Model theory, algebraic dynamics and local fields

Thomas Scanlon

University of California, Berkeley

7 June 2010

Model theory as a mathematical tool

In spite of its successes, the Model theory did not enter into a "tool box" of mathematicians and even many of mathematicians working on "Motivic integrations" are content to use the results logicians without understanding the details of the proofs.

Kazhdan on model theory

I don't know any mathematician who did not start as a logician and for whom it was "easy and natural" to learn the Model theory. Often the experience of learning of the Model theory is similar to the one of learning of Physics: for a [short] while everything is so simple and so easily reformulated in familiar terms that "there is nothing to learn" but suddenly one find himself in a place when Model theoreticians "jump from a tussock to a hummock" while we mathematicians don't see where to "put a foot" and are at a complete loss.

Kazhdan on model theory, continued

So we have two questions:
a) Why is the Model theory so useful in different areas of Mathematics?
b) Why is it so difficult for mathematicians to learn it ?

But really these two questions are almost the same- it is difficult to learn the Model theory since it appeals to different intuition. But exactly this new outlook leads to the successes of the Model theory.

What kinds of material will be covered?

With this tutorial I shall discuss

- some essential results from model theory which belong in every mathematician's tool box (*eg* the compactness theorem),
- some theorems in algebraic model theory which have direct applications to problems in number theory and geometry (*eg* the trichotomy theorem for difference fields), and
- the proofs of some theorems in Diophantine geometry using methods from model theory (*eg* Pila's proof of the André-Oort conjecture)

What will be omitted?

- Even with the parts of model theory most directly related to problems in Diophantine geometry, I will address only a small part of the theory.
- I will say a little about model theory as a subject in its own right, but I will focus on its interface with number theory. As such, we risk missing the source of the alternative intuitions provided by model theory.
- I will say nothing (other than to acknowledge now their existence) about the spectacular recent theorems of Hrushovski on approximate subgroups and of Goldbring on Hilbert's Fifth Problem.

Languages and structures

A model $\mathfrak{M}$ of a theory T is an $\mathscr{L}(\tau)$-structure for some signature τ which models every sentence from T.

- A signature τ consists of three sets $\mathscr{C}_\tau$ (constant symbols), $\mathscr{F}_\tau$ (function symbols), and $\mathscr{R}_\tau$ (relation symbols) together with functions arity : $\mathscr{F}_\tau \to \mathbb{Z}_+$ and arity : $\mathscr{R}_\tau \to \mathbb{Z}_+$
- An $\mathscr{L}(\tau)$-structure $\mathfrak{M}$ (sometimes called an interpretation) consists of a non-empty set M, for each $c \in \mathscr{C}_\tau$ an element $c^{\mathfrak{M}} \in M$, for each $f \in \mathscr{F}$ a function $f^{\mathfrak{M}} : M^{\text{arity}(f)} \to M$, and for each relation symbol $R \in \mathscr{R}_\tau$ a set $R^{\mathfrak{M}} =: R(\mathfrak{M}) \subseteq M^{\text{arity}(R)}$.

Example:Language of ordered rings

The signature τ for the language of ordered rings has two constant symbols 0 and 1, three function symbols $+$, $-$ and $\cdot$ where $\text{arity}(+) = \text{arity}(\cdot) = 2$ and $\text{arity}(-) = 1$, and a single relation symbol $\leq$ with $\text{arity}(\leq) = 2$.

Any ordered ring is naturally an $\mathscr{L}(\tau)$-structure, though we may have to write our functions in a somewhat nonstandard form in order to conform with the definition of an $\mathscr{L}(\tau)$-structure. For example, to regard $\mathbb{R}$ as an $\mathscr{L}(\tau)$-structure we would write $+^{\mathbb{R}}(x, y) = x + y$ where "$+$" on the right is the usual addition operation.

Just because we call τ the signature of ordered rings, there is no reason an $\mathscr{L}(\tau)$-structure must actually be an ordered ring.

Languages

Given a signature τ we build the language $\mathscr{L}(\tau)$ associated to τ by recursion.

- First, we define the set of terms, $\mathscr{T}(\tau)$, to be the smallest set containing $\mathscr{C}_\tau$, the set of variables $\{x_i : i \in \mathbb{N}\}$, and closed under the rule that if $f \in \mathscr{F}_\tau$, $t_1, \ldots, t_{\text{arity}(f)} \in \mathscr{T}(\tau)$, then so is $f(t_1, \ldots, t_{\text{arity}(f)})$.
- Next, we define the atomic formulae to be the expressions of the form $t = s$ and $R(t_1, \ldots, t_n)$ where $t, s, t_1, \ldots, t_n \in \mathscr{T}(\tau)$, $R \in \mathscr{R}_\tau$, and $n = \text{arity}(R)$.
- Finally, the language $\mathscr{L}(\tau)$ is the smallest set containing all of the atomic formulae and closed under the operations $\phi \in \mathscr{L}(\tau)$, then $\neg\phi \in \mathscr{L}(\tau)$, $\phi, \psi \in \mathscr{L}(\tau)$, then $(\phi \& \psi) \in \mathscr{L}(\tau)$ and $(\phi \vee \psi) \in \mathscr{L}(\tau)$, and $\phi \in \mathscr{L}(\tau)$ and $i \in \mathbb{N}$, then $(\exists x_i)\phi \in \mathscr{L}(\tau)$ and $(\forall x_i)\phi \in \mathscr{L}(\tau)$.

Truth

For an $\mathscr{L}(\tau)$-structure $\mathfrak{M}$ and sentence ϕ of $\mathscr{L}(\tau)$ we define the relation $\mathfrak{M} \models \phi$ (read "$\mathfrak{M}$ models ϕ" or "ϕ is true in $\mathfrak{M}$") by recursion on the construction of ϕ.

