] Only looking at $\mathcal{L}$.

**Remark.** Suppose $\mathcal{L} \supseteq \mathcal{L}_0$, and $\Gamma$ a set of $\mathcal{L}_0$-sentences, $\varphi$ on $\mathcal{L}_0$-sentence.

(a) $\Gamma \models_{\mathcal{L}_0} \varphi \Leftrightarrow \Gamma \models_{\mathcal{L}_1} \varphi$.

(b) $\Gamma \vdash_{\mathcal{L}_0} \varphi \Leftrightarrow \Gamma \vdash_{\mathcal{L}_1} \varphi$.

**Proof.** (a) and (b) are equivalent by the completeness theorem, and we prove (a).

Suppose $\Gamma \models_{\mathcal{L}_0} \varphi$. Suppose $\mathcal{M}_1$ is an $\mathcal{L}_1$-structure such that $\mathcal{M}_1 \models \Gamma$. Let $\mathcal{M}_0$ be the reduct of $\mathcal{M}_1$ to $\mathcal{L}_0$ and $\mathcal{M}_0 \models \Gamma$, so $\mathcal{M}_0 \models \varphi$, then $\mathcal{M}_1 \models \varphi$, thus $\Gamma \models_{\mathcal{L}_1} \varphi$.

Now, suppose $\Gamma \models_{\mathcal{L}_1} \varphi$. Suppose $\mathcal{M}_0$ is an $\mathcal{L}_0$-structure with $\mathcal{M}_0 \models \Gamma$. Expand $\mathcal{M}_0$ to an $\mathcal{L}_1$-structure $\mathcal{M}_1$ in any way. $\mathcal{M}_1 \models \Gamma$, so $\mathcal{M}_1 \models \varphi$. Thus, $\mathcal{M}_0 \models \varphi$, so $\Gamma \models_{\mathcal{L}_0} \varphi$. ⊛

What is important about the proof system?

**Definition 1.3.18** (Computably enumerable)**.** A set is *computably enumerable (ce)* or *computable listable* if there is a program that lists out its elements.

(1) Soundness and completeness, $\vdash \Leftrightarrow \models$.

(2) Proofs are finite, and use only finitely many hypotheses $\Rightarrow$ compactness.

(3) Computational properties. If $\mathcal{L}$ is finite, or computable (complete list of symbols and their arities).

   (a) We can compute with formulas.

   (b) Given a formula, it's computable to check whether it's a logical axiom.

   (c) It's computable to check whether a proof is valid.

   (d) If $\Gamma$ is a ce set of sentences, $\{\varphi \colon \Gamma \vdash \varphi\}$ is also ce.[5]

   (e) There is no program that given $\varphi$ can decide whether $\vdash \varphi$ at least for $\mathcal{L} = \{E\}$, $E$ binary.

[5] We can list out all the valid proofs from $\Gamma$ of any $\varphi$.

# Chapter 2

# The Beginning of Model Theory

## 2.1 Complete Theories

**Proposition 2.1.1.** Let $T$ be an $\mathcal{L}$-theory with an infinite model, and let $\kappa$ be an infinite cardinal with $\kappa \geq |\mathcal{L}|$. Then $T$ has a model of cardinality $\kappa$.

**Proof.** Let $\mathcal{C}$ be a set of $\kappa$-many new constants, and let $\mathcal{L}^* = \mathcal{L} \cup \mathcal{C}$. Let

$$T^* = T \cup \{c \neq d \mid c, d \in \mathcal{C} \text{ distinct}\}.$$

If $\mathcal{M} = T^*$, then $|M| \geq \kappa$. Also, if $T^*$ is satisfiable, it has a model of size at most $|\mathcal{L}^*| = \kappa$ since

$$\kappa = |\mathcal{C}| \leq |\mathcal{L}^*| \leq |\mathcal{C}| + |\mathcal{L}| \leq \kappa + \kappa = \kappa,$$

so if $T^*$ is satisfiable, it has a model $\mathcal{M}$ with $|M| = \kappa$.

**Claim.** $T^*$ is satisfiable.

**Proof.** By the compactness theorem, to show that $T^*$ is satisfiable, it's equivalent to show that every finite $\Gamma \subseteq T^*$ is satisfiable. Let $\mathcal{M}$ be infinite, and $\Gamma \subseteq T^*$ finite, then

$$\Gamma \subseteq T \cup \{c_i \neq c_j \mid i, j = 1, \ldots, n, i \neq j\}$$

for $c_1, \ldots, c_n \in \mathcal{C}$ since only finitely many $c_i$ are involved, and without loss of generality, $\Gamma = T \cup \{c_i \neq c_j \mid i, j = 1, \ldots, n, i \neq j\}$. Pick $a_1, \ldots, a_n \in M$, distinct, we then turn $\mathcal{M}$ into an $\mathcal{L}^*$-structure $\mathcal{M}^*$ with $c_i^{\mathcal{M}^*} = a_i$.[a] So $\mathcal{M}^* \models \Gamma$, thus $T^*$ is satisfiable. ⊛

[a] And each other $d \in \mathcal{C}$ with $d^{\mathcal{M}^*} = a_1$.

■

## Lecture 11: Algebraically Closed Fields

### 2.1.1 A Detour to Algebraically Closed Fields

9 Feb. 14:30

Algebraically closed fields are a great example of a *tame* theory (as opposed to e.g., $\mathbb{N}$, which are not *tame*). We detour to discuss some important and related definitions for the future discussion.

#### Rings

All rings $R$ we refer to will be commutative.

