Introduction to Model Theory

David Marker
University of Illinois at Chicago

My goal in these lectures is to introduce some of the basic concepts and results from model theory, starting from scratch. As my time is quite limited the topics covered will be tailored to the model theory of fields and the later lectures this week. I will be using algebraically closed fields to illustrate most of these ideas. The tools I will be describing are quite basic and most of this material is due either to Alfred Tarski or Abraham Robinson. At the end I will give some general references.

§1 Languages and Structures

What is a mathematical structure? Some examples of mathematical structures we have in mind are the ordered additive group of integers, the complex field, and the ordered real field with exponentiation.

To specify a structure we must specify the underlying set, some distinguished operations, some distinguished relations and some distinguished elements. For example, the ordered additive group of integers has underlying set $\mathbf{Z}$ and we distinguish the binary function $+$, the binary relation $<$ and the identity element 0. For the ordered field of real numbers with exponentation we have underlying set $\mathbf{R}$ and might distinguish the binary functions $+$ and $\times$, the unary function exp, the binary relation $<$ and the elements 0 and 1.

Here is the formal definition.

Definition 1.1 A *structure* $\mathcal{M}$ is given by the following data.

i) A set M called the *universe* or *underlying set* of $\mathcal{M}$.

ii) A collection of functions $\{f_i : i \in I_0\}$ where $f_i : M^{n_i} \to M$ for some $n_i \geq 1$.

iii) A collection of relations $\{R_i : i \in I_1\}$ where $R_i \subseteq M^{m_i}$ for some $m_i \geq 1$.

iv) A collection of distinguished elements $\{c_i : i \in I_3\} \subseteq M$.

Any (or all) of the sets I_0, I_1 and I_2 may be empty. We refer to n_i and m_j as the *arity* of f_i and R_j.

Here are some examples:

1) The ordered field of real numbers has domain $\mathbf{R}$, binary functions $+, -, \times$, relation $<$, and distinguished elements 0 and 1.

2) The valued field of p-adic numbers has domain $\mathbf{Q}_p$, binary functions $+, -, \times$, distinguished elements 0 and 1, and a unary relation $\mathbf{Z}_p$ for the ring of integers.

In mathematical logic we study structures by examining the sentences of first order logic true in those structures. To any structure we attach a language $\mathcal{L}$ where we have an n_i-ary function symbol $\widehat{f_i}$ for each f_i, an m_i-ary relation symbol $\widehat{R_i}$ for each R_i and constant symbols $\widehat{c_i}$ for each c_i.

An $\mathcal{L}$-*structure* is a structure $\mathcal{M}$ where we can interpret all of the symbols of $\mathcal{L}$. For example, let $\mathcal{L}$ be the language where we have a binary function symbol $\widehat{\times}$ and a constant symbol $\widehat{1}$. The following are examples of $\mathcal{L}$-structures:

1) $\mathcal{M}_1$ has underlying set $\mathbf{Q}$. We interpret $\widehat{\times}$ as $\times$ and $\widehat{1}$ as 1.

2) $\mathcal{M}_2$ has underlying set $\mathbf{Z}$. We interpret $\widehat{\times}$ as $+$ and $\widehat{1}$ as 0.

Of course we also could take the natural interpretation of $\mathcal{L}$ in $\mathbf{Z}$.

3) $\mathcal{M}_3$ has underlying set $\mathbf{Z}$. We interpret $\widehat{\times}$ as $\times$ and $\widehat{1}$ as 1.

Definition If $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{L}$-structures with underlying sets M and N, respectively, an $\mathcal{L}$-*embedding*, $\sigma : M \to N$ is an injective map that preserves the interpretation of all function symbols, relation symbols and constant symbols of $\mathcal{L}$. An $\mathcal{L}$-*isomorphism* is bijective $\mathcal{L}$-embedding.

We say that $\mathcal{M}$ is a substructure of $\mathcal{N}$ (and write $\mathcal{M} \subset \mathcal{N}$) if $M \subset N$ and the inclusion map is an $\mathcal{L} - embedding$.

Formulas in our language are finite strings made from the symbols of $\mathcal{L}$, the equality relation $=$, variables $x_0, x_1, \ldots$, the logical connectives $\neg, \wedge, \vee$, quantifiers $\exists$ and $\forall$ and parenthesis. * We interpret $\neg, \wedge, \vee$ as "not", "and" and "or" and $\exists$ and $\forall$ as "there exists" and "for all". I will use $x, y, z \ldots$ as variables and not use $\widehat{\ }$'s when no confusion arises.

Let $\mathcal{L}_{\mathrm{r}}$ be the language of rings where we have binary function symbols $+, -$ and $\times$ and constant symbols 0 and 1. The language of ordered rings, $\mathcal{L}_{\mathrm{or}}$ is $\mathcal{L}_{\mathrm{r}}$ with an additional binary relation symbol $<$. (As usual we will write $x + y$ instead of $+(x, y)$ and $x < y$ for $<(x, y)$.) Here are some examples of $\mathcal{L}_{\mathrm{or}}$-formulas.

$x_1 = 0 \vee x_1 > 0$
$\exists x_2 \ x_2 \times x_2 = x_1$
$\forall x_1 \ (x_1 = 0 \vee \exists x_2 \ x_2 \times x_1 = 1)$

Intuitively the first formula asserts that $x_1 \geq 0$, the second asserts that x_1 is a square and the third asserts that every nonzero element has a multiplicative inverse. We would like to define what it means for a formula to be true in a structure, but these examples already show one difficulty. While in any $\mathcal{L}_{\mathrm{or}}$-structure the third formula will either be true or false, the first two formulas express a property which may or may not be true of elements of the structure.

We say that a variable *occurs freely* in a formula ϕ if it is not inside the scope of a quantifier, otherwise we say it is *bound*. For example x_1 is free in the first two formulas and bound in the third, while x_2 is bound in both formulas.

We call a formula a *sentence* if it has no free variables. For any $\mathcal{L}$-structure each sentence of $\mathcal{L}$ is either true or false. If ϕ is a sentence we say that $\mathcal{M}$ is a model of ϕ and write $\mathcal{M} \models \phi$ if and only if ϕ is true in $\mathcal{M}$.

We often write $\phi(x_1, \ldots, x_n)$ to show that the variables $x_1, \ldots, x_n$ are free in the formula ϕ. We think of $\phi(x_1, \ldots, x_n)$ as describing a property of n-tuples from M. For example, the $\mathcal{L}_{\mathrm{or}}$ formula $\exists x_2 \ x_2 \times x_2 = x_1$, has the single free variable x_1 and describes

* I give precise definitions in the appendix.

the property "x_1 is a square". If $a_1, \ldots, a_n$ are elements of M we say $\mathcal{M} \models \phi(a_1, \ldots, a_n)$ if the property expressed by ϕ is true of the tuple $(a_1, \ldots, a_n)$.

We say that two $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent* if for all $\mathcal{L}$-sentences $\mathcal{M} \models \phi$ iff $\mathcal{N} \models \phi$.

Proposition 1.2 If $\mathcal{M}$ and $\mathcal{N}$ are isomorphic, then they are elementarily equivalent.

Proof

Show by induction on formulas that if $\phi(x_1, \ldots, x_n)$ is a formula, $\sigma : M \to N$ is an isomorphism and $a_1, \ldots, a_n \in M$, then

$$\mathcal{M} \models \phi(a_1, \ldots, a_n) \Leftrightarrow \mathcal{N} \models \phi(\sigma(a_1), \ldots, \sigma(a_n)).$$

We say that an $\mathcal{L}$-embedding $f : \mathcal{M} \to \mathcal{N}$ is *elementary* if for any $a_1, \ldots, a_n \in M$ and any formula $\phi(x_1, \ldots, x_n)$

$$\mathcal{M} \models \phi(a_1, \ldots, a_n) \Leftrightarrow \mathcal{N} \models \phi(f(a_1), \ldots, f(a_n)).$$

If $\mathcal{M} \subset \mathcal{N}$ we say that $\mathcal{M}$ is an *elementary substructure* if the inclusion map is elementary.

