MATH681
Mathematical Logic

Pingbang Hu

January 17, 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

1.1 What's Mathematical Logic?

5 Jan. 14:30

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.

> **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

1.2 Syntax and Semantics

1.2.1 Languages and Structures

Let's start with the fundamental object, language.

Definition 1.2.1 (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 σ rather than $\mathcal{L}$.

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

Remark. Any or all sets in Definition 1.2.1 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 1.2.2 (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 $c^{\mathcal{M}} \in M$.

Note (Interpretation). We call $f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}}$ the *interpretation in $\mathcal{M}$* of symbols f, R, c, 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, i.e., $\mathcal{L}_{\text{ring}}$, $\mathcal{L}_{\text{ord}}$, 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.

1.2.2 Embeddings and Isomorphisms

We can now consider the relation between structures.

Definition 1.2.3 (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 $f \in \mathcal{F}$ of arity n_f, and $a_1, \ldots, a_{n_f} \in \mathcal{M}$,

$$\eta(f^{\mathcal{M}}(a_1, \ldots, a_{n_f})) = f^{\mathcal{N}}(\eta(a_1), \ldots, \eta_{a_{n_f}});$$

(b) for each relation $R \in \mathcal{R}$ of arity n_R, and $a_1, \ldots, a_{n_R} \in \mathcal{M}$,

$$(a_1, \ldots, a_{n_R}) \in R^{\mathcal{M}} \Leftrightarrow (\eta(a_1), \ldots, \eta(a_{n_R})) \in R^{\mathcal{N}};$$

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

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

Definition 1.2.4 (Isomorphism)**.** An $\mathcal{L}$-*isomorphism* is a bijective $\mathcal{L}$-embedding.

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

Definition 1.2.5 (Substructure)**.** $\mathcal{M}$ is a *substructure* of $\mathcal{N}$.

Definition 1.2.6 (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 η be injective is the same as (b) in Definition 1.2.3 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.

Remark. Using $\mathcal{L}_2$, 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.

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

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.

1.3 First-Order Logic

1.3.1 Terms, Formulas, and Truths

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 1.3.1 (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, $t^{\mathcal{M}}(a_1, \ldots, a_n) = a_i$;

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

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 $2 \cdot (x+y)$.

Definition 1.3.2 (Formula)**.** The set of $\mathcal{L}$-*formulas* are defined inductively:

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

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

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

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

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

Notation (Atomic formula)**.** Definition 1.3.2 (a) and (b) are called *atomic formulas*.

Notation (Quantifier-free formula)**.** Definition 1.3.2 (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 1.3.3 (Free variable). The *free variables* $\mathrm{FV}(\varphi)$ of a formula φ 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) $\mathrm{FV}(\varphi\land\psi)=\mathrm{FV}(\varphi\lor\psi)=\mathrm{FV}(\varphi)\cup\mathrm{FV}(\psi)$.

(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 1.3.4 (Sentence). A formula φ is called a *sentence* if it has no free variables.

Notation. If φ 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 φ has no other free variables than $x_1,\ldots,x_n$.

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

Definition 1.3.5 (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 φ is *true* of $\overline{a}$ in $\mathcal{M}$,[a] denoted as $\mathcal{M}\models\varphi(\overline{a})$, as follows:

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

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

(d) If φ is $\psi_1\land\psi_2$, 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 φ is $\psi_1\lor\psi_2$, 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 φ is $\exists y\ \psi(\overline{x},y)$, then $\mathcal{M}\models\varphi(\overline{a})$ if there's $b\in\mathcal{M}$ such that $\mathcal{M}\models\psi(\overline{a},b)$.

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

12 Jan. 14:30

Notation (Material implication). The *material implication* $\varphi\to\psi$ between two formulas φ,ψ is an abbreviation of $\neg\varphi\lor\psi$.

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

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

where we see that any model of this sentence is undirected.

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

Definition 1.3.6 (Logical consequence). Let Φ be a set of sentences, and φ be a sentence. We say that φ is a *logical consequence* of Φ, written $\Phi \models \varphi$, if $\mathcal{M} \models \varphi$ whenever $\mathcal{M} \models \Phi$ in all models $\mathcal{M}$.

