B

Concepts from model theory

Model theory is a branch of mathematical logic which investigates the structure behind collections of mathematical objects satisfying a given set of axioms. Its main feature is that the language — the distinguished elements, functions and relations — which can be used in talking about these objects is rigorously restricted. Since at the core they both share a finitary, symbolic approach, algebra and model theory enjoy a synergy which becomes especially visible in (real) algebraic geometry. This exposition of the basic terminology from model theory closely follows [Mar02].

Language and formula. A *language* $\mathcal{L}$ consists of three parts: (1) a set of function symbols $\mathcal{F}$, each $f \in \mathcal{F}$ with a certain arity n_f, (2) a set of relation symbols $\mathcal{R}$, each $R \in \mathcal{R}$ with a certain arity n_R, and (3) a set of constant symbols $\mathcal{C}$. The language of rings $\mathcal{L}_{\mathrm{r}}$ has two binary function symbols $+$ and $\cdot$, no distinguished relation and two constants 0 and 1. The language of ordered rings $\mathcal{L}_{\mathrm{or}}$ extends $\mathcal{L}_{\mathrm{r}}$ by a binary relation symbol $<$. Note that we do not include the equality relation $=$ at this point because it is part of the definition of formulas below.

Given a language $\mathcal{L} = (\mathcal{F}, \mathcal{R}, \mathcal{C})$ the set of *$\mathcal{L}$-terms* is defined recursively: (1) every $c \in \mathcal{C}$ is a term, (2) we allow an unbounded number of variable symbols v_i, which are terms, or (3) for $f \in \mathcal{F}$ and terms $t_1, \ldots, t_{n_f}$, the formal expression $f(t_1, \ldots, t_{n_f})$ is a term. Terms are expressions thought of having "values" in our domain of discourse. From the terms, we define $\mathcal{L}$-formulas recursively as well. An *atomic $\mathcal{L}$-formula* is: (1) $t_1 = t_2$ for two terms, or (2) $R(t_1, \ldots, t_{n_R})$ for $R \in \mathcal{R}$. These are the possible ways of turning terms into truth values given our language. An *$\mathcal{L}$-formula* is then any boolean combination using operations $\neg$, $\wedge$ and $\vee$ of atomic $\mathcal{L}$-formulas or quantified $\mathcal{L}$-formulas $\exists v_i : \phi$ or $\forall v_i : \phi$. The *free variables* of a formula are also defined recursively. All variables appearing in a term and an atomic formula are free. Under boolean connectives, sets of free variables are joined. The quantifiers $\exists v_i$ and $\forall v_i$ *bind* the variable v_i and remove it from the free variables of the quantified subformula. A formula without free variables is a *sentence*.

By renaming variables we can always avoid confusing edge cases where the same variable name appears both quantified and unquantified in the same formula, for example $v_1 > 0 \vee \exists v_1 : v_1 = v_2$ has free variables $\{ v_1, v_2 \}$ even though v_1 also appears as a *different* variable bound to the existential quantifier on the right-hand side of the disjunction. We emphasize that terms and formulas are mere strings, i.e., formal objects without any inherent meaning. In particular the terms $1 + 0$, $0 + 1$ and 1 in the language of rings are regarded as different.

Structure and theory. Meaning is created by interpreting terms and formulas inside of an *$\mathcal{L}$-structure*. An $\mathcal{L}$-structure $\mathcal{M}$ consists of a set M, a function $f^{\mathcal{M}} : \mathcal{M}^{n_f} \to \mathcal{M}$ for each function symbol $f \in \mathcal{F}$, a relation $R^{\mathcal{M}} \subseteq \mathcal{M}^{n_R}$ for each relation symbol $R \in \mathcal{R}$, and a constant $c^{\mathcal{M}} \in \mathcal{M}$ for each constant symbol $c \in \mathcal{C}$. From the way terms and formulas have been defined, it is clear how to interpret them in a given structure by recursive substitution. Terms are M-valued expressions and hence they can be viewed as functions $M^k \to M$ where k is the number of variables appearing in the term; formulas make boolean assertions about relations of elements from M. It is important to note that quantifiers only range over elements of M. We cannot express the existence of an arbitrary subset, function or relation on M, for example. This restriction may be lifted by introducing additional quantifier symbols leading to higher-order logics, but we will not do so here. Instead, we remain in *first-order logic* where quantifiers range only over elements of the domain.