Definition We say that a set $X \subset M^n$ is *definable* in the $\mathcal{L}$-structure $\mathcal{M}$ if there is a formula $\phi(x_1, \ldots, x_{n+m})$ and elements $b_1, \ldots, b_m \in M$ such that

$$X = \{(a_1, \ldots, a_n) : \mathcal{M} \models \phi(a_1, \ldots, a_n, b_1, \ldots, b_m)\}.$$

We say that X is *A-definable* or *definable over A* where $A \subseteq M$, if we can choose that $b_1, \ldots, b_m \in A$. For example if $m = 0$ we say X is $\emptyset$-definable.

For example $\{x : x > \pi\}$ is definable over $\mathbf{R}$ but not $\emptyset$- definable, while $\{x : x > \sqrt{2}\}$ is $\emptyset$-definable by the formula $x \times x > 1 + 1 \wedge x > 0$. In the field $(\mathbf{Q}_p, +, -, \times, 0, 1)$ if $p \neq 2$ we can define the valuation ring $\mathbf{Z}_p$ by the formula $\exists y \; y^2 = px^2 + 1$.

We can give a very simple characterization of the definable sets.

Proposition 1.3 Suppose that D_n is a collection of subsets of M^n for all $n \geq 1$ such that $\mathcal{D} = (D_n : n \geq 1)$ is the smallest collection such that:

i) $M^n \in D_n$;

ii) for all n-ary functions f of $\mathcal{M}$, the graph of f is in D_{n+1};

iii) for all n-ary relations R of $\mathcal{M}$, $R \in D_n$;

iv) for all $i, j \leq n$, $\{(x_1, \ldots, x_n) \in M^n : x_i = x_j\} \in D_n$;

v) each D_n is closed under complement, union and intersection;

vi) if $X \in D^m$ and $\pi : M^n \to M^m$ is the projection map $(x_1, \ldots, x_n) \mapsto (x_{i_1}, \ldots, x_{i_m})$, then $\pi^{-1}(X) \in D_n$;

vii) if $X \in D^n$ and π is as above, then $\pi(X) \in D_m$.

viii) if $X \in D_{n+m}$ and $b \in M^m$, then $\{a \in M^n : (a, b) \in X\} \in D_n$.

Then $X \subseteq M^n$ is definable if and only if $X \in D_n$.

§2 Theories

An $\mathcal{L}$-*theory* is a set of $\mathcal{L}$-sentences. Theories arise naturally as we attempt to axiomatize the properties of mathematical structures. For example if $\mathcal{L}_{\rm r}$ is the language of rings we can write down the field axioms as $\mathcal{L}_{\rm r}$ sentences. We can give the theory of algebraically closed fields (ACF) by taking the field axioms plus for each $n \geq 1$, the axiom

$$\forall x_0 \forall x_1 \ldots \forall x_{n-1} \exists y \; y^n + x_{n-1}y^{n-1} + \ldots x_1 y + x_0 = 0.$$

We say that an $\mathcal{L}$-sentence ϕ is a *logical consequence* of an $\mathcal{L}$-theory T (and write $T \models \phi$) if and only if $\mathcal{M} \models \phi$ for all $\mathcal{M} \models T$. For example ACF$\models \forall x \forall y \exists z \; x^2 + y^2 = z^2$.

Gödel's Completeness Theorem (version 1) 2.1 $T \models \phi$ if and only if there is a formal proof of ϕ using assumptions from T.

This has a very useful reformulation with an important corollary. We say that an $\mathcal{L}$-theory T is *satisfiable* if and only if there is an $\mathcal{L}$-structure $\mathcal{M}$ with $\mathcal{M} \models T$ and we say that T is consistent if and only if we can not formally derive a contradiction from T.

Completeness Theorem (version 2) 2.2 T is satisfiable if and only if T is consistent. Moreover if T has infinite models then T has a model where the underlying set has cardinality κ, for all $\kappa \geq |\mathcal{L}| + \aleph_0$.

This has an easy consequence which is the cornerstone of model theory.

Compactness Theorem 2.3 If every finite subset of T is satisfiable, then T is satisfiable.

Proof If T is not satisfiable, then by 2.2 there is a proof of a contradiction from T. As proofs use only finitely many assumptions from T there is a finite inconsistent subset of T.

An important question when we try to axiomatize the properties of a structure is have we said everything we can say. An $\mathcal{L}$-theory T is *complete* if for all $\mathcal{L}$-sentences ϕ either $T \models \phi$ or $T \models \neg\phi$. Another way to say this is that a theory is complete if any two models are elementarily equivalent.

The easiest way to get a complete theory is to take the complete theory of a structure. If $\mathcal{M}$ is a structure, let $\mathrm{Th}(\mathcal{M}) = \{\phi : \mathcal{M} \models \phi\}$.

Gödel's incompleteness theorem says that Peano axioms are not complete (and there is no reasonable way to complete them). It is easy to see that ACF is not complete as it does not decide the characteristic. For p a prime number let ψ_p be the sentence

$$\forall x \;\; \underbrace{x + \ldots + x}_{p \text{ times}} = 0.$$

Clearly neither ψ_p nor $\neg\psi_p$ is a logical consequence of ACF. But this is the only obstruction. Let ACF_p be the theory obtained by adding ψ_p to ACF and let ACF_0 be the theory obtained by adding to ACF the sentences $\{\neg\psi_p : p \text{ a prime }\}$. We show shortly that ACF_p is complete.

If κ is a cardinal, we say that a theory T is *κ-categorical* if any two models of T where the underlying set has cardinality κ are isomorphic. Since algebraically closed fields are determined up to isomorphism by their characteristic and transcendence degree it is easy to see that ACF_p is κ-categorical for all $\kappa \geq \aleph_1$.

Vaught's Test 2.4 If all models of T are infinite and T is κ-categorical for some infinite cardinal κ, then T is complete.

Proof Suppose not. Then $T \cup \{\phi\}$ and $T \cup \{\neg\phi\}$ are satisfiable. By 2.2 we can find κ and $\mathcal{M}$ and $\mathcal{N}$ of cardinality κ such that $\mathcal{M} \models T + \phi$ and $\mathcal{N} \models T + \neg\phi$. But this is impossible as $\mathcal{M}$ must be isomorphic to $\mathcal{N}$.

Thus ACF_p is complete for $p \geq 0$. This can be thought of as a version of the Lefschetz principle.

Corollary 2.5 Let ϕ be an $\mathcal{L}_{\mathrm{r}}$-sentence. The following are equivalent.

i) ϕ is true in the complex numbers.

ii) ϕ is true in every algebraically closed field of characteristic zero.

iii) ϕ is true in some algebraically closed field of characteristic zero.

iv) There are arbitrarily large primes p such that ϕ is true in some algebraically closed field of characteristic p.

v) There is an m such that for all $p > m$, ϕ is true in all algebraically closed fields of characteristic p.

Proof

The equivalence of i)-iii) is just the completeness of ACF_0 and v)$\Rightarrow$ iv) is obvious.

For ii) $\Rightarrow$ v) suppose $\mathrm{ACF}_0 \models \phi$. By the completeness theorem, there is a proof of ϕ from ACF_0. That proof only uses finitely many assertions $\neg\psi_q$, thus for large enough p, $\mathrm{ACF}_p \models \phi$.

For iv$\Rightarrow$ii) suppose $\mathrm{ACF}_0 \not\models \phi$. By completeness $\mathrm{ACF}_0 \models \neg\phi$. By the above argument, $\mathrm{ACF}_p \models \neg\phi$ for sufficiently large p, thus iv) fails.

This result has a striking application.

Theorem 2.6 (Ax) Let $F : \mathbf{C}^n \to \mathbf{C}^n$ be an injective polynomial map, then F is surjective.

