Model-Theory of Fields: Background

David Pierce

2004.10.25

These notes are intended as a quick summary of first-order logic as used in model-theory and the model-theoretic study of fields. I originally wrote them for the algebra study group at METU in 2002, when we were looking at [3, ch. 6]. For less terse accounts, see [2] or [4] or even [1].

My notational conventions are these. The set of natural numbers is ω, and each natural number n is the set $\{0, \ldots, n-1\}$ of its predecessors. In particular, 0 is $\varnothing$. If $I \subseteq \omega$, and M is a set, then M^I is the set of functions from I to M. A typical element of M^I can be written $(a_i : i \in I)$ or just $\mathbf{a}$ or $\vec{a}$.

Model-theory begins with the distinctions indicated in the table on p. 2. Technical terms in **bold** are not defined further; those that are *slanted*, will be.

Formally, a **structure** with **signature** $\mathcal{L}$ can be defined as a pair $(M, \mathfrak{I})$, where M is a set, and $\mathfrak{I}$ is a function assigning an interpretation to each constant-, function- and relation-symbol in $\mathcal{L}$. (I may refer to relation-symbols as **predicates**, and to constant-symbols as **constants**.) The set M is called the **universe** of the structure. One rarely refers to $\mathfrak{I}$ explicitly, but one may write the structure as $\mathfrak{M}$ (in a more elaborate font) to indicate the presence of $\mathfrak{I}$.

The signature $\mathcal{L}_{\mathrm{r}}$ of (unital) rings and fields is

$$\{+, -, \cdot, 0, 1\},$$

where $+$ and $\cdot$ are binary, and $-$ is a unary, function-symbol, and 0 and 1 are constant-symbols. The signature $\mathcal{L}_{\mathrm{or}}$ of ordered rings and fields contains also the binary relation-symbol $\leqslant$. To indicate explicitly that the integers are to be thought of as composing an ordered ring, one might write this structure as

$$(\mathbb{Z}, +^{\mathbb{Z}}, -^{\mathbb{Z}}, \cdot^{\mathbb{Z}}, 0^{\mathbb{Z}}, 1^{\mathbb{Z}}, \leqslant^{\mathbb{Z}}).$$

However, the superscripts are rarely needed; one might write $(\mathbb{Z}, +, -, \cdot, 0, 1, \leqslant)$, or just refer to 'the ordered ring $\mathbb{Z}$'.

Terms can be defined thus (here f is as in the table):

($*$) Constant-symbols and variables are terms.

($\dagger$) If $t_0, \ldots, t_{n-1}$ are terms, then so is $ft_0 \ldots t_{n-1}$.

If t is a term, and I is a subset of ω containing the indices of all variables appearing in t, then $t^{\mathfrak{M}}$ can be understood in the obvious way as a function from M^I to M.

Informally, letters like x, y and z stand for variables. The definition of 'term' uses the so-called Polish notation, which needs no brackets. Conventionally, binary symbols are written between their arguments, so that $\cdot + x\, y\, z$ is written $(x+y)\cdot z$. The manner of writing terms is not mathematically important; what is important is that *a term of $\mathcal{L}$ is an unambiguous recipe for constructing a function in each $\mathcal{L}$-structure.*

For every commutative ring $\mathfrak{A}$, there is a unique homomorphism of $\mathbb{Z}$ into $\mathfrak{A}$; the image of $\mathbb{Z}$ in A is (the universe of) the **prime ring** of $\mathfrak{A}$. Every element of the prime ring is the interpretation of a term, namely $-(1+\cdots+1)$ or 0 or $1+\cdots+1$. Then every polynomial over the prime ring is the interpretation of a term of $\mathcal{L}_{\mathrm{r}}$, and every term has such an interpretation in $\mathfrak{A}$ (if A is infinite).