**Definition 2.1.1 (Ideal).** Let $R$ be a ring. An *ideal* $I$ of $R$ is a set $I \subseteq R$ such that

(a) $0 \in I$;

(b) if $a, b \in I$, then $a + b \in I$;

(c) if $a \in I$ and $r \in R$, $ra \in I$.

**Definition 2.1.2** (Proper)**.** An ideal is *proper* if $1 \notin I$, equivalently, $I \subsetneq R$.

**Definition.** Let $I$ be a proper ideal.

**Definition 2.1.3** (Radical)**.** $I$ is *radical* if $a^n \in I$, then $a \in I$.

**Definition 2.1.4** (Prime)**.** $I$ is *prime* if $ab \in I$, then $a \in I$ or $b \in I$.

**Definition 2.1.5** (Maximal)**.** $I$ is *maximal* if there is no proper ideal $J \supsetneq I$.

**Remark.** Maximal $\Rightarrow$ Prime $\Rightarrow$ Radical.

**Definition 2.1.6** (Polynomial ring)**.** Let $R$ be a ring. Then $R[x_1, \ldots, x_n]$ is the *polynomial ring* with coefficients in $R$ on indeterminates $x_1, \ldots, x_n$.

**Example.** Let $K$ be a field, $S \subseteq K^n$, and $I \subseteq K[x_1, \ldots, x_n]$ defined as

$$I = \{ f(\overline{x}) \mid f(\overline{s}) = 0 \text{ for all } \overline{s} \in S \} .$$

Then $I$ is a radical ideal.

**Theorem 2.1.1.** $K[x]$ is a principal ideal domain (PID): every ideal is generated by one element, $I = (f(x)) = \{ g(x)f(x) \mid g(x) \in K[x] \}$.

**Proof.** We can let $g$ be the polynomial of least degree in $I$. Then for any other $h \in I$, by long division, $h = gs + r$, with $\deg(r) < \deg(g)$. But then $r = h - gs \in I$, so if $r$ has lower degree than $g$, $r = 0$, hence $h = gs \in (g)$. ∎

**Definition 2.1.7** (Noetherian)**.** A ring $R$ is *Noetherian* if every ideal $I$ of $R$ is finitely generated.

**Remark.** Equivalently, there is no infinite proper ascending chain of ideals.

**Theorem 2.1.2** (Hilbert basis theorem)**.** If $R$ is a Noetherian ring, then $R[x]$ is also Noetherian. In particular, $K[x_1, \ldots, x_n]$ is Noetherian and so every ideal in $K[x_1, \ldots, x_n]$ is finitely generated.

**Theorem 2.1.3.** If $\alpha\colon R \to S$ is a ring homomorphism, then $\ker \alpha$ is an ideal of $R$, and the induced map $\overline{\alpha}\colon R / \ker \alpha \to S$ is injective.

**Theorem 2.1.4.** Let $R$ be a ring, and $I$ an ideal of $R$.[a]

(a) $R / I$ is an integral domain[b] if and only if $I$ is a prime.

(b) $R / I$ is a field if and only if $I$ is maximal.

[a] Then $\pi \colon R \to R / I$ is a ring homomorphism with kernel $I$.
[b] If $ab = 0$, then $a = 0$ or $b = 0$.

### Field Extensions

**Definition 2.1.8** (Field extension)**.** If $K \subseteq L$ is a subfield of $L$, we call $L / K$ a *field extension*.

Given a field extension $L / K$, then we have that $L$ is a $K$-vector space, which suggests the following natural notion.

**Definition 2.1.9** (Degree)**.** The *degree* of $L / K$ is the dimension of the $K$-vector space $L$.

**Notation** (Finite extension)**.** If $[L \colon K]$ is finite, then we say $L / K$ is a *finite extension*.

**Theorem 2.1.5.** If $M / L$ and $L / K$ are field extensions, then

$$[M \colon K] = [M \colon L][L \colon K].$$

### Algebraically Closed Fields

**Definition.** Let $L / K$ be a field extension, and $a \in L$.

**Definition 2.1.10** (Algebraic)**.** If there is a non-zero $f(x) \in K[x]$ such that $f(a) = 0$, then $a$ is *algebraic* over $K$.

**Definition 2.1.11** (Transcendental)**.** If $a$ is not algebraic, then it is *transcendental* over $K$.

**Definition 2.1.12** (Minimal polynomial)**.** If $a$ is algebraic over $K$, there is a non-zero, monic[a] $f(x) \in K[x]$ of least degree such that $f(a) = 0$ which we call the *minimal polynomial* of $a$ over $K$.

[a] This is a common practice.

**Remark.** A minimal polynomial is irreducible.

**Remark.** If $f(x)$ is a minimal polynomial, then

$$(f(x)) = \{g(x) \in K[x] \mid g(a) = 0\}.$$

**Example.** Consider a field extension $\mathbb{R} / \mathbb{Q}$ with $a = \sqrt{2} \in \mathbb{R}$. Then the minimal polynomial is $f(x) = x^2 - 2$.

**Theorem 2.1.6.** Let $L / K$ be a field extension and $a \in L$, then $a$ is algebraic over $K$ if and only if $n = [K(a) \colon K] < \infty$. Furthermore, if $a$ is algebraic over $K$, then $n$ is the degree of the minimal polynomial of $a$, and $1, a, \ldots, a^{n-1}$ is a basis for $K(a)$ as a $K$-vector space.