Proof Suppose not. Let $X = (X_1, \ldots, X_n)$. Let $F(X)$ be a counterexample where $F(X) = (F_1(X), \ldots, F_n(X))$ where each $F_i \in \mathbf{C}[X]$ has degree at most d. There is an $\mathcal{L}$-sentence $\Phi_{n,d}$ such that for K a field, $K \models \Phi_{n,d}$ if and only if every injective polynomial map $G : K^n \to K^n$ where each coordinate function has degree at most d is surjective. We can quantify over polynomials of degree at most d by quantifying over the coefficients. For example $\Phi_{2,2}$ is the sentence:

$\forall a_{0,0}\forall a_{0,1}\forall a_{0,2}\forall a_{1,0}\forall a_{1,1}\forall a_{2,0}\forall b_{0,0}\forall b_{0,1}\forall b_{0,2}\forall b_{1,0}\forall b_{1,1}\forall b_{2,0}\Big[(\forall x_1\forall y_1\forall x_2\forall y_2$ $((\sum a_{i,j}x_1^iy_1^j = \sum a_{i,j}x_2^iy_2^j \wedge \sum b_{i,j}x_1^iy_1^j = \sum b_{i,j}x_2^iy_2^j) \rightarrow (x_1 = x_2 \wedge y_1 = y_2)) \rightarrow$ $\forall u\forall v\exists x\exists y \sum a_{i,j}x^iy^j = u \wedge \sum b_{i,j}x^yy^j = v\Big].$

If K is a finite field then $K \models \Phi_{n,d}$. It follows that $\Phi_{n,d}$ holds in any increasing union of finite fields. In particular the algebraic closure of a finite field satisfies $\Phi_{n,d}$. Hence by 2.5, $\mathbf{C} \models \Phi_{n,d}$, a contradiction.

Originally logicians looked for completeness results because they lead to decidability results.

Corollary 2.7 The theory ACF_p is decidable for $p \geq 0$. That is, for each p there is an algorithm which for each sentence ϕ will determine if $\mathrm{ACF}_p \models \phi$.

Proof By the completeness of ACF_p and the completeness theorem either there is a proof of ϕ or a proof of $\neg\phi$ from ACF_p. We can systematically search all finite sequences of symbols and test each one to see if it is a valid proof of either ϕ or $\neg\phi$. Eventually we will find one or the other.

§3 Quantifier Elimination

Let F be a field. If $p(X_1,\ldots,X_n) \in F[X_1,\ldots,X_n]$, then $\{x \in F^n : p(x) = 0\}$ is defined by a quantifier free $\mathcal{L}_{\mathrm{r}}$-formula. We say that a subset of F^n is *constructible* if it is a boolean combination of zero sets of polynomials in $F[X_1,\ldots,X_n]$. It is easy to see that the subsets of F^n defined by quantifier free formulas are exactly the constructible subsets of F^n. If F is an algebraically closed field then Chevalley's theorem from algebraic geometry asserts that the projection of a constructible subset of F^{n+1} to F^n is constructible. Restating this model theoreticaly, this says that every definable set is constructible.

This is of course not true for non-algebraically closed fields. In the reals we can define the ordering by:

$$x < y \Leftrightarrow \exists z\ z \neq 0 \wedge x + z^2 = y,$$

but this is not a constructible subset of $\mathbf{R}^2$. Here this is the only problem. We say that a subset of an ordered field is *semialgebraic* if it is a boolean combination of zero sets of polynomials and polynomial inequalities (like $\{x : p(x) > 0\}$). It is easy to see that the semialgebraic sets are exacty the sets defined by quantifier free $\mathcal{L}_{\mathrm{or}}$-formulas. The Tarski-Seidenberg theorem says that in the reals (or more generally in a real closed fields) the projection of a semialgebraic set is semialgebraic. Thus in the real field the definable sets are exactly the semialgebraic sets.

In model theory we study the definable sets of a structure. Even when we can not eliminate quantifiers this is a rich, interesting and fruitful pursuit. Quantifier elimination results are very useful as often one can show the quantifier free definable sets have good geometric properties while the definable sets have strong closure properties. For example suppose $A \subseteq \mathbf{R}^n$ is semialgebraic. We want to show that the closure of A is also semialgebraic. Since A is definable there is an $\mathcal{L}_{\rm or}$-formula $\phi(x_1, \ldots, x_n, a_1, \ldots, a_m)$ that defines A. Then the formula

$$\forall \epsilon > 0 \exists y_1 \ldots \exists y_n \; (\phi(y_1, \ldots, y_n, a_1, \ldots, a_m) \wedge (x_1 - y_1)^2 + \ldots + (x_n - y_n)^2 < \epsilon)$$

defines the closure of A. Since the closure of A is definable it is semialgebraic.

In the structure $(\mathbf{Q}, +, \times, 0, 1)$ we can also define the ordering as nonnegative elements are sums of four squares. In fact things are much worse. Julia Robinson showed that the integers are definable in the field of rational numbers. By Gödel's incompleteness theorem this implies that the theory of the rational numbers is undecidable and the definable subsets are quite complicated.

There is a useful model theoretic test for quantifier elimiantion.

Theorem 3.1 Let $\mathcal{L}$ be a language containing at least one constant symbol. Let T be an $\mathcal{L}$ theory and let $\phi(v_1, \ldots, v_m)$ be an $\mathcal{L}$ formula with free variables $v_1, \ldots, v_m$ (we allow the possibility that $m = 0$). The following are equivalent:

i) There is a quantifier free $\mathcal{L}$-formula $\psi(v_1, \ldots, v_m)$ such that $T \models \forall \bar{v} \; (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$

ii) If $\mathcal{A}$ and $\mathcal{B}$ are models of T, $\mathcal{C} \subseteq \mathcal{A}$ and $\mathcal{C} \subseteq \mathcal{B}$, then $\mathcal{A} \models \phi(\bar{a})$ if and only if $\mathcal{B} \models \phi(\bar{a})$ for all $\bar{a} \in \mathcal{C}$.

Proof

[i) $\rightarrow$ ii)]: Suppose $T \models \forall \bar{v} \; (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$, where ψ is quantifier free. Let $\bar{a} \in \mathcal{C}$ where $\mathcal{C}$ is a substructure of $\mathcal{A}$ and $\mathcal{B}$ and the later two structures are models of T. Since quantifier free formulas are preserved under substructure and extension

$$\begin{aligned} \mathcal{A} \models \phi(\bar{a}) &\leftrightarrow \mathcal{A} \models \psi(\bar{a}) \\ &\leftrightarrow \mathcal{C} \models \psi(\bar{a}) \;\; \text{(since } \mathcal{C} \subseteq \mathcal{A}) \\ &\leftrightarrow \mathcal{B} \models \psi(\bar{a}) \;\; \text{(since } \mathcal{C} \subseteq \mathcal{B}) \\ &\leftrightarrow \mathcal{B} \models \phi(\bar{a}). \end{aligned}$$

[ii) $\rightarrow$ i)]. First, if $T \models \forall \bar{v} \; \phi(\bar{v})$, then $T \models \forall \bar{v} \; (\phi(\bar{v}) \leftrightarrow c = c)$. Second, if $T \models \forall \bar{v} \; \neg\phi(\bar{v})$, then $T \models \forall \bar{v} \; (\phi(\bar{v}) \leftrightarrow c \neq c)$. In fact, if ϕ is not a sentence we could use "$v_1 = v_1$" in place of $c = c$.

Thus we may assume that both $\phi(\bar{v})$ and $\neg\phi(\bar{v})$ are consistent with T.

Let $\Gamma(\bar{v}) = \{\psi(\bar{v}) : \psi$ is quantifier free and $T \models \forall \bar{v} \; (\phi(\bar{v}) \rightarrow \psi(\bar{v}))\}$. Let $d_1, \ldots, d_m$ be new constant symbols. We will show that $T + \Gamma(\bar{d}) \models \phi(\bar{d})$. Thus by compactness there are $\psi_1, \ldots, \psi_n \in \Gamma$ such that $T \models \forall \bar{v} \; (\bigwedge \psi_i(\bar{v}) \; \rightarrow \phi(\bar{v}))$. So $T \models \forall \bar{v} \; (\bigwedge \psi_i(\bar{v}) \; \leftrightarrow \phi(\bar{v}))$ and $\bigwedge \psi_i(\bar{v})$ is quantifier free. We need only prove the following claim.

claim. $T + \Gamma(\bar{d}) \models \phi(\bar{d})$.