Table 1: Model-theoretic symbols and meanings

IMAGE SYMBOL SYNTAX	REALITY INTERPRETATION SEMANTICS
signature $\mathcal{L}$	$\mathfrak{M}$, an *$\mathcal{L}$-structure*
	OPERATIONS ON M:
	BASIC OPERATIONS:
variable v_i	$\mathbf{a} \mapsto a_i : M^I \to M$, if $i \in I$
constant-symbol c	$c^{\mathfrak{M}}$, an element of M
n**-ary function-symbol** f	$f^{\mathfrak{M}} : M^n \to M$
term t	$t^{\mathfrak{M}}$, a composition of basic operations
LOGICAL SYMBOLS:	FUNCTIONS ON $\mathcal{P}(M^I)$
CONNECTIVES:	OPERATIONS:
$\wedge$	$\cap$
$\neg$	$A \mapsto A^{\mathrm{c}}$
$\vee$	$\cup$
$\to$	$(A,B) \mapsto A^{\mathrm{c}} \cup B$
$\leftrightarrow$	$(A,B) \mapsto (A^{\mathrm{c}} \cup B) \cap (A \cup B^{\mathrm{c}})$
QUANTIFIERS:	PROJECTIONS:
$\exists v_i$	$A \mapsto \{(a_j : j \in I \smallsetminus \{i\}) : \mathbf{a} \in A\}$
$\forall v_i$	$A \mapsto \{(a_j : j \in I \smallsetminus \{i\}) : \mathbf{a} \in A^{\mathrm{c}}\}^{\mathrm{c}}$
	RELATIONS ON M:
	BASIC RELATIONS:
$=$	equality
n**-ary relation-symbol** R	$R^{\mathfrak{M}}$, a subset of M^n
FORMULAS:	DEFINABLE RELATIONS:
atomic formula α	$\alpha^{\mathfrak{M}}$, a solution-set
open formula β	$\beta^{\mathfrak{M}}$, a *constructible* set
formula ϕ	$\phi^{\mathfrak{M}}$
sentence	true or false
$\vdash$	$\models$
$\models$	$\subseteq$

If we want to allow arbitrary coefficients from A, we introduce them into the signature. In general, if $B \subseteq M$, then $\mathcal{L}(B)$ is $\mathcal{L}$ with a new constant-symbol for each element of B.

Atomic formulas take the form $(t_0 = t_1)$ or $Rt_0 \dots t_{n-1}$ (where R is as in the table; the latter formula is in Polish notation.) The corresponding interpretations in $\mathfrak{M}$ are thus:

- $(t_0 = t_1)^{\mathfrak{M}}$ is the inverse image of $\{(a, a) : a \in M\}$ under $(t_0^{\mathfrak{M}}, t_1^{\mathfrak{M}})$, and
- $(Rt_0 \dots t_{n-1})^{\mathfrak{M}} = (t_0^{\mathfrak{M}}, \dots, t_{n-1}^{\mathfrak{M}})^{-1} R^{\mathfrak{M}}$.

In $\mathcal{L}_{\mathrm{r}}$, the atomic formulas correspond to polynomial equations over a prime ring; the interpretations of the formulas are the solution-sets of the equations. In $\mathcal{L}_{\mathrm{or}}$, some atomic formulas correspond to inequalities.

In the propositional calculus, the connectives $\wedge$ and $\neg$ are adequate to symbolize every truth-table. In particular, one has the equivalences:

$$P \vee Q \sim \neg P \wedge \neg Q; \quad P \to Q \sim \neg P \vee Q; \quad P \leftrightarrow Q \sim P \to Q \wedge Q \to P.$$

I shall use the arrows $\implies$ and $\iff$ not as formal symbols, but as abbreviations for ordinary expressions like 'implies' and 'if and only if' respectively.

Hence we can define **open** (or **basic**, or **quantifier-free**) formulas thus.

(∗) Atomic formulas are open.

(†) If α is open, then so is $\neg\alpha$.

(‡) If α and β are open, then so is $(\alpha \wedge \beta)$.

Informally, redundant brackets can be omitted. (Or one can use Polish notation.)

Arbitrary **formulas** are defined as open formulas are, with an extra provision:

(§) If ϕ is a formula, then so is $(\exists x\ \phi)$ for any variable x.

For every formula ϕ, there is a set $\mathrm{fv}(\phi)$ of indices of its **free variables**, given thus:

(∗) If α is atomic, then $\mathrm{fv}(\alpha)$ is the set of indices of variables appearing in ϕ.

(†) $\mathrm{fv}(\neg\phi) = \mathrm{fv}(\phi)$.