**Intuition.** Think about $f(a) = a^n + r_{n-1}a^{n-1} + \ldots + r_1 a + r_0 1 = 0$.

The following example illustrates how can we combine Theorem 2.1.5 and Theorem 2.1.6,

**Example.** Let $f(x) = x^2 - 2$, $\mathbb{Q}(\sqrt{2}) = \{a1 + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[6]{2}) & \\
\mathbb{Q}(\sqrt{2}) \arrow[ur, "3"] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[ul, "2"'] \\
 & \mathbb{Q} \arrow[ul, "2"] \arrow[ur, "3"'] \arrow[uu, "6"] &
\end{tikzcd}$$

**Theorem 2.1.7.** Let $L \,/\, K$ be a field extension, $a \in L$, and $f(x) \in K[x]$ be the minimal polynomial of $a$ over $K$.

(a) $K[x] \,/\, (f(x)) \cong K(a)$.[a]

(b) If $b \in L$ has the same minimal polynomial as $a$, then $K(a) \cong K[x] \,/\, (f(x)) \cong K(b)$.

[a] Let $x \in K[x]$, then $\overline{x} = x + (f(x)) \in K[x] \,/\, (f(x))$, i.e., $\overline{x}$ is a root of $f$, hence the isomorphism is given by $\overline{x} \mapsto a$.

**Example.** Let $a = \sqrt{2}, b = -\sqrt{2}$, and $f(x) = x^2 - 2$ with $K = \mathbb{Q}$. Then

$$\begin{array}{rclcl}
\mathbb{Q}(\sqrt{2}) \cong & \mathbb{Q}[x] \big/ (x^2 - 2) & \cong & \mathbb{Q}(-\sqrt{2}); \\
a + b\sqrt{2} \mapsto & [a + bx] & \mapsto & a - b\sqrt{2}.
\end{array}$$

**Definition 2.1.13** (Algebraic extension)**.** Let $L \,/\, K$ be a field extension. Then $L$ is an *algebraic extension* of $K$ if all $a \in L$ are algebraic over $K$.

If $a$ is algebraic over $K$, then $K(a) \,/\, K$ is algebraic: If $b \in K(a)$, then $K(b) \subseteq K(a)$, so $[K(b) \colon K] \leq [K(a) \colon K] < \infty$, so $b$ is algebraic over $K$.

**Theorem 2.1.8.** If $M \,/\, L$ and $L \,/\, K$ are algebraic extensions, then $M \,/\, K$ is an algebraic extension.

**Proof.** Let $a \in M$, and let $b_1, \ldots, b_n \in L$ be the coefficients of the minimal polynomial of $a$ over $L$. Then $b_1, \ldots, b_n$ are algebraic over $K$. Since

$$\begin{aligned}
[K(a) \colon K] &\leq [K(a, b_1, \ldots, b_n) \colon K] \\
&= [K(a, b_1, \ldots, b_n) \colon K(b_1, \ldots, b_n)] \cdot [K(b_1, \ldots, b_n) \colon K(b_2, \ldots, b_n)] \cdots [K(b_n) \colon K].
\end{aligned}$$

Since each of these is a finite extension, so $[K(a) \colon K] < \infty$. ■

**Definition 2.1.14** (Algebraically closed)**.** A field $L$ is *algebraically closed* if any non-constant $f(x) \in L[x]$ has a root in $L$.

**Definition 2.1.15** (Algebraically closure)**.** If $L \,/\, K$, then $L$ is an *algebraic closure* of $K$ if $L$ is algebraically closed and an algebraic extension of $K$.

**Example.** $\mathbb{C}$ is algebraically closed, while $\mathbb{R}$ is not.

Given $L \,/\, K$, $L$ is algebraically closed of $K$ if $L$ is algebraic over $K$.

**Example.** $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, and $[\mathbb{C} \colon \mathbb{R}] = 2$.

**Example.** $\mathbb{Q}^{\text{alg}} = \{a \in \mathbb{C} \mid a \text{ is algebraic over } \mathbb{Q}\}$ is the algebraic closure of $\mathbb{Q}$.

If $L$ is algebraic closed, any $f(x) \in L[x]$ factors completely as $f(x) = (x - a_1) \cdots (x - a_n)$ and $a_1, \ldots, a_n$ are the only roots of $f$.

**Theorem 2.1.9.** Every field $K$ has an algebraic closure. If $L / K$ and $M / K$ are algebraic closures over $K$, then $L \cong_K M$.[a]

[a] There exists $\alpha \colon L \to M$ such that $\alpha(a) = a$ for $a \in K$.

**Proof.** First, we show the existence. Assume $K$ . Let $f_1, f_2, \ldots$ be the polynomials over $K$. Start with $K = K_0$, let $g_1(x)$ be an irreducible factor of $f_1(x)$. Let

$$K_1 = {}^{K_0[x]}\Big/_{(g_1(x))}.$$

Since $g_1$ is irreducible, $(g_1(x))$ is maximal, so $K_1$ is a field with a root of $f_1$. Now, we build

$$K_1 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K^* = \bigcup_i K_i.$$

Since any $f(x) \in K$ has a root in $K^*$, so $K^* / K$ is algebraic. Now, take

$$K \subseteq K^* \subseteq K^{**} \subseteq K^{***} \subseteq \ldots \subseteq L = \bigcup K^{*\cdots},$$

then $L$ is the algebraic closure of $K$.

Now we prove the uniqueness.

**Lemma 2.1.1.** An algebraic closed field has no algebraic extension.

**Proof.** If $a$ is algebraic over an algebraic closed $L$, the minimal polynomial of $a$, $f(x)$, factors completely and is irreducible, so $f(x) = x - r$, $r \in L$. Then $f(a) = 0$ implies $a = r \in L$. ∎

**Lemma 2.1.2.** Let $L / K$ algebraic, $M / K$ algebraic closed. Then there is an embedding $\alpha \colon L \to M$ fixing $K$.