If $\Phi = \varnothing$ is the empty set, Definition 1.3.6 is written as $\models \varphi$, i.e., φ is true in all $\mathcal{L}$-structures.[1]

Definition 1.3.7 (Equivalent). Given two formulas φ, ψ, $\varphi(\overline{x})$ and $\psi(\overline{x})$ are *equivalent* if

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

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

Problem. Two sentences φ and ψ 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 1.3.1. 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 φ 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 φ 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 φ 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 φ 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 φ 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 $p > 0$, $\varphi_p \coloneqq \underbrace{1 + 1 + \ldots + 1}_{p} = 0$, which says the characteristic p. φ_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 $\varphi(x) \coloneqq \neg\exists y\ y + y = x$. We see that $\mathbb{Z} \models \varphi(1)$ but $\mathbb{Q} \models \neg\varphi(1)$.

Proposition 1.3.2. 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 φ is quantifier-free, so $\mathcal{B} \models \varphi(\overline{a}, b_1, \ldots, b_n)$ from Proposition 1.3.1, 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. In Proposition 1.3.2, formulas as in (a) are called *existential ($\exists_1$ or $\exists$) formulas*; and formulas as in (b) are called *universal ($\forall_1$ or $\forall$) formulas.*

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

- 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.

Remark. 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: Theory and Axioms

17 Jan. 14:30

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

Let G be a graph, viewed as a $\mathcal{L}_1$-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.[2]

For example, vEw is quantifier-free in $\mathcal{L}_1$, while

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

is not quantifier-free in $\mathcal{L}_2$.

[2] 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 $e \colon v \to w$.

Definition 1.3.8 (Theory). An $\mathcal{L}$-*theory* is a set of $\mathcal{L}$-sentences.

Definition 1.3.9 (Model). We say that $\mathcal{M}$ 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., $\{\forall x\ x \neq x\}$.

Definition 1.3.10 (Satisfiable). If a theory has a model, we say that it is *satisfiable*.

Definition 1.3.11 (Elementary class). A class $\mathcal{K}$ of $\mathcal{L}$ -structures is called an *elementary class* if there is an $\mathcal{L}$-theory T such that

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

Start with an $\mathcal{L}$-structure $\mathcal{M}$, then the theory of $\mathcal{M}$ is

$$\mathrm{Th}(\mathcal{M}) = \{\varphi \mid \mathcal{M} \models \varphi\}.$$

It's easy to see that $\mathcal{M} \models \mathrm{Th}(\mathcal{M})$.

Remark. $\mathrm{Th}(\mathcal{M})$ characterizes the structures satisfying the same sentences as $\mathcal{M}$.

Definition 1.3.12 (Complete). A theory T is *complete* if for any sentence φ, either $\varphi \in T$ or $\neg\varphi \in T$.

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

Definition 1.3.13 (Elementarily equivalent). $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent*$\mathcal{M} \equiv \mathcal{N}$ if for all sentences φ,

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

Remark (Non-standard model of arithmetic). 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*. $\mathcal{N}$ has *infinite element* larger than all of $\mathbb{M}$. Here, $\mathbb{N} = (\mathbb{N}, 0, 1, +, \cdot, -)$

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

Proof. We will show this on the homework. ⊛

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

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

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

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 $\mathcal{L}_{\text{group}} = \left\{e, \cdot, ^{-1}\right\}$, let T be the group axioms.

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

Definition 1.3.14 (Finitely axiomatizable). A theory is *finitely axiomatizable* if it has a finite axiomatization.

Given a theory, consider $T^{\models} = \{\varphi \colon T \models \varphi\}$,[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 Φ such that $T^{\models} = \Phi^{\models}$.

Definition 1.3.15 (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 $\overline{a} \in M$,

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

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 1.3.3. 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 φ, 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 1.3.1. 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, $\mathcal{M} \models \psi(\overline{a}, b)$, so $\mathcal{M} \models \varphi(\overline{a})$. ∎

Corollary 1.3.1. If $\mathcal{M} \cong \mathcal{N}$, then $\mathcal{M} \equiv \mathcal{N}$.

Definition 1.3.16 (Definable set). Let $\mathcal{M}$ be an $\mathcal{L}$-structure, and let $X \subseteq M^n$. X 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 $\varnothing$.

[3] Recall Definition 1.3.6.

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 (Langrange's four-square theorem)**.** Let $\mathbb{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$. Then $\mathbb{N}$ is $\varnothing$-definable in $\mathbb{Z}$ by

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

This follows 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, and the formula is very complicated.

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

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.