(‡) $\mathrm{fv}(\phi \wedge \psi) = \mathrm{fv}(\phi) \cup \mathrm{fv}(\psi)$.

(§) $\mathrm{fv}(\exists v_i\ \phi) = \mathrm{fv}(\phi) \smallsetminus \{i\}$.

If $\mathrm{fv}(\phi) = n$, then ϕ can be written as $\phi(v_0, \dots, v_{n-1})$, and $\phi^{\mathfrak{M}}$ should be a subset of M^n. Indeed, we define:

- $(\neg\phi)^{\mathfrak{M}} = (\phi^{\mathfrak{M}})^{\mathrm{c}}$;
- $(\phi \wedge \psi)^{\mathfrak{M}} = \phi^{\mathfrak{M}} \cap \psi^{\mathfrak{M}}$;
- $(\exists v_i\ \phi)^{\mathfrak{M}}$ is the image of $\phi^{\mathfrak{M}}$ under $\mathbf{a} \mapsto (a_j : j \in I \smallsetminus \{i\}) : M^I \to M^{I \smallsetminus \{i\}}$, where $\mathrm{fv}(\phi) \subseteq I$.

In $\mathfrak{M}$, the sets **definable over** $\varnothing$ are the interpretations of formulas of $\mathcal{L}$. These sets are also called 0-definable. If $B \subseteq M$, then the B-definable sets are the interpretations of formulas of $\mathcal{L}(B)$. Usually **definable** means M-definable.

In algebraic geometry, if $\mathfrak{K}$ is a field, then the **constructible** sets of $\mathfrak{K}$ are the sets definable by open formulas of $\mathcal{L}_{\mathrm{r}}(K)$. Chevalley's Theorem [5, § 4.4, p. 33] is that, if K is algebraically closed, then all definable sets of $\mathfrak{K}$ are constructible.

A **sentence** is a formula with no free variables. If σ is a sentence, then $\sigma^{\mathfrak{M}}$ is a subset of $M^{\varnothing}$. But $M^{\varnothing} = \{\varnothing\}$, whose subsets are $\varnothing$ and $\{\varnothing\}$, that is, 0 and 1, which can be considered as **false** and **true** respectively.

If $\sigma^{\mathfrak{M}} = 1$, then we write

$$\mathfrak{M} \models \sigma$$

and say that $\mathfrak{M}$ is a **model** of σ. In particular, if $\mathrm{fv}(\phi) = \{0\}$, then

$$\mathfrak{M} \models \exists v_0\ \phi \iff \phi^{\mathfrak{M}} \neq \varnothing.$$

If Γ is a set of sentences, then the expression

$$\mathfrak{M} \models \Gamma$$

has the obvious meaning. If $\mathfrak{M} \models \Gamma \implies \mathfrak{M} \models \sigma$ for all $\mathcal{L}$-structures $\mathfrak{M}$, then we write

$$\Gamma \models \sigma$$

and say σ is a **logical consequence** of Γ. One can define a notion of *formal proof*, and write $\Gamma \vdash \sigma$ ('σ is deducible from Γ') when there is a formal proof of σ from Γ. **Gödel's Completeness Theorem** is that the symbols $\vdash$ and $\models$ are interchangeable.

A **theory** is a set of sentences that contains all of its logical consequences. If T is a theory, and $\Gamma \models T$, then Γ is a set of **axioms** for T.

In $\mathcal{L}_{\mathrm{r}}$, the axioms for the (first-order) theory of fields are standard. They can be written in *universal* form, except for the axiom

$$\forall x\ \exists y\ (x = 0 \vee xy = 1).$$

The theory ACF of algebraically closed fields has the additional axioms

$$\forall v_0\ \forall v_1 \dots \forall v_{n-1}\ \exists y\ v_0 + v_1 y + \dots v_{n-1} x^{n-1} + y^n = 0.$$

The model-theoretic version of Chevalley's Theorem is that ACF admits **elimination of quantifiers**, that is, for all *positive* n, for every n-ary formula ϕ of $\mathcal{L}_{\mathrm{r}}$, there is an open formula α such that

$$\mathrm{ACF} \models \forall v_0 \dots \forall v_{n-1}\ (\phi \leftrightarrow \alpha).$$

One method of proof relies on the fact that a model of ACF is determined up to isomorphism by its characteristic and its transcendence-degree.