**Proof idea.** Consider the case that $L = K(a)$, then let $f(x)$ be the minimal polynomial of $a / K$. Let $b$ be a root of $f$ in $M$. $K(a) \cong K[x] / (f) \cong K(b) \subseteq L$, this is our $\alpha$.

Then, the full proof is to keep doing this and perhaps by using Zorn's lemma or transfinite induction. ∎

Now, if $L / K$ and $M / K$ are algebraic closures over $K$, then by Lemma 2.1.2, there is $\alpha \colon L \to M$. $M / \alpha(L)$ is an algebraic extension, and $\alpha(L) \cong L$ is algebraic closed, by Lemma 2.1.1, $M = \alpha(L)$, so $\alpha$ is an isomorphism $M \to L$ over $K$. ∎

## Lecture 12: ACF and Categorical

14 Feb. 14:30

**Definition 2.1.16** (Characteristic). A field $F$ has finite *characteristic* $p > 0$ if $\underbrace{1 + \ldots + 1}_{p \text{ times}} = 0$.

**Remark.** $p$ is always prime, otherwise, $F$ has characteristic $p = 0$, i.e., $1 + \ldots + 1 \neq 0$, always.

**Definition 2.1.17** (Prime field). The *prime field* $\mathbb{F}_p$ in characteristic $p$ such that $\mathbb{F}_p = \mathbb{Q}$ if $p = 0$, $\mathbb{F}_p = \mathbb{Z} / p\mathbb{Z}$ if $p > 0$.

**Definition 2.1.18** (Transcendence basis). Let $L / K$ be a field extension. A set $S \subseteq L$ is called a *transcendence basis* of $L / K$ if:

(a) $S$ is algebraically independent: no $a_1, \ldots, a_n \in S$ have non-zero polynomial $f(x_1, \ldots, x_n) \in K[\overline{x}]$ with $f(a_1, \ldots, a_n) = 0$;

(b) $L$ is an algebraic extension of $K(S)$, i.e., $S$ is maximal.

**Remark.** Every field extension has[a] a transcendence basis, and any two transcendence basis have the same size.

[a]Same as vector spaces.

**Example.** Let $K(t_1, \ldots, t_n)$ be the fraction field of $K[x_1, \ldots, x_n]$. $\{t_1, \ldots, t_n\}$ is a transcendence basis for $K(t_1, \ldots, t_n)$ over $K$.

**Definition 2.1.19** (Transcendence degree). The *transcendence degree* of $L$ over $K$ is the cardinality of any transcendence basis.

If we do not specify $K$, then $K$ is the prime field $K = \mathbb{F}_p$.

**Theorem 2.1.10.** Any two algebraically closed fields of the same characteristic $p$ and transcendence degree are isomorphic.

**Proof.** Let $L, K$ be those fields, with transcendence basis $S, T$ over $\mathbb{F}_p$. $L$ is the algebraically closure of $\mathbb{F}_p(S)$ and $K$ is the algebraically closure of $\mathbb{F}_p(T)$. There is a bijection $f \colon S \to T$, and then $f$ extends to $\overline{f} \colon \mathbb{F}_p(S) \to \mathbb{F}_p(T)$ such that

$$\overline{f}\left(\frac{\sum_\alpha r_\alpha \overline{x}^\alpha}{\sum_\alpha s_\alpha \overline{x}^\alpha}\right) = \frac{\sum_\alpha r_\alpha f(\overline{x})^\alpha}{\sum_\alpha s_\alpha f(\overline{x})^\alpha},$$

where $r_\alpha, s_\alpha \in \mathbb{F}_p$ and $\overline{x}^\alpha$ is some monomial from $S$, e.g., $x_1^2 x_2$ for $x_1, x_2 \in S$.[a]

$\mathbb{F}_p(S)$ and $\mathbb{F}_p(T)$ are the same (up to isomorphism), but the algebraically closures are unique, so $K \cong L$ via an isomorphism extending $\overline{f}$. ∎

[a]$\alpha$ can be thought as a tuple, in the case of $x_1^2 x_2$, $\alpha = (2, 1)$.

### 2.1.2 ACF

**Definition 2.1.20** (ACF). ACF is the theory of algebraically closed fields consists of the following.

(a) Field axioms.

(b) For every $n \geq 1$, $\forall a_0 \ldots \forall a_n \left(a_n \neq 0 \to \exists b\ a_n b^n + a_{n-1} b^{n-1} + \ldots + a_0 = 0\right)$.

**Remark.** The models of ACF are exactly the algebraically closed field, and the language $\mathcal{L} = \mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot\}$.

For $p > 0$ prime, let

$$\mathrm{ACF}_p = \mathrm{ACF} \cup \{\underbrace{1 + \ldots + 1}_{p} = 0\},$$

and

$$\mathrm{ACF}_p = \mathrm{ACF} \cup \{\underbrace{1 + \ldots + 1}_{n} \neq 0 \mid n \in \mathbb{N}\}.$$

**Definition 2.1.21** (Categorical)**.** Let $\kappa$ be an infinite cardinal and $T$ be an $\mathcal{L}$-theory. $T$ is *$\kappa$-categorical* if any $\mathcal{M}, \mathcal{N} \models T$ of size $\kappa$ have $\mathcal{M} \cong \mathcal{N}$.

**Definition 2.1.22** (Countably categorical)**.** If $\kappa$ is countable, then $T$ is *countably categorical.*

**Definition 2.1.23** (Uncountably categorical)**.** If $\kappa$ is uncountable, then $T$ is *uncountably categorical.*

We see that for being uncountably categorical, we only need one uncountable $\kappa$.

