MATH681
Mathematical Logic

Pingbang Hu

January 12, 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 σ 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 $c^{\mathcal{M}} \in M$.

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.

1.1.2 Embeddings and Isomorphisms

We can now consider the relation between structures.

Definition 1.1.3 (Embedding). Given a language $\mathcal{L}$ and 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 $a_1, \dots, a_{n_f} \in \mathcal{M}$,

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

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

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

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

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

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

Definition. Given a language $\mathcal{L}$ and 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 1.1.5 (Substructure).** $\mathcal{M}$ is a *substructure* of $\mathcal{N}$.

> **Definition 1.1.6 (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 kinds of mathematical structures.

Remark. Asking that η be injective is the same as (b) in Definition 1.1.3 for the relation $=$ of equality since

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

However, 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 OK at 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 for 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.

1.2 First-Order Logic

1.2.1 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 1.2.1 (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 $t^{\mathcal{M}} \colon M^n \to M$.

Then, we define t^m inductively 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
$$t^{\mathcal{M}}(a_1, \ldots, a_n) = f^{\mathcal{M}}\left(s_1^{\mathcal{M}}(a_1, \ldots, a_n), \ldots, s_k^{\mathcal{M}}(a_1, \ldots, a_n)\right).$$

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

Example. In $(\mathbb{R}, 0, 1, +, \cdot, -)$, 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
$$2 \cdot (x+y)$$

Then, what do the terms in the ring language look like? They are the polynomials with integer coefficients, assuming we interpret them in a ring.

Definition 1.2.2 (Formula)**.** Given a language $\mathcal{L}$, the $\mathcal{L}$*-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_1 is a variable, $\exists v_i\ \varphi$ and $\forall v_i\ \varphi$ are *formulas*.

Notation (Atomic formula)**.** Formulas of the form (a) and (b) in Definition 1.2.2 are called *atomic formulas*.

Notation (Quantifier-free formula)**.** Formulas of the form (a), (b), (c), and (d) in Definition 1.2.2 are called *quantifier-free formulas*.

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

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

while the first appearance of y is free, the second appearance of y is bound by $\exists y$, or we say that y is 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.

Definition 1.2.3 (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) $\mathrm{FV}(R(s_1, \dots, s_{n_R}))$ is the set of variables showing up in $s_1, \dots, s_{n_R}$.

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

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

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

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

Definition 1.2.5 (Truth)**.** Given a language $\mathcal{L}$ and an $\mathcal{L}$-structure $\mathcal{M}$, let $\varphi(x_1, \dots, x_n)$ be an $\mathcal{L}$-formula. Let $a_1, \dots, a_n \in \mathcal{M}$. Define $\mathcal{M} \models \varphi(\overline{a})$[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 $R(t_1, \dots, t_{n_R})$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\left(t_1^{\mathcal{M}}(\overline{a}), \dots, t_{n_R}^{\mathcal{M}}(\overline{a})\right) \in R^{\mathcal{M}}$.

(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 $\exists y\ \psi(\overline{x}, y)$,[b] 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] We read this as *φ is true of $\overline{a}$ in $\mathcal{M}$*.
[b] Recall that $\overline{x} = (x_1, \dots, x_n)$.

Lecture 3

As previously seen. If $\mathcal{M} \models \varphi(\overline{a})$, we say that $\mathcal{M}$ *satisfies* $\varphi(\overline{a})$, or $\varphi(\overline{a})$ *is true in* $\mathcal{M}$. And if φ is a sentence, we can write $\mathcal{M} \models \varphi$ or $\mathcal{M} \not\models \varphi \Leftrightarrow \mathcal{M} \models \neg\varphi$. 12 Jan. 14:30

Consider the language of graphs $\mathcal{L}_{\text{graph}} = \{E\}$, and consider the following examples.

Example (Material implication). An undirected graph can be written as

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

where we take $\to$ as an abbreviation such that $\varphi \to \psi$ means $\psi \lor \neg\varphi$, called *material implication*. 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. In terms of 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 first-order (FO) logic. ⊛

Example. 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). ⊛

We started with $\land, \lor, \neg, \forall, \exists$; but we could have started with on of $\land$ or $\lor$ or $\to$, and $\neg$, and one of $\forall$ or $\exists$. Then we would treat the other two as abbreviations.

Example. $\varphi \land \psi$ could be an abbreviation for $\neg(\neg\varphi \lor \neg\psi)$.

Example. $\exists x\ \varphi$ could be an abbreviation for $\neg(\forall x\ \neg\varphi)$.

Example. $\forall x\ \varphi$ could be an abbreviation for $\neg(\exists x\ \neg\varphi)$.

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

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

and we can use $\uparrow$ to define $\neg, \vee, \wedge$.

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 1.2.6 (Logical consequence). Let Φ be a set of sentences, and φ a sentence. 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, write $\models \varphi$, which means that φ is true in all $\mathcal{L}$-structures.[a]

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

Definition 1.2.7 (Equivalent). Say that $\varphi(\overline{x})$ and $\psi(\overline{x})$ are *equivalent* if

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

Notation. In Definition 1.2.7, $\leftrightarrow$ is the logical symbol (essentially $\to$ in both directions), showing up in formulas, and is different from $\Leftrightarrow$.

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 1.2.1. 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 will need to set $\mathcal{A}$ to be the Cartesian product with a fixed length, but we usually abbreviate it and drop the power.

Proof. We start with terms. We'll prove 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.

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

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

(3) If t is $f(s_1, \dots, s_n)$, 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

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

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 that $\mathcal{A} \models \varphi(\overline{a}) \Leftrightarrow \mathcal{B} \models \varphi(\overline{a})$ for $\overline{a} \in \mathcal{A}$. By induction on formulas,

(1) 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

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

(2) If φ is $R(s_1, \dots, s_n)$, then

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

(3) 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 $\Leftrightarrow$.

(4) If φ is $\psi_1 \vee \psi_2$,[a]

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

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 1.2.2. 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. It's easy to see that (b) is implied by (a), so we only prove (a). 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 $\mathcal{B} \models \varphi(\overline{a}, b_1, \ldots, b_n)$. Thus,

$$\mathcal{B} \models \exists y_1 \ldots \exists y_n\ \varphi(\overline{a}, y_1, \ldots, y_n).$$

■

Remark. In Proposition 1.2.2, 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.

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

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.