Ultra-products

Let $(\mathfrak{M}^{(i)} : i \in I)$ be an indexed set of $\mathcal{L}$-structures. We define a product-structure

$$\prod_{i \in I} \mathfrak{M}^{(i)},$$

or $\mathfrak{M}$ for short, as follows. The universe, M, is the product $\prod_{i\in I} M^{(i)}$. A typical element of this is $(a^{(i)} : i \in I)$, or simply a. Then each $\mathfrak{M}^{(i)}$ is an $\mathcal{L}(M)$-structure when we define

$$a^{\mathfrak{M}^{(i)}} = a^{(i)}.$$

For the symbols of $\mathcal{L}$, let this definition be a notational convention, so that $s^{(i)}$ means $s^{\mathfrak{M}^{(i)}}$ when $s \in \mathcal{L}$.

If σ is a sentence of $\mathcal{L}(M)$, then its **Boolean value**, $\|\sigma\|$, is defined to be the set

$$\{i \in I : \mathfrak{M}^{(i)} \models \sigma\}.$$

The map $\sigma \mapsto \|\sigma\|$ is a sort of homomorphism: $\|\sigma \wedge \tau\| = \|\sigma\| \cap \|\tau\|$ and $\|\neg\sigma\| = \|\sigma\|^{\mathrm{c}}$.

Having M, we define $\mathfrak{M}$ by:

- $c^{\mathfrak{M}} = (c^{\mathfrak{M}^{(i)}} : i \in I)$,
- $f^{\mathfrak{M}}(\mathbf{a}) = (f^{\mathfrak{M}^{(i)}}(\mathbf{a}^{(i)}) : i \in I)$,
- $\mathbf{a} \in R^{\mathfrak{M}} \iff \|R\mathbf{a}\| = I$.

Let $\mathfrak{F}$ be a filter on I (that is, the dual of an ideal of $\mathcal{P}(I)$). Define an equivalence-relation $\sim$ on M by:

$$a \sim b \iff \|a = b\| \in \mathfrak{F}.$$

(In case $\mathfrak{F} = \{I\}$, this relation is equality.) The **reduced product** $\mathfrak{M}/\mathfrak{F}$ has universe $M/{\sim}$, and:

- $c^{\mathfrak{M}/\mathfrak{F}} = c^{\mathfrak{M}}/{\sim}$,
- $f^{\mathfrak{M}/\mathfrak{F}}(\mathbf{a}/{\sim}) = f^{\mathfrak{M}}(\mathbf{a})/{\sim}$,
- $(\mathbf{a}/{\sim}) \in R^{\mathfrak{M}/\mathfrak{F}} \iff \|R\mathbf{a}\| \in \mathfrak{F}$.

The validity of this definition must be checked: If $\mathbf{a}, \mathbf{b} \in M^n$, then

$$\|a_0 = b_0 \wedge \ldots \wedge a_{n-1} = b_{n-1}\| \subseteq \|f(\mathbf{a}) = f(\mathbf{b})\|,$$

so $\mathbf{a} \sim \mathbf{b} \implies f(\mathbf{a}) \sim f(\mathbf{b})$. Also,

$$\|a_0 = b_0 \wedge \ldots \wedge a_{n-1} = b_{n-1}\| \cap \|R\mathbf{a}\| \subseteq \|R\mathbf{b}\|,$$

so $\mathbf{a} \sim \mathbf{b} \wedge \|R\mathbf{a}\| \in \mathfrak{F} \implies \|R\mathbf{b}\| \in \mathfrak{F}$.

Lemma. *Say σ_e $(e < 2)$ are sentences of $\mathcal{L}(M)$ such that*

$$\mathfrak{M}/\mathfrak{F} \models \sigma_e \iff \|\sigma_e\| \in \mathfrak{F}$$

in each case. Then $\mathfrak{M}/\mathfrak{F} \models \sigma_0 \wedge \sigma_1 \iff \|\sigma_0 \wedge \sigma_1\| \in \mathfrak{F}$.