**Example.** $(\mathbb{Q}, \leq)$ is countably categorical.

**Lemma 2.1.3.** If $K$ has transcendence degree $\lambda$, then $|K| = \lambda + \aleph_0$.

**Proof.** $K$ is algebraic over $\mathbb{F}_p(S)$, where $S$ is a transcendence basis of size $\lambda$. By counting, $|\mathbb{F}_p(S)| = \lambda + \aleph_0$, so $|\mathbb{F}_p(S)[x]| = \lambda + \aleph_0$. But since each element of $K$ satisfies some polynomials, and each polynomial has finitely many roots in $K$, so $|K| = \lambda + \aleph_0$. ■

**Theorem 2.1.11.** Fix $p$. $\mathrm{ACF}_p$ is $\kappa$-categorical for every uncountable $\kappa$.

**Proof.** Let $L, K$ be $\mathrm{ACF}_p$ for size $\kappa$, then $L, K$ have transcendence degree $\kappa$, and hence are isomorphic from Theorem 2.1.10. With the application of Lemma 2.1.3, we're done. ■

**Example.** $\mathbb{Q}^{\mathrm{alg}}$, the algebraically closure of $\mathbb{Q}$, has size $\aleph_0$, and has transcendence degree is 0.

**Example.** $\mathbb{Q}(t)^{\mathrm{alg}}$, the algebraically closure of $\mathbb{Q}(t) \cong \mathbb{Q}(\pi)$, has size $\aleph_0$, and has transcendence degree is 1.

**Proof.** We see that
$$\mathbb{Q}(t)^{\mathrm{alg}} = \{z \in \mathbb{C} \mid z \text{ is algebraic over } \mathbb{Q}(\pi)\ \} .$$
These are countable, but not isomorphic. $\mathrm{ACF}_0$ is not countably categorical. The same with $\mathrm{ACF}_0$ for $p > 0$. ⊛

**Note.** ACF is not uncountably categorical.

**Theorem 2.1.12** (Vaught's test)**.** Let $T$ be a satisfiable $\mathcal{L}$-theory with no finite models. If $T$ is $\kappa$-categorical for some infinite $\kappa \geq |\mathcal{L}|$, then $T$ is complete.

**Proof.** Suppose $T$ was not complete, so pick $\varphi$ with $T \not\models \varphi$ and $T \not\models \neg\varphi$, and hence $T \cup \{\varphi\}$ and $T \cup \{\neg\varphi\}$ are satisfiable. By a consequence of the proof of completeness theorem (with a compactness argument),

- $T \cup \{\varphi\}$ has a model $\mathcal{M}$ of size $\kappa$, and
- $T \cup \{\neg\varphi\}$ has a model $\mathcal{N}$ of size $\kappa$.

But $T$ is $\kappa$-categorical, so $\mathcal{M} \cong \mathcal{N}$, which is a contradiction ↯ ■

**Corollary 2.1.1.** $\mathrm{ACF}_p$ is complete for each $p$.

The axioms for $\mathrm{ACF}_p$ completely determines all of the first-order facts about algebraically closed fields of characteristic $p$.

**Remark** (Fact). The axioms for ACF or $\mathrm{ACF}_p$ can be listed computably. So $\{\varphi \mid \mathrm{ACF} \models \varphi\}$ and $\{\varphi \mid \mathrm{ACF}_p \models \varphi\}$ can be listed computably.

**Definition 2.1.24** (Decidable). A theory $T$ is *decidable* if there is a program that given $\varphi$, it determines whether $T \models \varphi$.

**Remark.** $\mathrm{ACF}_p$ is decidable.

**Proof.** Given $\varphi$, either $\mathrm{ACF}_p \models \varphi$ or $\mathrm{ACF}_p \models \neg\varphi$ since $\mathrm{ACF}_p$ is complete. By looking for a proof of $\varphi$ and a proof of $\neg\varphi$, eventually we will find one, telling us whether $\mathrm{ACF}_p \models \varphi$. ⊛

**Theorem 2.1.13.** ACF is decidable.

**Proof.** Given $\varphi$, simultaneously

(a) Look for a proof of $\mathrm{ACF} \vdash \varphi$, and

(b) Look for $p$ such that $\mathrm{ACF}_p \vdash \neg\varphi$ (so $\mathrm{ACF} \not\models \varphi$).[a]

The first case is fine. Suppose $\mathrm{ACF} \not\models \varphi$, so there is $\mathcal{M} \models \mathrm{ACF}$, $\mathcal{M} \models \neg\varphi$. There is $p$ such that $\mathcal{M} \models \mathrm{ACF}_p$. Since $\mathrm{ACF}_p$ is complete, $\mathrm{ACF}_p \models \neg\varphi$, so the search of the second case will half, so the whole search will eventually halt. ■

[a]We don't know $\mathrm{ACF} \models \neg\varphi$.

# Lecture 13: Upward Löwenheim-Skolem Theorem

16 Feb. 14:30

**Corollary 2.1.2** (Leftschetz principle). Let $\mathcal{L}$ be the language of rings. For an $\mathcal{L}$-sentence $\varphi$, the following are equivalent:

(i) $\mathbb{C} \models \varphi$

(ii) every algebraically closed field of characteristic $0 \models \varphi$

(iii) some algebraically closed fields of characteristic $0 \models \varphi$

(iv) for all sufficient large positive $p$, $\varphi$ is true in all algebraically closed fields of characteristic $p$

(v) for infinitely many positive $p$, $\varphi$ is true in all algebraically closed fields oof characteristic $p$

**Proof.** We only show the first three, others are left as homework. Let $K \models \mathrm{ACF}_0$, then since it's complete,

$$K \models \varphi \Leftrightarrow \mathrm{ACF}_0 \models \varphi.$$

■

**Theorem 2.1.14** (Ax-Grothendieck theorem). Let $f\colon \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map.[a] If $f$ is injective, then it's surjective. More generally, this is true for any $K \models \mathrm{ACF}_p$ for any $p$.