Suppose not. Let $\mathcal{A} \models T + \Gamma(\bar{d}) + \neg\phi(\bar{d})$. Let $\mathcal{C}$ be the substructure of $\mathcal{A}$ generated by $\bar{d}$. [Note: if $m = 0$ we need the constant symbol to ensure $\mathcal{C}$ is non-empty.]

Let Diag($\mathcal{C}$) be the set of all atomic and negated atomic formulas with parameters from $\mathcal{C}$ that are true in $\mathcal{C}$.

Let $\Sigma = T + \mathrm{Diag}(\mathcal{C}) + \phi(\bar{d})$. If Σ is inconsistent, then there are quantifier free formulas quantifier free formulas $\psi_1(\bar{d}), \ldots, \psi_n(\bar{d}) \in \mathrm{Diag}(\mathcal{C})$, such that $T \models \forall \bar{v}\ (\bigwedge \psi_i(\bar{v} \to \neg\phi(\bar{v}))$. But then $T \models \forall \bar{v}\ (\phi(\bar{v}) \to \bigvee \neg\psi_i(\bar{v}))$. So $\bigvee \neg\psi_i(\bar{v}) \in \Gamma$ and $\mathcal{C} \models \bigvee \neg\psi_i(\bar{d})$, a contradiction. Thus Σ is consistent.

Let $\mathcal{B} \models \Sigma$. Since $\Sigma \supseteq \mathrm{Diag}(\mathcal{C})$, we may assume that $\mathcal{C} \subseteq \mathcal{B}$. But by a), since $\mathcal{A} \models \neg\phi(\bar{d})$, $\mathcal{B} \models \neg\phi(\bar{d})$, a contradiction.

The next lemma shows that to prove quantifier elimination for a theory we need only prove quantifier elimination for formulas of a very simple form.

Lemma 3.2 Suppose that for every quantifier free $\mathcal{L}$-formula $\theta(\bar{v}, w)$, there is a quantifier free $\psi(\bar{v})$ such that $T \models \forall \bar{v}\ (\exists w\ \theta(\bar{v}, w) \leftrightarrow \psi(\bar{v}))$. Then every $\mathcal{L}$-formula $\phi(\bar{v})$ is provably equivalent to a quantifier free $\mathcal{L}$-formula.

Proof. We prove this by induction on the complexity of ϕ.

This is clear if $\phi(\bar{v})$ is quantifier free.

For $i = 0, 1$ suppose that $T \models \forall \bar{v}\ (\theta_i(\bar{v}) \leftrightarrow \psi_i(\bar{v}))$ where ψ_i is quantifier free.
If $\phi(\bar{v}) = \neg\theta_0(\bar{v})$, then $T \models \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow \neg\psi_0(\bar{v}))$.
If $\phi(\bar{v}) = \theta_0(\bar{v}) \wedge \theta_1(\bar{v})$, then $T \models \forall v\ (\phi(\bar{v}) \leftrightarrow (\psi_0(\bar{v}) \wedge \psi_1(\bar{v})))$.
In either case ϕ is provably equivalent to a quantifier free formula.

Suppose that $T \models \forall \bar{v}(\theta(\bar{v}, w) \leftrightarrow \psi_0(\bar{v}, w))$, where ψ is quantifier free. Suppose $\phi(\bar{v}) = \exists w\ \theta(\bar{v}, w)$. Then $T \models \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow \exists w(\psi(\bar{v}, w))$. By our assumptions there is a quantifier free $\psi(\bar{v})$ such that $T \models \forall \bar{v}\ (\exists w\ \psi_0(\bar{v}, w) \leftrightarrow \psi(\bar{v}))$. But then $T \models \forall \bar{v}\ (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$.

Thus to show that T has quantifier elimination we need only verify that condition ii) of theorem 3.1 holds for every formula $\phi(\bar{v})$ of the form $\exists w \theta(\bar{v}, w)$ where $\theta(\bar{v}, w)$ is quantifier free.

Theorem 3.3 The theory ACF has quantifier elimination.

Proof Let F be a field and let K and L be algebraically closed extensions of F. Suppose $\phi(v, \bar{w})$ is a quantifier free formula, $\bar{a} \in F$, $b \in K$ and $K \models \phi(b, \bar{a})$. We must show that $L \models \exists v\ \phi(v, \bar{a})$.

There are polynomials $f_{i,j}, g_{i,j} \in F[X]$ such that $\phi(v, \bar{a})$ is equivalent to

$$\bigvee_{i=1}^{l} \Big(\bigwedge_{j=1}^{m} f_{i,j}(v) = 0 \wedge \bigwedge_{j=1}^{n} g_{i,j}(v) \neq 0 \Big).$$

Then $K \models \bigwedge_{j=1}^{m} f_{i,j}(b) = 0 \wedge \bigwedge_{j=1}^{n} g_{i,j}(b)$ for some i.

Let $\widehat{F}$ be the algebraic closure of F. We can view $\widehat{F}$ as a subfield of both K and L. If any $f_{i,j}$ is not identically zero for $j = 1, \ldots, m$, then $b \in \widehat{F} \subseteq L$ and we are done.

Otherwise since

$$\bigwedge_{i=1}^{n} g_{i,j}(b) \neq 0,$$

$g_{i,j}(X) = 0$ has finitely many solutions. Let $\{c_1, \ldots, c_s\}$ be all of the elements o L where some $g_{i,j}$ vanishes for $j = 1, \ldots, m$. Thus if we pick any element d of L with $d \notin \{c_1, \ldots, c_s\}$, then $L \models \phi(d, \bar{a})$.

The next result summarizes some simple applications.

Corollary 3.4 Let K be an algebraically closed field.

i) If $X \subset K$ is definable, then either X or $K \setminus X$ is finite. (This property is called *strong minimality*).

ii) Suppose $f : K \to K$ is definable. If K has characteristic zero, there is a rational function g such that $f(x) = g(x)$ for all but fintely many x. If K has characteristic p there is a rational function g and $n \geq 0$ such that $f(x) = g(x)^{1/p^n}$ for all but finitely many x.

Proof

i) X is a boolean combination of sets of the form $\{x : f(x) = 0\}$ and these sets are finite.

ii) Assume K has characteristic 0 (the $p > 0$ case is similar). Let L be an elementary extension of K and let $a \in L \setminus K$. If σ is any automorphism of L fixing $K(a)$, then $\sigma(f(a)) = f(a)$. But then $f(a) \in K(a)$. Thus there is a rational function $g \in K(X)$ such that $f(a) = g(a)$. The set $\{x \in K : f(x) = g(x)\}$ is either finite or cotfinite by i). If it has size N, then the fact that it has exactly N elements is expressed by a sentence true of L and K. Then L would not contain any new elements of this set. Thus $f(x) = g(x)$ for all but finitely many x.

Indeed, (in characteristic zero) if f is definable there is a Zariski open O and a rational function g such that $f|O = g|O$.

The quantifer elimination test has many other applications. For example consider RCF, the theory of real closed ordered fields in the language $\mathcal{L}_{\rm or}$. The axioms for RCF consist of:

i) the axioms for ordered fields;

ii) $\forall x > 0 \exists y\ y^2 = x$;

iii) the axiom $\forall x_0 \ldots \forall x_{n-1} \exists y\ y^n + x_{n-1}y^{n-1} + \ldots + x_0 = 0$ for each odd $n > 0$.

Clearly RCF is part of the $\mathcal{L}_{\rm or}$-theory of the real field. We will see shortly that this theory is complete and hence axiomatizes the complete theory of the real field. First we show RCF has quantifier elimination. We use the algebraic facts that every ordered field has a unique real closed algebraic extension and over a real closed field any polynomial in one variable factors into a product of linear and irreducible quadratic factors (see for example Lang's *Algebra*).

Theorem 3.5 The theory RCF has quantifier elimination in $\mathcal{L}_{\rm or}$.