Proof. $\|\sigma_0\| \cap \|\sigma_1\| = \|\sigma_0 \wedge \sigma_1\| \subseteq \|\sigma_e\|$. □

Lemma. *Say ϕ is a formula of $\mathcal{L}(M)$ with one free variable, and*

$$\mathfrak{M}/\mathfrak{F} \models \phi(a) \iff \|\phi(a)\| \in \mathfrak{F}$$

for all a in M. Then $\mathfrak{M}/\mathfrak{F} \models \exists x\ \phi \iff \|\exists x\ \phi\| \in \mathfrak{F}$.

Proof. $\|\phi(a)\| \subseteq \|\exists x\ \phi\|$ for all a in M. Also, there a in M such that $\mathfrak{M}^{(i)} \models \phi(a)$ if $\mathfrak{M}^{(i)} \models \exists x\ \phi$. Then $\|\phi(a)\| = \|\exists x\ \phi\|$. □

Theorem (Łoś). *If $\mathfrak{U}$ is an ultrafilter on I, then*

$$\mathfrak{M}/\mathfrak{U} \models \sigma \iff \|\sigma\| \in \mathfrak{U} \tag{1}$$

for all sentences σ of $\mathcal{L}(M)$.

Proof. Since all sentences are constructed from atomic formulas using only $\wedge$, $\exists$ and $\neg$, it is enough to note that if (1) holds when $\sigma = \theta$, then it holds when $\sigma = \neg\theta$. □

Corollary (Compactness). *If every finite subset of a theory T has a model, then T has a model.*

Proof. Let I comprise the finite subsets of T. Each Γ in I determines a filter (Γ), namely the set

$$\{\Gamma' \in I : \Gamma \subseteq \Gamma'\}.$$

Any finite collection $\{(\Gamma_0), \dots, (\Gamma_{m-1})\}$ of subsets of I has intersection containing $\Gamma_0 \cup \dots \cup \Gamma_{m-1}$; so the intersection is non-empty. Hence some ultrafilter $\mathfrak{U}$ on I contains each (Γ). For each Γ in I, let $\mathfrak{M}^{(\Gamma)}$ be a model of Γ. If $\sigma \in T$, then $(\{\sigma\}) \subseteq \|\sigma\|$, so $\|\sigma\| \in \mathfrak{U}$. By the theorem of Łoś, $\prod_{\Gamma\in I} \mathfrak{M}^{(\Gamma)}/\mathfrak{U} \models T$. □

Let T be the set of sentences of $\mathcal{L}$ such that $\|\sigma\| \in \mathfrak{F}$. If $\mathfrak{U}$ is an ultrafilter on I that includes $\mathfrak{F}$, then

$$\mathfrak{M}/\mathfrak{U} \models T.$$

Conversely, suppose $\mathfrak{N} \models T$. The set $\{\|\sigma\| : \mathfrak{N} \models \sigma\}$ is closed under finite intersection. Also, if $\mathfrak{N} \models \sigma$, then $\|\sigma\|^{\mathrm{c}} \notin \mathfrak{F}$. Hence $\{\|\sigma\| : \mathfrak{N} \models \sigma\} \cup \mathfrak{F}$ is included in an ultrafilter $\mathfrak{U}$, such that

$$\mathfrak{N} \models \sigma \iff \|\sigma\| \in \mathfrak{U} \iff \mathfrak{M}/\mathfrak{U} \models \sigma$$

for all sentences σ of $\mathcal{L}$. We write

$$\mathfrak{N} \equiv \mathfrak{M}/\mathfrak{U},$$

and say that $\mathfrak{N}$ and $\mathfrak{M}/\mathfrak{U}$ are **elementarily equivalent**.

Example. Let T be the set of sentences of $\mathcal{L}_{\mathrm{r}}$, each of which is true in all but finitely many finite fields. Then

$$\prod_{q\in I} \mathbb{F}_q/\mathfrak{U} \models T,$$

where I is the set of prime powers, for all non-principal ultrafilters $\mathfrak{U}$ on I. Conversely, every model of T is elementarily equivalent to such an **ultraproduct**.

References

[1] Elisabeth Bouscaren, editor. *Model theory and algebraic geometry*, volume 1696 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1998. An introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture.

[2] C. C. Chang and H. J. Keisler. *Model theory*, volume 73 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, third edition, 1990.

[3] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1986.

[4] Wilfrid Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993.

[5] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.