Allow me to omit the formal definition, but I will note one place where one should take care. If $\phi = (\exists x_i)\psi$, then the meaning of $\mathfrak{M} \models \phi$ should be that there is some element a of M for which ψ is true of a in $\mathfrak{M}$. To formalize this, we ask that there be an expansion of $\mathfrak{M}$ to a structure $\mathfrak{M}'$ in a language with a new constant symbol c and that $\mathfrak{M}' \models \psi(c/x_i)$ where $\psi(c/x_i)$ is obtained from ϕ by substituting c for each free occurrence of x_i.

Given a set T of $\mathscr{L}(\tau)$-sentences we say that $\mathfrak{M} \models T$ if for every $\phi \in T$ we have $\mathfrak{M} \models T$

Examples

- The class of groups is axiomatizable in $\mathscr{L}(\cdot, e)$ by the usual axioms of group theory properly formalized. For example associativity is expressed by

$$(\forall x_1)(\forall x_2)(\forall x_3) \cdot (x_1, \cdot(x_2, x_3)) = \cdot(\cdot(x_1, x_2), x_3)$$

- The class of infinite groups may be axiomatized by the above sentence and the infinite set of sentences expressing that the cardinality is at least n for each natural number n:

$$(\exists x_1)(\exists x_2) \cdots (\exists x_n) \bigwedge_{i<j} \neg(x_i = x_j)$$

(Here we write $\bigwedge_{i \in I} \phi_i$ for the conjunction of all the formulae ϕ_i indexed by $i \in I$.

- The class of cyclic groups is not axiomatizable in first-order logic.

Definable sets

For an $\mathscr{L}(\tau)$-formula $\phi(x_1, \ldots, x_n)$ with free variables amongst $x_1, \ldots, x_n$ and an $\mathscr{L}(\sigma)$-structure $\mathfrak{M}$ the set defined by ϕ in $\mathfrak{M}$,

$$\phi(\mathfrak{M}) := \{(a_1, \ldots, a_n) \in M^n : \mathfrak{M} \models \phi(a_1, \ldots, a_n)\}$$

While we speak of a definable *set*, we really think of a definable set as an assignment (functor with the appropriate notion of morphism) from the category of $\mathscr{L}(\tau)$-structures to the category of sets, $\mathfrak{M} \mapsto \phi(\mathfrak{M})$. If we wish to specify the actual set of points $\phi(\mathfrak{M})$ we may speak of a definable set in $\mathfrak{M}$.

We usually implicitly allow the possibility that the formula ϕ uses parameters from the model. If we need to restrict the set of possible parameters to some set A, then we say that the set is A-definable.

Elementary extensions

The right notion of morphism to make a definable set a functor is that of an elementary embedding.

Definition

Given two $\mathscr{L}(\tau)$-structures $\mathfrak{M}$ and $\mathfrak{N}$ an elementary embedding $f : \mathfrak{M} \to \mathfrak{N}$ is given by a function $f : M \to N$ having the property that for any $\mathscr{L}(\tau)$ formula $\phi(x_1, \ldots, x_n)$ with free variables amongst $x_1, \ldots, x_n$ and tuple $a \in M^n$ we have $\mathfrak{M} \models \phi(a) \iff \mathfrak{N} \models \phi(f(a))$. We write $\mathfrak{M} \preceq \mathfrak{N}$ when $M \subseteq N$ and the inclusion is an elementary embedding.

Examples of elementary embeddings

- If $f : \mathfrak{M} \to \mathfrak{N}$ is an isomorphism, then it is an elementary embedding.
- The map $\Phi : \mathbb{C}(t) \to \mathbb{C}(t)$ given by $f(t) \mapsto f(t^2)$ is isomorphism between $\mathbb{C}(t)$ and the image of Φ, but it is is not elementary as $\mathbb{C}(t) \models \neg(\exists x)x^2 = t$ but $\mathbb{C}(t) \models (\exists x)x^2 = \Phi(t)$.
- It follows from the Hilbert Nullstellensatz that is $K \subseteq L$ is an extension of algebraically closed fields, then the extension is elementary.

Examples of definable sets

- If $(K, +, \times, 0, 1)$ is an algebraically closed field, then a definable in K is simply a Zariski-constructible set. An $\varnothing$-definable set is a Zariski-constructible set defined over $\mathbb{Z}$ (in the algebraic geometric sense).
- If τ is a signature having only a binary relation symbol R, then an $\mathscr{L}(\tau)$-structure is a directed graph. In any such graph, the set of points with at most two out arrows is definable, but the set of points with the same number of in arrows as out arrows is not definable.
- In a group $(G, \cdot, e)$ for any $a \in G$ the centralizer of a in G is definable with a as a parameter, but the group generated by a is not generally definable.

More examples: periodic points

Let k be any Noetherian commutative ring and $X \subseteq \mathbb{A}^n_k$ be a closed subscheme of affine n-space over the integers. Then the associated functor of points $h_X : k - \mathrm{Alg} \to \mathrm{Set}$ may be identified with a definable set (relative to the theory of k-algebras). However, it is not the case that every definable set has this form. For example, if $\phi(x) := (\exists y) y^2 = x$, then there are k-algebras R for which $\phi(R) = \{a \in R : (\exists b \in R) b^2 = a\}$ is not the set of R-valued points of any k-scheme.

If $f : X \to X$ is a regular self-map and $n \in \mathbb{Z}_+$ then the set of points of exact period n is definable, but unless the order of the f-periodic points is uniformly bounded, the set of periodic points is not definable, even though for specific k-algebras R the set of f-periodic points in $X(R)$ might be definable for accidental reasons.