Proof. We apply theorem 3.1. Let F_0 and F_1 be models of RCF and let $(R, <)$ be a common substructure. Then $(R, <)$ is an ordered domain. Let L be the real closure of the fraction field of R. By the uniqueness of real closures we can may assume that $(L, <)$ is a substructure of F_0 and F_1. Suppose $\phi(v, \bar{w})$ is quantifier free, $\bar{a} \in R$, $b \in F_0$ and $F_0 \models \phi(b, \bar{a})$. We need to show that $F_1 \models \exists v\ \phi(v, \bar{a})$. It suffices to show that $L \models \exists v\ \phi(v, \bar{a})$.

As in the proof of theorem 3.3 (and fooling around with the order), we may assume that there are polynomials $f_1, \dots, f_n, g_1, \dots, g_m \in R[X]$ such that $\phi(v, \bar{a})$ is

$$\bigwedge_{i=1}^{n} f_i(v) = 0 \wedge \bigwedge_{i=1}^{m} g_i(v) > 0.$$

If any of the f_i is not zero, then since $\phi(b, \bar{a})$, b is algebraic over R and thus in L. So we may assume $\phi(v, \bar{a})$ is

$$\bigwedge_{i=1}^{m} g_i(v) > 0.$$

Since L is a real closed field, we can factor each g_i as a product of factors of the form $(X - c)$ and $(X^2 + bX + c)$ where $b^2 - 4c < 0$. The linear factors change sign at c, while the quadratic factors do not change signs. If follows that we can find $\alpha_1, \dots, \alpha_l \in L \cup \{-\infty\}$ and $\beta_1, \dots, \beta_l \in L \cup \{+\infty\}$ such that for $v \in F_0$, $\phi(v, \bar{a})$ if and only if

$$\bigvee_{i=1}^{l} \alpha_i < v < \beta_i.$$

Since $F_0 \models \phi(b, \bar{a})$, for some i, $\alpha_i < b < \beta_i$. Then $L \models \phi(\frac{\alpha+\beta}{2}, \bar{a})$.

Corollary 3.6 RCF is complete and decidable.

Proof Let ϕ be a sentence. By quantifier elimination there is a quantifier free sentence ψ such that RCF$\models \phi \leftrightarrow \psi$. We can embed the rational numbers in any real closed field F and $F \models \psi$ if and only if $\mathbf{Q} \models \psi$. Thus $F \models \phi$ if and only if $\mathbf{Q} \models \psi$. In particular if F_1 and F_2 are real closed fields then $F_1 \models \phi$ if and only if $F_2 \models \phi$.

Hence RCF is complete. Decidability follows as in 2.7.

We also have an analog of 3.4.

Corollary 3.7 If R is real closed and $X \subset R$ is definable, then X is a finite union of points and intervals (this is called *o-minimality*).

Proof

Definable subsets of R are boolean combinations of $\{x : f(x) > 0\}$ which are finite unions of intervals.

§4 Model completeness

We say that a theory T is *model complete* if whenever $\mathcal{M}$ and $\mathcal{N}$ are models of T and $\mathcal{M} \subset \mathcal{N}$, then $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$.

Proposition 4.1 If T has quantifier elimination, then T is model complete.

Proof Let $\mathcal{M} \subset \mathcal{N}$. Suppose $\phi(\bar{v})$ is a formula and $\bar{a} \in M^n$. There is a quantifier free formula $\psi(\bar{v})$ such that in models of T

$$\phi(\bar{v}) \leftrightarrow \psi(\bar{v}).$$

Since ψ is quantifier free, $\mathcal{M} \models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \models \psi(\bar{a})$. Thus $\mathcal{M} \models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \models \psi(\bar{a})$.

Model completeness can arise in cases where quantifier elimination fails. For example, let T be the $\mathcal{L}_{\rm r}$-theory of the real numbers (with out a symbol for the order). The formula $\exists y\ y^2 = x$ is not equivalent to a quantifier free formula (recall that quantifier free definable sets in $\mathcal{L}_{\rm or}$ are constructible), so T does not have quantifier elimination. On the other hand the ordering of a real closed field is definable in the field language, thus if F and K are real closed fields and F is a subfield of K, then the ordering on F agrees with the ordering inherited from K (ie. F is an $\mathcal{L}_{\rm or}$-substructure of K). Thus, by quantifier elimination in $\mathcal{L}_{\rm or}$, F is an elementary substructure of K.

This example shows that "quantifier elimination" is sensitive to the exact choice of language. In general we can always enrich the language so that we have quantifier elimination. If T_0 is an $\mathcal{L}$-theory, we can add to our language an n-ary relation symbol R_ϕ for each formula ϕ with n free variables and we could let T be the theory where we add to T_0 axioms $\forall \bar{x}\ (\phi(\bar{x}) \leftrightarrow R_\phi(\bar{x}))$ for each formula ϕ. The theory T will have quantifier elimination, but this would be useless as we would not be able to say anything sensible about the quantifier free formulas. The goal is to show we have quantifer elimination in a language where the quantifier free formulas are simple.

Wilkie showed that the theory of $(R, +, -, \times, <, \exp)$ is model complete, but

$$y > 0 \wedge \exists w\ (wy = x \wedge z = y\exp(w))$$

is not equivalent to a quantifier free formula in the language $\{+, -, \times, <, 0, 1, \exp\}$ (or any expansion by total real analytic functions. Van den Dries, Macintyre and I showed that you can eliminate quantifiers in a much more expressive language, but we do not know the simplest language for quantifier elimination.

Model completeness itself has useful consequences. For example the model completeness of ACF leads to an easy proof of a version of the Nullstellensatz.

Theorem 4.2 Let F be an algebraically closed field and let $I \subset F[X_1, \ldots, X_n]$ be a prime ideal. Then there is $a \in F^n$ such that $f(a) = 0$ for all $f \in I$.

Proof
Let K be the algebraic closure of the fraction field of $F[X_1, \ldots, X_n]/I$. If $x_i \in K$ is X_i/I, then $f(x_1, \ldots, x_n) = 0$ for all $f \in I$. Choose $f_1, \ldots, f_m$ generating I. Then

$$K \models \exists y_1, \ldots, y_n \bigwedge_{i=1}^{m} f_i(y_1, \ldots, y_n) = 0.$$

As this is a sentence with parameters from F, by model completeness this sentence is also true in F. Thus there is $a \in F^n$ such that $f_i(a) = 0$ for $i = 1, \ldots, m$ and hence $f(a) = 0$ for all $f \in I$.

A very similar argument can be used to reprove Artin's solution to Hilbert's 17^{th} problem.

Theorem 4.3 Let F be a real closed field. Suppose $f(X_1, \ldots, X_n) \in F(X_1, \ldots, X_n)$ and $f(a) \geq 0$ for all $a \in F^n$ (we call f *positive semi-definite*). Then f is a sum of squares of rational functions.

Proof If not then we can extend the order of F to $F(X_1, \ldots, X_n)$ such that $f < 0$ (see Lang's *Algebra*). Let K be the real closure of $F(X_1, \ldots, X_n)$ with this ordering. Then

$$K \models \exists y_1 \ldots \exists y_n f(y_1, \ldots, y_n) < 0,$$

since we can use $X_1, \ldots, X_n$ as witnesses. By model completeness

$$F \models \exists y_1 \ldots \exists y_n f(y_1, \ldots, y_n) < 0.$$

Definition We say that a theory T is the *model companion* of a universal theory T_0 if:
i) every model of T is a model of T_0,
ii) every model of T_0 can be extended to a model of T, and
iii) T is model complete.

For example the theory of algebraically closed fields is the model companion of the theory of integral domains and the theory of real closed fields is the model companion of the theory of ordered domains. More interesting examples will arise in Chatzidakis' lecture.

Model theoretic methods can sometimes be used to obtain effective bounds. Compactness arguments alone can lead to crude bounds.

Proposition 4.4 There is a computable function $\tau(n, d)$ such if F is a real closed field and $f = g/h \in F(X_1, \ldots, X_n)$ where f and g are polynomials of degree at most d and f is positive semidefinite then f is the sum of squares of at most $\tau(n, d)$ rational functions with numerator and denominator of degree at most $\tau(n, d)$.