A sentence ϕ in language $\mathcal{L}$ has a truth value in every $\mathcal{L}$-structure $\mathcal{M}$. If this value is true, then $\mathcal{M}$ *satisfies* ϕ, or equivalently ϕ is *true* in $\mathcal{M}$, and we write $\mathcal{M} \models \phi$. For a general formula ϕ, the truth value depends on the values assigned to its free variables $v_{i_1}, \ldots, v_{i_k}$. We therefore view the formula as a function $\phi(v_{i_1}, \ldots, v_{i_k})$ and for each k-tuple $a \in M^k$ we obtain a sentence $\phi(a)$ with a well-defined truth value. This formula *satisfiable* in $\mathcal{M}$ if $\mathcal{M} \models \exists v_{i_1}, \ldots, v_{i_k} : \phi$ and *tautological* if $\mathcal{M} \models \forall v_{i_1}, \ldots, v_{i_k} : \phi$. The short summary of these definitions is that everything is exactly as a trained mathematician would expect it to be. We will usually be more lax with the notation, using for example $p \Rightarrow q$ as an abbreviation of $\neg p \vee q$, place parentheses only where necessary and write $+(1, 1)$ in the customary fashion as $1 + 1$.

So far anything can be an $\mathcal{L}$-structure. Even if we name the function symbols suggestively $+$ and $\cdot$ and the constants 0 and 1, their interpretation in an $\mathcal{L}$-structure does not have to conform with any requirements except the arity of functions and relations. To impose requirements, we write them down as $\mathcal{L}$-sentences and treat them as *axioms*. The axioms of rings can be written down as a finite collection $\mathfrak{A}$ of $\mathcal{L}_{\mathrm{r}}$-sentences then the $\mathcal{L}_{\mathrm{r}}$-structures $\mathcal{M}$ which satisfy every sentence in $\mathfrak{A}$, written $\mathcal{M} \models \mathfrak{A}$, are the *models* of $\mathfrak{A}$ — they must be rings. Conversely, given an $\mathcal{L}$-structure $\mathcal{M}$, we obtain the collection $\mathrm{Th}(\mathcal{L})$ of all $\mathcal{L}$-sentences true in $\mathcal{M}$ which is the *theory* of $\mathcal{M}$.

An *$\mathcal{L}$-theory* is any set of $\mathcal{L}$-sentences $\mathfrak{A}$. We can consider the enlarged set $\overline{\mathfrak{A}}$ containing all sentences ϕ such that $\mathcal{M} \models \phi$ for all models $\mathcal{M}$ of $\mathfrak{A}$. These ϕ are *consequences* of $\mathfrak{A}$ and we write $\mathfrak{A} \models \phi$. A theory is *sound* if does not contain ϕ and $\neg\phi$ for any sentence ϕ. It is *complete* if it contains at least one of the two.

For example, the $\mathcal{L}_{\mathrm{r}}$-sentence $\forall x, y : (xy = 0 \Rightarrow x = 0 \vee y = 0)$ forbids zero divisors in a ring and adding $\forall x : x = 0 \vee \exists y : xy = 1$ to the ring axioms axiomatizes fields. Algebraically closed fields are then axiomatized by adding countably infinitely many $\mathcal{L}_{\mathrm{r}}$-sentences, one for each degree that a polynomial can have:

$$\forall a_0, \ldots, a_n \exists x : a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

In this expression we use many convenient abbreviations like x^n from mathematical practise which are not covered by our definition of $\mathcal{L}_{\mathrm{r}}$-formula, but of course all these abbreviations can be expanded for each fixed n.