[a]I.e., $f(\overline{x}) = (f_1(\overline{x}), \ldots, f_n(\overline{x}))$ where $f_1, \ldots, f_n$ are polynomials.

**Proof.** The claim can be expressed by the sentences, so by Leftschetz principle, it's enough to prove that if for $K = \overline{\mathbb{F}_p}$, for each $p > 0$. Let $f\colon \overline{\mathbb{F}}_p^n \to \overline{\mathbb{F}}_p^n$ be an injective polynomial map and $\overline{y} \in \overline{\mathbb{F}}_p^n$. Then there is a finite subfield $L \subseteq \overline{\mathbb{F}}_p$ which contains $\overline{y}$ and the coefficients of $f$.then, $f$ restricts to an injective function $L^n \to L^n$, which is surjective because $L^n$ is finite, so $\exists \overline{x} \in L^n$ such that $f(\overline{x}) = \overline{y}$. ■

## 2.2 Up and Down

**Definition.** Let $\mathcal{M}$ be an $\mathcal{L}$-structure. Let $\mathcal{L}_M \supseteq \mathcal{L}$ be the expanded language with a new constant symbol $\underline{a}$ for each $a \in M$.

**Definition 2.2.1** (Atomic diagram)**.** The *atomic diagram* of $\mathcal{M}$ is the $\mathcal{L}_M$-theory

$$\mathrm{Diag}(\mathcal{M}) := \{\varphi(\underline{a}_1, \dots, \underline{a}_n) \mid \mathcal{M} \models \varphi \text{ and } \varphi \text{ is atomic or negated of atomic}\}.$$

**Definition 2.2.2** (Elementary diagram)**.** The *elementary diagram* of $\mathcal{M}$ is the $\mathcal{L}_M$-theory

$$\mathrm{Diag}_{\mathrm{el}}(\mathcal{M}) := \{\varphi(\underline{a}_1, \dots, \underline{a}_n) \mid \mathcal{M} \models \varphi \text{ and } \varphi \text{ an } \mathcal{L}\text{-formula}\}.$$

**Note.** There's a canonical way of expanding $\mathcal{M}$ to an $\mathcal{L}_M$-structure with $\underline{a}^{\mathcal{M}} := a$, i.e., we write $a$ for both the symbol and the element.

**Lemma 2.2.1.** Let $\mathcal{N}$ be an $\mathcal{L}_M$-structure.

(a) If $\mathcal{N} \models \mathrm{Diag}(\mathcal{M})$ then, viewing $\mathcal{N}$ as an $\mathcal{L}$-structure, there is an embedding $f \colon \mathcal{M} \to \mathcal{N}$.

(b) If $\mathcal{N} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$, then there is an elementary $\mathcal{L}$-embedding of $\mathcal{M}$ into $\mathcal{N}$.

**Proof.** Take $f(a) = \underline{a}^{\mathcal{N}}$, then $\mathcal{N} \models \mathrm{Diag}(\mathcal{M})$ means exactly that $f$ is an embedding, and $\mathcal{N} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ means that $f$ is an elementary embedding. ∎

**Theorem 2.2.1** (Upward Löwenheim-Skolem theorem)**.** Let $\mathcal{M}$ be an infinite $\mathcal{L}$-structure and let $\kappa$ be an infinite cardinal $\kappa \geq |\mathcal{M}| + |\mathcal{L}|$. Then there is an $\mathcal{L}$-structure $\mathcal{N}$ of cardinality $\kappa$ such that $j \colon \mathcal{M} \to \mathcal{N}$ is elementary.

**Proof.** $\mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$ is satisfiable since $\mathcal{M} \models \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$, so by Proposition 2.1.1, it has a model $\mathcal{N}$ of cardinality $\kappa \geq |\mathcal{L}_M|$, and by Lemma 2.2.1, there is an elementary embedding $\mathcal{M} \to \mathcal{N}$. ∎

**Proposition 2.2.1** (Tarski-Vaught Test)**.** Let $\mathcal{M}$ be a substructure of $\mathcal{N}$. Then $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$ if and only if for any formula $\varphi(x, \overline{y})$ and $\overline{a} \in M^n$, if there is $b \in N$ such that $\mathcal{N} \models \varphi(b, \overline{a})$, then there is $c \in M$ such that $\mathcal{N} \models \varphi(c, \overline{a})$.

**Proof.** The forward direction follows from the fact that $\mathcal{M}$ is an elementary substructure, so the truth of $\exists x\ \varphi(x, \overline{y})$ is proved.

For the backward direction, suppose the condition holds. We show that $\mathcal{M} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{N} \models \varphi(\overline{a})$ by induction on $\varphi$. Suppose the claim holds for $\varphi, \psi$. Then,

$$\mathcal{M} \models (\varphi \wedge \psi)(\overline{a}) \Leftrightarrow \mathcal{M} \models \varphi(\overline{a}) \text{ and } \mathcal{M} \models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models \varphi(\overline{a}) \text{ and } \mathcal{N} \models \psi(\overline{a}) \Leftrightarrow \mathcal{N} \models (\varphi \wedge \psi)(\overline{a}).$$

Finally, suppose the claim holds for $\varphi(x, \overline{y})$, then

$$\mathcal{M} \models \exists x\ \varphi(x, \overline{a}) \Leftrightarrow \exists b \in M\ \mathcal{M} \models \varphi(b, \overline{a}) \Leftrightarrow \exists b \in M\ \mathcal{N} \models \varphi(b, \overline{a})$$

by induction hypotheses. Conversely, $\mathcal{N} \models \exists x\ \varphi(x, \overline{a})$, then $\exists b \in N$ such that $\mathcal{N} \models \varphi(b, \overline{a})$ by the condition from the statement, so $\exists c \in M$ such that $\mathcal{N} \models \varphi(c, \overline{a})$. By the induction hypotheses, we further have $\mathcal{M} \models \varphi(c, \overline{a})$, hence $\mathcal{M} \models \exists x\ \varphi(x, \overline{a})$. ∎

**Example.** The ring $\mathbb{Z}$ is a substructure of $\mathbb{Q}$, but $\mathbb{Q} \models \exists x\ (x + x = 1)$ while $\mathbb{Z} \not\models \exists x\ (x + x = 1)$.