Proof Fix n, d. We claim that there is an M such that any positive semidefinite rational function in n variables with numerator and denominator of degree at most d is a sum of at most M squares of rational functions with numerator and denominator of degree at most M. Computability is free.

Suppose not Let $c_1, \ldots, c_N$ be new constants which will be coefficients of a rational function f in n-variables with numerator and denominator of degree at most d. Let Φ_M be a sentence asserting "f is not a sum of at most M squares of functions of degree at most M". Then RCF+ "f is positive semidefinite" + $\{\neg\Phi_M : M \geq 1\}$ is satisfiable contradicting Hilbert's 17th problem.

§5 Types

Suppose $\mathcal{M}$ is an $\mathcal{L}$-structure and $A \subseteq M$. Let $\mathcal{L}_A$ be the language obtained by adding to $\mathcal{L}$ constant symbols for all elements of A. Let $\mathrm{Th}_A(M)$ be the set of all $\mathcal{L}_A$-sentences true in $\mathcal{M}$.

Definition An *n-type* over A is a set of $\mathcal{L}_A$-formulas in free variables $x_1, \ldots, x_n$ that is consistent with $\mathrm{Th}_A(\mathcal{M})$. A *complete n-type* over A is a maximal n-type. In other words a complete type is a set p of $\mathcal{L}_A$-formulas consistent with $\mathrm{Th}_A(\mathcal{M})$ in the free variables $x_1, \ldots, x_n$ such that for any $\mathcal{L}_A$-formula $\phi(\bar{x})$ either $\phi(\bar{x}) \in p$ or $\neg\phi(\bar{x}) \in p$. Let $S_n(A)$ be the set of all complete n-types over A.

We sometimes refer to incomplete types as *partial types.*

By compactness every n-type over A is realized in some elementary extension of $\mathcal{M}$.

There is one easy way to get complete types. Suppose $\mathcal{N}$ is an elementary extension of $\mathcal{M}$ and $\bar{b} \in N^n$. Let $\mathrm{tp}(\bar{b}/A) = \{\phi(\bar{x}) \in \mathcal{L}_A : \mathcal{N} \models \phi(\bar{b})\}$. It is easy to see that $\mathrm{tp}(\bar{b}/A)$ is a complete type.

If $p \in S_n(A)$ we say that $\bar{b}$ *realizes* p if $\mathrm{tp}(\bar{b}/A) = p$.

What do types tell us?

Proposition 5.1 Suppose $\bar{a}, \bar{b} \in M^n$ and $\mathrm{tp}(\bar{a}/A) = \mathrm{tp}(\bar{b}/A)$. Then there is an elementary extension $\mathcal{N}$ of $\mathcal{M}$ and an $\mathcal{L}$-automorphism of $\mathcal{N}$ which fixes A and maps $\bar{a}$ to $\bar{b}$.

Proof We carefully iterate the following lemma.

Lemma 5.2 Suppose $\mathcal{M}$ is an $\mathcal{L}$-structure, $A \subset M$ and $f : A \to M$ is a partial elementary map (ie. $M \models \phi(a_1, \ldots, a_n)$ iff $\mathcal{M} \models \phi(f(a_1), \ldots, f(a_n))$. If $b \in M$, we can find $\mathcal{N}$ an elementary extension of $\mathcal{N}$ and extend f to a partial elementary map from $A \cup \{b\}$ into N.

Proof Let c be a new constant symbol. Let

$$\Gamma = \{\phi(c, f(a_1), \ldots, f(a_n)) : \mathcal{M} \models \phi(b, a_1, \ldots, a_n), a_1, \ldots, a_n \in A\} \cup \mathrm{Th}_M(\mathcal{M}).$$

Suppose we find a structure $\mathcal{N}$ and an element $c \in N$ satisfying all of the formulas in Γ. Since $\mathcal{N} \models \mathrm{Th}_M(\mathcal{M})$, $\mathcal{N}$ is an elementary extension of $\mathcal{M}$. It is also easy to see that we can extend f to an elementary map by $b \mapsto c$.

So it suffices to show that Γ is satisfiable. By compactness it suffices to show that every finite subset of Γ is satisfiable. Taking conjunctions it is enough to show that if $\mathcal{M} \models \phi(b, a_1, \ldots, a_n)$ then $\mathcal{M} \models \exists v\ \phi(v, f(a_1), \ldots, f(a_n))$. But this is clear since $\mathcal{M} \models \exists v \phi(v, a_1, \ldots, a_n)$ and f is elementary.

The type space $S_n(A)$ can be topologized as follows. For each $\mathcal{L}_A$-formula $\phi(x_1, \ldots, x_n)$ let $B_\phi = \{p \in S_n(A) : \phi \in p\}$. The *Stone topology* on $S_n(A)$ is the topology generated by using the sets B_ϕ as basic open sets.*

* Note: $S_n(A)$ can be thought of as the set of ultrafilters on the Boolean algebra of A-definable subsets of M^n so it is in fact the Stone space of a Boolean algebra.

Proposition 5.3 $S_n(A)$ is compact and totally disconnected.

Proof Suppose $\{B_{\phi_i} : i \in I\}$ is a cover of $S_n(A)$ by basic open sets. Suppose there is no finite subcover. Let $\Gamma = \{\neg\phi_i(x_1, \ldots, x_n) : i \in I\}$. Since there in no finite subcover every finite subset of Γ is satisfiable. By compactness Γ is satisfiable and this yields a type that is not contained in any B_{ϕ_i}.

Since $S_n(A) \setminus B_\phi = B_{\neg\phi}$, each B_ϕ is clopen. Thus $S_n(A)$ is totally disconnected.

Suppose K is an algebraically closed field and F is a subfield of K. What are the complete n-types over F? Suppose $p \in S_n(F)$. Let $I_p = \{f \in F[X_1, \ldots, X_n] :$ "$f(x_1, \ldots, x_n) = 0$" $\in p\}$. Let $\mathrm{Spec}(F[X_1, \ldots, X_n])$ be the set of prime ideals of $F[X_1, \ldots, X_n]$. We topologize this space by taking sub-basic open sets $\{P : f \notin P\}$, for $f \in F[\bar{X}]$.

Proposition 5.4 $p \mapsto I_p$ is a continuous bijection between $S_n(F)$ and $\mathrm{Spec}(F[\bar{X}])$.

Proof If $fg \in I_p$, then "$f(\bar{x})g(\bar{x}) = 0$" $\in p$. Since p is complete either "$f(\bar{x}) = 0$" $\in p$ or "$g(\bar{x}) = 0$" $\in p$. Thus I_p is prime. It is just as easy to see that it is an ideal.

If P is a prime ideal, then we can find a prime ideal $P_1 \in K[\bar{X}]$ such that $P_1 \cap F[\bar{X}] = P$. Let K_1 be the algebraic closure of $K[\bar{X}]/P_1$ and let $a_i = X_i/P$. For $f \in K[\bar{X}]$ $f(\bar{a}) = 0$ if and only if $f \in P_1$, thus $I_{\mathrm{tp}(\bar{a}/F)} = P$. Thus the map is surjective.

By quantifier elimination if $I_p \neq I_q$, then $p \neq q$.

Continuity is clear.

This shows that the Zariski topology on $\mathrm{Spec}(F[\bar{X}])$ is compact.

We can identify (as objects) $S_n(F)$ and $\mathrm{Spec}(F[\bar{X}])$, but the Stone topology is much finer that the Zariski topology. The Stone topology corresponds to the topology generated by the constructible sets.

If $p \in S_n(F)$, let $V = \{x \in K^n : f(x) = 0\}$ for all $f \in I_p\}$. Then the type p asserts that $\bar{x} \in V$ and $\bar{x} \notin W$ for any $W \subset V$ defined over F. Thus realizations of p are points of V generic over F.