Definability. Let $\mathcal{L}$ be a language and $\mathcal{M}$ an $\mathcal{L}$-structure. A subset $X \subseteq \mathcal{M}^n$ is *definable* if there is an $\mathcal{L}$-formula $\phi(v_1, \ldots, v_n, w_1, \ldots, w_m)$ with free variables $v_1, \ldots, v_n$ and $w_1, \ldots, w_m$ and a choice $b \in M^m$ such that

$$X = \{\, a \in M^n : \mathcal{M} \models \phi(a, b) \,\}.$$

To emphasize that b comes from a certain subset $B \subseteq M$, we also say that X is *B-definable* in $\mathcal{M}$.

Everything we can talk about — the axioms used to specify our class of models, the facts expressible about models and the formulas defining subsets — is restricted by the chosen language $\mathcal{L}$. The same structure may be studied in different languages, for example $\mathbb{R}$ may be studied as a field or as an ordered field or as an ordered commutative group. In the language of (ordered) rings and after imposing the ring axioms, every term is equivalent to a polynomial with integer coefficients. Hence, the sets definable in $\mathcal{L}_\mathrm{r}$ over a field using atomic formulas are varieties. The quantifier-free definable sets are finite unions and intersections of varieties or their complements. Over an algebraically closed field, these are in fact all the definable sets and they are called *constructible sets* in algebraic geometry.

Quantifier elimination. Since $\mathbb{R}$ is real-closed and by Corollary 1.17 the formulas $x > 0$ and $\exists y : y^2 x = 1$ define the same set of positive elements of $\mathbb{R}$. One of them is formulated in the sublanguage of rings but requires a quantifier while the other uses the language of ordered rings and is quantifier-free. A crucial question in model theory is whether a theory admits such an "elimination of quantifiers": can every first-order definable set be defined by quantifier-free formulas?

An $\mathcal{L}$-theory $\mathfrak{A}$ has *quantifier elimination* if for every $\mathcal{L}$-formula ϕ there exists a quantifier-free $\mathcal{L}$-formula ψ such that $\mathfrak{A} \models \phi \Leftrightarrow \psi$. In particular, this property makes all definable sets quantifier-free definable. Quantifier elimination has desirable algorithmic consequences: the naïve approach to deciding whether a given formula is satisfiable is to iterate over all elements of the domain to check if plugging them in makes the formula true. This algorithm is successful (but inefficient) if the domain is finite, it may not terminate if the domain is countably infinite (recursively enumerable to be precise) and it is not sensible if the domain is uncountable. However, quantifier elimination removes all quantifiers and thus the need for searching in the domain. If quantifier elimination can be done algorithmically and if the set of quantifier-free sentences is decidable in the given theory, then the entire first-order theory is decidable.

Quantifier elimination in ACF. The theory ACF of algebraically closed fields has quantifier elimination in the language $\mathcal{L}_\mathrm{r}$ and it is decidable. Furthermore, each theory ACF_p of algebraically closed fields of characteristic p (prime or zero) has quantifier elimination in $\mathcal{L}_\mathrm{r}$ and they are all complete and decidable.

In particular every sentence such as $\forall x : px = 0$, where p is a fixed integer, is equivalent to a quantifier-free formula ψ, but in a sentence every variable is bound by a quantifier, so ψ cannot contain any variables. It follows that any such ψ is a boolean formula over variable-less sentences in the language of rings. These are all of the form $m = n$ for integers m, n. The sentence $\forall x : px = 0$, for example, is equivalent to $p = 0$.

The boolean combination of these sentences points out exactly which characteristics make the sentence true.

The reason why ACF is not complete is because there exist algebraically closed fields of different characteristics. So a sentence like $2 = 0$ is neither correct (there exist algebraically closed fields where this is false) nor is its negation correct (there also exist algebraically closed fields where $2 = 0$ is true). The completeness of ACF_p shows that these are the only type of sentence obstructing the completeness of ACF.

The fact that existential quantifiers can be eliminated in the language of rings, given the theory of algebraically closed fields, implies that the image of a coordinate projection of any constructible set is constructible:

Chevalley's Theorem. Over an algebraically closed field, a projection of a constructible set is constructible.

The goal of Chapter 3 is to prove that the theory of real-closed fields, likewise, has quantifier elimination in the language of ordered rings. This entails that projections of semialgebraic sets are semialgebraic and many other important theorems in real algebraic geometry, which are the subject of Chapter 4.