# Lecture 14: Downward Löwenheim-Skolem theorem

21 Feb. 14:30

**Definition 2.2.3** (Built-in Skolem functions). We say an $\mathcal{L}$-theory $T$ has *built-in Skolem functions* if for all $\mathcal{L}$-formulas $\varphi(x, y_1, \ldots, y_n)$, there is a function symbol $f$ such that

$$T \models \forall \overline{y}\ (\exists x\ \varphi(x, \overline{y}) \to \varphi(f(\overline{y}), \overline{y})).$$

**Lemma 2.2.2.** Let $T$ be an $\mathcal{L}$-theory, then there are $\mathcal{L}^* \supseteq \mathcal{L}$ and $T^* \supseteq T$ an $\mathcal{L}^*$-theory such that $T^*$ has built-in Skolem functions. Moreover, if $\mathcal{M} \models T$, then we can expand $\mathcal{M}$ to $\mathcal{M}^* \models T^*$.

**Proof.** Start with $\mathcal{L}_0 = \mathcal{L}$ and $T_0 = T$, we build $\mathcal{L}^* = \bigcup_i \mathcal{L}_i$ and $T^* = \bigcup_i T_i$. Given $\mathcal{L}_i$ and $T_i$, define

$$\mathcal{L}_{i+1} = \mathcal{L}_i \cup \{f_\varphi \mid \varphi(x, \overline{y}) \text{ is an } \mathcal{L}_i\text{-formulas}\}$$

where the arity of $f_\varphi$ is the same as $\overline{y}$, and

$$T_{i+1} = Tvi \cup \{\forall \overline{y}\ (\exists x\ \varphi(x, \overline{y}) \to \varphi(f_\varphi(\overline{y}), \overline{y}))\}.$$

Now, we argue that if $\mathcal{M} \models T_i$, we can expand it to a model $\mathcal{M}^*$ of $T_{i+1}$. Pick $c \in M$ a "default value." Given $\varphi$ and $\overline{a}$, define $f_\varphi^{\mathcal{M}^*}(\overline{a})$ to be some $b$ with $\mathcal{M} \models \varphi(b, \overline{a})$ if such a $b$ exists, or $c$ otherwise. Then, $\mathcal{M}^* \models T_{i+1}$.

Now, $T^*$ has built-in Skolem functions. Suppose $\mathcal{M} \models T$, i.e., $\mathcal{M} = \mathcal{M}_0 \models T_0$. Then $\mathcal{M}_0$ has an expansion $\mathcal{M}_1 \models T_1$, which has an expansion $\mathcal{M}_2 \models T_2$, etc. Then, $\mathcal{M}^* = \bigcup_i \mathcal{M}_i$ is a model of $T^*$, and by counting, we have $|\mathcal{L}^*| = |\mathcal{L}| + \aleph_0$. ∎

**Notation** (Skolemization). We call $T^*$ in Lemma 2.2.2 a *Skolemization* of $T$.

**Theorem 2.2.2** (Downward Löwenheim-Skolem theorem). Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $X \subseteq M$. Then there is an elementary substructure $X \subseteq \mathcal{N}$ of $\mathcal{M}$ of cardinality $|\mathcal{N}| \leq |\mathcal{L}| + \aleph_0 + |X|$.

**Proof.** By expanding the language, we get $\mathcal{M}^*$ and $\mathcal{L}^*$-structure with $\mathrm{Th}(\mathcal{M}^*)$ has built-in Skolem functions (where $T = \mathrm{Th}(\mathcal{M})$ in Lemma 2.2.2). Replacing $\mathcal{M}$ by $\mathcal{M}^*$, etc., we may assume that we already had built-in Skolem functions.

Start with $X_0 = X \cup \{c^{\mathcal{M}} \mid c \text{ a constant symbol}\}$. Given $X_i$, define $X_{i+1}$ as

$$X_{i+1} = X_i \cup \{f(\overline{a}) \mid f \text{ a function symbol}, \overline{a} \in X_i\}.$$

Let $N = \bigcup_i X_i$, let $\mathcal{N}$ be the substructure of $\mathcal{M}$ with domain $N$.[a] Now, to show that $\mathcal{N}$ is an elementary substructure of $\mathcal{M}$, we use the Tarski-Vaught test. Suppose that we have an $\mathcal{L}$-formula $\varphi(x, \overline{y})$, $\overline{a} \in N$, $b \in M$ such that $\mathcal{M} \models \varphi(b, \overline{a})$ (we must replace $b$ by $c \in N$). Since $\mathcal{M} \models \exists x\ \varphi(x, \overline{a})$, so $\mathcal{M} \models \varphi(f_\varphi(\overline{a}), \overline{a})$. But since $\overline{a} \in N$, so $f_\varphi(\overline{a}) \in N$, so the Tarski-Vaught test says $\mathcal{N}$ is an elementary substructure of $\mathcal{M}$.