What about real closed fields? If F is an ordered subfield of a real closed field and p is an n-type, let I_p be as above and let $C_p = \{f/I_p : f \in F[\bar{X}]$ and "$f(\bar{x}) > 0 \in p\}$. Then $p \mapsto (I_p, C_p)$ is a bijection onto the set of pairs of real prime ideals P (prime ideals where $-1 \neq \sum a_i b_i^2$ where $a_i > 0$, $a_i \in F[\bar{X}]$, $b_i \in P$) and orderings of $F[\bar{X}]/P$. This is the *real spectrum* of $F[\bar{X}]$.

In particular if R is a real closed field, then elements of $S_1(R)$ correspond to either elements of R or cuts in the ordering of R.

§6 Saturation

It is often useful to work in a very rich model of a theory. For example it is sometimes easier to prove things in an algebraically closed field of infinite transcendence degree. Or when dealing with the reals it is useful to use nonstandard methods by assuming there are infinite elements. In model theory we make this precise in the following way.

Definition Let κ be an infinite cardinal. We say that a structure $\mathcal{M}$ is *κ-saturated* if for every $A \subset M$ with $|A| < \kappa$ if $p \in S_1(A)$, then there is b in M such that b realizes p. An easy induction shows that in this case every n-type over A is also realized in $\mathcal{M}$.

We say that $\mathcal{M}$ is *saturated* if it is $|M|$-saturated.

Lemma 6.2 If $\mathcal{M}$ is saturated, $A \subset M$ and $|A| < |M|$, then $\mathrm{tp}(\bar{a}/A) = \mathrm{tp}(\bar{b}/A)$ if and only if there is an automorphism of M fixing A mapping $\bar{a}$ to $\bar{b}$.

Proof The argument from 5.1 can be done completely inside M.

Proposition 6.3 An algebraically closed field K is saturated if and only if it has infinite transcendence degree.

Proof

Suppose $A \subset K$ is finite and F is the field generated by A. Let p be the 1-type over A which says that x is transcendental over F. If K is $\aleph_0$-saturated, then p must be realized in K. Thus every $\aleph_0$-saturated algebraically closed field has infinite transcendence degree.

On the other hand suppose K has infinite transcendence degree and $F \subset K$ is a field generated by fewer that $|K|$ elements. Let $p \in S_1(F)$ and let I_p be as in 5.4. If $I_p = \{0\}$, then p simply says "x is transcendental over F", and we can find a realization in K. If I_p is generated by $f(X)$, then any zero of f realizes p and we can find a realization in K.

Unfortunately saturated models are not so easy to come by in general. In general $|S_n(A)|$ can be as large as $2^{|A|+|\mathcal{L}|+\aleph_0}$. For example 1-types over $\mathbf{Q}$ in the theory of real closed fields, correspond to cuts in the rationals so $|S_1(\mathbf{Q})| = 2^{\aleph_0}$. Thus set theoretic problems arise. Under assumptions like the generalized continuum hypothesis or the existence of inaccessible cardinals we can find saturated models, but it is also possible that there are no saturated real closed fields.

Suppose $|\mathcal{L}| \leq \aleph_0$ and λ is an infinite cardinal. We say that an $\mathcal{L}$-theory T is *λ-stable* if and only for all $\mathcal{M} \models T$ and all $A \subset M$, if $|A| = \lambda$, then $|S_n(A)| = \lambda$. It is easy to see that algebraically closed fields are λ-stable for all infinite λ.

Proposition 6.4 If T is λ-stable, then T has a saturated model of size λ^+.

Proof We build a saturated model of size λ^+ as a union of an elementary chain of models $(\mathcal{M}_\alpha : \alpha < \lambda^+)$ where each $\mathcal{M}_\alpha$ has size λ. Let $\mathcal{M}_0$ be any model of size λ. For α a limit let $\mathcal{M}_\alpha$ be the union of the $\mathcal{M}_\beta$, for $\beta < \alpha$.

Given $\mathcal{M}_\alpha$. Let $(p_\beta : \beta < \lambda)$ list all 1-types over M_α. Build a chain of elementary extensions $(\mathcal{N}_\beta,\, \beta < \lambda)$ where $\mathcal{N}_0 = \mathcal{M}_\alpha$ and where $\mathcal{N}_\beta$ contains a realization of p_β. Let $\mathcal{M}_{\alpha+1}$ be the union of the $\mathcal{N}_\beta$.

Let $\mathcal{M} = \bigcup_{\alpha<\lambda^+} \mathcal{M}_\alpha$. Then $|M| = \lambda^+$. If $A \subset M$ and $|A| = \lambda$, then $A \subset M_\alpha$ for some α. Thus any 1-type over A is already realized in $\mathcal{M}_{\alpha+1}$.

§7 Interpretability and Imaginaries.

It is often very useful to study the structures which can be defined inside a give structure. For example, let K be a field and let G be the group $\mathrm{GL}_2(K)$. Let $X = \{(a,b,c,d) \in K^4 : ad - bc \neq 0\}$. Let $f : X^2 \to X$ by

$$f((a_1,b_1,c_1,d_1),(a_2,b_2,c_2,d_2)) = (a_1a_2 + b_1c_2, a_1b_2 + b_1c_2, c_1a_2 + d_1c_2, c_1b_2 + d_1d_2).$$

Clearly X and f are definable and the set X with the operation f is isomorphic to $\mathrm{GL}_2(K)$.

We say that an $\mathcal{L}_0$-structure $\mathcal{N}$ is *definable* in an $\mathcal{L}$-structure $\mathcal{M}$ if and only if we can find a definable (in $\mathcal{L}$) subset X of M^n for some n and we can interpret the symbols of $\mathcal{L}_0$ as definable subsets and functions on X so that the resulting $\mathcal{L}_0$-structure is isomorphic to $\mathcal{N}$.

The above example shows that $\mathrm{GL}_n(K)$ is definable in K. It is also easy to see that any linear algebraic group is definable in K.

We give a more interesting example. Let F be a field and let G be the group of matricies of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

where $a, b \in K, a \neq 0$. We will show that F is definable in the group G. Let

$$\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} \tau & 0 \\ 0 & 1 \end{pmatrix}$$

where $\tau \neq 0, 1$. Let

$$A = \{g \in G : g\alpha = \alpha g\} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in F \right\}$$

and

$$B = \{g \in G : g\beta = \beta g\} = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} : x \neq 0 \right\}.$$

Clearly A and B are definable.

B acts on A by conjugation

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{y}{x} \\ 0 & 1 \end{pmatrix}.$$

Clearly the action $(a,b) \mapsto b^{-1}ab$ is definable. We can define the map $i : A \setminus \{1\} \to B$ by $i(a) = b$ iff $b^{-1}ab = 1$, ie.

$$i\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.$$

Define an operation $*$ on A by

$$a * b = \begin{cases} i(b)^{-1}ab & \text{if } b \neq 1 \\ 1 & \text{if } b = 1 \end{cases}.$$

It is now easy to see that $(F, +, \times, 0, 1)$ is isomorphic to $(A, \cdot, *, 1, \alpha)$. Thus the field is definable in G.

This will not be true for all algebraic groups. For example if E is an elliptic curve and $\oplus$ is the addition law on E then we can not interpret a field in the group $(E, \oplus)$.

Often we want to do more general constructions. For example, suppose we have a definable group G and a definable normal subgroup H. We might want to look at the group G/H. It is possible that G/H does not correspond to a definable group in our structure. But it does correspond to the cosets of a definable equivalence relation.

We say that an $\mathcal{L}_0$-structure $\mathcal{N}$ is *interpretable* in an $\mathcal{L}$-structure M if there is a definable set X, a definable equivalence relation E on X, and for each symbol of $\mathcal{L}$ we can find definable E-invariant sets on X, such that X/E with the induced structure is isomorphic to $\mathcal{N}$.