Finally, we see that $|X_0| \leq |X| + |\mathcal{L}| + \aleph_0$, and since $N$ is a countable union, so

$$|N| \leq |X| + |\mathcal{L}| + \aleph_0.$$

∎

[a] Here, $\mathcal{N}$ is called the *substructure generated by* $X$.

**Example** (Countable real closed filed). Consider $\mathbb{R} = (\mathbb{R}, 0, 1, +, -, \cdot, \leq)$. Let $X \subseteq \mathbb{R}$ be countable, e.g., $X = \varnothing$ or $X = \{\pi, e\}$. Then there is $X \subseteq R \preceq \mathbb{R}$ such that $R$ is countable. In particular, $\mathrm{Th}(R) = \mathrm{Th}(\mathbb{R})$. In this way, $R$ is a *countable real closed filed*:

(a) $-1$ is not a sum of squares;

(b) for all $a$, there is $b$ such that $a = b^2$ or $a = -b^2$;

(c) every odd degree polynomial has a root.

**Example** (Skolem's paradox). Let $\mathcal{L} = \{\in\}$, where $\in$ a binary relation symbol. Let $T = \mathrm{ZFC}$. Suppose that ZFC is a satisfiable,[a] and let $\mathcal{M} \models T$. Then there is $\mathcal{N} \preceq \mathcal{M}$ with $\mathcal{N}$ countable. Then,

$$\mathcal{N} \models \text{"there is no bijection between } \mathbb{R}^{\mathcal{N}} \text{ and } \mathbb{N}^{\mathcal{N}}\text{"}.$$

$\mathcal{N}$ thinks that it contains an uncountable set $\mathbb{R}^{\mathcal{N}}$, but $\left\{a \in N \mid \mathcal{N} \models a \in \mathbb{R}^{\mathcal{N}}\right\} \subseteq N$ is countable. This is called *Skolem's paradox*.

[a] From Gödel's incompleteness theorem, in ZFC, one can't prove that ZFC is consistent.

**Definition 2.2.4** (Universallly axiomatizable). Let $T$ be an $\mathcal{L}$-theory, then $T$ is *universallly axiomatizable* if there is a set $\Gamma$ of universal sentences such that $T \models \Gamma$ and $\Gamma \models T$.

**Theorem 2.2.3.** Let $T$ be an $\mathcal{L}$-theory. $T$ is universallly axiomatized if and only if whenever $\mathcal{N} \models T$ and $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} \models T$.

**Proof.** We already know the forward direction. Now, to prove the backward direction, suppose that if $\mathcal{N} \models T$, $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} \models T$. Define

$$\Gamma = \{\varphi \text{ universal} \mid T \models \varphi\},$$

then $T \models \Gamma$. Now, we show that $\Gamma \models T$. We may assume that $T$ is satisfiable[a] and let $\mathcal{M} \models \Gamma$.we must prove that $\mathcal{M} \models T$. We will do this by finding $\mathcal{N} \supseteq \mathcal{M}$, $\mathcal{N} \models T$, which implies $\mathcal{M} \models T$. We build such an $\mathcal{N}$ by showing that $\mathrm{Diag}(\mathcal{M}) \cup T$ is satisfiable with compactness theorem. Let $\Delta \subseteq \mathrm{Diag}(\mathcal{M}) \cup T$ be finite, then there is a finite set of atomic or negated atomic formulas $\varphi_1, \ldots, \varphi_\ell$ and $m_1, \ldots, m_k \in M$ such that

$$\Delta \subseteq \{\varphi_1(\overline{m}), \ldots, \varphi_\ell(\overline{m})\} \cup T.$$

We may assume that they are actually equal. To show that $\Delta$ is satisfiable, it is enough to show that

$$\{\exists x_1 \ldots \exists x_k\ (\varphi_1(\overline{x}) \land \ldots \land \varphi_\ell(\overline{x}))\} \cup T$$

is satisfiable. If not, then $T \models \forall x_1 \ldots \forall x_k\ \neg(\varphi_1(\overline{x}) \land \ldots \land \varphi_\ell(\overline{x}))$. But this is universal, hence in $\Gamma$, so it is true in $\mathcal{M}$, i.e., $\mathcal{M} \models \varphi_1(\overline{m}) \land \ldots \land \varphi_\ell(\overline{m})$ and $\mathcal{M} \models \forall x_1 \ldots \forall x_k\ \neg(\varphi_1(\overline{x}) \land \ldots \land \varphi_\ell(\overline{x}))$, a contradiction $\lightning$ Hence, $\Delta$ is satisfiable, so any finite subset is satisfiable, by compactness theorem, we're done. ∎

[a] Since otherwise $\Gamma \ni \forall x\ x \neq x$.

# Appendix

# Bibliography


[HH97] W. Hodges and S.M.S.W. Hodges. *A Shorter Model Theory*. Cambridge University Press, 1997. ISBN: 9780521587136. URL: https://books.google.com/books?id=S6QYeuo4p1EC.

[Hin05] P.G. Hinman. *Fundamentals of Mathematical Logic*. Taylor & Francis, 2005. ISBN: 9781568812625. URL: https://books.google.com/books?id=xA6D8o72qAgC.

[Mar02] D. Marker. *Model Theory : An Introduction*. Graduate Texts in Mathematics. Springer New York, 2002. ISBN: 9780387987606. URL: https://books.google.com/books?id=gkvogoiEnuYC.

[Rob49] Julia Robinson. "Definability and decision problems in arithmetic". In: *The Journal of Symbolic Logic* 14.2 (1949), pp. 98–114. DOI: 10.2307/2266510.