As an example let us show that we can interpret the additive group of integers in the field $\mathbf{Q}_p$. First note that we can define $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : \exists y\ y^2 = px^2 + 1\}$ (at least for $p \neq 2$). Let $U = \{x \in \mathbf{Z}_p : \exists y \in \mathbf{Z}_p : xy = 1\}$ be the units of $\mathbf{Z}_p$. Then $(\mathbf{Z}, +)$ is isomorphic to the multiplicative group $\mathbf{Q}_p^*/U$. We can define the ordering on $\mathbf{Q}_p^*/U$ by $x/U \geq y/U \Leftrightarrow \frac{x}{y} \in \mathbf{Z}_p$.

Quotient constructions are so useful that we often enrich our structure so that we can deal with all quotients as elements of the structure. Let $\mathcal{M}$ be an $\mathcal{L}$-structure. If E is a $\emptyset$-definable equivalene relation on M^n, let $S_E = M^n/E$ and let $\pi_E : M^n \to M^n/E$ be the quotient map. Let $\mathcal{M}^{\mathrm{eq}}$ be the structure whose underlying set is the disjoint union of $\mathcal{M}$ and all of the S_E for E a $\emptyset$-definable equivalence relation. In addition to the relations and functions of $\mathcal{L}$, we add function symbols for each map π_E. We call the new elements of $\mathcal{M}^{\mathrm{eq}}$ *imaginary* elements.

If a structure $\mathcal{N}$ is interpretable in $\mathcal{M}$, then $\mathcal{N}$ is definable in $\mathcal{M}^{\mathrm{eq}}$. On other hand, not much has changed, if $X \subseteq M^n$ is definable in $\mathcal{M}^{\mathrm{eq}}$ then X is already definable in $\mathcal{M}$.

An important property of many of the theories of fields that we will consider is that the passage from K to K^{eq} is unnecessary.

Van den Dries showed that in real closed fields any definable equivalence relation has a definable set of representatives. Nothing this strong could be true in algebraically closed fields as a set of represntatives for the equivalence relation $xEy \leftrightarrow x^2 = y^2$ would be infinite and coinfinite.

We say that $\mathcal{M}$ has *elimination of imaginaries* if whenever E is a definable equivalence relation on M^n, there is a definable function $f : M^n \to M^m$ for some m, such that xEy iff $f(x) = f(y)$.

Theorem 7.1 (Poizat) Algebraically closed fields have elimination of imaginaries.

In other words if X is a constructible set and E is a constructible equivalence relation on X, then X/E can be viewed as a constructible set.

The proof of 7.1 proceeds by first showing that a theory has elimination of imaginaries if and only if for any saturated model $\mathcal{M}$ and any $X \subset M^n$ definable there is $\bar{a} \in M^m$ for some m such that for all automorphisms σ of $\mathcal{M}$, σ fixes X setwise if and only if $\sigma(\bar{a}) = \bar{a}$. We call $\bar{a}$ *canonical parameter for* X. If X is defined by $\phi(\bar{x}, \bar{b})$, we could define an equivalence relation $\bar{b}_1 E \bar{b}_2$ iff $\phi(\bar{x}, \bar{b}_1) \leftrightarrow \phi(\bar{x}, \bar{b}_2)$. Then $\bar{b}/E$ is a canonical parameter for X. In general canonical parameters will only be found in $\mathcal{M}^{\rm eq}$.

Suppose K is an algebraically closed field and X is an irreducible variety. There is a smallest subfield $k \subset K$ such that X is fixed by an automorphism iff k is fixed pointwise (k is called the *field of definition* of X). k must be finitely generated and if $\bar{a}$ generates k, then $\bar{a}$ is a canonical parameter. From this observation and quantifier elimination one can derive elimination of imaginaries.

The field of p-adics is a natural example where elimination of imaginaries fails. We saw above that we can interpret the integers in $\mathbf{Q}_p$. Analysis using quantifier elimination for the p-adics, shows that any definable set is either finite or uncountable, so the integers can not be isomorphic to a definable set.

Here is another instructive example where elimination of imaginaries fails. Let K be an algebraically closed field of characteristic zero. Let C be curve of genus at least one and let $\mathcal{C}$ be the structure with underlying set C and relation symbols for all constructible subsets of C^n. Since there is a rational map $\pi : C \to K$, we can intepret the field on C using the equivalence relation xEy iff $\pi(x) = \pi(y)$. If C/E was definably isomorphic to a definable set $X \subset C^n$, this would give rise to a definable map $f : K \to C$. But (by 3.4) there is a rational map $g : K \to C$ which agrees with f on all but a finite set. By genus considerations g is constant.

It is often very important to understand the groups and fields interpretable in a structure. For algebraically closed fields we get a very satisfying answer. It is easy to see that if K is an algebraically closed field any algebraic group defined over K is interpretable in K and hence, by elimination of imaginaries, isomorphic to a definable group. The following theorem is related to Weil's theorems on group chunks.

Theorem 7.2 i) (van den Dries/Hrushovski) If a group G is definable in an algebraically closed field K, then G is definably isomorphic to the K-rational points of an algebraic group defined over K.

ii) (Poizat) If F is an infinite field definable in an algebraically closed field, then F is definably isomorphic to K.

Appendix A: Formulas

Throughout the notes I have been discussing formulas. Here I will give a precise definition. Let $\mathcal{L}$ be a language.

Definition The set of *$\mathcal{L}$-terms* is the smallest set $\mathcal{T}$ such that:

i) all constant symbols of $\mathcal{L}$ are in $\mathcal{T}$,

ii) all variables are in $\mathcal{T}$, and

iii) if $t_1, \ldots, t_n$ are in $\mathcal{T}$ and $\widehat{f}$ is an n-ary function symbol of $\mathcal{L}$, then $\widehat{f}(t_1, \ldots, t_n) \in \mathcal{T}$.

The set of *atomic $\mathcal{L}$-formulas* is the smallest set $\mathcal{A}$ such that:

i) if t_1 and t_2 are terms, then $t_1 = t_2$ is in $\mathcal{A}$, and

ii) if $t_1, \ldots, t_n$, are terms and $\widehat{R}$ is an n-ary function symbol, then $\widehat{R}(t_1, \ldots, t_n)$ is in $\mathcal{A}$.

The set of $\mathcal{L}$-formulas is the smallest set $\mathcal{F}$ such that

i) every atomic $\mathcal{L}$-formula is in $\mathcal{F}$,

ii) if $\phi \in \mathcal{F}$, then $\neg\phi \in \mathcal{F}$

iii) if ϕ and ψ are in $\mathcal{F}$, then $(\phi \vee \psi)$ and $(\phi \wedge \psi)$ are in $\mathcal{F}$,

iv) if ϕ is in $\mathcal{F}$ and x_i is a variable, then $\exists x_i \phi$ and $\forall x_i \phi$ are in $\mathcal{F}$.

For example $x_1+(x_2\times(x_1+1))$ is an $\mathcal{L}_{\mathrm{or}}$-term, $x_1\times(x_2+x_3) = x_1+1$ and $x_1 < x_3+x_7$ are atomic $\mathcal{L}_{\mathrm{or}}$-formulas, and $\exists x_1(x_1 \times (x_2 + x_3) = x_1 + 1 \wedge x_2 < x_1)$ is an $\mathcal{L}_{\mathrm{or}}$-formula.

References

The following are good basic texts.

C.C. Chang and H.J. Keisler, *Model Theory*, North Holland (1977).

W. Hodges, *Model Theory*, Cambridge (1993).

W. Hodges, *A Shorter Model Theory*, Cambridge (1997).

B. Poizat, *Cours de Théorie des Modèles*, Nur al-Mantiq wal Ma'rifah (1985).

G. Sacks, *Saturated Model Theory*, Bejamin (1972).

For an introduction to the model theory of algebraically closed, real closed, differentially closed and separably closed fields.

D. Marker, M. Messmer and A. Pillay, *Model Theory of Fields*, Springer Lecture Notes in Logic #5, Springer-Verlag (1996).

Proofs of 7.1 can be found in the volume above or in

B. Poizat, An introduction to algebraically closed fields and varieties, *The Model Theory of Groups*, A. Nesin and A. Pillay ed., Notre Dame (1989).

A proof of 7.2 can be found in

B. Poizat, *Groupes Stables*, Nur al-Mantiq wal Ma'rifah (1987).